UNIVERSITY OF READING

U.S. Strategic Cyber Deterrence Options

Doctor of Philosophy in Politics

Department of Politics & International Relations

Scott Jasper

March 2018

Contents

Abstract

The U.S. government appears incapable of creating an adequate strategy to alter the behavior of the wide variety of malicious actors seeking to inflict harm or damage through cyberspace. This thesis provides a systematic analysis of contemporary deterrence strategies and offers the U.S. the strategic option of active cyber defense designed for continuous cybered conflict. It examines the methods and motivations of the wide array of malicious actors operating in the cyber domain. The thesis explores how the theories of strategy and deterrence underpin the creation of strategic deterrence options and what role deterrence plays with respect to strategies, as a subset, a backup, an element of one or another strategic choice. It looks at what the government and industry are doing to convince malicious actors that their attacks will fail and that risk of consequences exists. The thesis finds that contemporary deterrence strategies of retaliation, denial and entanglement lack the conditions of capability, credibility, and communications that are necessary to change the behavior of malicious actors in cyberspace. This research offers a midrange theory of active cyber defense as a way to compensate for these failings through internal systemic resilience and tailored disruption capacities that both frustrate and punish the wide range of malicious actors regardless of origin or intentions. The thesis shows how active cyber defense is technically capable and legally viable as an alternative strategy in the U.S. to strengthen the deterrence of cyber attacks.

Abbreviations

A2/AD	Anti-access/Area denial
ACD	Active Cyber Defense
AIS	Automated Indicator Sharing
APT	Advanced Persistent Threat
BPHS	Bulletproof Hosting Services
CBM	Confidence-Building Measure
CFAA	Computer Fraud and Abuse Act
CIS	Center for Internet Security
CISP	Cybersecurity Strategy and Implementation Plan
CMF	Cyber Mission Force
CSC	Critical Security Controls
DCO	Defensive Cyberspace Operations
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DIUx	Defense Innovation Unit Experimental
DNC	Democratic National Committee
DNS	Domain Name System
DOD	Department of Defense
EEZ	Exclusive Economic Zone
EU	European Union
FBI	Federal Bureau of Investigation
FS	Financial Services
FTP	File Transfer Protocol
GDP	Gross Domestic Product
GLACY	Global Action on Cybercrime
GOP	Guardians of Peace
G-20	Group of Twenty
GPS	Global Positioning System

GSCI	Global Socio-Cyber Infrastructure
HM	Her Majesty’s
HTTP(S)	Hypertext Transfer Protocol (Secure)
IACD	Integrated Adaptive Cyber Defense
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
ICS-CERT	Industrial Control System – Computer Emergency Response Team
ICT	Information and Communication Technology
IDM	Internal Defensive Measures
IP	Intellectual Property
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISIS	Islamic State of Iraq and Syria
NSA	National Security Agency
NATO	North Atlantic Treaty Organization
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OPM	Office of Personnel Management
OSCE	Organization for Security and Co-operation in Europe
PII	Personally Identifiable Information
PIN	Personal Identification Number
POS	Point-of-Sale
PPD	Presidential Policy Directive
PLA	People’s Liberation Army
RA	Response Actions
RAM	Remote Access Memory
RAT	Remote Access Trojan
SIEM	Security Information and Event Management
SSL	Secure Sockets Layer

STIX	Structured Threat Information eXpression
SQL	Structured Query Language
TAXII	Trusted Automated eXchange of Indicator Information
TTP	Tactics, Techniques and Procedures
UK	United Kingdom
UN	United Nations
UNCLOS	UN Convention on Law of the Sea
URL	uniform resource locator
XML	Extensible Markup Language

Introduction

Headlines in May 2017 were dominated by the massive WannaCry ransomware attack that hit 74 countries across Europe and Asia, affecting more than a dozen hospitals in England's National Health System.[1] Even worse than this criminal activity is the threat to critical infrastructure as seen by the malware infections at electrical distribution companies in Ukraine that caused outages to 225,000 customers in late 2015.[2] Furthermore, recent reports on alleged Russian hacks into the U.S. Democratic National Committee and the staff of French candidate Emmanuel Macron, coupled with subsequent release of emails or content in coercive campaigns to apparently influence Presidential Elections have brought national attention to the inadequacy of cyber deterrence.[3] All sectors of the economy rely on the networks, systems, and services that form cyberspace.[4]

Information and Communication Technologies [ICTs] form the technical backbone of these networks and are equally essential to the defense sector, especially during the conduct of military operations. Yet protecting cyberspace is challenging because it is currently borderless, subject to dynamic change, and open to all comers. The cybered society is probed and penetrated by nation states, hacker groups, criminal organizations, and terrorist groups or lone wolves. These entities called malicious or threat actors can be partially or wholly responsible for

---

[1] Robert McMillian, Jenny Gross, and Denise Roland, "Major Cyberattack Sweeps Globe, Hitting FedEx, U.K. Hospitals, Spanish Companies," *The Wall Street Journal*, May 12, 2017.

[2] Electrical Information Sharing and Analysis Center, "Analysis of the Cyber Attack on the Ukrainian Power Grid," March 18, 2016: 1-25.

[3] Adam Nossiter, David E. Sanger and Nicole Perlroth, "Hackers Came, But the French Were Prepared," *New York Times*, May 10, 2017.

[4] The basis of this introduction first appeared in *Strategic Studies Quarterly* Vol. 9, No. 1 (Spring 2015). The thesis is drawn from recent publication of my book titled *Strategic Cyber Deterrence: The Active Cyber Defense Option* (New York, Rowman & Littlefield: July 2017).

a cyber incident that dramatically reduces an organization's security.[5] Many of these malicious actors seek state secrets, trade secrets, technology, and ideas, or they develop the ability to strike critical infrastructure and harm advanced economies.[6] Hacker groups and criminal gangs often work in concert with state actors, under some form of control, direction, incitement or other more nebulous arrangement. That intertwined relationship allows foreign governments to hide their malicious activity and claim innocence if confronted.[7] In addition, malicious actors use common tools, techniques and talent, available for purchase at very low prices on illicit web sites on the worldwide underground market.[8] This convergence of actor relationships, motivations, tactics, and capabilities complicates attribution of an attack[9] and makes using a single option to change the behavior of an individual actor, such as the nation state, impossible and impractical to counter cyber attacks.

Malicious actor attacks, via cyberspace, target "an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/ infrastructure; or destroying the integrity of the data or stealing controlled information."[10] Recent incidents show cyber attacks are employed and refined in a systematic, coordinated manner in an effort to achieve actor objectives. Criminal exploitation, military or

[5] Ivy Wigmore, "Threat Actor Definition," Security Threats and Countermeasures Glossary, January 2016.

[6] Robert Anderson, Jr. "Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland," testimony before the Committee on Homeland Security and Government Affairs, US Senate, September 10, 2014.

[7] Ian Duncan, "Cyber Command chief: Foreign governments use criminals to hack U.S. systems," *The Baltimore Sun*, March 16, 2016.

[8] Dell Secure Works, "Underground Hacker Markets," Annual Report, April 2016: 1-22.

[9] Mandiant, "M Trends 2015: A View From the Front Lines," Alexandria, Virginia, June 2015; 20-22.

[10] National Institute of Standards and Technology, "Glossary of Key Information Security Terms," NISTIR 7298 Revision 2, May 2013: 57.

industrial espionage, nationalist hacker protests, and infrastructure infiltration or sabotage are prominent in actor operations and campaigns. The motivations to conduct malicious activity vary, from criminals looking for financial gain, hacktivists promoting a cause, and state actors engaging in espionage (military or economic) or infiltrating critical infrastructure.[11] In many cases the actors conducting crime, espionage or disruption are the same. Even more so, all malicious actors in cyberspace have one thing in common: an increasing choice of attack methods. In deciding to attack, each actor will assess the effort against the expected benefit under their own criteria or rationality. As a strategic response to the threat of cyber attacks, deterrence seeks to change adversary perceptions of costs, benefits and restraint.[12] A daunting and critical question is whether contemporary deterrence strategies are sufficient to deter malicious actors in cyberspace in a multi-faceted approach or would an alternative strategy be more effective?

Governments have every reason to search for responses to challenges in cyberspace and deterrence is a key response. Deterrence is "the prevention of an adversary's undesired action."[13] Contemporary deterrence occurs when an adversary's believes that a threat of retaliation exists, the intended action cannot succeed, or the costs outweigh the benefits of acting.[14] Therefore deterrence centers on ways to impose costs, deny benefit, or encourage restraint. The strategic debate during the Cold War over how best to deter the threat of nuclear attack was separated into first 'deterrence by punishment' (threat of retaliation that imposes

[11] Adam Bromwich, Symantec, "Emerging Cyber Threats to the United States," Testimony before House Committee on Homeland Security, February 25, 2016.

[12] U.S. Department of Defense, *The DOD Cyber Strategy*, April 2015: 11.

[13] U.S. Department of Defense, *Joint Operation Planning,* Joint Publication 5-0 (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, August 11, 2011): E-2.

[14] U.S. Department of Defense, *Joint Operations,* Joint Publication 3-0, (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 17 January 2017): VI-4.

costs) and second into ‘deterrence by denial’ (limitation of damage by denial of success).[15] Since U.S. policy would not condone today the punishment of another country, a more appropriate view of the first method would simply be ‘deterrence by retaliation.’ In contemplation of strategic interdependence spawn from contemporary globalization, one might also add a third method titled ‘deterrence by entanglement’ (presumably cooperation on mutual interests encourages restraint to avoid unintended consequences and antagonizing third parties).[16] These three contemporary strategic deterrence options could conceivably apply in some fashion for cyberspace. Although an argument can be made that especially in the Cold War, deterrence functions worked only amongst stable actors and in situations of overall stability. Some actors (e.g. ISIS) cannot be deterred by traditional thinking.

Cyberspace – A National Achilles Heel?

Cyberspace is defined by the military as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”[17] For social, technical, and economic purposes, cyberspace can be considered as more than a domain but a substrate. In this usage, a “substrate” is an underlying physical layer on which modern society is built.[18] Cyberspace uniquely underpins every facet of social, technical and economic systems in developed societies. This

---

[15] Schuyler Forester, “Theoretical Foundations: Deterrence in the Nuclear Age,” in *American Defense Policy,* Schuyler Foerster and Edward Wright, eds., 6th ed. (Baltimore, MD: Johns Hopkins University Press, 1990): 47-51.

[16] Roger Harrison et al., “Space Deterrence: The Delicate Balance of Risk,” *Space and Defense* 3 (Summer 2009).

[17] See Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, As Amended Through 15 October 2016), 60.

[18] David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power,* (Routledge, 2011): 37.

substrate has a topology that is largely territorial, built by people unlike other traditional domains of warfare. The services relied upon in daily life, such as water distribution, healthcare, electricity generation, transportation, and financial transactions, depend on this underlying information technology infrastructure.[19] Systems or assets supporting these services are designated as critical infrastructure, deemed so because their incapacity or destruction would have "a debilitating impact" on national or economic security, public health or safety.[20] Because most critical infrastructure supports military operations, any significant disruption to the integrity of their networks could compromise the military's abilities to protect the nation.[21] In talking about the hypothetical dangers of what has been called a 'Cyber Pearl Harbor,' Representative Mike Rogers stated in 2014 that "the threat of a catastrophic and damaging cyberattack in the United States critical infrastructure like our power or financial networks is actually becoming less hypothetical every day."[22]

Not only has the volume of malicious code, known as malware, that threatens the functioning of critical infrastructure, increased to over 390,000 new programs each day,[23] but also the means of malware delivery have expanded to take advantage of human or technological weaknesses and modern day platforms. A specific method used to access equipment, computers or systems to deliver malware or other hostile outcomes is called a 'cyber attack vector' by

---

[19] Sean P. McGurk, National Cybersecurity and Communications Integration Center Director, "The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure," Testimony before the US House Committee on Homeland Security, April 15, 2011.

[20] Executive Office of the President, "Executive Order -- Improving Critical Infrastructure Cybersecurity," (Washington: The White House, February 12, 2013).

[21] William J. Lynn III, Deputy Secretary of Defense, "Remarks on the Department of Defense Cyber Strategy," Delivered at National Defense University, Washington, DC, July 14, 2011.

[22] Mike Rogers, "Cybersecurity Threats: The Way Forward," Hearing of the House (Select) Intelligence Committee, Washington, DC, November 20, 2014.

[23] AV Test, The Independent IT-Security Institute, *Malware Statistics*, August 9, 2016: https://www.av-test.org/en/statistics/malware/.

security professionals.[24] Vast arrays of vectors threaten industrial, commercial, governmental and military systems and devices. These attack methods have grown in complexity and sophistication, ranging from emails specifically tailored by attackers, using information found in social sites (a technique call social engineering), to spark interest of individuals to click on links or open attachments loaded with malware in 'spear phishing' attacks, or the planting of malicious code on legitimate sites visited by targeted individuals in what is called a 'watering hole' attack.[25] Auxiliary means for malware delivery include compromises of physical devices, like when an infected flash drive inserted into a U.S. military laptop spread code onto network systems,[26] or compromises of third party vendors of services and supplies that have trusted access to corporate networks, which is becoming a common occurrence.[27] The most sensational and publicized methods are intrusions by groups of attackers categorized as an "advanced persistent threat" (APT) and assaults using distributed denial of service (DDoS) methods. The APT group's form of hacking is designed to covertly penetrate networks and systems to steal or alter information, manipulate data, or cause damage. DDoS assaults disrupt website availability by overwhelming network equipment with high volume requests by compromised computers or by consuming application processing resources.[28]

[24] Kevin G. Coleman, "The Cyber Commander's eHandbook: The Strategies and Tactics of Digital Conflict," version 4, Technolytics, 2013, 52-80.

[25] Symantec, "Internet Security Threat Report," Volume 19, April 2014: 26 and 34.

[26] William J. Lynn III, Deputy Secretary of Defense, "Defending a New Domain," *Foreign Affairs,* Vol. 89, No. 5, September/October 2010.

[27] Chris Strohm, "U.S. Intelligence to help Companies avert Supply-Chain Hacking," *Bloomberg News,* August 10, 2016.

[28] Securosis, "Defending Against Denial of Service Attacks," White Paper, Version 1.3, October 31, 2012: 1-24.

New Emergent Forms of Peacetime Conflict

As a result of 'cyber attack vector' proliferation, highly motivated threat actors at any level now have myriad methods to conduct malicious activity in cyberspace. Primary areas of malicious activity are the theft or exploitation of data; disruption or denial of access or service; and destructive action comprising corruption, manipulation, and damage or the alteration of data – at rest and in motion. The buying or renting of malicious code viruses, exploits of code vulnerabilities (software and computer configuration flaws – including zero days), botnets (collections of compromised computers), and command and control servers (used for instructions) provides these actors with a ready array of tools and services. Some actors use these tools and services in "cyber warfare", which is a widely used and contested term. U.S. military joint terminology defines cyber warfare as "an armed conflict conducted in whole or part by cyber means."[29] Here an attacker could launch a military confrontation during a period of tension by attacking civilian infrastructure, a cyber attack just prior to or simultaneously with a surprise military attack, or wait until war starts to activate implanted exploits.[30] In addition to "military operations to deny an opposing force the effective use of cyberspace systems and weapons in a conflict,"[31] state cyber campaign doctrine appears to include disruption of governmental services, financial enterprises, and media outlets. For example in August 2008, when Russian troops engaged Georgian forces during their ground invasion, six command and control servers, managed by a cybercrime group, issued DDoS attack commands on select Georgian government, news and banking sites.[32] This instance and many others since indicate

---

[29] James E. Cartwright, "Joint Terminology for Cyberspace Operations" (Washington, DC: Office of the Vice Chairman of the Joint Chiefs of Staff, November 2010), 8.

[30] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, (Santa Monica, California: RAND Corporation, 2009): 143-149.

[31] Joint Terminology for Cyberspace Operations, 8.

[32] Jeff Carr, "Russia/Georgia Cyber War – Findings and Analysis," Project Grey Goose: Phase I Report, October 17, 2008.

that disruptive and destructive cyber attacks on critical infrastructure are becoming a part of modern conflict.

Although "cyber warfare" as defined above has entered into the common lexicon, the term "cybered conflict" or "cyber enabled conflict" characterizes more appropriately the essential nature of modern military operations. Cybered conflict frames the complexity and ambiguity of struggle involving cyberspace, including hybrid warfare (multi modes) and insurgent campaigns that exploit the domain or use attack methods in the form discussed previously.[33] Cybered conflict symbolizes "old and new forms of conflict born of, enabled through, or dramatically altered by cyberspace."[34] For instance, malicious activity occurred in cyberspace during Russian military operations in Crimea. Operations started with the seizure of *Ukrtelecom* offices and the physical cutting of telephone and internet cables.[35] Groups like OpRussia and Russian Cyber Command (Rucyborg)[36] that opposed annexation conducted DDoS attacks against Russian sites,[37] while pro-Russian CyberBerkut was active against NATO, in particular targeting their main public website before Crimea's vote in March 2014 to secede from Ukraine and join Russia.[38] Berkut is a reference to the feared riot squads of ousted pro-Russian President Victor Yanukovich. CyberBerkut also compromised the Central Election Commission during Ukraine's presidential election in May 2014, disabling real-time display updates in the

---

[33] Chris Demchak, "Cybered Conflict, Cyber Power, and Security Resilience as Strategy," *Cyberspace and National Security,* (Georgetown University Press, 2012): 121-136.

[34] Peter Dombrowski and Chris Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review,* April 1, 2014: 3.

[35] John Leyden, "Battle apparently underway in Russia-Ukraine conflict, *The Register*, March 4, 2014.

[36] Meto Ddihadzijanev, "Hacktivists of the Russian Cyber Command," *Scribd*, April 10, 2014.

[37] Mark Clayton, "Massive cyberattacks slam official sites in Russia, Ukraine," *Christian Science Monitor,* March 18, 2014.

[38] Adrian Croft and Peter Apps, "NATO Websites hit in cyber attack linked to Crimea tension," *Reuters*, March 16, 2014.

vote count and posting false results.[39] Political conflicts between nations have also spawned cyber attacks against Western news organizations.[40] The Syrian Electronic Army, a group of pro-regime hackers, has compromised external-facing websites and social media accounts of *The New York Times, The Associated Press, CNN, The Huffington Post* and *Forbes,* to promote the embattled Syrian regime.[41]

Rising State-level Security Concerns

The former U.S. Secretary of Defense Leon Panetta warned that the attacks on energy companies in the Arabian Gulf and on banks in the United States mark a significant escalation of the cyber threat and renewed concerns over still more destructive scenarios.[42] *Shamoon* malware, which is intended to destroy data, infected some 30,000 workstations at Saudi Aramco Oil Company in August 2012, rendering them unusable.[43] A partial photo showing the burning of an American flag was used to overwrite the content of the files. Weeks later, Qatar's RasGas suffered a major malware attack that shut down its website and email servers but not production systems.[44] In September 2012, six major American banks were hit in a wave of DDoS attacks that caused Internet blackouts and delays in online banking. Even though the attackers

---

[39] Nikolay Koval, "Revolution Hacking," *Cyber War in Perspective: Russian aggression against Ukraine,* Chapter 6, (Tallinn, Estonia, NATO Cooperative Cyber Defense Center of Excellence Publications, 2015): 55-58.

[40] Mandiant, "M Trends: Beyond the Breach," Alexandria, Virginia, April 2014: 1-7.

[41] Patrick Tucker, "Syrian Electronic Army Threatens to Hack CENTCOM," *Defense One*, March 3, 2014.

[42] Leon E. Panetta, "Defending the Nation from Cyber Attack," Business Executives for National Security, New York, October 11, 2012.

[43] Kelly Jackson Higgins, "Shamoon Code 'Amateur' But Effective," *Dark Reading*, September 11, 2012.

[44] Danielle Walker, "Natural gas giant RasGas targeted in cyber attack," *SC Magazine*, August 31, 2012.

announced the time and targets in advance, the financial institutions were unable to prevent their websites from being disrupted.[45] In Ukraine in December 2015, three different regional electricity distribution companies were attacked by malware infections that caused outages to approximately 225,000 customers. A third party entered into company computer and control systems to remote control distribution management systems and shut off substation breakers.[46] The delineations between the various phases of the operation suggest different levels of actors worked on different parts and possible collaboration between cyber criminals and state actors.[47]

While most attacks to date have not spilled far beyond the digital world, security experts seem to agree that the threat to critical infrastructure is real. For example, Meredith Patterson, an information security expert says "It is remarkably easy to just mess with the temperature someplace in a natural gas plant and catch the entire plant on fire."[48] Just because attacks on critical infrastructure do not happen very often does not mean they are not possible.

As of today, preparations for cybered conflict are already included in the Phase Zero or "Shape" Phase found in the notional six-phase model of joint and multinational operations described in US joint doctrine. This doctrine presents military operations leading to "war" as a natural progression of activities, from shaping, deterring, seizing initiative, dominating, stabilizing to enabling civil authority.[49] Certainly two major adversaries are attempting to shape

---

[45] Nicole Perlroth, "Attacks on 6 Banks Frustrate Customers," *The New York Times*, September 30, 2012.

[46] Electrical Information Sharing and Analysis Center, "Analysis of the Cyber Attack on the Ukrainian Power Grid," March 18, 2016: 1-25.

[47] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016.

[48] Lorenzo Franceschi-Bicchierai, "How Cyberattacks on Critical Infrastructure Could Cause Real-Life Disasters," *Motherboard*, August 16, 2016.

[49] U.S. Department of Defense, *Joint Operation Planning*, US Joint Publication 5-0, (Washington, DC: The Joint Staff, August, 11 2011), III-38 through III-44.

the world's and each other's perceptions of threat and response. The commander of U.S. Cyber Command stated in his 2012 Congressional testimony that China was responsible for the advanced persistent threat (APT) intrusion into the security firm RSA patented SecurID systems for multi-factor authentication.[50] Duplicate 'SecurID' electronic keys made with extracted information, explicitly by China, were then used to penetrate the networks of Lockheed Martin and several other US defense contractors in May 2011.[51] The Pentagon made further allegations against China in its 2013 annual report, alluding to the use of "computer network exploitation capability to support intelligence collection against the US diplomatic, economic, and defense industrial base sectors."[52] Exposure by an American company of a hacking campaign based in Shanghai focused on drone technology[53] confirmed the Washington Post published list of two dozen military systems compromised by cyber espionage emanating from China.[54]

At the Shangri-La Dialogue in Singapore in June of 2013, Defense Secretary Chuck Hagel voiced this concern about "the growing threat of cyber intrusions, some of which appear to be tied to the Chinese government and military." [55] In May 2014 the Justice Department indicted five members of the Chinese Military on charges of computer fraud, damaging a computer,

---

[50] Kelly Jackson Higgins, "China Hacked RSA, U.S. Official Says," *Dark Reading*, March 29, 2012.

[51] Jim Finkle and Andrea Shalal-Esa, "Hackers breached U.S. defense contractors," *Reuters*, May 27, 2011.

[52] U.S. Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," May 2013: 36.

[53] Edward Wong, "China's push for drones fueled by U.S. secrets," *International Herald Tribune*," September 23, 2013: 1.

[54] Oliver Knox, "Chinese hackers breach key US weapons designs," *Yahoo News*, May 28, 2013, and later further confirmation by Agence France-Presse, "Report: Chinese Soldiers Linked to US Military Hacking Case," *Defense News*, January 20, 2016.

[55] Reuben F. Johnson and James Hardy, "Hagel Reiterates Cyber Charges against China," *Jane's Defense Weekly*, June 12, 2013.

aggravated identify theft and economic espionage.[56] Officials noted that the difference in U.S. cyber activity is that economic advantage is obtained if China or others provide state-owned enterprises with extracted information to improve their competitive edge and reduce cost.[57] The cost to the United States in all kinds of intellectual property (product plans, research results, and customer lists) and confidential business information (trade secrets, exploration data, and negotiating strategies) theft amounts at least to "$200 to $250 billion annually."[58] While most of the intrusions seen to date originating from China appear to be for the purpose of collecting intelligence rather than launching attacks, each objective requires access and a compromise for espionage could become disruptive or destructive with little notice by the same actor.[59]

China has in return made much of what it calls the U.S.' "global" cyber activity, evidenced by the discovery in June 2010 of the Stuxnet virus infecting nuclear facilities in Iran.[60] More recent revelations prominently disparaged by Chinese statements include the United States penetrating of the servers of the telecommunications firm Huawei to learn how to conduct surveillance or offensive cyber operations against countries that buy the Chinese-made equipment.[61] After Washington filed criminal charges against the Chinese military officers in 2014, an editorial in the Global Times, a subsidiary of the People's Daily, the official journal of China's Communist Party said "Regarding the issue of network security, the US is such a

---

[56] United States District Court, Indictment, Criminal No. 14-118, Filed May 1, 2014: 1-48.

[57] Scott Jasper, "Are US and Chinese Cyber Intrusions So Different?" *The Diplomat*, September 9, 2013.

[58] McAfee, "Net Losses: Estimating the Global Cost of Cybercrime," with Center for Strategic and International Studies, June 2014: 1-23.

[59] United States, Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," April 2014: 34-35.

[60] David E. Sanger, "Obama Order Sped up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012.

[61] David E. Sanger, "N.S.A Breached Chinese Servers Seen as Security Threat," *New York Times*, March 22, 2014.

mincing rascal that we must stop developing any illusions about it." The Global Times asserted that the United States "spies both home and abroad with the PRISM program of the National Security Agency (NSA)" and "still owes an apology to Beijing" over the NSA hacking of its network.[62]

The challenge for national security is that, while the accusations are flying around, the deceiving, penetrating, exploiting and extracting continues to increase. The current responses are clearly insufficient and moving out of cybered conflict Phase Zero is highly undesirable. In China, the state–criminal nexus is apparent as cyber intruders who commit crimes and espionage use similar methods, for instance by employing the same Remote Access Trojan tools (that capture and extract information) to include Poison Ivy, Ghost, and PlugX.[63] Some state actors also 'moonlight' for financial gain, further complicating attribution. China also uses professional hackers for hire, like the Hidden Lynx group, located in China. Hidden Lynx hackers steal very specific information that could be used to gain competitive advantages at both the corporate and nation state level.[64] They have been engaged in several high-profile campaigns, to include Operation Aurora, the intrusions on Google and more than 30 other companies disclosed in 2010 that revealed the complexity and obscurity of advanced persistent threats (APTs).[65] Part of China and Iran's anti-access and area denial strategies to blunt outside interference is the condoning or out-sourcing of cyber power to proxy groups. An activist group known as the Cutting Sword of Justice took responsibility for the cyber destruction at Saudi Aramco. A hacker group called Izz ad-Din al-Qassam Cyber Fighters took credit in online posts for the previously

---

[62] "High-level hooligan: Chinese media vents spleen over US cybercrime charges," *RT News*, May 21, 2014.

[63] Kelly Jackson Higgins, "Chinese Cyberespionage Tool Updated For Traditional Cybercrime," *Dark Reading*, November 27, 2012.

[64] Stephen Doherty,Jozsef Gegeny, Branko Spasojevic, and Jonell Baltazar, "Hidden Lynx – Professional Hackers for Hire," Version 1.0, Symantec, September 17, 2013.

[65] William Jackson, "How Google Attacks Changed the Security Game," *Government Computer News*, September 1, 2010.

mentioned U.S. Bank assault in September 2012, supposedly in retaliation for an anti-Islam video that mocks the Prophet Muhammad. Investigators eventually traced attack signatures in both cases to Iranian hackers with government ties.[66] This multiplicity of instances by a nexus of nation states, hacker groups, and criminal organizations that are now in the public domain is presumably matched by many more not publicly known.

Deterrence – The Preferred Alternative to War

The number of actors to be deterred is the first of many challenges in applying the contemporary deterrence approach. For a deterrence strategy to be implemented well and to be effective, however, three elements are essential: capability (possessing the means to influence behavior), credibility (instilling believability that counter actions may actually be deployed), and communication (sending the right message to the desired audience).[67] The achievement of these conditions for effective deterrence is extremely difficult in cybered conflict. State capabilities to influence the behavior of malicious actors in cyberspace are constrained by their ability to operate with anonymity, impunity and deniability. Even if actors are convinced that counter actions may be deployed, their rationality cannot be assumed; and the audience of actors conducting cyber attacks is vast and varied in motivations and intentions.

The point of deterrence is to add another consideration to the attacker's decision making calculus[68] and (for the U.S. and others) this lends itself to extended deterrence to friends and allies and multiple actors such as NATO and the EU. Yet affecting a wide array of actors in cyberspace is a problem since deterrence has to work in the mind of each attacker under different

---

[66] Siobhan Gorman and Julian E. Barnes, "U.S. Says Iranian Hackers Are Behind Electronic Assaults on U.S. Banks, Foreign Energy," *The Wall Street Journal*, October 12, 2012.

[67] Department of Defense. *Joint Operations.* Joint Publication 3-0. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 17 January 2017): xxii.

[68] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, (Santa Monica, California: RAND Corporation, 2009): 6-37.

circumstances. Even if the attacker is rational, their motivations to achieve political objectives, national pride, personal satisfaction or monetary gain are not easily deterable. Rationality was a big part of Cold War nuclear deterrence thinking which has informed the cyber deterrence debate. Chris Demchak has offered an alternative "theory of action" in which a malicious actor or group's decision is a function of legitimacy, need, and confidence related to the act itself, the latter primarily through transforming the ease of action, irrespective of actor culture,[69] which means increased confidence by any party that the act will succeed. The more each of those elements is pushed below a threshold; the malicious act is 'disrupted.' But pushing the elements for a wide range of actors simultaneously is difficult, making retaliation and entanglement hard to implement.

Hence a new means of deterrence is required for a cybered world. Recognizing the need to "integrate newer behavioral approaches outside a rational state based actor construct," the Assistant Chief of Staff for U.S. Strategic Deterrence and Nuclear Integration recommended moving beyond reliance solely on "imposition of costs to integrate denial of benefits and other methods for encouraging restraint."[70] Therefore to move beyond Cold War relics, the focus must be on closer linking deterrence to the desired effect of altering behavior, regardless of the actor being deterred.[71] For rational state actors, the strategy of deterrence by entanglement can encourage responsible behavior (to not conduct, endorse or allow malicious cyber activity in their territory) through cooperation based on economic and political relationships between governments. However for the wider array of malicious actors, a different paradigm or concept has to be considered to achieve the central premise of deterrence – altering behavior.[72]

---

[69] Chris Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*, (University of Georgia Press, September 2011).

[70] William A. Chambers, "Foreword," in *Thinking About Deterrence*, Adam Lowther, editor, (Maxwell Air Force Base, Alabama: Air University Press, 2014): xii.

[71] Adam Lowther, "The Evolution of Deterrence," in *Thinking About Deterrence,* Adam Lowther, editor, (Maxwell Air Force Base, Alabama: Air University Press, 2014): 3-4.

[72] Ibid.

An updated strategic option and the main concern of this work – is one designed for this new form of continuous cybered conflict, titled "active cyber defense". The strategy reinforces both deterrence by denial and deterrence by retaliation. It combines internal systemic resilience to halt malicious cyber activity after an intrusion with tailored disruption capacities to thwart malicious actor objectives.[73] Hence active cyber defense supports denial by making it harder to carry out a cyber attack and supports retaliation by providing more options to inflict punishment, to include a series of offensive cyber options. As a combined and new means to achieve deterrence, active cyber defense also enhances adversary propensity for restraint in peacetime cybered conflict by shaping the adversary's perceptions of costs and benefits of a cyber attack irrespective of the character or number of actors to be deterred.[74] Active cyber defense involves the synchronized detection, analysis and mitigation of network security breaches in cyber relevant time combined with the aggressive use of legal countermeasures deployed outside the victim's network by authorized entities.[75] Inside the defender's network, active cyber defense stops or limits damage through detective controls and remediation actions, seamlessly automated in a common framework of integration – which is offered by many companies. The promise of active cyber defense is in internal countermeasures that act without regard to the identity or type of malicious actor or their motivations, only to detect, isolate or eradicate their malware. Outside

---

[73] Chris C. Demchak, "Economic and Political Coercion and a Rising Cyber Westphalia," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 595-620. This work introduces the concepts of *systemic resilience* and *disruption capacities* in socio-technical-economic systems as key components of relative national power in a cybered world. My thesis expands the concepts and repurposes them for a different intent in arguing for a new means for deterrence.

[74] Schulyer Forester, "Strategies of Deterrence," *Conflict and Cooperation in the Global Commons,* (Georgetown University Press, September 2012): 55-67.

[75] Robert S. Dewar, "The Triptych of Cyber Security: A Classification of Active Cyber Defense," in *Proceedings 6th International Conference on Cyber Conflict* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, June 2014): 7-21.

the victim's network, active cyber defense offers a range of countermeasures for use by the state or private organization depending on technical feasibility and legal authorities. The selection of countermeasures will vary for the type of malicious actor based on circumstances and risk, which is not a small issue whether in the U.S. or in other liberal democracies to different degrees, and can take time, at the right level, and with the necessary expertise to correctly analyze it.

The main issue today was summed up well by Senator Inhope, during the 2014 Senate Hearing to consider the nomination of the new commander for U.S. Cyber Command, who said, "the lack of a cyber-deterrence policy... [has] left us more vulnerable to continued cyber aggression." When the nominee was asked "how do we prevent that," Vice Admiral Rogers responded "We're generating capability, we're generating capacity...But in the end I believe we've got to get some idea of deterrence within the cyber arena."[76] The concept of contemporary deterrence is still debatable because of its origin in traditional nuclear deterrence which relies on an adversary having knowledge of the destruction that will result from misbehaviors. That clarity, however, is not possible in cyber since the secrecy about cyber weapons is necessary to preserve their effectiveness.[77] The strategy of active cyber defense, however, does not intrinsically require clear adversary knowledge of the mechanisms that defeat attacks. It also appears less likely to escalate conflict by requiring the deterring state to make demands or posture in a threatening manner either. The promise of active cyber defense warrants examination of evidence to determine if it is more likely to alter behavior than current methods attempted for contemporary deterrence strategies in the emerging forum of peacetime conflict. Nuclear deterrence theories are cannot be read across directly into cyber. Among the reasons are the range of actors and the low barriers to entry.

---

[76] "Hearing to consider the Nominations of ... VADM Michael S. Rogers, USN to be Admiral and Director, National Security Agency/ Chief, Central Security Services/ Commander, U.S. Cyber Command," Statements Before the Senate Committee on Armed Services," 11 March, 2014.

[77] Zachary Fryer-Biggs, "US Cyber Moves Beyond Protection," *Defense News*, March 16, 2014.

Thesis Research Question

To what extent, in a deeply cybered world, does active cyber defense for a largescale modern state mitigate the systemic security losses of transnational cyber attacks more comprehensively than the contemporary deterrence strategies of retaliation, denial, or entanglement?

Given the breadth, speed, and volume of cyberspace's predators, active cyber defense technologies will be automated and have the ability to interdict, isolate or remove threats. As a means to strengthen deterrence, the intent of active cyber defense is to deny benefits to adversaries by ensuring systemic resilience, by engaging, deceiving or stopping adversaries, and by imposing costs through disruption capacities, regardless of the source. The concept of "systemic resilience" means a defender's state or network has the capacity of combined social and technical systems to proactively recognize, adapt to, absorb, and innovate around disturbances or disruptions.[78] Given how the nature of cyber attacks has changed, it would be ideal to develop comprehensive, overarching internal systemic resilience and tailored disruption capacities[79] to meet the failings, or limits, of contemporary deterrence strategies. However that level of comprehensive deterrence will take time. The implementation of this form of robust cyber power will require unprecedented peacetime cooperation among all stakeholders in industry, government and defense spheres due to the inherent complexity in socio-economic-technical systems. The necessary self-organizing order in interactions between these complex adaptive systems with so many interconnected parts will take a long time to establish.

In the interim, the nation's national security community needs to consider less all-inclusive strategies for deterrence such as active cyber defense, those that center on collaborative

---

[78] Louise K. Comfort, Arjen Boin, and Chris C. Demchak, *Designing Resilience: Preparing for Extreme Events*, (University of Pittsburgh, September 2010.): 1-12.

[79] Chris C. Demchak, "Economic and Political Coercion and a Rising Cyber Westphalia," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 595-620.

efforts with fewer actors to achieve some greater measure of deterrent '*emergence'* in complex systems. The property of *emergence* is roughly described by the common phrase "the action of the whole is more than the sum of the actions of the parts."[80] As a first step, the 2009 U.S. Cyberspace Policy Review identified the need for a comprehensive framework to facilitate coordinated response by government, the private sector, and allies to a significant cyber threat or incident. The report recognized that "addressing network security issues requires a public-private partnership as well as international cooperation and norms."[81] Likewise, the 2014 U.S. Joint Staff Unity of Effort Framework Solution Guide recognized that the government and the private sector have to coordinate their activities to prepare for cyber threats. The Joint Staff realized that achieving unity of effort to meet national security goals is problematic due to challenges in information sharing, competing priorities, and uncoordinated activities.[82] PPD-41 issued by the White House in 2016 codified that "significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors."[83]

NATO experiences offer an example of how to design a comprehensive approach for operations in a domain of interest (like cyber deterrence). The former director of the National Security Agency (NSA) argued "government, industry and our allies have to work together" to prepare for catastrophic cyber attacks in our future.[84] The North Atlantic Treaty Organization

---

[80] John H. Holland, *Complexity: A Very Short Introduction*, (Oxford University Press, 2014).

[81] United States, Executive Office of the President, "Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communication Infrastructure" (Washington, DC: The White House, May 2009), i.

[82] US Department of Defense, *Unity of Effort Framework Solution Guide*, (Suffolk, Virginia: US Joint Staff J-7, August 31, 2014) Foreword.

[83] Executive Office of the President, *Presidential Policy Directive – United States Cyber Incident Coordination*, PPD-41, (Washington, DC: The White House, July 26, 2016).

[84] Cheryl Pellerin, "Alexander: Defending Against Cyberattacks Requires Collaboration," News Article, Defense.gov, October 30, 2013.

(NATO) has for decades aligned parties in various operations through a comprehensive approach based on shared “principles and collaborative processes that enhance the likelihood of favorable and enduring outcomes within a particular situation.”[85] NATO stated “the need to promote a comprehensive approach applies not only to operations, but more broadly to many of NATO’s efforts to deal with 21st century security challenges, such as…protecting against cyber attacks.”[86] To be effective in continuous cybered conflict, the NATO methodology has to be adapted for different operational conditions, structural characteristics, and prominent partners, to include private sector actors. The White House has also embraced a comprehensive approach for cyber deterrence by endorsing public and private sector partnerships for cyber defense of critical infrastructure sectors.[87] Within this context, a partnership would be defined as close cooperation between parties having common interests in achieving a shared vision. The 2010 Comprehensive National Cybersecurity Initiative sought to create such an approach to cyber defense strategy that deters “interference” and attack in cyberspace.

The challenge is to align the efforts of all parties for a common purpose in all means of deterrence. However, if one accepts that contemporary deterrence does not work well in a cybered conflict world, and this partnership lags in its unity of effort in a whole of nation approach, then active cyber defense offers a means to strengthen deterrence by combining systemic resilience and disruption capacities in the interim period, allowing time for all participants to adjust and align efforts for a longer term, comprehensive deterrence strategy. An analysis of the sufficiency of strategic cyber deterrence options (retaliation, denial, entanglement or active cyber defense) to alter malicious actor behavior in cyberspace requires answers to the following questions:

---

[85] United Kingdom, Ministry of Defence, “The Comprehensive Approach,” Joint Discussion Note 4/05, Shrivenham: Joint Doctrine and Concepts Centre, 2006: 1-4 to 1-5.

[86] North Atlantic Treaty Organization, “A Comprehensive Approach,” 27 October 2010.

[87] United States, Executive Office of the President, *The Comprehensive National Cybersecurity Initiative*, Initiative #10 and 12, March 2010: 5.

Sub-questions

1. *To what extent will the threat of the use of all necessary means, often in kind, in response to hostile acts in cyberspace achieve deterrence by retaliation?*
2. *By what degree do protective measures improve the security of networks and systems to deny adversaries the benefit of attack?*
3. *To what level will cooperative measures for entanglement based on mutual interests restrain behavior in conducting, endorsing or allowing malicious cyber activity?*
4. *By what extent does evidence show that active cyber defense is technically capable and legally viable as a comprehensive means for dissuading and deterring malicious actors?*

Research Design

Grounded theory research methods were used to examine deterrence strategy options based on empirical evidence. This approach requires pursuing empirical research guided by the theories of *strategy* and *deterrence* while allowing the data to manifest elements emergent in a cybered world and not anticipated in the other approaches. *Strategy* is described as the direction and use made of means by chosen ways in order to achieve the desired ends of national policy.[88] *Deterrence* is about decisively influencing decision making by threatening to impose costs, or denying benefits, while encouraging restraint.[89] This process of research grounded in qualitative data,[90] is intended to produce a proposed midrange theory of deterrence by *active cyber defense*. The discussion starts with the empirical phenomenon and abstracts from it to create general

---

[88] Arthur F. Lykke, Jr. "Toward an Understanding of Military Strategy," *Guide to Strategy*, (Carlisle Barracks: US Army War College, 1983), February 2001: 179-185.

[89] Kevin Chilton and Greg Weaver, "Waging Deterrence in the Twenty-First Century," *Strategic Studies Quarterly*, Vol. 3, Issue 1, (Spring 2009): 31-42.

[90] Kathy Charmaz, *Constructing Grounded Theory,* 2nd Edition, (London: SAGE Publications Ltd, 2014): 1-21.

concepts that can be verified by data.[91] In particular, concepts of *systemic resilience* and *disruption capacities*,[92] both essential to security from attacks, are the tests of comprehension, for all deterrence methods and data is analyzed to demonstrate the relative effectiveness of the contemporary and new deterrence methods.

Source material is drawn from a combination of informative meetings and literature review. The data is primarily qualitative. Informative meetings were conducted with public agency and private sector decision makers, program experts, and security practitioners in the fields of national security and cyber strategy. For instance, meetings were held at U.S. Cyber Command, the National Security Agency, Commander, U.S. Tenth Fleet, U.S. Department of Homeland Security (Office of Cybersecurity & Communications and Intelligence & Analysis), and the John's Hopkins Applied Physics Lab. In the United Kingdom, the thesis was discussed with the Foreign & Commonwealth Office, the Development, Concepts and Doctrine Centre, Royal United Services Institute, Defence Academy of the United Kingdom, Chatham House, and RAND Europe. Consultations on security technologies were conducted with Palo Alto Networks, Hexis Corporation, Akamai, Carbon Black, Crowdstrike, Cylance, Dell, FireEye, Hewlett Packard, IBM, LightCyber, LogRhythm, Looking Glass, Sophos, Splunk, Watchguard and others in the range of solutions. Primary literature consists of testimony, documents, concepts, publications, reports, papers, media outlets and blogs that form raw intelligence, and secondary literature was used in the form of published books, chapters, essays, articles, and studies. The data was constructed and unearthed data observations, interactions and materials gathered on the topics in the Research Sub-questions and also study of related empirical events and experiences. Simultaneous data collection and analysis occurred through constant comparison, with pauses to capture instantaneous realizations of analytical connections.

---

[91] Robert K. Merton, "On Sociological Theories of the Middle Range," *Classical Sociological Theory*, Third Edition, (West Sussex, United Kingdom: Blackwell Publishing, 2012): 531-542.
[92] Chris C. Demchak, "Economic and Political Coercion and a Rising Cyber Westphalia," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 595-620.

The initial collection and consideration of data started an iterative process of interpretation of categories based on segments of data. The rich and voluminous array of malicious actors, their methods in incidents, and their campaigns of malicious cyber activity provide considerable data for categorization to compare and contrast analyses. The analysis addresses the evidence of limits to or constraints on the effectiveness of the strategic deterrence options of retaliation, denial, entanglement and active cyber defense as formally stated in the research sub-questions. Specific measures of attacks, time, and costs are used where applicable to evaluate option utility and sufficiency. For example, at the tactical level, the analysis considers the impact of the options on attacks (number of attempted or successful penetrations by the attacker), time (of threat detection, response and mitigation by the defender), and costs (for the attacker or defender). Then at the strategic level, the analysis considers the impact of the options on attacks (volume of noise across social, technical and economic systems generated by the attacker), time (in mitigation of systemic security losses by the defender), and costs (in the order of magnitude of gross domestic products for the defender), although difficult to accurately judge. The measures are used to determine whether these options are more or less comprehensive than the concepts of *systemic resilience* and *disruption capacities.* The result is a midrange theory of *active cyber defense.*

Key Options for Analysis

A summary of the initiatives, issues and constraints identified and analyzed in the four strategic option sections is presented below:

Deterrence by Retaliation is defined by the effort to directly impose costs for hostile acts in cyberspace. Retaliation is based on “the right to use all necessary means” in order “to defend our Nation, our allies, our partners and our interests.”[93] Means for a proportional and justified

[93] Executive Office of the President, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 14.

response include "diplomatic, informational, military, and economic, as appropriate and consistent with applicable international law."[94] Military response options may include the employment of cyber (or cyber physical) and/or kinetic capabilities. Under some circumstances, hostile acts in cyberspace could constitute an armed attack within the meaning of Article 51 of the UN Charter.[95] Established principles would apply in the context of an armed attack (*Jus ad bellum*).[96] First, the right of self-defense applies against an imminent or actual armed attack whether the attacker is a State or non-State actor.[97] Second, the use of force in self-defense must be limited to what is necessary and proportionate to address the nature of the threat.[98] Third, States are required to take measures to ensure their territories are not used for purposes of armed activities against other States. The use of cyber tools in the context of armed conflict (*Jus in bello*) is addressed by existing rules and principles of the international law of armed conflict.[99]

Hostile acts include armed attack, and damage. On whether or not a cyber operation constitutes an armed attack, according to the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Rule 71), "depends on the scale and effects."[100] Cyber operations that result in death or injury of individuals or destruction or damage of objects could be defined as an armed attack.[101] Although Stuxnet caused physical damage, the international

---

94 Ibid.

95 Office of General Counsel, *Department of Defense Law of War Manual*, June 2015 (Updated May 2016). 1016-17.

96 Ibid, 1015.

97 Ibid, 1018.

98 Ibid.

99 Ibid, 1020-22.

100 Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017), 339.

101 Michael N. Schmitt, "Attack as a Term of Art in International Law: The Cyber Operations Context," *Proceedings 4th International Conference on Cyber Conflict*," (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2012): 283-293.

group of experts who authored the Tallinn Manual was divided on whether the damage constituted an armed attack. Future cyber attacks could be designed to transmit data or modify, degrade or corrupt data in a malicious but not immediately noticeable manner that could avoid the obvious damage threshold and yet be damaging.[102] The NATO Enhanced Cyber Defense Policy affirms that cyber defense is part of NATO's core task of collective defense. Any decision as to whether a cyber attack would invoke Article 5 of the Washington Treaty is subject to political decisions by the North Atlantic Council on a case-by-case basis.[103] Although the manner in which the North Atlantic Council would assess each cyber attack remains ambiguous. No standards for assessment exist and countries hold various and differing internal criteria.[104] This ambiguity gives an adversary the option to use cyber as a method of attack against critical infrastructure.[105]

The imposition of costs in deterrence by retaliation is intended to reduce any threat actor's willingness or ability to initiate or continue an offensive operation. While some argue the fundamental interconnectedness of networks means the effects of responsive cyber operations cannot be limited, others claim as a point of debate that contained operations are possible even within broadly connected systems.[106] However, deliberate, inadvertent or accidental escalation could trigger a chain reaction that raises the level of conflict beyond any contemplated by any

---

[102] Martin R. Stytz and Sheila B. Banks, "Toward Attaining Cyber Dominance," *Strategic Studies Quarterly* Vol. 8, Issue 1 (Spring 2014): 60.

[103] North Atlantic Treaty Organization, "Wales Summit Declaration", Paragraph 72, September 5, 2014.

[104] Stephen Jackson, "NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack," Center for Infrastructure Protection & Homeland Security, George Mason University, August 16, 2016.

[105] V. Joubert, "Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?" *Research Paper*, No. 76, Rome: NATO Defense College, May 2012: 5.

[106] Maren Leed, "Offensive Cyber Capabilities at the Operational Level," Center for Strategic & International Studies," September 2013: 2-3.

party to the conflict.[107] In the United States only the president can approve a cyber operation likely to result in significant consequences, a tough decision due to an inability to predict collateral damage and uncertainty over political effects.[108] Equally, the threat of massive cyber retribution would probably encourage actors to seek low levels of cyber attacks that fall below the threshold that would trigger such retaliation in kind.[109] In many cases, victim countries may be constrained to seek justice rather than retribution. In court, victim states can press for access to individuals or information and use refusal to cooperate as a justification for retaliation. However, until retaliation by any means does ensue, there is no punishment and hence, this deterrence option is extremely limited in a world of cybered conflict.[110]

Deterrence by Denial is defined as the effort to withhold any benefit from malicious activity in cyberspace and thereby over time encourage perceptions of cyber attacks as pointless endeavors. Denial of any malicious actor's objectives occurs by increasing the security of networks and systems. In this context, security is "a condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems."[111] In this context, protective measures limit damage by reducing the risk of an attack succeeding. Specific actions for risk reduction can include the promulgation of security strategies or policies to avoid

---

[107] Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, Vol. 6, Issue 3, (Fall 2012): 52-55.

[108] James Lewis, "Low-level cyberattacks are common but truly damaging ones are rare," *The Washington Post*, October 9, 2013.

[109] Sean Lawson, "Putting the war in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States," *First Monday*, Volume 17, Number 7, July 2, 2012.

[110] Martin Libicki, "Pulling Punches in Cyberspace," *Proceedings of a Workshop on Deterring Cyberattacks*, (Washington, D.C.: The National Academies Press, 2010). 123-147.

[111] Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST), "Glossary of Key Information Security Terms," NISTIR 7298, Revision 2, May 2013: 173.

or accept risk; the implementation of security controls to mitigate or diminish risk; and organizational arrangements to share or transfer risk.[112] A variety of protective measures are contained and endorsed in best practice guidelines for businesses, organizations and consumers. An example of a best practice for security strategies is the employment of a defense-in-depth approach that emphasizes "multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method."[113] Examples of best practices regarding security policies include the use of encryption to protect sensitive data, the restriction of removable media, and the enforcement of effective passwords.

While best practice guidelines help reduce risk from cyber threats, more methodical approaches for the identification and application of other protective measures, like specific safeguards, are contained in a variety of frameworks. Safeguards are prescribed to protect the confidentiality, integrity, and availability (the CIA triad) of an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Safeguards are synonymous with security controls.[114] The Center for Internet Security (CIS) produced Critical Security Controls for Effective Cyber Defense offers a set of actions based on the combined knowledge of actual attacks and effective defenses.[115] The controls deny benefit of attack by monitoring networks and systems, detecting attack attempts, identifying compromised machines, and interrupting infiltration. The top three

---

[112] Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST), "Managing Information Security Risk," NIST Special Publication 800-39, March 2011:41.

[113] Symantec Corporation, "Internet Security Threat Report," Volume 19, April 2014: 87-89.

[114] Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST), "Security and Privacy Controls for Federal Information Systems and Organizations," NIST Special Publication 800-53, Revision 4, Appendix B, April 2013: B-20.

[115] The Center for Internet Security, "The CIS Critical Security Controls for Effective Cyber Defense," Version 6.0, October 15, 2015: 1- 89.

drivers for adopting the controls are increasing visibility of attacks, improving response and reducing risk.[116] When the U.S. Congress failed to pass necessary legislation, President Obama signed an Executive Order for the development of a Cybersecurity Framework that incorporates voluntary consensus standards and industry best practices. The initial Cybersecurity Framework is built around the core functions of identify, protect, detect, respond, and recover.[117] The Critical Security Controls are part of the Framework's informative references that illustrate ways to accomplish core functions and thereby make attacks on systems either less possible or less costly even if they succeed initially.

Cyber intelligence on threats and vulnerabilities leads to better risk-informed decision making on investments in relevant security controls. Organizational arrangements for the sharing of cyber intelligence are another form of protective measures to reduce risk, although horizontal sharing may lead to leaks. As mandated in the 2013 Executive Order, the National Cybersecurity and Communications Integration Center (NCCIC) coordinates with the private sector, and also government and international partners as a mechanism in deterrence by denial. The NCCIC integrates analysis and data into a comprehensive series of actionable and shareable information products. In addition, the NCCIC cooperates with information sharing and analysis centers (ISACs) to protect portions of critical information technology that they interact with, operate, manage, or own. For example, the NCCIC worked with the Financial Services ISAC during the 2012 series of DDoS assaults on U.S. major banks to provide technical data and assistance to financial institutions. Data included DDoS related IP addresses and supporting

[116] John Pescatore and Tony Sager, "Critical Security Controls Survey: Moving From Awareness to Action," A SANS Whitepaper, June 2013.

[117] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, February 12, 2014.

contextual information, which was also given to over 120 international partners.[118] The NCCIC has been designated by PPD-41 as the lead coordinator for asset response.[119]

The deterrence option, however, is limited in its comprehensive potential due to the need for real time, actionable data sharing among competitors for markets and with government agencies. Critical actors in agencies and companies acknowledge the need to share more individual information about threats across enterprise boundaries but are worried about their organization's liability and the ambiguities of cybered risk. Commercial offerings to share data - such as the Internet Identity's (IID) Active Trust platform – allow contributors to retain ownership of data and control dissemination.[120] Yet in reality, only cybersecurity legislation can permit the private sector to share real-time cyber threat activity detected on its networks without fear of violating civil liberties and rights to privacy of citizens.[121] In December 2015, President Obama signed the "Cybersecurity Act of 2015" as part of an emergency budget omnibus bill. The legislation gives liability protection to companies that share information with the government but requires them to strip away personal data first.[122] Even with passage of this legislation, participation in sharing arrangements - and adoption of industry best practices - for securing cyberspace remains voluntary for the private sector that largely owns the Nation's

[118] Roberta Stempfley and Lawrence Zelvin, "Statement Before the House Committee on Homeland Security," May 16, 2013.

[119] DHS Press Office, "Statement By Secretary Jeh C. Johnson Regarding PPD-41, Cyber Incident Coordination," July 26, 2016.

[120] William Jackson, "Social platform for sharing cyber threat intel opens up," *Government Computer News*, March 2014: 6.

[121] Keith B. Alexander, "Statement Before the House Committee on Armed Services," March 12, 2014.

[122] U.S. Congress, "Consolidated Appropriations Act, 2016," Division N- Cybersecurity Act of 2015, December 15, 2015: 1728-1770.

critical infrastructure.[123] This is the same private sector that routinely discovers 85% of cyber breeches from an external party usually many months after an intrusion.[124] Today the average is around 150 days after the breach.[125] This private sector laggardly participation remains despite the reality that it is not a matter of if a company will be breached, but when.[126] Hence, this deterrence option is also limited in its effectiveness for the near term cybered conflict.

Deterrence by entanglement is defined as an effort to encourage responsible state behavior (and thus restrain malicious behavior) by raising the perceived value of maintaining and not endangering the returns from government to government cooperation on mutual interests. To some extent, nations share political, economic, commercial, and strategic interdependence in cyberspace and so all too some degree share vulnerability. The United Nations Secretary General has stated "While all Nations appreciate the enormous benefits of ICTs [Information and Communication Technologies], there is also broad recognition that misuse of the cyberspace substrate poses risks to international peace and security."[127] The 2013 report by the Group of Governmental Experts (GGE) emphasized this shared vulnerability by observing that the "development and spread of sophisticated malicious tools and techniques" for cyber attack increases "the risk of mistaken attribution and unintended escalation."[128] The GGE report also noted that states have affirmed the need for cooperative action against threats resulting from misuse of ICTs. While states have to lead these efforts, effective cooperation also rests on

---

[123] Department of Homeland Security, "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," March 2013: 1-14.

[124] Verizon, "2014 Data Breach Investigations Report," June 2014: 41.

[125] Mandiant, "M-Trends 2016," Special Report, February 2016: 4.

[126] Danny Palmer, "It is not about if you will be penetrated, but when, warns NSA Chief," *Computing News*, July 16, 2015.

[127] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, 24 June 2013: 4.

[128] Ibid, 6-7.

participation by the private sector and civil society to achieve a comprehensive result as required. The 2013 report, and an updated version in 2015, specified an array of actions, to include norms, rules and principles of responsible State behavior in cyberspace, such as prohibiting harm to critical infrastructure and emergency response systems, and other confidence building measures intended to further deterrence through risk reduction.[129]

One action to strengthen deterrence by entanglement is the formal implementation of binding agreements between states. Arms control treaties aim to establish legal regimes that make conflict less likely by reducing the existence of, or restricting the use of certain weapons. However, imposing limitations on the development and proliferation of what has been called "cyber-weapons" is difficult. Their properties - especially their ubiquitous ease of deception and opaqueness, speed of action, and complexity - are incompatible with the conditions of standing arms control treaties.[130] The lack of universal consensus on what even constitutes a "cyber-weapon" complicates verification of compliance. Most of the technology relied on in an offensive capacity is inherently dual-use. The means, control and distribution are created, held, and employed by a large array of non-state as well as state actors. Vulnerability assessment tools that scan an organization's systems and data for security gaps can relatively easily be reused in an attack to gain illegal access.[131] Otherwise helpful software can be repurposed with minimal effort for a variety of malicious actions.[132] Another hindrance for arms control enforcement is that the creator or source of the weapon is often not the user. For example, in state sponsored

---

[129] Ibid, United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, 22 July 2015: 8-9.

[130] Louise Arimatsu, "A Treaty for Governing Cyber-Weapons," *Proceedings 4th International Conference on Cyber Conflict*, (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2012): 91-109.

[131] Brad Causey, "Finding Vulnerabilities by Attacking Your Own Environment," *Information Week Reports*, November 2012.

[132] United States, Department of Defense, *Cyberspace Policy Report*, November, 2011: 8.

hacktivist campaigns, cyber tools with instructions are often provided by third parties to patriotic hackers supporting a cause or casual opportunists who happen to join in the attack.[133]

Absent useful formal treaties, a broad assortment of other more cooperative measures has been promoted to restrain state activity, or state sponsored or endorsed activity, from malicious activity in cyberspace. Internationally acceptable norms, rules and principles of responsible behavior by states could ensure order in cyber activity if fully implemented and enforced. They start with the premise that international law, and in particular the Charter of the United Nations is applicable to cyberspace and thereby enforceable with the same mechanisms. The Seoul Conference on Cyberspace in 2013 resulted in a 'Framework for and Commitment to Open and Secure Cyberspace' that offers guidelines for governments and organizations on coping with cybercrime and cyberwar.[134] These guidelines include verbatim norms of behavior proposed in 2013 by the UN Group of Government Experts for States to meet their international obligations regarding wrongful acts attributed to them, refrain from using proxies to commit wrongful acts, and ensure their territories are not used by non-State actors for unlawful acts.[135] The fourth Global Conference on Cyberspace in The Hague in 2015 is a particularly good exemplar of these entanglement – as – deterrence efforts. The meeting gathered representatives from governments, private sector and civil society "to promote practical cooperation in cyberspace, to enhance cyber capacity building, and to discuss norms for responsible behavior in cyberspace."[136]

---

[133] Parmy Olson, *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (New York: Back Bay Books: May 14, 2013).

[134] H.E. Yun Byung-se, Minister of Foreign Affairs, "Seoul Conference on Cyberspace," Seoul, South Korea, October 17-18, 2013.

[135] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, 24 June 2013: 8.

[136] "About the Global Conference on CyberSpace," The Hague, 16-17, April 2015.

Regional or bilateral dialogue have been able to establish voluntary confidence-building measures to promote trust and assurance, such as those agreed upon by the United States and Russia in 2013 for sharing of cyber threat indicators.[137] Other practical measures to increase predictability and reduce misperception include exchange of views on national policies, like an informative briefing by the Obama Administration in 2014 to Chinese officials on Pentagon doctrine for defending against and conducting cyber attacks.[138] Finally, capacity-building assistance is recognized as a likely need for some States to fulfil their responsibilities in any form of agreement for securing cyberspace. Efforts for assistance range from developing technical skill and sharing best practices, to strengthening national legal frameworks.[139]

Overall, cooperative measures do have the potential to address cyber related threats, vulnerabilities and risks in some considerable measure, but they require extensive cooperation that is often thwarted by a clash of competing state interests in addition to the role of non-state actors. For example China suspended a Sino – US working group on cyber issues after the indictment of the Unit 61398 members, citing "we should encourage organizations and individuals whose rights have been infringed to stand up and sue Washington."[140] Reasons for tension in cooperation with China on matters of international governance can be explained by standard international relations theory. Realists argue that China "did not have a hand in creating" the existing architecture and, as China becomes more powerful, it would naturally seek

---

[137] Executive Office of the President, "Fact Sheet: US–Russian Cooperation on Information and Communications Technology Security" (Washington: The White House, June 17, 2013).

[138] David E. Sanger, "U.S. Tries Candor to Assure China on Cyberattacks," *New York Times,* April 6, 2014.

[139] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7 February 2013: 1-20.

[140] "High-level hooligan: Chinese media vents spleen over US cybercrime charges," *RT News*, May 21, 2014.

to alter international institutions.[141] Others say the authoritarian regime is "uncomfortable with a multi-stakeholder system" guided by concerns for the rights of individuals and flexible attitudes toward state sovereignty.[142] Chinese leaders state that "China has been a 'rule-taker,' but is becoming a 'rule-maker' who is promoting new norms and rules of the game that fit its national interests."[143] Likewise, the Russian mantra of "new rules or no rules"[144] obstructs cooperation on international governance with civil society democracies in particular.[145]

This discussion demonstrates how each of three contemporary deterrence strategies are not comprehensive enough to adapt to the needs of cyber conflict in the near or possibly longer term. The strategic option of active cyber defense, however, is a fourth choice potentially capable of reinforcing the other three in the near and long term. In this work, *active cyber defense* is defined as the automated real-time detection, analysis and mitigation of network security breaches for systemic resilience combined with the aggressive use of legal countermeasures beyond network and state territorial boundaries for tailored disruption. It is designed to meet the gaps in comprehensiveness present in the other deterrence options but needed urgently for a robust national cybered defense. Scholars have described active cyber defense as a range of actions that engage the adversary before and - especially - during a cyber incident. Their listings of the gamut of applicable activities include the use of honeypots, beaconing, sinkholing, and deception – all of which increase adversary costs through

[141] Scott Kennedy, "China in Global Governance: What Kind of Status Quo Power?" Chapter One, *From Rule Takers to Rule Makers: the Growing Role of Chinese in Global Governance*, Co-published by the Research Center for Chinese Politics and Business and the International Centre for Trade and Sustainable Development, September 2012: 9.

[142] Ibid.

[143] Ibid.

[144] Stephan Blank, "How the U.S. should counter Putin's unbridled expansionism," *Newsweek*, September 9, 2015.

[145] Fyodor Lukyanov and Ivan Krastev, "New Rules or No Rules?" XI Annual Valdai Discussion Club Meeting Participants Report, Moscow, 2015: 1-28.

interference, delay, obstruction, or trickery.[146] Typical examples of these techniques, in order of the above intent, would be use of a honeypot to see which files the adversary wants to steal, remotely tracking stolen files by passive watermarks, redirecting the malware on an infected computer to communicate not with an attacker but with a safe server, or allowing the attacker to steal files that contain false or misleading information.[147] More aggressive countermeasures outside of the victim's network include "taking control of remote computers to stop attacks" or "launching denial of service attacks against attacking machines."[148]

Today the cyber security industry is shifting to more reactive forms of active cyber defense, predicated on automated and integrated technologies that have the ability to identify, interdict, isolate or remove threats inside the network within defined action limits.[149] Active cyber defense, as an announced strategy strengthens deterrence against attacks by combining systemic resilience and disruption capacities. Part of the failure of the three contemporary options is that they do not easily operate to defeat the attack at the speed and scale needed for cyberspace and thereby add failure to perpetrators' calculations about costs and benefits of such operations. An early pioneer in the field was Hexis Cyber Solutions, which created and fielded HawkEye G as an automated threat removal platform – an early prototype for active defense capabilities.[150] This next generation cyber security platform, now acquired by Watchguard

---

[146] Franklin D. Kramer and Melanie J. Teplinsky, "Cybersecurity and Tailored Deterrence," Atlantic Council, December 2013: 6.

[147] Irving Lachow, "Active Cyber Defense: A Framework for Policy Makers," Center for a New American Security, February 2013: 1-10.

[148] Matthew Monte, *Network Attacks and Exploitation: A Framework* (Indianapolis, IN, John Wiley & Sons, Inc: August 2015).

[149] James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival: Global Politics and Strategy*, Vol. 54, Issue 4, August 1, 2012: 110.

[150] Hexis Cyber Solutions, "HawkEye G," Data Sheet, 2015: 1-2.

Technologies,[151] provides endpoint and network sensing, threat detection analytics, and automated countermeasures that "remove advanced threats at machine speed from within the network" before adversaries can "steal data, compromise intellectual property or cause process disruption."[152] Once HawkEye G detects and investigates a cyber threat, it deploys network-based countermeasures (like blocking traffic or redirecting it to a Bot Trap) and host-based countermeasures (such as killing the malware process or quarantining malicious files) to remediate and remove the threat.[153] In respect for corporate reluctance to adopt machine-enabled defensives for fear of algorithmic misfires with unexpected results, Hexis provided choices for HawkEye G settings, either to use corporate policies to control automatic countermeasure execution or to allow machine-guided execution to optimize human-in-the loop threat response and removal. HawkEye G was selected due to its unique capabilities by the U.S. Intelligence Community as part of an integrated active cyber defense solution named SHORTSTOP for protecting federal agencies' networks against advanced adversaries.[154]

For active defense outside the network of specific organizations, Rule 20 of the Tallinn Manual 2.0 says "A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State."[155] Furthermore the Manual states there is in existing international law "no prohibition against injured States turning to a private firm, including foreign companies, to conduct cyber

---

[151] Chris Warfield, "WatchGuard Acquires Hexis HawkEye G to Deliver Holistic Network Security From the Network to the Endpoint," WatchGuard Technologies, Press Release, June 7, 2016.

[152] Hexis Cyber Solutions, "How to Automate Cyber Threat Removal," A HawkEye G Technical White Paper, Release 3.1, October 2015: 3.

[153] Ibid, 9.

[154] Hexis Cyber Solutions, "HawkEye G Selected As Part of an Active Cyber Defense System to Protect Federal Networks from Advanced Cyber Attacks," Press Release, March 12, 2015.

[155] Michael Schmitt (editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 111.

countermeasures on their behalf against responsible States."[156] This use of a proxy for defense is complicated, however, by the rules in westernized states or companies themselves. On the contrary "hack-back" is when the victim acts on its own initiative with a counterstrike to stop an ongoing attack, or even hack into their network to delete or alter stolen information.[157] Although it is alleged that "an increasing number of U.S. companies are taking retaliatory action,"[158] for private sector actors to act on their own using hack-back, existing legal constraints would have to be adapted to allow use of these tactics.[159] The primary law in the United States that applies to private sector use of hack-back techniques is the Computer Fraud and Abuse Act (CFAA), codified as Title 18, Section 1030. A company's defenders can violate the CFAA by accessing a "protected computer" without authorization or by exceeding authorized access.[160] Currently in the United States "it's illegal to chase bad guys up the wire, even if you have the capability to do so -- it's illegal to shoot back."[161] However, one could argue that U.S. common law admits certain rights of self-defense and defense of property in preventing the commission of a crime against an individual or a corporation. Applying the latter for hostile cyber attacks, the range of permitted actions is roughly comparable to the range for *non-lethal* self-defense. While individuals are not permitted to engage in revenge or retaliation for a crime, they are— in some instances—entitled to take otherwise-prohibited actions for the purpose of preventing or averting an imminent crime or one that is in progress. Yet in most cases, challenges in quickly obtaining

[156] Ibid, 131.

[157] Scott Cohn, "Companies Battle Cyberattacks Using 'Hack Back'," *CNBC News,* June 4, 2013.

[158] Joseph Menn, "Hacked companies fight back with controversial steps," *Reuters,* June 18, 2012.

[159] Jeffery Carr, "Cyber laws may need tweaking," *SC Magazine*, December 2012: 50.

[160] 18 U.S. Code § 1030 - Fraud and related activity in connection with computers.

[161] Patience Wait, "Cyberthreats Grow More Ominous: Former NSA Chief," *Information Week,* October 11, 2013.

definitive attribution preclude exercising this right.[162] Therefore today a private sector actor may realistically and legally only use countermeasures within its own network, unless granted authority on behalf of the state to use countermeasures outside the network under international law constraints, which might not be the case in practice.

The U.S. Department of Defense (DoD) has already embraced the use of active cyber defense as a means to defend military operations and thereby compensate for the failure of contemporary deterrence strategies in cybered conflict. The Department defines the concept as the "synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities" against its own operational networks.[163] For the military, these tasks are very similar to defensive cyberspace operations described by the Director of Operations at U.S. Cyber Command as "passive and active cyberspace defense activities that allow us to outmaneuver an adversary."[164] Defensive cyberspace operations provide the ability to discover, detect, analyze, and mitigate threats with malicious capability and intent to affect key cyber terrain. Subcategories of these operations are internal defensive measures (IDM), actions taken inside networks, and response actions (RA), actions taken outside networks. Tasks for IDM are "hunting" on units within DoD network space for threats and directing allowable responses, whereas RA is "about going after the shooter" outside DoD network space to stop the attack.[165] The Commander, Fleet Cyber Command has stated "we have people that hunt bad actors,"

---

[162] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington DC: National Academies Press, 2009): 204-205.

[163] U.S. Department of Defense, *Strategy for Operating in Cyberspace*, July, 2011: 13.

[164] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Number 73, 2nd Quarter 2014: 12-19.

[165] Ibid.

indicating a propensity to actively defend the network vice waiting to respond to or deny the benefit of cyber attacks, or even waiting for cooperative measures to work. [166]

Illustrative Case of Insufficient Contemporary Strategies

The U.S. Chairman of the Joint Chiefs of Staff has said "cyber attacks are incredibly disruptive and could disable his country's critical infrastructure."[167] While tangible evidence readily supports that assertion, like the cyber attack on the Ukraine power grid, not all cyber attacks rise to that level of harm against key resources, but they can have a significant economic or political effect. Take for instance, the 2016 hack into the Democratic National Committee (DNC) network that created political fallout through what could be considered a coercive campaign. The breach offers an illustrative case for an initial look at the sufficiency of contemporary deterrence strategies or an alternative strategy. The Washington Post reported in June that "Russian government hackers penetrated the computer network of the Democratic National Committee and gained access to the entire database of opposition research on GOP presidential candidate Donald Trump."[168] Committee officials said the intruders also were able to read all email and chat traffic. After discovering the intrusion in late April, the Committee reached out immediately to the cyber firm CrowdStrike to investigate. In May, CrowdStrike identified two separate Russian intelligence-affiliated hacker groups present in the network. One group named Cozy Bear (APT29) had gained access the prior summer and the other named Fancy Bear (APT28) in April.[169] A comparative analysis of malware samples for coding

---

[166] Richard R. Burgass, "Fleet Cyber Commander: "We Have People That Hunt Bad Actors," Seapower Magazine Online, December 2, 2014.

[167] Martin E. Dempsey, "Cyber attacks could disable critical US infrastructure," Interview, Press TV, January 12, 2015.

[168] Ellen Nakashima, "Russian government hackers penetrated DNC, stole opposition research on Trump," *The Washington Post*, June 14, 2016.

[169] Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," CrowdStrike Blog, June 15, 2016.

structures and obfuscation techniques by Fidelis Cybersecurity supported the CrowdStrike findings.[170]

Dmitry Peskov, a spokesman for President Vladimir Putin, immediately told foreign journalists in Moscow that "I absolutely rule out the possibility that the government or government agencies were involved in this."[171] Although Russia denied the DNC hack, both groups in question have been accused of hacking on their behalf. FireEye has documented a series of cyber espionage campaigns by APT28 in Eastern Europe and European security organizations that would likely benefit the Russian government.[172] Likewise, CrowdStrike claims that APT29 hacked the White House, State Department and U.S. Joint Chiefs of Staff.[173] The purpose of the DNC hacks appeared to be presidential candidate Donald Trump. In late July 2016 WikiLeaks dumped nearly 20,000 emails from top DNC officials. Several of the released emails revealed that officials floated ideas about ways to undermine the candidacy of former presidential candidate Bernie Sanders[174] contrary to Democratic party leader' statements meant to appear unified behind presumptive presidential nominee Hillary Clinton.[175] The immediate fallout for the DNC was severe. One day before the Democratic convention was ready to begin,

---

170 Teri Robinson, "Guccifer 2.0 out – Cozy Bear, Fancy Bear hacked DNC, Fidelis analysis shows," SC Magazine, June 21, 2016.

171 Andrew Roth, "Russia denies DNC hack and says maybe someone forgot the password," *The Washington Post, June 15, 2016.*

172 FireEye, "APT28: A Window into Russia's Cyber Espionage Operations," Special Report, 2014: 1-28.

173 Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," CrowdStrike Blog, June 15, 2016.

174 Alana Abramson and Shushannah Walshe, "The 4 Most Damaging Emails from the DNC WikiLeaks dump," *ABC News*, July 25, 2016: http://abcnews.go.com/Politics/damaging-emails-dnc-wikileaks-dump/story?id=40852448

175 Julian Routh, "Emails Show DNC Taking Aim at Sanders," *The Wall Street Journal*, July 26, 2016.

the DNC Chairwoman announced her resignation, and enraged Sanders supporters protested and disrupted the convention.[176] Multiple Democrats alleged "the Russian government stole the emails and provided them to WikiLeaks in an effort to help Republican presidential nominee Donald Trump win the November election."[177] The leaks of damaging emails related to the Clinton campaign continued all the way up to the election and beyond.[178]

Since no financial information was reported to be abused after any penetrations by the Russian hacker groups - only personal details of wealthy donors including celebrities,[179] it appears their motivations or those of their state sponsor were not for profit but political in nature, apparently to understand and influence political decisions in the United States. After all, Russia had set precedent for this sort of coercive activity by interfering through proxy hacker groups in the presidential elections in Ukraine in 2014 and allegedly in the UK Brexit referendum of 2016.[180] On October 7, 2016, the U.S. Director of National Intelligence stated with confidence "that the Russian Government directed the recent compromises of e-mails from U.S. persons and institutions, including U.S. political organizations. ... We believe based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these

[176] Jeff Zeleny, MJ Lee and Eric Bradner, "Dems open convention without Wasserman Schultz," *CNN Politics*, July 25, 2016.

[177] Damian Paletta and Devlin Barrett, "Russians Accused of Hacking DNC," *The Wall Street Journal*, July 26, 2016.

[178] Dave Boyer, "Obama briefed on intel report of Russian hacking in election," *The Washington Times*, January 5, 2017 and David Sherfinski, "State Department: 'Pretty obvious' Russia was trying to hurt Hillary Clinton," *The Washington Times*, January 6, 2017.

[179] Greg Masters, "Fallout from DNC hack broadens to donors, including celebrities," *SC Magazine*, August 12, 2016.

[180] Nikolay Koval, "Revolution Hacking," *Cyber War in Perspective: Russian aggression against Ukraine*, Chapter 6, (Tallinn, Estonia, NATO Cooperative Cyber Defense Center of Excellence Publications, 2015): 55-58.

activities."[181] Countering that statement, WikiLeaks founder Julian Assange adamantly claimed that the source for the hacked emails "is not the Russian government and it is not a state party."[182] Six months later, in late May 2017, President Putin still "denied the Russian State had directed any hacking operations designed to influence the U.S. election – though he did say Russian patriots could have been behind the plot on their own accord."[183] Although new details revealed by the Washington Post, finally in late June 2017, revealed that the "CIA had obtained intelligence from sources inside the Russian government by early August [2016] that captured the Russian leader's specific instructions to subordinates on the operation's objectives: disparage and seek to defeat the Democratic nominee Hilary Clinton while helping to deliver the White House to Trump."[184]

Interfering in the integrity of democratic society elections is part of cybered conflict, or hybrid warfare, and will be difficult to deter by either retaliation, denial, or entanglement. A proportional and justified response to the DNC incident would not include military means for deterrence by retaliation for according to Tallinn Manual general editor Michael Schmitt, "it's not a situation that would allow the U.S. to respond in self-defense militarily."[185] The effectiveness of other means to impose costs such as diplomatic overtures and legal indictments would be doubtful. The Kremlin called the U.S. allegations "nonsense" and its leaders would

[181] Director of National Intelligence, "Joint DHS and ODNI Election Security Statement," Press Release, October 7, 2016: 1.

[182] Sean Hannity, "Assange: Russian government not the source of WikiLeaks emails, *Fox News*, January 3, 2017.

[183] Associated Press, "Vladimir Putin fights election-tampering accusations with his own shots at US," *Fox News*, June 2, 2017

[184] Greg Miller, "Putin denied meddling in the U.S. election. The CIA caught him doing just that," *The Washington Post*, June 23, 2017.

[185] Ellen Nakashima, "Russia's apparent meddling in U.S. election is not an act of war, cyber expert says," *The Washington Post*, February 7, 2017.

likely not cooperate."[186] For deterrence by denial, any layered protective measures in place on the DNC network obviously failed. Significant investment will be necessary to counter the advanced techniques of this type of sophisticated actor and credibility will be difficult to re-establish save over time. For deterrence by entanglement, the United States does have a cooperation pact but not a formal enforceable binding agreement with Russia for protection of the information resources of their states. Although Russia has tacitly agreed to international norms in 2015 through participation in the UN Group of Government Experts findings, it can challenge attribution to the act or to employing the proxies and it would be difficult to hold them legally accountable. National security expert James Lewis sums up the situation well in stating "If we couldn't deter Moscow from going into the Ukraine, we're not going to deter them from hacking us."[187] Clearly deterrence by retaliation or punishment, denial and entanglement failed because they are not comprehensive enough strategies for a cybered world.

Active cyber defense is the only option that is likely to have been effective in advance; its implementation would have invoked an earlier response. While the initial entry in the network by social engineering would not have been blocked, the breach could have been detected sooner by automated capabilities that discover and interpret subtle behaviors in enterprise activity and attributed quickly for action. Given the importance of fair elections, subsequent verifiable alerts could have enabled state-level tailored disruptive countermeasure considerations, for which Schmitt said unlawful intervention gave the United States grounds to undertake.[188] Only if active cyber defense had been in place would the results have been less likely because the strategy is more comprehensive as a strategic option to a cybered world. A detailed analysis of all four strategic options and the actual U.S. response will be presented in the final conclusion.

---

[186] Dmitry Solovyov, "Moscow says U.S. cyber attack claims fan 'anti-Russian hysteria,'" *Reuters*, October 8, 2016.

[187] David E. Sanger and Nicole Perlroth, "What Options Does the U.S. Have After Accusing Russia of Hacks?" *The New York Times*, October 8, 2016.

[188] Ellen Nakashima, "Russia's apparent meddling in U.S. election is not an act of war, cyber expert says," *The Washington Post*, February 7, 2017.

Expected Outcomes

In the illustrative case of alleged state-sponsored espionage, and in other disruptive or destructive cyber attacks, each contemporary deterrence strategy has limits in effectiveness in preventing malicious activity. Deterrence convinces adversaries not to take malicious actions by "means of decisive influence over their decision making."[189] Decisive influence is achieved by threatening to impose costs, or deny benefits, while encouraging restraint.[190] There are ways to overcome the current shortcomings of contemporary deterrence strategies for a cybered world by a deterrence strategy that imposes real consequences (retaliation), employs proactive defenses (denial), and pursues diplomatic concessions (entanglement). Incidents like the DNC hack can be learning experiences because they force states to recognize the potential risks and threats, and perhaps pursue laws and norms they otherwise would not have endorsed.[191] Deterrence options are not mutually exclusive. U.S. doctrine, for instance, uses a mixed approach, especially across diplomatic, legal, economic and military dimensions. However whether these options can achieve decisive influence on their own or whether the strategy of active cyber defense is necessary to fill in the existing gaps is the key question of this work. The data shows these contemporary methods do not work as planned or needed in cybered conflict. As offered here, a midrange theory of *active cyber defense* provides the framework to compensate for these contemporary deterrence failings through systemic resilience and disruption capacities that both frustrate and punish the wide range of malicious actors regardless of origin or intentions.

This project will make an original contribution to knowledge by correlating actual threat incident details to public assertions of effectiveness in order to assess the effectiveness of

---

189 U.S. Department of Defense, *Deterrence Operations Joint Operating Concept*, Version 2.0, (Washington, DC: US Strategic Command, December 2006), 8.

190 Ibid.

191 Mark Pomerleau, "Hope for global cyber norms struggles following Russian hacking allegations," *C4ISRNET*, January 5, 2017.

contemporary deterrent responses to the threat of cyber attack. Although conceptual literature[192] and workshop proceedings[193] exist on cyber deterrence theory, there is little empirical work of this nature attempting to compare contemporary strategies across complex social and technical issues equally. For application of a more comprehensive approach, a variety of conferences[194] and speeches[195] have addressed the subject but lack a unified framework. In response to the void, this project provides an empirically grounded midrange theory in active cyber defense is the key strategic deterrence option most likely to influence the behavior of malicious actors in cyberspace. As stated earlier by Vice Admiral Michael Rogers, the proliferation of malicious actors and cyber attack vectors does not allow much time to "get some idea of deterrence within the cyber arena."[196]

Thesis Structure

The thesis is divided into three sections, which examine in total the broad themes outlined above. The sections are succinctly entitled: *Thinking about Deterrence, Contemporary Deterrence Strategies*, and *A New Strategic Option*. These sections will contain chapters which

[192] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly*, Vol. 4, Issue 3 (Fall 2010): 102-135.

[193] National Research Council, *Proceedings of a Workshop on Deterring CyberAttacks*, The National Academies Press, 2012.

[194] Organization for Security and Co-operation in Europe (2011), "A Comprehensive Approach to Cyber Security: Exploring the future OSCE Role," Conference, Hofburg, Vienna, 9-10 May.

[195] James Lewis, "Rethinking Cyber Security – A Comprehensive Approach," Sasakawa Peace Foundation, Tokyo, September 12, 2011.

[196] "Hearing to consider the Nominations of ... VADM Michael S. Rogers, USN to be Admiral and Director, National Security Agency/ Chief, Central Security Services/ Commander, U.S. Cyber Command," Statements Before the Senate Committee on Armed Services," 11 March, 2014.

analyze thematically a different sub-theme within the section followed by a conclusion and appendix.

Section One: *Thinking about Deterrence*

The first section explores the current literature and the nature of the cyber threat to ascertain what theoretical foundations can be applied to deter cyberattacks.

Chapter I presents the literature review which reveals that adequate sources exist to express the underlying logic of the thesis. The constantly changing array of malicious actors, attack methods and motivations in cyberspace mandates use of the most current reference material for critical analysis of deterrence strategy options and to draw out conceptual theories. Therefore the evidence base is very young and can be at times problematic. Primary sources that would directly document cyber attacks – who made them, when and how, and with what reasoning – do not often exist in unclassified documents. As most attacks are illegal, the best evidence will be hidden from view by attackers, governments, and often victims themselves. The only sources we can draw upon are thus ones indicating that an attack occurred and sometimes giving results pointing at suspects. This thesis therefore draws on testimony, documents, concepts, publications, reports, papers, media outlets and blogs as raw intelligence to construct compelling answers to propositions.

While there are academic treatises of the topics pertaining to contemporary cyber deterrence strategies and the alternative of active cyber defense, an integrated examination does not exist. Much secondary literature only describes cyber threats, doctrinal approaches, offensive tactics, and defensive procedures while other works consider individual aspects of technology, policy and warfare. In order to form the most comprehensive arguments for the research questions, secondary literature in the form of published books, chapters, essays, articles, and studies will be used to examine applicable theories, occurrences, or initiatives.

Chapter II examines the most common types of attack methods available to all levels of malicious actors operating in global cybered conflict. It starts with discussion on how malicious code is spread through exploitation of vulnerabilities by cyber attack vectors. The chapter then provides technical detail on in particular, five vectors for compromise of information systems - spear phishing, watering hole, point-of-sale, web application, and distributed denial of service attacks - along with examples of their use in actual cyber incidents. The discussion then outlines – key malicious and defending actors and presents their motivations in campaigns of malicious or pre-emptive cyber activity. Specifically, the chapter will describe and examine the doctrine and capabilities of nation states, to include North Korea, Iran, China, Russia, and even the United States, hacker groups, criminal organizations, and terrorist groups – using recent cyber incidents to better understand their position and intent on cyber operations. The chapter will finish further elevating the nationally significant consequences of these cyber attacks upon complex socio-technical-economic systems of defending nations.

Chapter III explains conceptually how theories of *strategy* and *deterrence* underpin the creation of contemporary strategic cyber deterrence options or would inform the adaptation of an alternative option that would most likely influence malicious actor behavior in cyberspace. It begins with a review of seminal scholars' thinking on the role of deterrence to illustrate the relationship between deterrence strategies, as a subset, a backup, an element of one or another national strategic choice. The discussion explores national strategic choices made in three historical periods. Specifically, the chapter examines the use of coercive diplomacy and preemption before World War II, escalation dominance and countervailing strategy during the Cold War, and superiority in cyberspace and other domains or functional models in an era of Rising Cybered Conflict. In each of the three historical periods, the chapter explores how theories of deterrence found in these periods apply or not in the formulation and implementation of strategic cyber deterrence options. Finally in recognition of the intrinsic complexity and vulnerabilities found in various socio-economic-technical systems, the chapter concludes with an explanation of why a comprehensive approach enhances the multi-sector and largescale organizational interaction needed for the deterrence of malicious actors in cyberspace.

Section Two: *Contemporary Deterrence Strategies*

The second section analyses the utility and sufficiency of the contemporary deterrence strategies of retaliation, denial and entanglement for influencing malicious actor behavior in cyberspace.

Chapter IV assesses the effectiveness of deterrence by retaliation through use of a range of means to impose costs for hostile acts in cyberspace. Specifically it reviews the utility of military cyber operations, diplomatic engagements, law enforcement measures, economic sanctions, and even the use of kinetic capabilities, to change an actor's perceptions under varying conditions and circumstances. The chapter starts with an illustrative case that depicts an example of a justified and proportionate response by the United States government to a destructive and vindictive cyber attack by a foreign government on the private company Sony Pictures in 2014. The chapter next reviews the challenges in military response options, to include cyber weapon selection and usage constraints, both in the context of armed attack and of armed conflict. It then considers the virtues of other response options in a whole-of-government approach using the tools of global diplomacy, law enforcement expertise, and economic clout. The chapter finishes with an assessment of whether retaliation meets the conditions of effective deterrence for cybered conflict, given a greater tolerance for risk in malicious actors generated from government hesitancy to use all necessary means to change their behavior.

Chapter V evaluates the effectiveness of deterrence by denial of benefit to malicious cyber activity. Specifically it ascertains whether protective measures - including the promulgation of security strategies, the implementation of security controls, and the sharing of cyber threat information or intelligence - can limit actor willingness to attack over time. The chapter starts with an illustrative case that depicts the failure of deterrence by denial of benefit in a massive breach at the U.S. Office of Personnel Management in 2015. The chapter then examines the utility of protective measures designed to reduce risk, beginning with a defense-in-depth strategy that places preventive and detective security controls informed by cyber threat intelligence across what the cyber security industry labels the "cyber kill chain."[197] The chapter next evaluates security control frameworks to institute industry best practices and security solutions. The chapter then addresses whether threat intelligence sources and information sharing arrangements can stay ahead of the threat. After an explanation of risk management efforts to limit damage, the chapter finishes with an assessment of whether denial meets the conditions of effective deterrence for cybered conflict, given the apparent ease by which malicious actors are able to quickly penetrate systems with low cost, readily available attack tools.

Chapter VI appraises the effectiveness of deterrence by entanglement to ensure restraint in malicious cyber activity. Specifically it ascertains whether cooperative measures, including international norms, confidence building measures, and capacity building assistance, can restrain state behavior in conducting, endorsing or allowing malicious cyber activity originating from territory under their jurisdiction. The chapter starts with an illustrative case that depicts an example of the use of coercive diplomacy by the United States government to reach an unprecedented cyber arms agreement with China in 2015. The chapter then examines premises and principles for responsible state behavior found in global interdependence and international law. After discussion of the current inability to obtain formal binding obligations for cyberspace, the chapter presents initiatives and related setbacks in a broad assortment of cooperative measures under development by international bodies, organizations and corporations. The chapter finishes with an assessment of whether entanglement meets the conditions of effective deterrence for cybered conflict, given the divergence of state objectives, views, and values regarding the use of cyberspace.

---

[197] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, March 2011

Section Three: *A New Strategic Option*

The third section assesses whether evidence supports the assertion that active cyber defense compensates for the shortcomings of the contemporary deterrence strategies and is technically capable and legally viable as an effective, alternative cyber deterrence strategy.

Chapter VII describes and evaluates the range of actions for active cyber defense (ACD) in the context of the real time detection, analysis, and mitigation of network security breaches combined with the aggressive use of legal countermeasures beyond network and state territorial boundaries. The chapter starts with an illustrative case of actual cyber attacks in 2013 and 2014 affecting two U.S. mega retailers, Target and Home Depot, that depict the virtues of active cyber defense capabilities applied across the cyber kill chain. It then examines how implementation of this concept creates internal systemic resilience to withstand a potential attack using typical proactive activities, such as honeypots or sinkholes, and more recently new cyber security industry driven reactive approaches, using automated and integrated capabilities in a single security platform. Next the chapter outlines how the concept employs tailored disruption capacities to punish the attacker under the permissive legal conditions contained in international law. The chapter then explores employment options and restrictions for use of countermeasures by private companies, licensed privateers, and government agencies. The chapter concludes with arguments for considering active cyber defense as an alternative or part of deterrence strategy.

The *Conclusion* summarizes whether the data unearthed and considered is sufficient evidence to base a verdict on the proposed midrange theory of active cyber defense applicable to the world of cybered conflict emerging to challenge state security today. The final chapter reviews malicious actor advantages in cyberspace, particularly in terms of scale, proximity and precision.[198] It then examines the potential for systemic sector consequences in terms of

---

[198] Peter Dombrowski and Chris Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review*, April 1, 2014: 83. Malicious actors can scale attacking

cascading effects from disruptive or destructive cyber attacks. The chapter next presents an assessment at the strategic level of the impact of the contemporary deterrence strategies in terms of these three measures: on attacks (volume of noise across social, technical and economic systems), time (in mitigation of systemic security losses), and costs (in the order of magnitude of gross domestic products). Given the shortfalls of existing deterrence options demonstrated over the previous chapters the conclusion then consolidates the evidence showing how the midrange theory of active cyber defense is technically capable and legally viable as a means for deterring malicious actors. After review of multiple factors for application of active cyber defense activities inside and outside the network, the illustrative case of politically disruptive and coercive cyber attacks upon the Democratic National Committee network outlined in the introduction is examined in more detail to depict a recent example of why active cyber defense is the preferred and available means to strengthen deterrence and compensate for the shortcomings of other options. The chapter finishes with how active cyber defense meets the conditions of capability, credibility and communication to be considered an empirically grounded midrange theory for effective cyber deterrence.

An *Appendix* presents a national strategy agenda for creating internal systemic resilience and tailored disruption capacities through implementation of active cyber defense. The agenda's intent is to induce in an actor the belief that a threat of retaliation credibly exists, the intended action cannot fully succeed, or the costs outweigh any benefits of acting. The appendix will delineate how the strategic pillars of resilience and disruption play roles in the current cyber security strategies of international organizations and multiple nations when enabled through an effective comprehensive cyber deterrence approach. The appendix then explores architectures and arrangements already in place in the United States to strengthen the two strategic pillars. The appendix finishes with priority suggestions and policy recommendations to guide tradeoffs and choices in a national strategy agenda aimed to provide comprehensive deterrence in a conflictual, complex, cybered world.

---

units, operate outside close physical proximity, and vary "the precision of their targeting from a single person to cities, regions, or entire nations."

Section One:

Thinking about Deterrence

CHAPTER I

Literature Review

Primary Sources

The constantly evolving array of malicious actors, attack methods and motivations in cyberspace forces the use of the most current reference material to acquire data for critical analysis of deterrence strategy options. Primary sources used here include testimony, documents, articles, speeches, concepts, publications, reports, papers, media outlets and blogs. The phenomena is too new to rely on published works by academics and too diverse and dynamic to rely on formal institutional documents. The secrecy surrounding the subject area makes the finding of reliable sources of any form very difficult. Only the nature of cyber threats and actual attacks can be gleaned from past testimony and documents.

Government Testimony and Documents

The subject area is so dynamic that only very current material plays a prominent role in analysis. The testimony of government officials serves to establish published positions and policies on the risk and mitigation of cyber threats and vulnerabilities. Sean McGurk, the Director of the National Cybersecurity and Communications Integration Center, delineated in 2011 how malicious actors in cyberspace, including nation states, terrorist networks, and criminal groups, "have varying levels of access and technical sophistication, but all have nefarious intent."[199] McGurk later spoke of how a cyber event impacting control systems in the electric, nuclear, water, transportation or communications sectors could have implications at all

---

[199] Sean P. McGurk, National Cybersecurity and Communications Integration Center Director, Testimony before the House Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, April 14, 2011: https://www.dhs.gov/news/2011/04/14/testimony-national-cybersecurity-and-communications-integration-center-director-se%C3%A1n

levels of government and the private sector with potentially cascading effects upon all critical infrastructure sectors.[200] In 2012, General Keith Alexander, the Commander of U.S. Cyber Command, remarked that "it is only a matter of time before someone employs capabilities that could cause significant disruption to civilian or government networks and to our critical infrastructure."[201] Alexander went on to state in the context of cyber espionage and attack "against the United States as well as our allies and partners", that "our cyber capabilities represent key components of deterrence."[202] General Alexander adjusted his position the following year by saying we have "some confidence in our ability to deter major state-on-state attacks but we are not deterring the seemingly low-level harassment of private and public sites, property, and data."[203]

Jane Hall Lute, the Deputy Secretary, U.S. Department of Homeland Security, outlined in 2013, malicious actor methods to Congress to include distributed denial of service attacks and social engineering to malware introduced through thumb drives, supply chain exploitation, and trusted insider access. She contended the success of efforts "to reduce cybersecurity risk depends on effective identification of cyber threats and vulnerabilities, analysis, and enhanced information sharing...from all levels of government, the private sector, and international

---

[200] Roberta Stempfley, Acting Assistant Secretary, Office of Cyber Security and Communications, and Sean P. McGurk, Testimony before the House Subcommittee on Oversight and Investigations, July 26, 2011: https://www.wired.com/images_blogs/threatlevel/2011/07/StempflyMcgurk-1.pdf.

[201] Keith B. Alexander, Commander, United States Cyber Command, Testimony before the House Committee on Armed Services, March 20, 2012: http://www.au.af.mil/au/awc/awcgate/postures/posture_cybercom_20mar2012.pdf.

[202] Ibid.

[203] Keith B. Alexander, Commander, United States Cyber Command, Statement before the Senate Committee on Armed Services, March 12, 2013: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-091.pdf.

entities."[204] In 2013 Roberta Stempfley, the Acting Assistant Secretary, U.S. Department of Homeland Security asserted that carefully crafted information sharing provisions, as part of cyber security legislation, are essential to improve the Nation's cybersecurity posture. Accordingly, Stempfley argued that "Congress should enact legislation to incorporate privacy, confidentiality, and civil liberties safeguards into all aspects of cyber security" and promote "the establishment and adoption of standards for critical infrastructure."[205]

In 2013 Larry Wortzel, a senior member of the U.S.-China Economic and Security Review Commission, testified that Chinese cyber espionage poses a major threat to U.S. business interests and military readiness, by using intrusions to fill gaps in China's research programs. In case of conflict, he asserted military doctrine in China "calls for attacks on critical infrastructure of an opponent's homeland."[206] Admiral Rogers, the Commander, U.S. Cyber Command, the successor to Alexander, verified China, along with one or two other countries, already has cyber capabilities that "could shut down the electric grid in parts of the United States."[207] Alexander

[204] Jane Hall Lute, Deputy Secretary, US Department of Homeland Security, Statement before the House Committee on Homeland Security, March 13, 2013: http://docs.house.gov/meetings/HM/HM00/20130313/100390/HHRG-113-HM00-Wstate-LuteJ-20130313.pdf.

[205] Roberta Stempfley and Lawrence Zelvin, National Cybersecurity and Communications Integration Center Director, Statement before the House Committee on Homeland Security," May 16, 2013: https://www.dhs.gov/news/2013/05/16/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-hearing.

[206] Larry M. Wortzel, "Cyber Espionage and the Theft of US Intellectual Property and Technology," Testimony before the House Committee on Energy and Commerce, July 9, 2013: http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf.

[207] Catherine Herridge, "NSA Director: China can damage US power grid," *Fox News*, November 20, 2014: http://www.foxnews.com/politics/2014/11/20/nsa-director-china-can-damage-us-power-grid.html.

stated prior that the U.S. Cyber Command and Components, when directed, will defend the "nation against attacks in cyberspace."[208] Robert Anderson, an Executive Assistant Director, at the Federal Bureau of Investigation (FBI), expanded the range of malicious actors in cyberspace in 2014 to include "state-sponsored hackers, hackers for hire, global cyber syndicates, and terrorists."[209] The same year, James Clapper, the Director of National Intelligence (DNI), highlighted how "terrorist organizations have expressed interest in developing offensive capabilities," in addition to using cyberspace for influence, propaganda, finance and recruitment. Clapper commented on how "cyber criminals play a major role in the international development, modification and proliferation of malicious software," while nations like "Iran and North Korea are unpredictable actors" whose cyber capabilities might "provoke or destabilize the United States or its partners."[210] In 2015, Robert Work, the Deputy Secretary of Defense, recognized that for the United States "we are not where we need to be in our deterrent posture."[211] A year later in 2016, Lieutenant General McLaughlin, the Deputy Commander, U.S. Cyber Command, pronounced that "one of the [Defense] Department's key policy goals in cyberspace is to deter

---

[208] Keith B. Alexander, Commander, United States Cyber Command, Statement Before the House Committee on Armed Services, March 12, 2014: http://docs.house.gov/meetings/AS/AS26/20140312/101883/HHRG-113-AS26-Wstate-AlexanderUSAK-20140312.pdf .

[209] Robert Anderson, Jr. "Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland," Testimony before the Senate Committee on Homeland Security and Government Affairs, September 10, 2014: https://www.hsgac.senate.gov/hearings/cybersecurity-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland.

[210] James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the House Permanent Select Committee on Intelligence," February 4, 2014: https://www.dni.gov/index.php/newsroom/testimonies/203-congressional-testimonies-2014/1011-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community-hpsci.

[211] Cheryl Pellerin, "Defense, Intel Leaders: Cybersecurity Priorities are Defense, Deterrence," DoD News, Defense.gov, September 29, 2015.

cyberattacks" and therefore the Department is "supporting a comprehensive, whole-of-government cyber deterrence strategy" in line with the approach of this thesis.[212]

Government documents promulgate regional or national strategy, policy, plans or orders to secure or defend cyberspace from the threat of cyber attack. In the United States in particular, a lineage of products has been issued over nearly fifteen years that attempt to keep pace with the evolving threat. They start with the *2003 National Strategy to Secure Cyberspace* which is obviously quite outdated, although it does properly highlight public-private engagement as a key component to secure cyberspace. The Strategy priorities stress continuity plans for resilience, law enforcement capabilities, national training and awareness, secure technology programs, and international cooperation to deter malicious actors and the same would apply today.[213] The *2009 Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure* maintains emphasis on a public-private partnership for addressing network security issues, as well as international cooperation and norms. The Review delineates need for "a comprehensive framework to ensure coordinated response and recovery by the government, the private sector, and our allies to a significant [cyber] incident or threat."[214] The *2010 Comprehensive National Cybersecurity Initiative* consists of a number of mutually reinforcing

[212] Mr. Thomas Atkin, Lieutenant General James K. McLaughlin, United States Cyber Command, and Brigadier General Charles L. Moore, Statement Before the House Armed Services Committee, June 22, 2016: http://docs.house.gov/meetings/AS/AS00/20160622/105099/HHRG-114-AS00-Wstate-AtkinT-20160622.pdf.

[213] Executive Office of the President, *The National Strategy to Secure Cyberspace*, (Washington, DC: The White House, February 2003): https://www.dhs.gov/national-strategy-secure-cyberspace.

[214] Executive Office of the President, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure*, (Washington, DC: The White House, May 2009): https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf.

initiatives designed as key elements of a broader national strategy. Initiative number ten intends to define and develop enduring deterrence strategies and programs upon realization that contemporary measures have not achieved the needed level of security.[215] When Congress failed to enact cyber security legislation, the President signed in 2013 an *Executive Order -- Improving Critical Infrastructure Cybersecurity* to improve information sharing and develop a cyber security framework,[216] and the *Framework for Improving Critical Infrastructure Cybersecurity* was released a year later.[217] In parallel, the President issued PPD-21 in 2013 titled *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*,[218] which was followed shortly by *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* to better manage risks to critical infrastructure by identifying threats, reducing vulnerabilities and mitigating consequences of incidents through an integrated approach across a diverse community.[219]

---

[215] Executive Office of the President, *The Comprehensive National Cybersecurity Initiative,* (Washington, DC: The White House, March 5, 2010): http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf.

[216] Executive Office of the President, *Executive Order -- Improving Critical Infrastructure Cybersecurity*, (Washington, DC: The White House, February 12, 2013): https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[217] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[218] Executive Office of the President, *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*, PPD-21, (Washington, DC: The White House, February 12, 2013): https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[219] Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*, March 2013:

Three releases by the United States in 2011 clarified the nation's positions on cyberspace. The first *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* released in May 2011 illuminated the combination of diplomacy, defense, and development to enhance prosperity, security, and openness.[220] The defense objective sets pertinent policy for this book in stating that the "United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate."[221] Next the U.S. Department of Defense *Strategy for Operating in Cyberspace* published in July 2011 designates cyberspace as an operational domain to organize, train and equip as armed forces do in air, land, maritime, and space. Department efforts in 2011 focus on mission assurance supported by the development of increasingly resilient networks and systems.[222] The Department's *Cyberspace Policy Report* issued in November 2011 provides indications of how the United States will respond to hostile acts in cyberspace.[223] The same year the NATO promulgated their initial policies for collective defense response in a 2011 document titled *Defending the Networks, The NATO Policy on Cyber*

---

https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

[220] Executive Office of the President, *International Strategy for Cyberspace*, (Washington, DC: The White House, May 2011): https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[221] Ibid, 12.

[222] U.S. Department of Defense, *Strategy for Operating in Cyberspace*, July 2011: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[223] U.S. Department of Defense, *Cyberspace Policy Report*, November, 2011: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf.

Defence.[224] The European Union (EU) followed suit with their *2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace Cybersecurity Strategy* outlining principles, priorities, actions and roles to achieve an open, safe and secure cyberspace.[225] This document is supplemented by national strategy objectives, such as in *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* that emphasizes detecting and defeating threats while pursuing internationally-agreed upon rules of the road on the use of cyberspace.[226] The UK strategy was updated in 2015 at the same time as establishment of a new National Cyber Security Centre. In 2015 the United States updated their *Department of Defense Cyber Strategy* to strengthen both cyber defense and cyber deterrence postures, in particular adding the need to "strengthen the overall resilience of U.S. systems to withstand a potential attack if it penetrates the United States' defenses," which forms the basis for the concept of internal systemic resilience found in this book.[227] The U.S. Defense Department is tasked to defend the nation against cyberattacks of significant consequence, which includes working with other agencies of the government.

---

[224] North Atlantic Treaty Organization (2011), *Defending the Networks, The NATO Policy on Cyber Defence,* approved by NATO defense ministers on June 8, 2011: http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

[225] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* July 2, 2013: https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace.

[226] *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world,* November 2011: https://www.gov.uk/government/publications/cyber-security-strategy.

[227] U.S. Department of Defense, *The DoD Cyber Strategy*, April 2015: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Official Articles and Speeches

Articles or speeches by senior officials in the United States provide tangible reasons why cyber defense policy initiatives should include use of contemporary deterrence strategies. In 2008, Defense Deputy Secretary William Lynn revealed in *Foreign Affairs* a significant compromise of the U.S. Department of Defense military networks by an infected flash drive that was inserted into a U.S. military laptop at an operating base in the Middle East. Lynn stated the operation to counter this previously classified attack "marked a turning point in U.S. cyber defense strategy."[228] One year after the Pentagon released their strategy, Lynn used the same academic forum to remark that "the danger of cyber warfare rivals that of traditional war."[229] Citing a "strategic shift in the cyber threat" from exploitation to disruption (which can be both depending on purpose and actor), Lynn stated that "cyber technologies now exist that are capable of destroying critical networks, causing physical damage, or altering the performance of key systems."[230] In 2012, former U.S. Defense Secretary Leon Panetta used examples of these sorts of attacks on energy companies in the Middle East as evidence for his contention of "a significant escalation of the cyber threat and renewed concerns over still more destructive scenarios that could unfold" as part of a cyber-Pearl Harbor scenario.[231]

The former U.S. Chairman of the Joint Chiefs of Staff, General Martin Dempsey amplified in a speech in 2013 that those "disruptive and destructive attacks are becoming a part

---

[228] William J. Lynn III, "Defending a New Domain," *Foreign Affairs,* Vol. 89, No. 5, September–October 2010: 97–108.

[229] William J. Lynn III, "The Pentagon's Cyberstrategy, One Year Later," *Foreign Affairs,* Snapshot, September 28, 2011: 1-4.

[230] Ibid.

[231] Leon E. Panetta, "Defending the Nation from Cyber Attack," Business Executives for National Security, October 11, 2012.

of conflict between states, within states, and among non state actors."[232] In this conflict, he remarked that "civilian infrastructure and business are often targeted first", which makes sense since softer targets.[233] He went on to say that the Department of Defense is therefore "taking on a new mission when asked, with interagency partners that is defending the nation from cyber attacks."[234] However the question lingers as to whether defense strategy is adequate to maintain superiority against this rapidly changing threat landscape, when certainly under challenge.[235] General Keith Alexander, the Commander of U.S. Cyber Command, and his colleagues contended in *The National Interest* that even as the United States confronts mounting threats, an historical opportunity exists to deter them, through "an evolving set of capabilities and activities that have not yet reached their collective potential."[236] Alexander said progress has been made, but more can be done to provide: "authority to respond to threats," "legislation that facilitates information sharing with the private sector, established security standards for critical infrastructure," and doctrine for "the conduct of military operations in cyberspace." – which arguably conflate issues and are very difficult to tackle.[237]

Military Concepts and Publications

In the United States, military concepts are critical to identify problems and propose solutions for innovative ways to conduct operations. Ideally they will produce capabilities that

---

[232] Martin E. Dempsey, "Defending the Nation at Network Speed," The Brookings Institution, June 27, 2013: 1-44.

[233] Ibid.

[234] Ibid.

[235] Thomas M. Chen, "An Assessment of the Department of Defense Strategy for Operating in Cyberspace," *The Letort Papers,* Strategic Studies Institute, US Army War College, September 2013: 1-45.

[236] Keith B. Alexander, Emily Goldman and Michael Warner, "Defending America in Cyberspace," *The National Interest*, November/December 2013: 18.

[237] Ibid, 23.

render previous ways of warfighting obsolete while changing measures of success in operations. The *Deterrence Operations Joint Operating Concept*, December 2006, Version 2.0, states that deterrence strategy must "be tailored to the perceptions, values and interests of specific adversaries." It also states that deterrence operations "convince adversaries not to take actions that threaten interests" by "means of decisive influence over their decision-making." Decisive influence is "achieved by credibly threatening to deny benefits and/or impose costs while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome."[238] U.S. Joint Staff doctrine states that success in preparation and response to cyber threats "is dependent upon unity of effort enabled by collaboration and coordination" among partners. Their *Unity of Effort Framework Solution Guide,* August 2013, provides procedures, templates, and definitions to aid planners in improving unity of effort for complex problems.[239]

Joint and service publications provide the doctrinal foundations, fundamental principles and specific considerations that guide the armed forces in operations. The *DOD Dictionary of Military and Associated Terms,* as of March 2017, sets forth standard US military terminology but is limited in expressions of cyberspace and deterrence.[240] Joint Publication 3-0 for *Joint Operations*, January 2017, views deterrence as a phase (Deter) in a flexible model to arrange combat and stability operations,[241] where more detail on individual phases is found in Joint

---

[238] U.S. Department of Defense, *Deterrence Operations Joint Operating Concept*, Version 2.0, (Washington, DC: US Strategic Command, December 2006), 1-53: http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf.

[239] U.S. Department of Defense, *Unity of Effort Framework Solution Guide,* (Suffolk, Virginia: US Joint Staff J-7, August 31, 2013), 1-68: http://www.dtic.mil/doctrine/doctrine/jwfc/uef_solution_guide.pdf.

[240] U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms,* (Washington, DC: The Joint Staff, As of March 2017): http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf.

[241] U.S. Department of Defense, *Joint Operations*, Joint Publication 3-0, (Washington, DC: The Joint Staff, 17 January 2017), V-7 to V-10: http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

Publication 5-0 for *Joint Operation Planning*, August 2011.[242] Joint Publication 3-24 for *Counterinsurgency*, November 2013, provides a glimpse of how the comprehensive approach can frame unified action by key actors for unity of effort in operations.[243] Joint Publication 3-12 (R) for *Cyberspace Operations*, February 2013, provides military guidance and joint doctrine for "the planning, preparation, execution and assessment of joint cyberspace operations."[244] Joint Publication 1-04 for *Legal Support to Military Operations*, August 2016, describes the law of war principles of military necessity, humanity, distinction, and proportionality to be used in all joint military operations.[245] The Department of Defense *Law of War Manual*, updated May 2016, devotes an entire chapter on how law of war principles and rules apply to cyber capabilities and the cyber domain, in particular for cyber operations in both *jus ad bellum* and *jus in bello*.[246] Joint Publication 3-01 for *Countering Air and Missile Threats*, March 2012, illuminates how passive and active measures for Ballistic Missile Defense are very similar in context to Defensive Cyberspace Operations.[247] Air Force Doctrine Document 3-12 for *Cyberspace*

---

[242] U.S. Department of Defense, *Joint Operation Planning*, Joint Publication 5-0, (Washington, DC: The Joint Staff, August 11, 2011), III-38 through III-44: http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

[243] U.S. Department of Defense, *Counterinsurgency*, Joint Publication 3-24, (Washington, DC: The Joint Staff, November 22, 2013), III-4 to III-5: http://www.dtic.mil/doctrine/new_pubs/jp3_24.pdf.

[244] U.S. Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (R), (Washington, DC: The Joint Staff, February 5, 2013): http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[245] U.S. Department of Defense, *Legal Support to Military Operations*, Joint Publication 1-04, (Washington, DC: The Joint Staff, August 2, 2016): http://www.dtic.mil/doctrine/new_pubs/jp1_04.pdf.

[246] Office of General Counsel, *Department of Defense Law of War Manual*, June 2015 (Updated May 2016): https://www.defense.gov/Portals/1/Documents/DoD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf.

[247] U.S. Department of Defense, *Countering Air and Missile Threats*, Joint Publication 3-01,

Operations, November 2011, Change 1, addresses unique challenges, such as mission assurance, compressed decision cycles, and anonymity from inherent attribution.[248] Other Department of Homeland Security and Commerce publications provide information security terms,[249] practices,[250] standards,[251] and guidelines.[252]

Industry Reports and Papers

Commercial cyber security vendors conduct research and produce various synopses on multiple aspects of the cyber threat. Their annual or special reports and papers are the most

---

(Washington, DC: The Joint Staff, March 23, 2012): I-4: http://www.dtic.mil/doctrine/new_pubs/jp3_01.pdf.

[248] Major General Maurice H. Forsyth, USAF, "Cyberspace Operations," Air Force Doctrine Document 3-12, 15 July 2010, Incorporating Change 1, 30 November 2011: 1-10: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-060.pdf.

[249] National Institute of Standards and Technology, "Glossary of Key Information Security Terms," NISTIR 7298 Revision 2, (Washington, DC: US Department of Commerce June 5, 2013): https://www.nist.gov/publications/glossary-key-information-security-terms-1.

[250] Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, (Washington, DC: National Cyber Security Division, September 2016): https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[251] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, (Washington, DC: US Department of Commerce, January 2014): https://www.nist.gov/publications/security-and-privacy-controls-federal-information-systems-and-organizations-including-0.

[252] National Institute of Standards and Technology, *Guide to Cyber Threat Information Sharing*, Special Publication 800-150, (Washington, DC: US Department of Commerce, October 4, 2016): https://www.nist.gov/publications/guide-cyber-threat-information-sharing.

current and detailed source of evidence on the magnitude and mitigation of the cyber threat. Scholars of cyber security or strategy related topics cannot rely on traditional academic sources that are dated and limited in explanation and understanding of the pervasive and evolving threat. For example, the annual *Internet Security Threat Report* by Symantec reviews the ever changing types and number of breaches and attacks plus delivery tactics while recommending appropriate best practices and security controls.[253] Whereas Verizon's annual *Data Breach Investigations Report* centers on developing data breech statistics and attack methods categorized in basic patterns with recommended and suitable controls.[254] The annual *Global Threat Report* by CrowdStrike reveals the latest malicious activity and techniques used by state and non-state actors.[255] Other primary sources of current threat summaries or expert predictions include FireEye *M-Trends*,[256] Kaspersky *Security Bulletins*[257] and McAfee *Threat Predictions*.[258] More detailed and foundational analysis on specific threat delivery mechanisms call threat vectors and the cyber kill chain are found in special releases by companies such as RSA[259] or Lockheed

[253] Symantec Corporation, "Internet Security Threat Report," Volume 22, April 2017: https://www.symantec.com/security-center/threat-report.

[254] Verizon, "2017 Data Breach Investigations Report," May 2017: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

[255] CrowdStrike, "2015 Global Threat Report, February 2016: https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf.

[256] FireEye, "M-Trends 2017," Milpitas, California, April 2017: https://www.fireeye.com/current-threats/annual-threat-report.html.

[257] Kaspersky Lab, "Security Bulletin 2016," December 2016: https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary/.

[258] McAfee Labs, "2017 Threat Predictions," November 2016: https://www.mcafee.com/au/resources/reports/rp-threats-predictions-2017.pdf.

[259] Sam Curry, Bret Hartman, David P. Hunter, David Martin, Dennis R. Moreau, Alina Oprea, Uri Rivner, and Dana Elizabeth Wolf, "Mobilizing Intelligent Security Operations for Advanced

Martin.[260] Exacting reviews of actual "advanced persistent threat" groups and their organizations, locations, affiliations, activities, targets, and methods are produced according to nations, such as China by Mandiant for APT1[261] and Russia by FireEye for APT28.[262] Other cyber security companies, like Imperva, break down the motivations and tactics of different actors, like Anonymous (the hacker collective) use of Distributed Denial of Service type methods.[263] Other actor campaigns identified in a host of illustrious names are captured and explained by security firms, such as *Night Dragon* and *Operation Troy* by McAfee,[264] or *Red October* and *NetTraveler* by Kaspersky[265] and *Operation Blockbuster* by Novetta.[266]

Persistent Threats," *RSA Security Brief,* February 2011: http://www.cnmeonline.com/news/rsa-introduces-new-model-to-battle-persistent-threats/.

[260] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, March 2011: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

[261] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 27, 2013: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[262] FireEye, "APT28: A Window into Russia's Cyber Espionage Operations?" October 28, 2014: https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf.

[263] Imperva, "Hacker Intelligence Summary Report: The Anatomy of an Anonymous Attack," Redwood Shores, CA, 2012: https://www.imperva.com/docs/HII_The_Anatomy_of_an_Anonymous_Attack.pdf.

[264] McAfee, "Global Energy Cyberattacks: Night Dragon," Santa Clara, CA, 2011, and "Dissecting Operation Troy: Cyberespionage in South Korea," Santa Clara, CA, 2013.

[265] Kasperskey, "Red October," Global Research and Analysis Team, January 2013, and "The NetTraveler (aka Travnet)," Global Research and Analysis Team, June 2013.

[266] Novetta, "Operation Blockbuster: Unraveling the Long Threat of the Sony Attack," February 2016: https://www.novetta.com/2016/02/operation-blockbuster-unraveling-the-long-thread-of-the-sony-attack/.

Commercial cyber security firms also produce unique technical analysis of attacks or occurrences leading to suggested security solutions that are unavailable for use elsewhere. Almost all government analysis is classified and thus not accessible to the general public. A scholar that possesses an appropriate clearance and views classified information risks inadvertent disclosure in discussion and publication. An example of useable material is a FireEye paper that explained how their product solutions would disrupt the 2010 Aurora attack upon U.S. companies at each stage of the infection lifecycle.[267] Similarly Lumension identified how a defense-in-depth approach can protect against the weaponized malware used in the Flame virus attacks upon Iran.[268] Other security companies identify cyber defense solution requirements to detect and defend across all attack process stages.[269] These suggested defensive measures are similar to the Critical Security Controls endorsed by the SANS Institute.[270] The Ponemon Institute assists organizations in creating a business case to adopt these security controls through publication of periodic studies depicting risks in endpoints[271] and costs of breaches.[272] A plethora of industry papers recommend products and practices to protect companies from advanced threats, like by Kaspersky on targeted cyber attacks.[273] Though some security firms claim that prevention alone is not enough, and defenders need technologies that automate

---

[267] FireEye, "Breaking the Operation Aurora Infection Lifecycle" Milpitas, CA, 2012.

[268] Lumension, "Preventing Weaponized Malware Payloads in Advanced Persistent Threats," Scottsdale, Arizona, February 2013: 1-12.

[269] Verdasys, "Cyber Attack Defense: A Kill Chain Strategy," Waltham, MA, 2013: 1-13.

[270] John Pescatore and Tony Sager, "Critical Security Controls Survey: Moving From Awareness to Action," A SANS Whitepaper, June 2013.

[271] Ponemon Institute, "2016 State of Endpoint Report," April 2016: 1-26: https://cdn2.hubspot.net/hubfs/150964/2016_State_of_Endpoint_Report.pdf.

[272] Ponemon Institute, "2016 Cost of Data Breach Study," June 2016: 1-30: https://securityintelligence.com/media/2016-cost-data-breach-study/.

[273] Kaspersky, "Step out of the Bull's-Eye: Protecting your company from advanced threats and targeted cyberattacks," January 2013: 1-18.

responses to advanced cyber threats. For example, Hexis Solutions declared Hawkeye G can detect, investigate and remove threats at the speed of a machine, without human intervention, from within the network.[274]

Media Outlets and Blogs

Analysis of viable strategies to counter emerging and pressing cyber threats requires dynamic reporting of incidents and policies. Quite a number of electronic and print media resources provide credible cyber security industry expert evaluations and senior government official positions on cyber threats and vulnerabilities coupled with related reactions and initiatives. In many cases the only news of significant cyber attacks comes from daily papers or their online sites, such as the New York Times, Reuters, Bloomberg, Washington Post and the Wall Street Journal. Without access to and use of these sources, patterns of evidence cannot be developed and fused to reach conclusions on the usefulness of proposed strategies in this thesis. Furthermore exclusive reporting is only contained at specific locations such as the Dark Reading site which posts stories, news, commentary and conversations on attacks or beeches, vulnerabilities and threats, plus cloud, application, endpoint, mobile and perimeter security.[275] More essential and unique details can be found in blogs, like at the InfoSec Institute Resources Site or IANS Blogs at IANS Perspective, and in sites, like Ars Technica for Risk Assessment at Security & Hacktivism or Cyber Attack at the Hacker News site. The applicability of cyber attacks in warfare is elaborately presented in magazines, such as Jane's Defense Weekly, or in blogs, such as Digital Conflict Blog at the Defense Systems site. Daily recaps of important federal cyber security and information technology initiatives can only be found in posts by the groups like FedCyber and FedScoop. Finally, pertinent information on current cyber security solutions is available in print journals such as Government Computer News and SC Magazine.

---

[274] Hexis Cyber Solutions, "HawkEye G: The Active Defense Grid," White Paper, Hanover, Maryland, 2013.

[275] See *Dark Reading* at: https://www.darkreading.com/

Secondary Literature

Academic treatises of the multiple topics pertaining to contemporary cyber deterrence strategies have not yet achieved an adequately inclusive or integrated examination. Many sources are devoted only to various cyber threats, doctrinal approaches, offensive tactics, and defensive procedures while others consider only individual aspects of technology, policy or warfare. In order to form expansive arguments for the research questions, this volume of disparate information will be fused with a variety of applicable theories, occurrences, or initiatives found in published books, chapters, essays, articles, and studies.

Cyber Threats

For this work, a clear understanding of technical aspects of cyber threats is critical to evaluate the utility of security controls, initiatives and regimes designed to counter cyber attacks. However only a limited set of technically oriented books and chapters exist that outline various cyber threats and state of the art attack methods. Kevin Coleman, a reputable columnist for the magazine Defense Systems, defined a "cyber attack vector" as "a category of software or code vulnerability, along with the path and method used to exploit it."[276] In his electronic book, Coleman not only described nearly fifty types of vectors, but also graded each along a risk scale (1 to 5) for threat, use, maturity, and defenses. Robert Koch, on the Faculty of Computer Science at the Universitat der Bundeswehr Munchen, presented attack trends for the purpose of evaluating weaknesses in current security systems. He claimed the most important methods are application layer attacks (like a code injection into a Web forum input box for a specific action to be performed on a database), zero day exploits (a program exploiting a flaw in software, such as operating systems or web browsers, that is available before the vendor knows about the flaw), social engineering (an intrusion that relies on human interaction for installation), dissemination routes (for malware, e.g. through data storage media), and insider attacks (that result in data

---

[276] Kevin Coleman, "The Cyber Commander's eHandbook: The Weaponry and Strategies of Digital Conflict," version 4, Technolytics, 2013, 52-80.

leakage) or all of them and more.[277] Christopher Elisan, a principal malware scientist at the security firm RSA Netwitness, classified means by which malware (software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system)[278] is able to infiltrate a targets system as 'infection vectors'.[279] While Marcus Maybaum, a German Air Force Information Technology professional,[280] and Ed Skoudis, a network security consultant for Intelguardians Network Intelligence,[281] analyzed specific tools and techniques for intrusion along the phases of the cyber attack process defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objectives.

A major form of cyber threat called the "advanced persistent threat" covertly obtains unauthorized access and uses stealthy techniques along the phases of the cyber attack process to steal valuable information usually in long-term surveillance operations against targets. Case

---

[277] Robert Koch, Bjorn Stelte and Mario Golling, "Attack Trends in Present Computer Networks," *Proceedings 4th International Conference on Cyber Conflict*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012): 269-282.

[278] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, Appendix B, (Washington, DC: US Department of Commerce, April 2013).

[279] Christopher C. Elison, "Infection Vectors," *Malware, Rootkits & Botnets,* (McGraw Hill, 2012): 155-184.

[280] Markus Maybaum, "Technical Methods, Techniques, Tools and Effects of Cyber Operations," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 103-131.

[281] Ed Skoudis with Tom Liston, "Attack Phases 1-5,"*Counter Hack Reloaded*, Second Edition, (Upper Saddle River, New Jersey: Prentice Hall, 2006): 183-668.

studies of APT group attacks reveal common tools, techniques, and indicators.[282] Mauno Pihelgas, a security technology researcher at the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), described ways in which APTs and other malicious actors operate to avoid detection and association with their true identity in order to maintain anonymity. He prescribed the use of "back-tracing" as a way to identify the originating source of communication, using processes or tools such as "traceroute" to find the route of network packets, which could determine attribution for an appropriate response to an attack.[283] Cyber threat intelligence strives to understand the type, motivation and capability of APTs and other malicious actors, as well as potential impacts. In his short summary, Bob Gourley, a partner at Cognito Corporation, advocated that cyber threat intelligence drives decisions on defenses and provides sources of cyber threat intelligence from a range of providers.[284]

A broad examination of cyber actors and their intentions is offered by Mike McConnell, former Director of the NSA National Security Agency. He observed that malicious actors posing the greatest threats to cyberspace have shifted in the last 20 years from those causing operational nuisances or financial impacts to "terrorist groups and nation-states whose strategic intent is to cause long-term harm" to U.S. economic well-being and national security.[285] Several prominent books illuminate the type of operations conducted by these actors. Eneken Tikk, a well-known

---

[282] Stuart McClure, Joel Scambray and George Kurtz, "Cybercrime and Advanced Persistent Threats," *Hacking Exposed 7: Network Security Secrets and Solutions*, (McGraw Hill, 2012) 313-368.

[283] Mauno Pihelgas, "Back-Tracing and Anonymity in Cyberspace," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 31-60.

[284] Bob Gourley, *The Cyber Threat,* (Create Space Independent Publishing Platform, September 23, 2014).

[285] Mike McConnell, "Cyber Insecurities: The 21st Century Threatscape," *America's Cyber Future: Security and Prosperity in the Information Age,* (Washington, DC: Center for a New American Security, June 2011): 27-39.

international lawyer, masterfully annotated the timelines, means, targets, origins and effects of suspected state-sponsored disruptive cyber conflicts in Estonia and Georgia in her treatise on legal considerations.[286] Jason Healey, the Director of the Cyber Statecraft Initiative of the Atlantic Council, provided a chronological narrative of a quarter century of conflict in cyberspace, looking in particular at the militarization phase of cyber history containing espionage and disruptive attacks, to include the former by Chinese affiliated APT groups. His analysis revealed that the "probability and consequences of disruptive conflict have often been hyped; while the real impacts of cyber intrusions have been consistently under-appreciated."[287]

A variety of seminal articles and essays help outline the objectives and methods of attacker campaigns, which are a series of extended and connected major operations aimed at achieving specific goals, in cyberspace. In some cases, actors seek to merely influence others through, and by means of, cyberspace. Christian Czosseck, a German Army Information Technology professional, outlined how state cyber power can be wielded by dedicated national capabilities and also by proxies of different types in ways not possible before cyberspace, especially leveraging the global outreach and anonymity of the internet.[288] For example Iftach Amit, Managing Partner, Security & Innovation, linked Russian cyber warfare activities in Estonia and Georgia to cybercrime groups,[289] mechanisms that states would not have used in previous eras. For the Ukraine conflict, Mark Clayton examined whether similar attacks tied to

[286] Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2009): 14-32.

[287] Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, (Cyber Conflict Studies Association, 2013).

[288] Christian Czosseck, "State Actors and their Proxies in Cyberspace, *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 1-30.

[289] Iftach Ian Amit, "Cyber [Crime/War]," Security and Innovation, Defcon Paper, 2010.

two large criminal botnets have any national allegiance.[290] John Bumgarner, the Chief Technology Officer for the U.S. Cyber Consequences Unit, argued Russia did not run the same playbook used in Georgia since it did not blind the Ukrainian government with massive cyber attacks when its forces invaded Crimea.[291] While Bryan Krekel, from Northrop Grumman, pointed out that in China organized cyber criminals and state-sponsored intelligence professionals often operate in the same environment and against similar targets.[292]

Some senior sources link attacks to a "war" equivalent often. Larry Wortzel a senior member of the U.S.-China Economic and Security Review Commission, presented evidence that "the Chinese government is directing and executing a large scale cyber espionage campaign against the United States."[293] He claimed intrusions into government and defense industries pose a major threat to US military operations and readiness. Wortzel said the Chinese government provides state-owned enterprises information and data exfiltrated through espionage to out-compete US companies.[294] In their Center for Strategic and International Studies (CSIS) report, Lewis and Baker examine the impact of cyber espionage and also cybercrime in terms of cost but conclude "the cost of malicious cyber activity involves more than the loss of financial assets or intellectual property. There are opportunity costs, damage to brand and reputation, consumer losses from fraud, the opportunity costs of service disruptions...and the cost of increased

---

290 Mark Clayton, "Massive cyberattacks slam official sites in Russia, Ukraine," *Christian Science Monitor,* March 18, 2014.

291 John Bumgarner, "A Cyber History of the Ukraine Conflict," Commentary, Dark Reading, March 27, 2014.

292 Bryan Krekel, Patton Adams and George Bakos, "Chinese Capabilities for Computer Network Operations and Cyber Espionage," Prepared for The US-China Economic and Security Review Commission, 7 March 2012: 8-13.

293 Dr. Larry M. Wortzel, "China's Military Modernization and Cyber Activities," *Strategic Studies Quarterly,* Vol. 8, Issue 1 (Spring 2014): 10.

294 Ibid, 11-15.

spending on cybersecurity."[295] According to the works of cyber warfare specialists Richard Clarke and Robert Knake, recent cyber attacks constitute a form of "cyber war" due to the conditions and effects of these attacks.[296]

Contrarian views on whether cyber attacks achieve a "war" equivalent are necessary in considerations in this work regarding legal thresholds for military responses. By contrast, well recognized scholar Thomas Rid of King's College argued that past and present cyber attacks are forms of political violence (sabotage, espionage and subversion) that just remove direct human action.[297] Others agree that research indicates the actual magnitude and pace of attacks do not match popular perception of war.[298] In looking at the strategic aspects of how cyber war affects the will of the adversary directly, Martin Libicki from the RAND Corporation differentiated how cyber warfare is about the conduct of war, carried out to improve the performance of combat in the physical domain.[299] Chatham House scholar Paul Cornish' and his co-authors agreed that cyber warfare "cannot be separated from conflict in the physical domain."[300] Finally Thomas Mahnken concluded cyber warfare uses "the cyber instrument as a dimension of a larger military conflict," aiding lethal forms of warfare, whereas "the independent use of the cyber instrument"

---

[295] James Lewis and Stewart Baker, "The Economic Impact of Cybercrime and Cyber Espionage," Center for Strategic and International Studies, July 2013.

[296] Richard A. Clarke and Robert K. Knake, *Cyber War,* (New York, NY: Harper Collins Publishers, 2010).

[297] Thomas Rid, *Cyber War Will Not Take Place*, (Oxford University Press, September 1, 2013).

[298] Brandon Valeriano and Ryan Maness, "The Fog of Cyberwar," *Foreign Affairs*, November 21, 2012.

[299] Martin C. Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," *Strategic Studies Quarterly,* Vol. 8, Issue 1 (Spring 2014): 23-39.

[300] Paul Cornish, et al, "On Cyber Warfare," A Chatham House Report, November, 2010: 1-38.

is termed "cyber war."[301] Overall, the terms cyber war and warfare are poorly defined, contested, and misunderstood.

Strategic Theory

Numerous books and chapters by distinguished authors depict dimensions of strategic theory for national defense, or simply the theory of strategy. These works are necessary to understand the role, and use, or threat, of force in this work. Beatrice Heuser referred to strategy as how people think about the link between political aims and the use of force, or its threat. She presented how the term strategy as the "art of the general" in antiquity evolved into the "science of the supreme commander" in early 1800, in contrast to "the use of engagements for the object of war" according to Clausewitz. She noted a return to the use of technical definitions by generals in the early twentieth century did not allow for the political directives under which strategy operated. Eventually though it appears today's military thinkers have formed consensus that strategy is about "the pursuit of political aims by the use or possession of military means."[302] Edward Luttwak considered strategy to be "a body of reoccurring objective phenomena that arise from human conflict." He contended that the normative Clausewitz version continued to dominate American interpretations while preferring a succinct French definition along the lines of "the art of wills that use force to resolve conflict."[303] Likewise, French General Andre

---

[301] Thomas G. Mahnken, "Cyberwar and Cyber Warfare," *America's Cyber Future: Security and Prosperity in the Information Age,* (Washington, DC: Center for a New American Security, June 2011): 57-64.

[302] Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present*, (Cambridge University Press, 2010).

[303] Edward N. Luttwak, *Strategy: The Logic of War and Peace,* (Cambridge and London: The Belknap Press of Harvard University Press, 1987).

Beaufre had a tendency to speak of strategy as “the art of the dialectic of force, or more precisely, the dialectic of opposing wills, which use force for the settlement of their disputes.”[304]

Colin Gray endeavored to show that strategy is an inclusive rather than exclusive realm of thought and behavior, where different perspectives are sources both of constraint and opportunity. He reiterated that military strategy pertains to the use and threat of force for the purposes of policy as decided by policy, an important connotation for use of the threat of retaliation.[305] Sir Basil Henry Liddell Hart, an English military theorist, recognized strategy depends on a sound calculation and coordination of the ends (policy) and the means (ability). He opined that strategy has to overcome resistance, manifested by human will.[306] To that extent, Lawrence Freedman explored whether it is possible to manipulate and shape the environment or fall victim to forces beyond control. His treatment of rational actor theory is most revealing regarding tendencies of self-interest overcome by coalitions and cooperation in strategic situations. However, the theory works well only if people are reasonable and sensible, and thoughtful about consequences, which bounds the notion of rational behavior.[307] Arthur F. Lykke, Jr. added the third element of ways (methods) in characterizing the *Strategy = Ends + Ways + Means* paradigm, to illustrate the need to examination courses of action to achieve objectives by available resources, such as to prevent undesirable behavior.[308]

Keith Payne and Dale Walton state that Cold War nuclear deterrence strategies assumed that challengers would be rational and reasonable and thus predictable. However they countered

---

304 Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present*, (Cambridge University Press, 2010): 17.

305 Colin S. Gray, *Perspectives on Strategy*, (Oxford University Press, 2013).

306 B.H. Liddell Hart, “The Theory of Strategy,” *Military Strategy: Theory and Application*, (Carlisle Barracks: US Army War College, 1983), 3-22 to 3-27.

307 Lawrence Freedman, *Strategy*, (Oxford University Press, 2013).

308 Arthur F. Lykke, Jr. “Toward an Understanding of Military Strategy,” *Guide to Strategy*, (Carlisle Barracks: US Army War College, 1983), February 2001: 179-185.

that "even the most brilliantly conceived and presented deterrence threats may be discounted or misunderstood" by "desperate or confident leaders intent on their chosen course," which could apply to the type of actors operating in cyberspace.[309] Colin Gray pointed out that nuclear weapons in the Cold War were instruments of policy capable of functioning in the ends-means context of strategy in time of and deterrence of war.[310] While Lawrence Freedman noted nuclear "forces were not being used to compel a change in the status quo but only to contain an enemy."[311] In his view Soviet expansionism "could only be held through the threat of force and if necessary, the realization of this threat at those points where it looked as if it might break out of limits." Therefore Freedman concluded that "containment as an objective lent itself to deterrence as a method."[312] Although Freedman did consider nuclear weapons as a problem in strategy in terms of military means to be related to political ends, and reached the conclusion that security problems can be eased only by stronger conventional forces, similar to their role in cyber deterrence as an alternative means to respond to a cyber attack.[313]

In Marc Trachtenberg's study of the influence of historical experience on strategy, he attempted to make sense of a world of thermonuclear weapons in citing Bernard Brodie's conclusion that what was needed was a comprehensive and radically different framework for thinking about strategic issues.[314] In thinking about the current security environment, Michael Carns stated the United States has little choice but to rethink security and deterrence as they apply to the various state, non-state, and trans-national threats that have heretofore been ignored

---

[309] Keith B. Payne and C. Dale Walton, "Deterrence in the Post-Cold War World," Strategy in the Contemporary World, (Oxford, 2002), 171.

[310] Colin S. Gray, "Strategy in the Nuclear Age: The United States, 1945-1991," *The Making of Strategy*, (Cambridge University Press, 1994): 579-613.

[311] Lawrence Freedman, *Deterrence*, (Cambridge: Polity Press, 2004): 11.

[312] Ibid.

[313] Lawrence Freedman, "The First Two Generations of Nuclear Strategists," *Makers of Modern Strategy*, (Princeton University Press, 1986): 735-778.

[314] Marc Trachtenberg, *History & Strategy*, (Princeton University Press, 1991): 261.

or wished away, which astutely applies to attempts to address today's cyber threats in this work. Carns stated the first step would be to craft a holistic national security policy that deters, or at least manages, emergent threats, because the promise is great and the alternative unacceptable.[315] Colin Gray recapped that if one discusses strategic ideas, like deterrence, to remember that strategy inalienably is a practical subject pervaded with political meaning. The challenge of deterrence is thus the challenge of strategy. Gray reminded the reader that the purpose of strategy, according to Clausewitz, is "to impose our will on the enemy' and hence 'an enemy who chooses to be deterred is an enemy who chooses to subordinate his will to ours"[316] and the enemy examined in this work is the malicious actor in cyberspace.

Cyber Strategy

In 2010 U.S. President Barak Obama appeared to adhere to Michael Carns advice that the first step to deter or manage emerging threats is to craft a holistic national security policy by ordering, shortly after taking office, "the development of a comprehensive approach to securing America's digital infrastructure."[317] A key element of the approach, labeled number 10, of the President's subsequent 2010 *Comprehensive National Cybersecurity Initiative* is to "Define and develop enduring deterrence strategies and programs."[318] The Initiative stated that "senior policymakers must think through the long-range strategic options available" which inspired the illumination of those offered in this work. The Initiative provided some useful considerations for this work in articulating "an approach to cyber defense that deters interference and attack in

[315] Michael P.C. Carns, "Reopening the Deterrence Debate: Thinking about a Peaceful and Prosperous Tomorrow," *Deterrence in the 21st Century,* (New York, NY: Frank Cass, 2001): 7-16.

[316] Colin S. Gray, "Deterrence and the Nature of Strategy," *Deterrence in the 21st Century,* (New York, NY: Frank Cass, 2001): 17-26.

[317] Executive Office of the President, *The Comprehensive National Cybersecurity Initiative,* (Washington, DC: The White House, March 5, 2010):1.

[318] Ibid, 5.

cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors," although these responses have not been developed as evidenced in many attacks since.[319] In regard to warning, security expert James Lewis identified a widening gap between offensive and defensive capabilities where most companies find out they have been hacked months later, usually by a third party. Therefore Lewis contended that any cyber strategy should set expectations for the sharing of threat information between and among parties that can act on the data. In regard to roles for international partners, he stated cyber strategy should also reflect the importance of international cooperation and governance that requires common norms to create an atmosphere that encourages responsible behavior.[320] Both observations by Lewis, on threat information sharing and common international norms, highlight the need for mechanisms used in this work for deterrence by denial and by entanglement, respectively.

National cyber security strategies suggest a myriad of actions and initiatives to secure cyberspace, including creative ways to deter malicious actors. In his seminal book on the subject, Kenneth Geers, a U.S. Representative to the NATO CCD COE, described cyber attack mitigation strategies that fall into the categories of technical solutions, military doctrine, attack deterrence, and arms control. Geers highlighted useful opportunities or limitations on each category, specifically in the potential for new protocols that provide enhanced security features; objective calculations for offensive operations; credibility challenges in deterrence due to attribution and asymmetry; and cyber arms control model difficulties because of prohibition and inspection challenges.[321] In a later release from Tallinn on a theoretical framework for facets of national cyber security according to different levels of public policy, Alexander Klimburg, a nonresident senior fellow with the think tank Atlantic Council, examined political aims, strategic

[319] Ibid.

[320] James Andrew Lewis, "Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage," Center for Strategic and International Studies, March 2014: 1-8.

[321] Kenneth Geers, *Strategic Cyber Security*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2011).

goals, organizational considerations, and international agreements and regulations.[322] His mandate for governmental, societal and international stakeholders to work together in order to succeed in cyber security implores the application of a comprehensive approach as a means of cooperation as seen in this work.

Any cyber strategy to deter or manage emerging threats should outline a vision and approach to understanding and managing risk while balancing civil rights and liberties, as espoused in this work under the chapter on deterrence by denial. Christin Goodwin and Paul Nicholas, from the Microsoft Corporation contribute to this vision and approach by providing a clear set of principles that serve as the basis for a risk-based strategy, where risk is assessed by identifying threats, vulnerabilities and consequences; then managed through costs or controls.[323] A report by Herbert Lin, a renowned researcher at Stanford University, and his associates recognized that tensions exist between cybersecurity and other public policy concerns, especially the aforementioned civil rights and liberties due to their informational dimension. For example a policy to inspect Internet traffic for malware could be regarded as a violation of privacy. Likewise the sharing of technical information raises concerns about possible privacy or antitrust violations, which is accommodated by legislative proposals identified in this work.[324]

The formulation of strategic options for deterrence in this thesis is not limited to the consideration of only U.S. strategy and policy decisions and initiatives. The thesis also draws upon academic pieces that frame official cyber defense policy established by the North Atlantic Treaty Organization (NATO) and the European Union (EU). For example, Diana De Viva at the NATO Defence College summarized a range of useful NATO efforts and arrangements leading to

---

[322] Alexander Klimburg, *National Cyber Security Framework Manual,* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012).

[323] Christin Flynn Goodwin and J. Paul Nicholas, "Developing a National Strategy for Cybersecurity," Microsoft Corporation, October 2013: 1-23.

[324] David Clark, Thomas Berson, and Herbert S. Lin, *At the Nexus of Cybersecurity and Public Policy* (Washington, D.C.: National Research Council, 2014).

release of their Enhanced Cyber Defense Policy in 2014.[325] While Hannes Krause, an Assistant Defence Counselor, Permanent Representation of Estonia to NATO looked at progress and challenges since adoption of the original NATO Policy in 2011, in areas such as use of the defense planning process in the cyber context and information sharing as a political goal.[326] Others authors have captured lessons after attacks from legal, operational and strategic perspectives, to include the feasibility of deterrence by denial or by punishment,[327] and also the international perspective on cyber conflict, that leads to cooperation on areas of agreement.[328] Giles Merritt, the Chairman of the Security and Defence Agenda expressed EU leader views on proposals for private-public, in addition to international cooperation.[329] Meanwhile, renowned U.S. expert Jason Healey portrayed NATO's policies and capabilities in terms of defensive improvements, political governance and operational steps. Given difficulties in keeping attackers out of systems, Healey emphasized resilience as the way to secure strategic objectives.[330]

Deterrence Theory

A variety of books provide historical and practical foundations for deterrence theory as the basis for foreign policy, which are necessary to understand the object and use of strategic options in this work. Gordon Craig and Alexander George laid out a process to weigh the

---

[325] Diana De Viva, "NATO Enhanced Policy on Cyber Defense: Towards the Wales Summit," NATO Defense College, *Vox Collegii* Volume IX, September 2014: 16-20.

[326] Hannes Krause, "NATO on its way towards a comfort zone in Cyber Defence," *The Tallinn Papers*, Vol. 1, No. 3 2014: 1-6.

[327] V. Joubert, "Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?" *Research Paper,* No. 76, Rome: NATO Defense College, May 2012.

[328] Ilmar Tamm, "Cyber Ready," *C4ISR Journal*, January/February 2012: 38-40.

[329] Giles Merritt, "What next for European cyber-security?" *Cyber-security: Problems outpace solutions,* Security and Defence Agenda, March 19, 2013: 6-14.

[330] Jason Healey and Klara Tothova Jordan, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," *Atlantic Council Issue Brief,* September 2014: 1-9.

interest of the country, convey a commitment to defend those interests, and back its commitment by threats to respond if the opponent acts.[331] This process applies to a potential malicious act in cyberspace. The authors admit the general theory of deterrence they draw upon is found in a manuscript by Alexander George and Richard Smoke that presents an in-depth assessment of deterrence theory applied in American foreign policy since the end of World War II. That book focuses on efforts to deter limited conflicts and the authors conclude the "theory has been markedly less useful to policy-makers than it might have been" by relying too heavily on "deterrent threats in lieu of the more flexible instruments of inter-nation influence associated with classical diplomacy," which relates directly to ongoing international engagements concerning cyberspace.[332] In their new approach for "Perfect Deterrence," Frank Zagare and Marc Kilgore focused on connections among capability, preferences, credibility and outcomes in both mutual direct and to extended deterrence relationships.[333] Adam Lowther framed policy applications in terms of deterrence instruments, failure and consequences that are helpful for use of deterrence theory in this century.[334]

General Kevin Chilton, commander, U.S. Strategic Command, and senior advisor Greg Weaver judged "deterrence should and will remain a core concept in our twenty-first century national security policy... because the concept itself is just as relevant today as it was during the

---

[331] Gordon A. Craig and Alexander L. George, *Force and Statecraft: Diplomatic Problems of our Time*, (Oxford University Press, 1995).

[332] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, (New York, NY: Columbia University Press, 1974.)

[333] Frank C. Zagare and D. Marc Kilgour, *Perfect Deterrence*, (Cambridge University Press, 2000).

[334] Adam Lowther, "Framing Deterrence in the Twenty-first Century," *Proceedings of Deterrence in the Twenty-first Century,* (Maxwell Air Force Base, Alabama: Air University Press, May 2009).

Cold War."[335] With a seminal analysis of Cold War observations, Schuyler Forester's primer is useful to this work because it lays out the basic elements of traditional deterrence (by denial and by punishment) and highlights inherent contradictions. Discussions of deterrence must be specific about *whom* and *what* to deter before solving the question of *how*. Most poignant is Forester's realization that "deterrence must be most effective in circumstances when rationality can least be assumed."[336] According to, Janice Stein, the rationality of adversaries is one of the principal threads of the debate about deterrence as theory and strategy. She addressed the meaning of rationality, the construction of the threat and the structure of the international system. Stein found the problem of rationality is compounded by the complex and uncertain global system, a useful finding considering the vast motivations of malicious actors in cyberspace that exploit globalization gains for malicious acts.[337] Chris Demchak outlined a theory of action that involves addressing the malicious actor's or group's sense of legitimacy, need, and confidence related to the act itself.[338] She claimed "humans in general are motivated by perceptions of legitimacy (often called beliefs), needs (usually monetized), and confidence (historically tied to the ability to wield decisive force)."[339] These motivators reflect the three fields of constructivism, institutionalism, and realism described by Michael Doyle.[340] The motivators map to the three schools of international relations in the following way: "beliefs are the focus of

---

[335] Kevin Chilton and Greg Weaver, "Waging Deterrence in the Twenty-First Century," *Strategic Studies Quarterly*, Vol. 3, Issue 1 (Spring 2009): 31-42.

[336] Schuyler Forester, "Theoretical Foundations: Deterrence in the Nuclear Age," in *American Defense Policy*, Schuyler Foerster and Edward Wright, eds., 6th ed. (Baltimore, MD: Johns Hopkins University Press, 1990): 42-51.

[337] Janice Gross Stein, "Rational Deterrence against "Irrational" Adversaries," *Complex Deterrence: Strategy in the Global Age*, (The University of Chicago Press, 2009): 58-82.

[338] Chris Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*, (University of Georgia Press, September 2011): 38.

[339] Ibid.

[340] Michael W. Doyle, *Ways of War and Peace*, (New York/London: W. W. Norton and Company, 1997).

constructivism, money is the focus of liberal institutionalism, and force is the focus of realism."[341] Demchak argued that coercion works best in diminishing confidence, by transforming the ease of actions, irrespective of local culture, to find and frustrate the malicious actor. Her argument is helpful in examining how strategic options influence decisions to attack based on beliefs (legitimacy), money (need) and ability (confidence).

Major General William Chambers, the U.S. Air Force Assistant Chief of Staff for Strategic Deterrence and Nuclear Integration, proclaimed the necessity to retain classic deterrence methodologies and integrate newer behavioural approaches outside a rational state-based actor construct.[342] Adam Lowther, an Air Force research professor, aptly noted "today's diversity of challenges increases the complexity of formulating successful deterrence strategies." Therefore Lowther suggested states "develop coherent and comprehensive approaches that are applicable to the global security environment" and that "deliberately employ all instruments of power,"[343] consistent with the bearing of this work. Senior defence analyst Michael Johnson and RAND program director Terrence Kelly emphasize tailored approaches to deter principal threats to national security, seizing upon basic tenets such as to deny objectives or impose costs, which provides a useful paradigm for exploring an alternative strategy in this work. They suggest deterring aggression by China in multiple domains with a defensive approach capable of limiting ability to attack.[344] A RAND study by Abram Shulsky examines the particular requirements for

---

[341] Chris Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*, (University of Georgia Press, September 2011): 39.

[342] William A. Chambers, "Foreword," in *Thinking About Deterrence*, Adam Lowther, editor, (Maxwell Air Force Base, Alabama: Air University Press, 2014): xii.

[343] Adam Lowther, "Introduction: The Evolution of Deterrence," *Thinking About Deterrence*, (Maxwell Air Force Base, Alabama: Air University Press, December 2013): 3-16.

[344] Michael Johnson and Terrence K. Kelly, "Tailored Deterrence: Strategic Context to Guide Joint Force 2020," *Joint Force Quarterly*, Number 74, 3rd Quarter 2014: 22-29.

deterrence of China while reaching a different conclusion that the best means is by diplomatic action,[345] which validates a different approach also examined in the work.

Cyber Deterrence

In the leading book on cyber deterrence, Martin Libicki applied the concept and components of deterrence in the context of strategic and operational cyberwar. Libicki masterfully examined what makes deterrence in cyberspace different in terms of attribution, signaling, thresholds, and escalation, which contributes to views on retaliation in this work.[346] Esteemed scholar Patrick Morgan believed for cyber attacks, the limits on deterrence based on retaliation, the largest being credibility to demonstrate will, must be compensated for by deterrence supplied by defense, which is the reverse of the U.S. situation during the Cold War.[347] Furthermore, Will Goodman, a defense advisor to Senator Patrick Leahy, explained that the credibility of a deterrent declaration is defined by capability, intent and incontestability. He proclaimed "states must maintain effective denial measures and threaten credible penalties,"[348] which lends credence to efforts for denial in this work. Given cumulative challenges of attack detection, precise attribution and credible retaliation, expert views by Dimitri Alperovitch from the cyber security firm McAfee, are appropriate for thinking of how to establish a cyberspace deterrence strategy. After arguing that "attacks on confidentially cannot be subject to deterrence in the current international framework," Alperovitch put forth a strategy that can "enhance

[345] Abram N. Shulsky, *Deterrence Theory and Chinese Behavior*, (Santa Monica, California: RAND Corporation, 2014).

[346] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, (Santa Monica, California: RAND Corporation, 2009).

[347] Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," *Proceedings of a Workshop on Deterring Cyberattacks*, (Washington, D.C.: The National Academies Press, 2010). 55-76.

[348] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly*, Vol. 4, Issue 3 (Fall 2010): 102-135.

national security against devastating cyber attacks through a credible declaratory retaliation capability that establishes red lines that may trigger a counter strike against all identifiable responsible parties,"[349] part of the basis for active defense in this work.

Jeffrey Cooper, a vice president for technology at Science Applications International Corporation, recognized the calculus of deterrence is a function of decision makers evaluating, within a matrix of values and expectations, possible gain versus loss for opportunities filled with consequences and uncertainties. Thus Cooper introduced a cooperation, competition and conflict framework for cyber deterrence that sees actors driven by and pursuing self-interest,[350] a relevant component of entanglement in this work. Franklin Kramer, distinguished fellow for the Brent Scowcroft Center, and Melanie Teplinsky, adjunct professional lecturer at American University's Washington College of Law, proposed development of a tailored deterrence approach to reduce adversarial cyber intrusions. Their unique approach emphasized raising costs of, and reducing benefits from, cyber attacks, to include use of cyber sanctions, mandatory standards for protection and resilience, international agreements, and certified active defense,[351] that are analogous to elements of the four strategic options in this work. Lieutenant Colonel Corinda Rujillo, U.S. Air Force provided similar options for cyber deterrence that comprise strengthening defense (security and resilience), pursing partnerships, and advancing policy and legislative solutions, which are highly realist and U.S.-led.[352] Kamal Jabbour, a senior scientist for information assurance, and Paul Ratazzi, a principal engineer for cyber assurance, suggested a

---

[349] Dimitri Alperovitch, "Towards Establishment of Cyberspace Deterrence Strategy," *Proceedings 3rd International Conference on Cyber Conflict* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, June 2011): 87-94.

[350] Jeffrey R. Cooper, "A New Framework for Cyber Deterrence," *Cyberspace and National Security*, (Georgetown University Press, 2012): 105-120.

[351] Franklin D. Kramer and Melanie J. Teplinsky, "Cybersecurity and Tailored Deterrence," Atlantic Council, December 2013: 1-10.

[352] Corinda Trujillo, "The Limits of Cyberspace Deterrence," *Joint Force Quarterly*, Number 75, 4th Quarter 2014: 43-52.

new strategy for securing cyberspace must employ new technical solutions based on warfighting concepts found in other domains, like the notion of offensive and defensive operations occurring simultaneously and in concert,[353] which are useful ideas for the application of active cyber defense in this work.

In order to better understand how defensive and offensive systems relate and interact in warfighting concepts in other domains for the translation of the simultaneous operations model to the cyber domain, national security expert Leon Sloss proposed looking at the strategic perspective of ballistic missile defense. Sloss then examined how ballistic missile defense does or does not play a role in deterrence strategies.[354] Although ballistic missile defense has demonstrated limited tactical success, Schulyer Forester, the Brent Scowcroft Professor of National Security Studies at the U.S. Air Force Academy, remarked that active defenses confront the tyranny of an offense dominant environment in the global commons (maritime, air, space and cyberspace domains). As an alternative, Forester presented deterrence by entanglement as a way to entrench potential adversaries in a network that would not attack because of shared interests,[355] the basis for the third strategic concept in this work. Other scholars evaluate the usefulness of the "commons" analogy for resolving issues nations face in regard to cyber security, and for guiding regulatory frameworks for cyberspace, such as those envisioned in the theory of entanglement suggested by Forester.[356] Vincent Manzo, a research analyst at the National Defense University, postulated that the United States may seek to deter attacks in

---

[353] Kamal T. Jabbour and E. Paul Ratazzi, "Deterrence in Cyberspace," *Thinking About Deterrence*, (Maxwell Air Force Base, Alabama: Air University Press, December 2013): 37-50.

[354] Leon Sloss, "The Strategist's Perspective," in *Ballistic Missile Defense*, Ashton B. Carter and David N. Schwartz, editors (Washington, DC: The Brookings Institute, 1984): 24-48.

[355] Schulyer Forester, "Strategies of Deterrence," in *Conflict and Cooperation in the Global Commons*, Scott Jasper, editor (Washington, DC: Georgetown University Press, 2012): 55-67.

[356] Julie J. C. H. Ryan, Daniel J. Ryan, and Eneken Tikk, "Cybersecurity Regulation: Using Analogies to Develop Frameworks for Regulation," 76-99.

cyberspace by threatening proportionate cross-domain responses, which adversaries could perceive as clearer and more credible.[357]

In maturing the concept of cyberspace as an operational domain, General Larry Welch, U.S. Air Force, former president of the Institute of Defense Analysis, treated "cyber as a place, not a mission," in, from, and through which "military operations create intended effects."[358] Parallel to this view, Lieutenant Colonel Lincoln Bonner, of the U.S. Air Force, defined "cyber power" as the ability to "exploit cyberspace to create advantages and influence events."[359] This ability to "create intended effects" and "influence events" through cyber power relates closely to the central premise of cyber deterrence - altering an adversary's behavior.[360] Thus David Betz, senior lecturer at King's College, and Tim Stevens, an associate at King's College, posit four distinct forms of cyber power. The first form uses direct coercion to modify the behavior or conditions of existence of another actor; the second involves the indirect control of an actor through the mediation of an institution; the third works to maintain structures to permit or constrain actors; and the fourth uses social discourses to constrain or facilitate social actions.[361] Joseph Nye, a renowned American political scientist, considered three aspects of relational power in the cyber domain which each use hard and/or soft power in or through cyberspace to obtain preferred outcomes. The first aspect uses an ability to make others "do something

---

357 Vincent Manzo, "Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit," *Strategic Forum*, No. 272, National Defense University, December 2011: 1-8.

358 Larry D. Welch, "Cyberspace – The Fifth Operational Domain," *Research Notes,* Institute of Defense Analysis, Summer 2011: 2-7.

359 E. Lincoln Bonner III, "Cyber Power for 21st- Century Joint Warfare," *Joint Force Quarterly,* Number 74, 3rd Quarter 2014: 102-109.

360 Adam Lowther, "The Evolution of Deterrence," in *Thinking About Deterrence*, Adam Lowther, editor, (Maxwell Air Force Base, Alabama: Air University Press, 2014): 4.

361 David J. Betz and Tim Stevens, "Power and Cyberspace," *Cyberspace and the State*, (Routledge, 2011): 35-53.

contrary to their initial preferences," the second aspect uses agenda setting that "precludes the choices of another by exclusion of their strategies," and the third aspect shapes "another's initial preferences so that some strategies are not even considered."[362] The Betz and Nye forms of cyber power are helpful in thinking of how to influence uncooperative state actors to abide by international norms established by international institutions contrary to their preferences. Stuart Starr, a distinguished research fellow at the National Defense University, went further to advance the theory of cyber power in regard to the development of strategy. He recommended assessments of military risk in relying so heavily on cyberspace and analyses of other levers of power (political, diplomatic and economic),[363] which are useful views on coercive means for altering an adversary's behavior.

Retaliation in a Cybered Conflict

This form of deterrence is based on credible threats of retaliation that impose unacceptable costs for hostile acts in cyberspace. An assortment of books and articles outline political and legal issues in determining circumstances and thresholds for retaliation in cybered conflict. Professor Michael Schmitt, the Chairman of the Stockton Center for the Study of International Law at the United States Naval War College, examined in a NATO CCD COE 2012 conference proceeding the meaning of the term attack in international law in a cyber operations context, both in the conduct of *jus ad bellum* (governs when a state may resort to force) and *jus in bello* (governs how operations may be conducted during armed conflict).[364] More than a decade before in his seminal paper, Schmitt provided six criteria for evaluating

---

[362] Joseph S. Nye, Jr. "Cyber Power," Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010: 7-9.

[363] Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," *Cyberpower and National Security*, (Washington, DC: National Defense University Press, 2009): 43-87.

[364] Michael Schmitt, "Attack as a Term of Art in International Law," *Proceedings 4th International Conference on Cyber Conflict*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012): 283-294.

cyber attacks as a use of armed force, specifically in severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.[365] Building upon these criteria, Schmitt chaired, an international group of experts, to produce two versions of the *Tallinn Manual,* as the authoritarian view on international law applicable to cyber operations, the latest version containing one hundred and fifty-four rules governing such operations. The *Manual 2.0* addresses topics such as sovereignty, jurisdiction, international responsibility, the use of force, the conduct of hostilities, and neutrality.[366]

Conversely a study by Keir Giles, the director of the Conflict Studies Research Centre, with Andrew Monaghan, a Research Fellow at Chatham House found "a range of foreign states use definitions for cyber conflict that are entirely different," which extends to different concepts of what constitutes hostile cyber activity and even a state of war, such as a shifting boundary between war and peace.[367] This finding complicates use of a consistent threshold to respond to cyber attacks in this thesis since an adversary "could be operating according to an entirely different understanding of international law."[368] Commander Ramberto Torruella, U.S. Navy offered how to determine what constitutes a hostile act using a variety of legal frameworks (instrument-, effects-, and target-based plus kinetic equivalency) combined with the Schmitt criteria.[369] Colonel Jonathan Rice, of the U.S. Air Force also proposed cyber attack guidance

---

[365] Michael Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *The Colombia Journal of Transnational Law*, Volume 37, 1999: 885-937.

[366] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second Edition (Cambridge: Cambridge University Press, 2017).

[367] Keir Giles with Andrew Monaghan, "Legality in Cyberspace: An Adversary View," *The Letort Papers*, Strategic Studies Institute, March 2014: 1-42.

[368] Ibid.

[369] Ramberto A. Torruella, "Determining Hostile Intent in Cyberspace," *Joint Force Quarterly*, Number 75, 4th Quarter 2014: 114-121.

based on foundational elements of context, spectrum, focus, and circumstances.[370] For a decision to respond to hostile cyber acts in kind, Major Steven Smart applied joint targeting principles according to the Law of War to military operations in cyberspace, to include differentiating between offensive and defensive cyber targeting.[371] The latter is most helpful, since Smart identified five key areas that complicate cyber targeting, specifically "positive identification of the target; location of the target; attribution of attack; capability/target pairing; and assessment of potential collateral damage." A premier example of the application of the Law of War that centers on the core principles of distinction and proportionality is contained in a report by John Richardson, the President of JMR Portfolio Intelligence, Inc. on the Stuxnet worm attack upon Iranian nuclear facilities.[372]

An analysis by Herbert Lin, a senior research scholar at Stanford University and his associates provided a foundation for understanding the basic characteristics, technologies and principles of a cyber attack, and what U.S. policy goals these actions might serve, is helpful because it integrates technical capacity with policy experience, which is the aim of this thesis.[373] Other articles address in detail what constitutes a cyber weapon and their ethical usage. Thomas Rid, now moved to John Hopkins University, and Peter McBurney, a Professor in the Agents and Intelligent Systems Group at King's College define and group cyber weapons along a spectrum

---

[370] Jonathan C. Rice, "Core Questions for Cyber Attack Guidance," *Joint Force Quarterly,* Number 71, 4th Quarter 2013: 32-39.

[371] Steven Smart, "Joint Targeting in Cyberspace," *Air & Space Power Journal*, Winter 2011: 65-74.

[372] John Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield," July 22, 2011: 1-39.

[373] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington, D.C.: The National Academies Press, 2009): 1-390.

ranging from malicious software to autonomous smart bombs.[374] While authors Gregory Rattray, of the Internet Corporation for Assigned Names and Numbers (ICANN) and Numbers, and Jason Healey categorize "offensive cyber capabilities across a range of potential scenarios to help further the dialogue on cyber deterrence,"[375] and this is useful for this work because it separates below-legal threshold campaigns from more overt military operations. Maren Leed, a senior advisor at the Center for Strategic and International Studies examined policy considerations, technical feasibility and intelligence concerns in the use of offensive cyber tools.[376] On ethical deliberations, Neil Rowe, a Professor of Computer Science at the Naval Postgraduate School discussed the unreliability of cyberweapons and the problems of damage assessment, counter attacks and collateral damage, arguing that cyberweapons "can create serious harms like any weapon."[377] A NATO organized ethics workshop tackled the applicability of traditional Just War Theory along Law of War criteria to military cyber operations[378] and of other theories of the morality of war, citing instances of cyber warfare in more slippery moral terrain, such as intrusion into information systems or placing inactive malware to eventually cause harm,

---

[374] Thomas Rid and Peter McBurney, "Cyber Weapons," The RUSI Journal, 157:1, February 29, 2012: 6-13.

[375] Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," *Proceedings of a Workshop on Deterring Cyberattacks*, (Washington, D.C.: The National Academies Press, 2010). 77-97.

[376] Maren Leed, "Offensive Cyber Capabilities at the Operational Level," Center for Strategic & International Studies," September 2013: 2-3.

[377] Neil C. Rowe, "The Ethics of Cyberweapons in Warfare," International Journal of Technoethics," January-March 2010: 20-31.

[378] Edward T. Barrett, "The Applicability of the Just War Tradition to Military Cyber Operations," *1st Workshop on Ethics of Cyber Conflict Proceedings* (NATO Cooperative Cyber Defense Centre of Excellence: Tallinn, Estonia: 2014): 26-32.

meaning some methods for retaliation reviewed in this work might be ethically or/and legally questionable.[379]

Several articles explore escalatory issues that relate to decisions to retaliate in response to a hostile act in cyberspace. Martin Libicki cited that cyber attacks carried out in the name of deterrence may be considered "after-the-fact retaliation to convince the attacker to stop attacking, and deter it from contemplating further mischief."[380] Accordingly Herbert Lin's work examined how to deter escalation (chain reactions), terminate conflict (cease fire agreements), and prevent kinetic escalation (off-limit targets) which is difficult in practice.[381] Another article by Irving Lachow, a Portfolio Manager for International Cyber at the MITRE Corporation and his associates identified the important precept that unlike kinetic actions that can generally be identified and measured, the failure to detect intentions, moves, and origins in cyberspace could lead to overreactions and miscalculations, hence escalation.[382]

<u>Denial in a Cybered Context</u>

This form of deterrence is based on capability that ensures denial of an adversary's objectives in cyberspace. Although limited academic material on the topic of protective measures is available since cyber security solutions are usually promulgated in industry releases, Emin Caliskan, a Computer Scientist, and Raimo Peterson, Chief of Research & Development,

---

379 Randall R. Dipert, "Distinctive Ethical Issues of Cyberwarfare," *1st Workshop on Ethics of Cyber Conflict Proceedings* (NATO Cooperative Cyber Defense Centre of Excellence: Tallinn, Estonia: 2014): 33-40.

380 Martin Libicki, "Pulling Punches in Cyberspace," *Proceedings of a Workshop on Deterring Cyberattacks*, (Washington, D.C.: The National Academies Press, 2010). 123-147.

381 Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, Vol. 6, Issue 3 (Fall 2012): 52-55.

382 Robert A. Miller, Daniel T. Kuehl, and Irving Lachow, "Cyber War: Issues in Attack and Defense," *Joint Force Quarterly*, Issue 61, 2nd Quarter 2011: 18-23.

both at the NATO CCD COE, have explained the main technical methods and techniques for cyber defense, with some coverage of security applications and devices, such as firewalls, detection and prevention systems, and honeypots (a computing resource whose purpose is to be accessed in an unauthorized way in order to collect information about the attack and the attacker.)[383] Richard Andres, a Professor at the U.S. National War College highlighted the dynamics in cyber defense as an element of cyber deterrence and the reasons the traditional defense model is failing under cyber threats.[384] Relatedly, David Aucsmith, Chief Scientist at the Applied Physics Lab of the University of Washington laid out in his article on cyber defense a fundamental factor in a computer system is their complexity that guarantees vulnerabilities and the lack of a systemic way to find all of them.[385]

According to cyber security professionals Jason Andreas and Steve Winterfeld "one of the more important principles of a successful defensive strategy is defense-in-depth," which "proposes a layered approach to security."[386] In this case defenses would be at the network, host, application, and data levels, in addition physical security and user awareness training are integrated into layers of security.[387] In regard to sample defenses, Robert Koch gave a useful overview of intrusion detection and data leakage prevention systems to investigate their

---

[383] Emin Caliskan and Raimo Peterson, "Technical Defense Methods, Techniques, Tools and Effects," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 61-101.

[384] Richard B. Andres, "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," *Cyberspace and National Security*, (Georgetown University Press, 2012): 89-103.

[385] David W. Aucsmith, "Rethinking Cyber Defense," *High Frontier*, Volume 7, Number 3, May 2011: 35-37.

[386] Jason Andreas and Steve Winterfeld, *Cyber Warfare Techniques, Tactics and Tools for Security Practitioners*, Second Edition, (Walton, MA: Syngress, 2014): 203.

[387] Ibid, 204.

shortcomings while recommending architecture for next generation systems.[388] According to a report on Strategic Cyber Intelligence, in addition to tactical level intelligence to help understand a network attack, a great need exists at a higher level to better understand the goals, objectives and inter-relationships associated with these tactical attacks. This knowledge will lead to risk-informed decision making on investments in defensive measures relevant to the threat and better choices across deterrence options.[389]

Larry Clinton, the president of the Internet Security Alliance, a civil society group, wrote about value of public-private partnerships in promoting cyber threat information sharing, in particular the sharing of classified and sensitive information by the government with the private sector to defend its systems and deny benefit of an attack.[390] Several other articles address sharing of cyber threat and also system vulnerability information between the public and private sectors. This practice could warn either about likely attacks or specific problems in software which would help defenders harden systems. Sharing of information should not include personal or sensitive details, just sources of threats or vulnerabilities in coding.[391] Therefore in the United States a number of impediments for sharing exist, starting with a narrow legislative focus since the 9/11 attacks on counterterrorism and agency over-classification of relevant data. The recent Presidential Executive Order 13636, titled Improving Critical Infrastructure Cybersecurity, takes steps to improve information dissemination, with an emphasis on producing unclassified reports

---

[388] Robert Koch, "Towards Next-Generation Intrusion Detection," *Proceedings 3rd[h] International Conference on Cyber Conflict* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence , June 2011): 87-94.

[389] Intelligence and National Security Alliance, "Strategic Cyber Intelligence," March 2014: 1-12.

[390] Larry Clinton, "Improving our Nation's Cybersecurity through the Public-Private Partnership," Internet Security Alliance, March 8, 2011: 1-26.

[391] David Inserra and Paul Rosenzweig, "Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," *The Heritage Foundation,* No. 2899, April 1, 2014: 1-13.

or granting security clearances when a report cannot be declassified but is crucial to the defense of critical infrastructure.[392] The Senate Intelligence Committee passed the Cybersecurity Information Act (CISA) of 2014 however it could be improved with reasonable clearer privacy protections and more protection from regulatory use.[393]

Entanglement in a Cybered World

This form of deterrence is based on cooperation on mutual interests that encourages responsible behavior (and thus restrains malicious behavior) in cyberspace. Cooperation at the hemispheric, regional or global level is relevant to deterrence because it is often seen as the surrogate indicator of conflict reduction by entanglement. For example, Brian Bow, the director of the Centre for Foreign Policy Studies and an Associate Professor at Dalhousie University stated that apprehensions about cybersecurity serve as a political lever for progress between the United States, Canada and Mexico on coordinated national policies for critical infrastructure security and resilience.[394] Thomas Renard, a senior research fellow at Egmont-Royal Institute for International Relations assessed the extent and limits of cooperation between the European Union and its strategic partners on cyber security, to include achieving cyber resilience and cooperating with like-minded international stakeholders to make the internet safe and stable. Renard reviewed cooperation on the exchange of information and best practices, strengthening multilateral instruments and shaping internet governance.[395] Joseph Nye, a Distinguished Service Professor at Harvard University took a global view on internet governance, using regime

---

[392] Veronica A. Chinn, Lee T. Furches, and Barian A. Woodward, "Information-Sharing with the Private Sector," *Joint Force Quarterly,* Number 73, 2nd Quarter 2014: 32-38.

[393] David Inserra, "Senate Cyber Information-Sharing Bill on the Right Track but Improvements Needed," *The Heritage Foundation*, No. 4269, September 2, 2014: 1-3.

[394] Brian Bow, "Now for the Hard Part: Renewing Regional Cooperation on Critical Infrastructure Security and Resilience," Wilson Center, September 2014: 1-18.

[395] Thomas Renard, "The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security," European Strategic Partnerships Observatory, Working Paper 7, June 2014: 1-31.

theory to describe loosely coupled norms and institutions in a mapped regime complex. Nye contended this loose coupling among issues permits cooperation among actors in some areas, like economic prosperity, while they disagree in others, such as in human rights and content control.[396]

Joseph Nye separated norms from entanglement in describing complex mechanisms to prevent harm in cyberspace, evening calling norms a fourth major means of deterrence. Although Nye readily admitted that normative considerations "can deter actions by imposing reputational costs that can damage an actor's soft power beyond the value gained for a given attack." Since reputation is "something highly valuable to lose," potential costs in this regard may contribute to self-restraint, which Nye labeled an element of entanglement that "may result from rational calculations of interest."[397] Hence normative considerations encourage restraint, or in effect serve to implement entanglement. A report by the United Nations Secretary General recognizes that the application of norms derived from existing international law relevant to information and communication technologies is essential to reduce risks to international security.[398] An understanding of the general principles of international law and their application to cyberspace is necessary to evaluate the efficacy of norms. Katharina Ziolkowski, a legal advisor to the German Armed Forces, stated that although "cyber specific international custom is absent and contractual regulation is scarce," the "competing freedoms of the coexisting

---

[396] Joseph S. Nye, Jr., "The Regime Complex for Managing Global Cyber Activities," Chatham House, Paper Series: No-1, May 2014: 1-15.

[397] Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security,* Vol.41, No. 3, Winter 2016/2017: 58.

[398] Secretary General, United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, 24 June 2013: 1-13.

sovereign States are guided (and de-conflicted) by general principles of international law."[399] Kristen Eichensher, a visiting Assistant Professor at the UCLA School of Law, addressed pressing state-to-state issues in regulation of cyberspace, starting with the presumption that existing legal regimes for the high seas and outer space establish a baseline for the assessment of cyber governance. She argued for multi-stakeholder governance in cyberspace and governance through norms (and not by treaties), which can serve as instruments for cooperation among actors in deterrence by entanglement.[400]

Other authors also discount the use of treaties for cyber governance as a form of arms control relevant to deterrence and de-escalation of cybered conflict is contested among experts. Paul Meyer, a Canadian Foreign Service Officer explained policy-makers can draw upon past arms control models to accommodate the specific challenges of cyberspace, in particular examples for prevention and for regulation. However, Meyer concluded that arms control efforts for cyberspace are premature due to problems of attribution, transparency, and verification, but some aspects, like confidence building measures have merit.[401] Neil Rowe and his associates argue however, that recent technology provides some tools for cyber weapons control and therefore international cyber arms agreements could provide for forensics and usage monitoring, while encouraging more responsible cyber weapons use by stipulating attribution and reversibility.[402] Louise Arimatsu, in the International Law Program at Chatham House, finds that,

[399] Katharina Ziolkowski, "General Principles of International Law as Applicable in Cyberspace," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 135-188.

[400] Kristen Eichensehr, "The Cyber-Law of Nations," *Georgetown Law Journal*, Vol. 103, No. 2, August 6, 2014: 1-74.

[401] Paul Meyer, "Cyber-Security Through Arms Control," *RUSI Journal,* Vol. 156, No. 2, April/May 2011: 22-27.

[402] Neil C. Rowe, Simson L. Garfinkel, Robert Beverly, and Panayotis Yannakogeorgos, "Challenges in Monitoring Cyberarms Compliance," *International Journal of Cyber Warfare & Terrorism*, January-March 2011: 1-14.

although chances for a cyber arms control treaty cannot be dismissed, reasoning from historical experience is a poor guide; for contrary to kinetic weapons; cyber weapons are relatively inexpensive, widely accessible, easily concealable, and impossible to destroy all copies.[403]

Michael Schmitt discussed in a Tallinn paper the two sources of international law – treaties and custom – and explained the different challenges cyberspace poses to their formation, identification and application. He deduced that the conclusion of new treaties or the crystallisation of new customary law norms to govern cyber activities is doubtful, and instead, the application and interpretative evolution of existing international law is the most likely near-term prospect.[404] Other authors are more hopeful for success in international norms, such as Panayotis Yannakogeorgos, the Dean of the Air Force Cyber College and Adam Lowther, an Air Force research professor, who write that "nation-states should be held culpable for the malicious actions and other cyber threats originating in or transiting information systems within their borders, or owned by registered corporate entities therein," under clear and accepted norms of responsible state behavior in cyberspace.[405] Their work assumes attribution problems can be resolved with "not only technical methods, but also legal/policy solutions as well."[406]

This work assumes the right of a cyber Westphalia in which nations will be choosing deterrence options for themselves. David Betz and Tim Stevens consider the notion of

---

[403] Louise Arimatsu, "A Treaty for Governing Cyber-Weapons," *Proceedings 4th International Conference on Cyber Conflict*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012): 91-109.

[404] Michael N. Schmitt and Luis Vihul, "The Nature of International Law Cyber Norms," Tallinn Paper No. 5, A NATO CCD COE Publication, 2014: 1-31.

[405] Panayotis A. Yannakogeorgos and Adam B Lowther, "The Prospects for Cyber Deterrence: American Sponsorship of Global Norms," *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, (Taylor & Francis Group, July 2013): 51.

[406] Panayotis A. Yannakogeorgos, *Strategies for Resolving the Cyber Attribution Challenge*, (Maxwell Air Force Base, Alabama: Air University Press, December 2013): 1-85.

Westphalia (as a right of internal decision-making) in their interpretations of cyberspace and sovereignty, in addition to domestic (entails authority and control); interdependence (control flows across territorial boundaries); and also international legal (recognition of state authority). They detect these forms of sovereignty interact with each other and are subject to compromise.[407] Brigid Grauman, an independent Brussels-based journalist presented judgements by experts, such as Vytautas Butrimas, Lithuania's Cyber Security adviser at the Ministry of Defense that "we need an international agreement that makes every country responsible for its sovereign cyber-space" and by U.S. Lawyer Stewart Baker that "an international treaty is a waste of time."[408] Jason Healey, a senior research scholar at Columbia University and a Senior Fellow at the Atlantic Council crossed this chasm in opinions with proposed cyber confidence-building measures that increase stability in cyberspace without extensive legal or political action by states.[409] Legal scholar Katharina Ziolkowski attested to the value of confidence-building measures as "a verified instrument of international politics, which aims to prevent the outbreak of war or an (international) armed conflict by miscalculation or misperception of the risk,"[410] yet affirmed their development for cyberspace proves to be difficult because of the specific attributes of the internet.

---

[407] David J. Betz and Tim Stevens, "Cyberspace and Sovereignty," *Cyberspace and the State*, (Routledge, 2011): 55-74.

[408] Brigid Grauman, "Cyber-Security: The Vexed Question of Global Rules. An Independent Report on Cyber-preparedness around the World," Santa Clara, CA: McAfee, 2012.

[409] Jason Healey, John C. Mallery, Klara Tothova Jordan, and Nathaniel V. Yould, "Confidence-Building Measures in Cyberspace," Atlantic Council, November 2014: 1-19.

[410] Katharina Ziolkowski, "Confidence Building Measures for Cyberspace – Legal Implications," (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2013): 12.

Systemic Resilience

The concept of systemic resilience is relevant to the argument in this thesis because the development of overarching internal systemic resilience is a way to meet the failings of the contemporary deterrence strategies of retaliation, denial and entanglement. Systemic resilience in this work means a defender's state or network has the capacity of combined social and technical systems to proactively recognize, adapt to, absorb, and innovate around disturbances or disruptions.[411] Numerous books and chapters by esteemed authors illustrate the value of resilience in general as a key element of national security strategy. This value is apparent in an edited volume by Louise Comfort, Arjen Boin, and Chris Demchak on the topic of resilience in the context of low-chance, high impact events, such as natural disasters, terrorist attacks, pandemics or critical infrastructure failures, sometimes called Black Swan events. The authors use this forum to inquire into the characteristics, causes, consequences, and measurement of resilience, while studying societal capacity to deal with emerging contingencies in terms of resilience.[412] For why resilience against cyber attacks is important, P.W. Singer, the director of the Center for 21st Century Security and Intelligence, and Allan Friedman, the research director of the Center for Technology Innovation, both at the Brookings Institution illuminate the need to build resilience against shocks (like losing internet access) that have impact on things like politics and economics. They think about resilience in terms of systems and organizations that are prepared for attacks and can maintain some functionality while under attack.[413] Chris Demchak observes that cybered conflict greatly increases the potential for unexpected outcomes across the complex critical systems of modern society. Therefore, a national security resilience

---

[411] Louise K. Comfort, Arjen Boin, and Chris C. Demchak, *Designing Resilience: Preparing for Extreme Events,* (University of Pittsburgh, September 2010.): 1-12.

[412] Louise K. Comfort, Arjen Boin, and Chris C. Demchak, *Designing Resilience: Preparing for Extreme Events,* (University of Pittsburgh, September 2010)

[413] P.W. Singer and Allan Friedman, "Rethink Security: What is Resilience and Why is it Important," *Cybersecurity and Cyberwar*, (New York, NY: Oxford University Press, 2014): 169-173.

strategy is necessary to guide the coordination of society's cyber resilience with national military capabilities,[414] and could be relevant to strengthen deterrence, by halting malicious cyber activity after an intrusion, and by using tailored disruption capacities to thwart malicious actor objectives.

Kamal Jabbour, at the Air Force Institute of Technology, and Sarah Muccio, at the Air Force Research Lab write on the challenges of mission assurance, similar to the functional continuity aspects of resilience, for national security systems and with a direct relevance to discussions of deterrence. They introduce an approach to mapping mission dependence on cyber systems and discuss time dependent mission assurance, specified for a finite duration, rather than indefinitely.[415] Academic treatise for critical infrastructure protection advances these themes along practical examples starting with an edited book by Maurizio Martellini, from the International Working Group-Landau Network Centro Volta, that proposes methods for security and resilience for industrial control systems.[416] Joseph Weiss, an industry expert on control systems formerly at the Electric Power Research Institute, concentrates on protecting systems from malicious threats while maintaining their mission, given their convergence with but also differences between information technology systems.[417] Other experts at the U.S. Department of Homeland Security respond to industrial control system vulnerabilities with suggestions for

[414] Chris Demchak, "Cybered Conflict, Cyber Power, and Security Resilience as Strategy," *Cyberspace and National Security*, (Georgetown University Press, 2012): 121-136.

[415] Kamal Jabbour and Sarah Muccio, "On Mission Assurance," *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, (Taylor & Francis Group, July 2013): 107-126.

[416] Maurizio Martellini, Cyber Security: Deterrence and IT Protection for Critical Infrastructure, (Springer, October 2013).

[417] Joseph Weiss, *Protecting Industrial Control Systems from Electronic Threats*, (New York, NY: Momentum Press, 2010).

defense-in-depth strategies that create an aggregated security posture which isolates and protects critical assets.[418]

Robert Jervis asserts in his book that many systems are contingent on strategies that "produce aggregate behavior that is complex and ordered, although not necessarily predictable and stable."[419] He stated that everything in a system will not remain constant and a change at one point will have wide ranging and multiple effects. Therefore based on his premise that in a system the whole is *different from*, not *greater than*, the sum of the parts, Jervis examines effects, often delayed and indirect, that occur from interactions of the parts, with the belief that since systems are designed to cope with adversity, the breakage of one point rarely destroys them.[420] Jervis cites how Robert Gilpin in his most important realist text addresses the vital role that feedback, both positive and negative, plays in most systems, especially in the system structure of world politics when confronted by stimuli.[421] Jervis in particular contributes to an argument to strengthen deterrence through systemic resilience because the vast majority of large-scale socio-economic-technical systems from electrical grids to manufacturing supply chains have become vulnerable to nasty surprises in cyberspace and if a surprise can cascade over enough nodes, the wide ranging and multiple effects will become a systemic event.[422]

---

418 Department of Homeland Security, "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies," October 2009: 1-34.

419 Robert Jervis, *Systemic Effects: Complexity in Political and Social Life,* (Princeton University Press, 1997):7.

420 Ibid, 8-19.

421 Robert Galpin, *War and Change in International Politics*, (Cambridge University Press, 1981).

422 Chris C. Demchak, "Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)," *Journal of Comparative Policy Analysis: Research and Practice*, July 12, 2012: 254-258.

Complexity Theory and Socio-Technical Systems Literature

Chris Demchak argued that not only systemic resilience, but also disruption capacities in large-scale socio-technical-economic systems are key components of relative cyber power, and therefore are used as conceptual elements in this work. Demchak observed that cybered coercers use deception and opaqueness in campaigns against these complex systems designed, used and maintained by humans. Therefore national cyber power needs to be both resilient to unskilled bad actors assaulting society and able to disrupt organized hackers employed by states or transnational organizations. Since cybered coercion is theoretically a struggle between whole systems, the understanding of cumulative effects across the wide range of actors and complex systems requires reframing along systemic terms.[423] Professor Alicia Juarrero said complex systems are grouped into interlinked levels of organization determined by the functional task of interest. In her article she proclaimed that "complexity is a systemic property." According to Juarrero, complexity is the order that results from the connectivity and interaction among multiple agents,[424] which helps to understand the systemic nature of complex systems that are at risk from cyber attack.

Edward Smith, an executive strategist at the Boeing Company, labeled military organizations and government agencies as multi-tiered living systems that have a recognizable order, where simultaneous interactions with multiple actors occur on many different levels. In a full length study, he examined complexity in the context of effects-based approaches to operations. Here Smith viewed complexity as "a continually changing array of interdependent variables in which the chain of causes and effects between action and outcome will seldom if

---

[423] Chris C. Demchak, "Economic and Political Coercion and a Rising Cyber Westphalia," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 595-620.

[424] Alicia Juarrero, "Complex Dynamical Systems Theory," Cognitive-Edge.com, 2010: 1-11.

ever be the same."[425] Furthermore, Professors William Rouse and Nicoleta Serban at the Georgia Institute of Technology explained how understanding change in complex systems requires understanding the fundamental nature of causality. They argued the difficulty in determining causes of system states increases with the complexity of the system.[426] David Berteau and his fellow authors saw complexity as a result of non-linear, unpredictable interaction of elements combined in new ways. Their paper provided ways to measure or access success in managing complex programs, while cultivating flexibility and resiliency in the organization, integral to defending against cyber attacks.[427]

Professor John Holland at the University of Michigan also saw complexity as a web of interactions between objects with interconnected parts. He contended each complex system exhibits a distinctive property called *emergence* which is roughly described by the common phrase "the action of the whole is more than the sum of the actions of the parts." His short book looks at ways in which systems exhibit emergent properties. Holland split the field of complexity studies into two subfields that study emergence: complex physical systems and complex adaptive systems.[428] Doctor Mitchell Waldrop, a writer and correspondent for Science magazine, discussed this adaptive phenomenon in his classic book on complexity. He observed the richness of independent agents "interacting with each other in a great many ways" allows "the system as a whole to undergo spontaneous self-organization."[429] Furthermore he argued

---

[425] Edward A. Smith, "Complexity, Networking & Effects-Based Approaches to Operations," Command and Control Research Program Publication Series, 2006.

[426] William B. Rouse and Nicoleta Serban, "Understanding change in complex socio-technical systems: An exploration of causality, complexity and modeling," *Information Knowledge Systems Management*, (IOS Press, 2012): 25-49.

[427] David J. Berteau, Guy Ben-Ari, and Matthew Zlatnik, "Organizing for a Complex World: The Way Ahead," Center for Strategic and International Studies, 2009: 1-16.

[428] John H. Holland, *Complexity: A Very Short Introduction*, (Oxford University Press, 2014).

[429] M. Mitchell Waldrop, *Complexity: The Emerging Science at the Edge of Order and Chaos*, (New York: Simon and Schuster Paperbacks, 1992): 11.

these "self-organizing systems are adaptive in that they don't just passively respond to events," but actively "try to turn whatever happens to their advantage."[430] Waldrop concluded that "complex, self-organizing, adaptive systems [possess] a kind of dynamism that makes them qualitatively different from merely complicated static objects."[431]

A comprehensive approach is one way for stakeholders to deal with the inherent complexity in socio-economic-technical systems. A key test for this work is whether each of the deterrent options is comprehensive enough for an emerging cybered world. The comprehensive approach seeks "to apply a wide spectrum of civil and military instruments in a concerted effort that takes into account their respective strengths and mandates."[432] The pivotal study of the approach reveals from operational experience that coherence could only be achieved if processes, planning and objectives are harmonized across all instruments and agencies.[433] Fundamentals of the comprehensive approach include interdependence, cooperation, prioritization, nesting of imperatives with objectives, flexibility of sequencing and timing, and measurements of progress.[434] Accordingly, essential elements for implementation of the approach are proactive coordination mechanisms, shared understanding, outcome-based thinking and collaborative working guidelines. While many of the fundamentals and elements are reflected in some manner in the four strategic options in this work, yet their absence signifies insufficiency in the contemporary deterrence strategies.

---

[430] Ibid.

[431] Ibid, 11-12.

[432] Brooke Smith-Windsor, "Hasten Slowly: NATO's Effects Based and Comprehensive Approach to Operations," NATO Defence College, Research Paper No. 38, Rome, 2008.

[433] United Kingdom, Ministry of Defence, "The Comprehensive Approach," joint discussion note 4/05 (Shrivenham: Joint Doctrine and Concepts Centre, 2006), 1-4 to 1-7.

[434] United States Institute of Peace, "Fundamentals of a Comprehensive Approach," in *Guiding Principles for Stabilization and Reconstruction*, (Washington, DC: United States Institute of Peace Press, 2009): 5-30 to 5-32.

Part of the reason for lack of coherence in practice, according to Phillipp Rotmann, a fellow at the Global Public Policy Institute in Berlin, is that obstacles to an effective comprehensive approach include institutional and political fragmentation of mandates, conflicts between organizational and professional cultures, and political-strategic differences.[435] Two edited volumes best examine how the comprehensive approach can be translated and applied for different situations, conditions and players, to include in an emerging cybered world. In the first, Kristina Rintakoski and Mikko Autti, editors for the Crisis Management Initiative, state the comprehensive approach is a way of thinking or a method rather than a mechanical process. They argue it is all about developing mechanisms and cultures of understanding, sharing and collaboration.[436] Therefore the comprehensive approach enhances organizational interaction to deal with inherent complexity. Michael Hallet and Oke Thorngren, on the staff of NATO's Supreme Allied Command Transformation, state the approach aims for congruence of purpose. It enables the development of new means of influencing (seducing some, coercing others) actors to shape the environment. Most importantly, this influence can be exerted in preventing conflict, not only responding to it, to include in the cyber domain under the guise of cyber deterrence.[437]

Active Cyber Defense

In this work, Active Cyber Defense is posited as a more comprehensive and thereby useful deterrent option for nations mired in cybered conflict. It's defined here as the real-time

[435] Phillipp Rotmann, "Built on Shaky Ground: The Comprehensive Approach in Practice," NATO Defence College, Research Paper No. 63, Rome, 2010.

[436] Kristina Rintakoski and Mikko Autti, *Trends, Challenges and Possibilities for Cooperation in Crisis Prevention and Management*, (Helsinki, Finland: Crisis Management Initiative, June 17, 2008), 1-34.

[437] Michael Hallet and Oke Thorngren, "Attempting a Comprehensive Approach Definition and Its Implications for Reconceptualizing Capability Development," Chapter 3, *Capability Development in Support of Comprehensive Approaches*, (National Defense University, December 2011): 35-50.

detection, analysis and mitigation of network security breaches combined with the aggressive use of legal countermeasures beyond network and state territorial boundaries.[438] The newness of the concept and of the environment in which it is emerging makes a literature review more challenging than the previous discussions of terms such as denial, entanglement or norms. Nonetheless a growing field of works deals with the concept directly or relatedly. Some are more explicit and advanced than others but all offer some aspect of Active Cyber Defense relevant to this argument. Professor Jay Kesan and his research assistant Carol Hayes at the University of Illinois at Urbana-Champaign in a workshop proceeding in 2010 identified the concept as a controversial option that returns fire at hackers in order to prevent further disruption. They claim a combination of intrusion detection systems and traceback technology provides the source of the attacks for counterstrikes. Although already a practice in the IT industry to some extent, the authors question if counterstriking should be regulated and standardized.[439] For in reality, Herbert Lin, a senior research scholar at Stanford University argued the private sector has only two ways that are incontrovertibly legal under current law, either to take defensive measures within its organizational boundaries or seek the assistance of law enforcement. Lin characterized any offensive operations chosen by the private sector for defensive purposes as "self-help," which if condoned by US policy might serve as a deterrent against the cyber threat.[440]

In 2013, Irving Lachow, a Portfolio Manager for International Cyber at the MITRE Corporation took a broader view on the topic in describing the term active cyber defense as "a

---

[438] Robert S. Dewar, "The Triptych of Cyber Security: A Classification of Active Cyber Defense," in *Proceedings 6th International Conference on Cyber Conflict* (Tallinn, Estonia: CCD COE, June 2014): 7-21.

[439] Jay P. Kesan, and Carol M. Hayes, "Thinking Through Active Defense in Cyberspace," *Proceedings of a Workshop on Deterring Cyberattacks*, (Washington, D.C.: The National Academies Press, 2010). 327-341.

[440] Herbert S. Lin, "Defining Self-Defense for the Private Sector in Cyberspace," *World Politics Review*, February 6, 2013: 1-4.

range of proactive actions that engage the adversary before and during a cyber incident."[441] These actions enable detection and forensics, deception and attack termination. However he argued any use of active cyber defense techniques must not violate the primary law that applies in such situations, the U.S. Computer Fraud and Abuse Act of 1984.[442] A way to comply with this law described by Martin Stytz, the Collegiate Professor for Cybersecurity at the University of Maryland, and Sheila Banks, the president of Calculated Insight is to "erect an ever-varying maze of tactical cyber defenses based on virtual machines, each with a different combination of properties and operational characteristics that serve to complicate the tactical cyber-attackers' challenge."[443] In essence the tactical cyber defenses that operate inside the network to remain inside the law are "based upon an active, dynamic layered cyber defense-in-depth" architecture. Attorney James Farwell and Rafal Rohozinski, a principal of the SecDev Group observed in 2012 that the military's notion of active cyber defense was unformed.[444] This assertion remained true until finally in 2014, the Director of Operations at U.S. Cyber Command described passive and active defense activities by the military in the concept of defensive cyberspace operations.[445]

Although there is a growing number of trade, military, and other articles related to the concept, currently only one book exists with the title Active Cyber Defense, an edited volume that captures the proceedings of an international conference held in Tallinn, Estonia by the NATO Cooperative Cyber Defence Centre of Excellence in 2014. In the volume, Robert Dewar, a researcher in the Politics Department at the University of Glasgow suggested a concept

---

[441] Irving Lachow, "Active Cyber Defense: A Framework for Policy Makers," Center for a New American Security, February 2013: 1-10.

[442] Ibid.

[443] Martin R. Stytz and Sheila B. Banks, "Toward Attaining Cyber Dominance," *Strategic Studies Quarterly*, Vol. 8, Issue 1 (Spring 2014): 55-71.

[444] James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival: Global Politics and Strategy*, Vol 54, Issue 4, August 1, 2012: 110.

[445] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Number 73, 2nd Quarter 2014: 12-19.

definition based on characteristics identified in academic and policy literature, where active cyber defense is predicated upon proactive measures not only to detect, analyze, and mitigate breaches in real time, but also upon aggressive countermeasures outside the victim network, which directly informs the definition used in this work.[446] In hearing a rising chorus of voices in favor of external countermeasures, Oona Hathaway, the Gerard C. and Bernice Latrobe Smith Professor of International Law at the Yale Law School outlined both legal and policy concerns in her chapter, primarily drawn on the correlation between "hack back" to a "use of force."[447] In contrast, Jason Rivera, U.S. Army posted at the Georgetown School of Foreign Service, and Forrest Hare, U.S. Air Force at the Johns Hopkins School of Advanced International Studies, spun the book's focus to internally based cyber threat countermeasures that proactively engage threatening actions independent of a requirement to achieve attribution. They contend effective internal countermeasures will deter malicious actors by affecting their cost/benefit calculus.[448] NikosVirvilis and Oscar Serrano, both at the NATO Communications and Information Agency, and Bart Vanautgaerden, a consultant for NATO Office of Security, InfoSec, at NATO Headquarters, concur with the use of internal countermeasure in their chapter by proposing the use of multiple deception techniques, like honey tokens or social network avatars, at stages of the attack phase to protect the resources of an organization.[449]

---

[446] Robert S. Dewar, "The Triptych of Cyber Security: A Classification of Active Cyber Defense," *Proceedings 6th International Conference on Cyber Conflict* (Tallinn, Estonia: CCD COE, June 2014): 7-21.

[447] Oona A. Hathaway, "The Drawbacks and Dangers of Active Defense," *Proceedings 6th International Conference on Cyber Conflict* (Tallinn, Estonia: CCD COE, June 2014): 39-52.

[448] Jason Rivera and Forrest Hare, "The Deployment of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures," *Proceedings 6th International Conference on Cyber Conflict* (Tallinn, Estonia: CCD COE, June 2014): 99-116.

[449] Oscar Serrano, Bart Vanautgaerden, and Nikolaos Virvilis-Kollitirus, "Changing the Game: The art of deceiving sophisticated hackers," *Proceedings 6th International Conference on Cyber Conflict* (Tallinn, Estonia: CCD COE, June 2014): 87-98.

A number of recent studies and reports by academics and researchers have examined, suggested or neglected the use of active cyber defense. The most prominent report is aptly titled *Into the Gray Zone* sponsored by the Center for Cyber & Homeland Security at the George Washington University. The most useful aspect of this Project Report is the depiction of the "spectrum of proactive cybersecurity measures that fall between traditional passive defense and offense."[450] Their definition and evaluation of active defense techniques informed the range of countermeasures listed in this work and their applicability to types of malicious actors in various scenarios. While those countermeasures act outside the network, Liam Nevill and Zoe Hawkins, from the Australian Strategic Policy Institute, affirm the value of automated technologies that act within one's own defense to "interdict, isolate or remove threat vectors."[451] Furthermore, the Center for Long-Term Cybersecurity at UC Berkley released Policy Ideas for a New Presidency that included "norm development in the active defense space." Although considered risky, the Center tacitly promoted private active defense as "a limited freedom, for a cabined window of time," made "in coordination with the government,"[452] to increase capabilities to respond to cyber attacks. Paul Rosenzweig and associates at the Heritage Foundation reached the same conclusion in saying "the U.S. should expressly allow active defenses that annoy adversaries while allowing only certified actors to engage in attribution-level active defenses,"[453] which endorsed the proposed application of tailored disruption capacities in this work. Finally, the Defense Science Board report, co-chaired by James Miller and James Gosler, both senior fellows at the Johns Hopkins University Applied Physics Laboratory focused primarily on tailored

---

[450] Center for Cyber & Homeland Security, "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," Project Report, The George Washington University, October 2016

[451] Liam Nevill and Zoe Hawkins, "Deterrence in Cyberspace: Different domain, different rules," Special Report, International Policy Centre, July 2016: 1-24.

[452] Jesse Goldhammer, et al, Center for Long-Term Cybersecurity, "Cybersecurity Policy Ideas for a New Presidency," UC Berkeley, November 2016.

[453] Paul Rosenzweig, et al, "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense," Backgrounder, No. 3188, May 5, 2017.

deterrence campaigns for the "most likely" and the "most dangerous" types of cyber attacks. However, their definition of cyber attack included only effects on availability and/or integrity, of mostly weapon and affiliated military systems, omitting confidentially, the third element of the standard security triad for information systems. Although the authors concluded "it is clear that a more proactive and systematic approach to U.S. cyber deterrence is urgently needed," the report neglected to even consider active cyber defense, only mentioning vague "innovative technologies aimed at breakthrough improvements in cyber security." Except for discussions on the development of a playbook of scalable response options, the report is not very applicable for this work.[454]

Review Summary

Adequate sources exist to articulate in detail the underlying logic of the thesis. Primary literature is sufficient to describe the typology of malicious actors, attack methods and their motivations for exploiting their inherent advantages in the cyber substrate. Current reference material is available to explore how cyber acts through complex system's surprise to result in nationally significant socio-tech-economic system (STES) consequences. Secondary literature is suitable to describe the role of deterrence in national strategic choices to address the burdens and cost of these consequences. Ample academic treatises exists, except for active cyber defense itself, to provide the foundation for the comparison and weighing of deterrence implementation options, to include the strategic option of active cyber defense.

[454] James Miller and James Gosler, "Task Force on Cyber Deterrence," Defense Science Board, February 23, 2017: 1-36.

CHAPTER II

Global Cybered Conflict

An attack in cyberspace is defined as "any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself."[455] Malicious activity includes the theft or exploitation of data; disruption or denial of access or service; and destructive action including corruption, manipulation, alteration of data and damage to systems. The array of actors conducting malicious activity is vast and varied in their motivations. They usually desire to achieve some form of reputation, satisfaction, monetary gain, national pride or advantage. Their actual decision to act is based on meeting the actor's sense of legitimacy, need, and confidence related to the act itself.[456] Actors use malicious code to steal data, tarnish reputations, disrupt services, or sabotage systems. They operate with no discernible legal or ethical restraints.[457] The targets for their attacks are not just private companies, but also military installations, government offices, energy supply and transportation control facilities, financial and telecommunications systems, and other critical infrastructure nodes, i.e., the critical functions of a nation as a system.

Cyber attacks are increasing in scale and severity of impact, while the cyber networks, systems and services that support military, commercial and social activities remain vulnerable to theft, espionage, disruption and destruction. The Director of National Intelligence foresees an ongoing series of cyber attacks from a variety of sources "will impose cumulative costs on US

---

[455] National Institute of Standards and Technology, "Glossary of Key Information Security Terms," NISTIR 7298 Revision 2, May 2013: 11.

[456] Chris Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*, (University of Georgia Press, September 2011).

[457] Michael S. Rogers, Statement before the House Committee on Armed Services, March 4, 2015.

economic competitiveness and national security."[458] An Institute survey found in 2014 that the most costly attacks for large organizations in all industry sectors were by web-based attacks, denial of services, malicious insiders, and malicious code, to include Structured Query Language (SQL) injection. The average time to contain a cyber attack was 31 days, during which business disruption accounted for 38 percent of total external costs.[459] Another Industry survey of over 800 IT security decision makers and practitioners across North America and Europe, of those who knew or admitted to it, revealed 71 percent of their networks were breached in 2014, again a nearly 10 percent increase from the previous year. Phishing/spear-phishing, malware, and zero-day attacks were perceived as the greatest risk for responding organizations.[460]

The tactical imbalance of power impedes the fundamental premise of contemporary deterrence strategies, which is convincing the attacker that costs outweigh benefits. The Commander, US Cyber Command has admitted "despite your best efforts, you must prepare and assume that you will be penetrated."[461] This undeniable truth is a direct result of the gap between an organization's ability to defend itself and the adversaries' ability to circumvent those defenses.[462] The adversary has considerable resources and expertise at their disposal to conduct attacks, while victim organizations often have limited resources and budgets to launch an

---

[458] James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record for the Senate Armed Services Committee, February 26, 2015: 1-3.

[459] Ponemon Institute, "2014 Global Report on the Cost of Cyber Crime," Research Report, October 2014: 1-29.

[460] CyberEdge Group, "2015 Cyberthreat Defense Report: North America & Europe," March, 2015: 1-18.

[461] Robert Wall and Alexis Flynn, "NSA Chief Expects More Cyberattacks Like OPM Hack," *The Wall Street Journal*, July 15, 2015.

[462] Kevin Mandia, "Advanced Cyber Threats Facing Our Nation," Written Testimony before the Permanent Select Committee on Intelligence, U.S. House of Representatives, February 14, 2013: 1-3.

adequate defense. It is an unfair and asymmetric fight, because offense is easier and cheaper.[463] This chapter will present why cyber attacks matter to states if they happen and how bad it can get if defenders cannot deter malicious actors. It will start by examining the relative ease by which all levels of malicious actors' access information systems through various types of attack methods. These actors operate from distant locations without any real risks or repercussions. They can with impunity freely choose "the scale, proximity, and precision" of their attacks.[464] Using examples of actual cyber incidents, the chapter will delineate the wide range of malicious actors, and their methods and motivations in their campaigns of malicious activity. It will end on the need to deter malicious actors from causing significant consequences though cyber attacks on complex socio-technical-economic systems.

Attack Methods

The asymmetric nature of the cyber threat that undermines contemporary deterrence strategies demands an understanding of how exactly and easily a malicious actor can access equipment, computers or systems. Malicious actors use various methods, termed 'cyber attack vectors' by industry professionals, to access microprocessor controlled equipment, computers or systems in order to deliver a hostile payload or a malicious outcome. [465] The attack vector creates a path to exploit a software or code vulnerability that compromises the equipment, computer or system for the installation of malicious code, also known as malware. Malicious code is "software or firmware intended to perform an unauthorized process that will have

---

[463] Nick Woltman, "Cyber-Security Expert Kevin Mandia Addresses Local Business Leaders," Live Events, twincities.com, February 20, 2014.

[464] Peter Dombrowski and Chris Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review*, April 1, 2014: 83.

[465] Kevin G. Coleman, "The Cyber Commander's eHandbook: The Strategies and Tactics of Digital Conflict," version 4, Technolytics, 2013, 55-81.

adverse impact on the confidentiality, integrity, or availability of an information system."[466] Common forms of malware include worms (that spread freely), viruses (that activate upon execution), and Trojans (that allow remote control of the infected system). Ransomware is a type of malware that inflects computers and restricts user access to systems or data unless a ransom is paid.[467] Most malicious code attempts to evade detection, by various means such as the use of polymorphism to automatically change its code whenever it is downloaded, allowing the malware to escape traditional signature-based antivirus sensors.

The term vulnerability implies a weakness in a system or in a piece of software, commonly called a software "bug." Software exploits are used to take advantage of these flaws or misconfigurations in operating systems and applications. They can be found in exploit kits available for purchase on hacking forums, the most active in 2015 is entitled Angler. The average price for exploit kits is $800-$1500 a month.[468] The kits include software exploits for known vulnerabilities in end user technologies such as Internet Explorer, Adobe Flash and Oracle Java. Over 80 percent of the vulnerabilities in exploit kits were published in the past two years. The speed with which exploit kit developers deploy new exploits takes advantage of the gap in time between initial vulnerability disclosure and the implementation of software patches at an organization. [469] Yet vulnerability scanning data reveals that 21 percent of client vulnerabilities found in every industry sector are more than three years old, meaning the organization does not patch it and it is open for exploitation.[470] The exploit kit scans victim systems to find those open or zero-day vulnerabilities, identifies effective exploits for those vulnerabilities, exploits the target system vulnerability, and drops into the system the attacker's

---

[466] Computer Security Resource Center, Information Technology Laboratory, National Institute of Standards and Technology (NIST), Glossary: https://beta.csrc.nist.gov/Glossary/?term=5370

[467] United States Computer Emergency Readiness Team, "TA16-091A: Ransomware and Recent Variants," National Cyber Awareness System, March 31, 2016: 1-4.

[468] Websense, "2015 Threat Report," White Paper, Websense Security Labs, 2015: 5.

[469] Solutionary, "Global Threat Intelligence Report," 2015 NTT Group, 15-27.

[470] Solutionary, "Global Threat Intelligence Report," 2016 NTT Group, 13-14.

payload of malware.[471] Exploit kits continue to evolve at a much faster pace than the people defending and using the systems can respond.[472]

The most common attack vectors to exploit vulnerabilities and spread malicious code are 'spear phishing' by sending an email to a specific person in the hope they will run a malicious attachment or click a malicious link, or by so called 'drive by download' which occurs when visiting a compromised web page.[473] These personalized attacks are difficult to prevent because they capitalize on human behaviors[474] such as trust, compassion, or curiosity.[475] More so, human behavioral trends and advanced technique trends are the reason that if targeted by an advanced attacker, a breach is inevitable. The following sections will examine the most successful attack methods by which malicious actors deliver a hostile payload or harmful outcome.

Spear Phishing

Social Engineering. It is almost certain that in a 'spear phishing' campaign, some member of an organization will click upon a malicious attachment or link. The security firm FireEye-Mandiant analyzed over eight million results of sanctioned phishing tests in 2015 to find that 30 percent of phishing messages were opened by the target and about 12 percent went on to click on the attachment or link.[476] The reason is because phishing attacks have evolved from

---

[471] Websense, "The Seven Stages of Advanced Threats," White Paper, Websense Security Labs, 2013: 2.

[472] Nick Lewis, "Exploit kits evolved: How to defend against the latest attack toolkits," Tech Target, August 31, 2015.

[473] David Emm, "The Threat Landscape," Kaspersky Lab, 2013.

[474] Symantec, "Fraud Alert: Phishing – The Latest Tactics and Potential Business Impacts," White Paper, 2014: 1-8.

[475] Greg Otto, "Research looks at why phishing attacks are so hard to avoid," *FedScoop*, August 4, 2016: http://fedscoop.com/phishing-attacks-email-facebook-black-hat-2016

[476] Verizon, "2016 Data Breach Investigations Report," May 2016: 18.

mass emails with blatantly phony messages to lower volume and highly targeted emails that appear more legitimate. The spear phishing attack process usually starts by hackers gathering intelligence on targets from social networking websites; then they compromise a legitimate domain familiar to the target to gain access to a reputable email address; from which they send a socially engineered email to the target recipient. A large percentage of recipients act on the email by clicking on a malicious attachment or an embedded URL (web address) that links to a legitimate but compromised website that downloads exploits and malware.[477] Cyber criminals send messages that appear to come from a company's domain, leaving customers vulnerable to phishing attacks. For the healthcare, banking, and payments industry, malicious emails trick people into sharing sensitive information with hackers, leading to identity theft, while eroding customer trust.[478]

Spear phishing lures unsuspecting people to act or provide information via seemingly trustworthy electronic communications. In some cases victims are asked to input their login credentials and they comply on what are fake sites. Arguably one of most notable examples of phishing success is seen in the Operation Aurora attacks in 2010 on Google, Adobe and over 30 other U.S. corporations. Hackers used a high level of target profiling and social engineering to employ fake but personalized emails to trick employees and ultimately download malware which exploited a zero-day vulnerability (also not yet patched) in Internet Explorer.[479] Today's spear phishing attacks are more sophisticated in content, and even more effective. For instance, the technique was used to penetrate the unclassified networks of both the White House in 2014[480]

---

[477] Websense, "Defending against today's targeted phishing attacks," White Paper, 2012: 1-5.

[478] Agari, "The State of Email Trust 2014," White Paper, 2014: 1-8.

[479] Mathew J. Schwartz, "Leaked Cables Indicate Chinese Military Hackers Attacked U.S." *Information Week,* April 19, 2011.

[480] Evan Perez and Shimon Prokupecz, "How the U.S. thinks Russians hacked the White House, *CNN.com,* April 8, 2015.

and the U.S. Joint Staff in 2015.[481] Also today, the volume of attack attempts are astonishingly high, as the number of phishing emails reached 6.3 million in the first quarter of 2016, with 93 percent containing ransomware.[482]

Watering hole

Web-Based Attack. Watering hole attacks have advantages over spear phishing, such as the ability to bypass email filtering security technologies.[483] These web-based attacks occur when malicious actors infect a legitimate website with malware by SQL injection attack or some other means for the purpose of targeting visitors of that site. In a watering hole attack, the individual target does not need to be socially engineered into acting; instead all that is required is for a website of interest to a target group to be compromised and the attacker to wait like a predatory tiger for its prey. State sponsored hackers use watering hole attacks alongside other methods to compromise large groups within the same industry; like an attack on the IHS.com website which is the parent of Jane's Information Group and other sources of military, intelligence, or political analysis, by the Chinese state-sponsored group known as "FlowerLady." When users visited the compromised site, a PlugX file was downloaded onto the victim's machine and within 10 seconds this Remote Access Trojan received commands and sent data to an attacker controlled domain. Although users can be trained to detect spear phishing, there is no way for the user to recognize a compromised and legitimate popular website.[484]

---

[481] David Martin, "Russian hack almost brought the U.S. military to its knees," *CBS News,* December 15, 2016, with initial report by Craig Whitlock and Missy Ryan, "U.S. suspects Russia in hack of Pentagon computer network," *The Washington Post,* August 6, 2015.

[482] Chloe Green, "93% of phishing emails now contain ransomware," *Information Age*, security blog post, June 6, 2016.

[483] Brandan Blevins, "Spear phishing still popular, but more watering hole attacks coming," *Tech Target,* January 24, 2014.

[484] News, "Water Hole Replacing Spear-Phishing as State-Sponsored Weapon of Choice," infosecurity-magazine.com, July 17, 2013.

Exploits of zero-day vulnerabilities are occasionally deployed in watering hole attacks, such as the incident of a newly uncovered flaw in Internet Explorer served up through the U.S. Veterans of Foreign War's website.[485] In a similar incident, two zero-day vulnerabilities, this time in Adobe Flash and Internet Explorer, were leveraged in a watering hole attack on the Forbes website. The Chinese hacking group Codoso infected the 'Thought of the Day' widget with the intent to perform 'drive by download' attacks.[486] For days only certain visitors who clicked on the widget were redirected to another site where their computers could be infected with malware. The attack targeted only companies within the defense industry and financial services industries despite the broad audience of the Forbes site.[487] Although attackers must compromise a legitimate website in this attack vector, surprisingly scans of public websites have found that 16 percent are vulnerable enough to allow attackers to access and alter website content, signifying watering hole attacks are not going away.[488]

Point-of-Sale

RAM Scraping. Headlines of breaches at several large retailers through Point-of -Sale (POS) intrusions highlight the use of low cost malware available on criminal forums to achieve disproportionate financial gains. This vector begins with the compromise of a POS device (terminals where customers swipe a payment card at a checkout counter) that is open to the Internet and protected with weak or default passwords, by issuing likely credentials (called Brute

---

[485] Brandan Blevins, "FireEye finds active watering hole attack using IE zero-day exploit," *Tech Target,* February 14, 2014.

[486] Ericka Chickowski, "Chinese Hacking Group Codoso Team Uses Forbes.com As Watering Hole," *Dark Reading*, February 10, 2015.

[487] Andrea Peterson, "Forbes Web site was compromised by Chinese cyberespionage group, researchers say," *The Washington Post*, February 10, 2015.

[488] Symantec, "Internet Security Threat Report," Volume 19, April 2014: 34.

force) to access the device.[489] Or the vendor using the POS is compromised by an email or web attack lure. Then RAM (Remote Access Memory) scrapper malware is installed which captures payment card data while processed in memory before it is encrypted for storage or transmission. The data is written to a text file which is later sent to an offsite server.[490] This credit or debit card data is usually offered for sale on the Dark Web.[491] Often discovery of the payment card breach does not occur until the criminals are noticed to be using the data for fraud and other illicit purposes by law enforcement or fraud detection entities. Payment card track data is more valued in the criminal marketplace than just names, numbers, dates and codes because it can be used to manufacture counterfeit credit cards.[492]

In the POS breach at U.S. based retailer Target in late 2013 actors were able to steal data for as many as 70 million credit card and debit card accounts.[493] Within weeks of the breach, underground markets were flooded with stolen account information, selling in batches of one million cards and going from $20 to more than $100 per card.[494] The malware that infected POS devices was a hybrid of Kaptoxa and Reedum, both derived from the BlackPOS code sold on cybercrime forums. The BlackPOS malware is small in size, designed to bypass firewall software and costs only $2,300.[495] The malware continuously scanned the memory of infected devices for patterns that looked like payment card numbers and logged them to a file that was

---

[489] Verizon, "2014 Data Breach Investigations Report," June 2014: 16-18.

[490] Websense, "Point-of-Sale Malware and the Seven Stages Attack Model," White Paper, Websense Security Labs, 2014: 1.

[491] SurfWatch Labs, "Dark Web Situational Awareness Report," White Paper, 2015: 3.

[492] CrowdStrike, "Global Threat Intel Report," 2014: 15.

[493] Maggie McGrath, "Target Data Breach Spilled Info On As Many As 70 Million Customers," *Forbes*, January 10, 2014.

[494] Brian Krebs, "Cards Stolen in Target Breach Flood Underground Markets," krebsonsecurity.com, December 20, 2013.

[495] Brian Krebs, "A First Look at the Target Intrusion, Malware," krebsonsecurity.com, January 15, 2014.

transferred to an internal site at regular intervals until exfiltrated to external servers. In 2015 headline making remote payment card breaches shifted from large retailers to hotel chains.[496] Twenty hotels including Marriott, Hyatt, Le Meridien, Sheraton, Westin and the Intercontinental chains, reported payment card data hacks by POS malware from December 2015 to June 2016.[497] Although in early 2017, the fast food restaurant chain Arby's suffered a point-of-sale breach at up to 1,110 stores affecting 355,000 cards.[498]

Web Application

SQL Injection. Web application attacks typically target an organization's internet facing applications. A 2014 survey by the Ponemon Institute showed "42 percent of all data breaches are due, at least in part, to SQL injection."[499] This vector allows attackers to exploit a web application vulnerability in order to access or change data. This means they type computer code in the fields of a web form input box, instead of something like a last name or credit card number. The technique takes advantage of applications that do not correctly validate requests before passing them to back-end databases.[500] The SQL commands can dupe the database system into running code that outputs sensitive information, like intellectual property or customer accounts. The SQL code can also allow the attacker to steal the site's administrator password, manipulate data enabling for example the defacement of the website, or compromise the site to host malware for 'drive by download' by visitors. The risk of SQL injection is compounded by automated tools that detect and exploit Web application vulnerabilities, such as

---

[496] 2016 Data Breach Investigations Report, 31.

[497] Warwick Ashford, "PoS malware attacks highlights need for security standards in hotel industry," *Computer Weekly,* August 16, 2016.

[498] Doug Olenick, "Arby's hit with POS breach, 1,100 stores possibly affected," *SC Magazine,* February 9, 2017.

[499] Ponemon Institute, "The SQL Injection Threat Study," Research Report, April 2014:1.

[500] Michael Cobb, "How to prevent SQL injection attacks by validating user input," *Tech Target,* March 31, 2015.

the open source tool Sqlmap or the Iranian built tool Havij.[501] Comprehensive features make Havij stand out from other tools, such as capabilities to bypass security products, like Web Application Firewalls or Intrusion Detection Systems.[502]

The Ponemon Institute study in 2014 also revealed that 65 percent of the organizations surveyed experienced a SQL injection attack in the last 12 months.[503] Famous breaches by SQL injection include at Heartland Payment Systems, Sony, Nokia, and Adobe.[504] The Navy Marine Corps Intranet network, consisting of 800,000 users at 2,500 locations, was also deeply penetrated by SQL injection in 2013. Hackers entered through a Navy website available to the public and found their way to unprotected databases.[505] Even the NASDAQ Stock Exchange fell victim to an SQL injection in a global hacking operation. One hacker identified a vulnerability in a password-reminder page of the NASDAQ website, crafted a text string that injected SQL programming code and obtained encrypted login credentials.[506] While never penetrating the main servers supporting trading operations, the hacking ring eventually had enough information to perform network or systems administrator functions on the servers.[507]

---

[501] Imperva, "An Anatomy of a SQL Injection Attack," Hacker Intelligence Summary Report, Monthly Trend Report #4, September 2011: 1-4.

[502] Nick Lewis, "Defend against the SQL injection tool Havij, other SQL injection tools," *Tech Target*, March 31, 2015.

[503] Ponemon Institute, "The SQL Injection Threat Study," Research Report, April 2014:1.

[504] Kelley Jackson Higgins, "Adobe Hacker Says He Used SQL Injection To Grab Database of 150,000 User Accounts," *Dark Reading*, November 14, 2012.

[505] Siobhan Gorman, "Navy Hacking Blamed on Iran Tied to H-P Contract," *The Wall Street Journal*, March 6, 2014.

[506] Dan Goodwin, "NASDAQ is owned," Risk Assessment/Security & Hacktivism Blog, arstechnica.com, July 25, 2013.

[507] Nathaniel Popper, "Wall Street's Exposure to Hacking Laid Bare," *The New York Times*, July 25, 2013.

Distributed Denial of Service (DDoS)

DDoS Methods. Distributed Denial of Service attacks are popular because of access to high performance virtual machines, massive botnets, and service offerings. Assailants can perform the attacks with a high probability of success and a low probability of getting caught. DDoS attacks typically flood a target server with thousands of communication requests originating from multiple compromised machines known as a botnet. DDoS assaults serve a variety of purposes, such as to make social or political statements or take down or interrupt government or commercial sites in cybered conflict. DDoS attacks are also used as a part of multi-vector blended attacks or as a distraction mechanism. For example, during a large barrage on a victim's server, an attacker can conduct an SQL injection, hoping the noise covers the hack attempt.[508] Or in a hack on financial services institution accounts, a DDoS attack can flood the bank's network and keep the IT department busy while criminals transfer funds and cover their tracks.[509] For instance, in the Dyre Wolf malware campaign, a cybercrime gang based in Eastern Europe distracted banks with DDoS attacks that shut down websites to draw attention away from wire transfers to their offshore accounts.[510]

There are two types of DDoS attacks, either a network centric attack that uses up bandwidth or application layer attack which overloads a service.[511] In a volumetric attack targeting the network and transport layers,[512] large amounts of data packets and other traffic

---

[508] Stephen Lawton, "DDoS: Back in vogue," ebook: An SC Magazine publication, Sponsored by f5, 2015: 1-9.

[509] Rik Turner, "Tackling the DDoS Threat to Banking in 2014," Ovum, White Paper, January 27, 2014: 1-10.

[510] Maxim Tamarov, "Dyre malware returns to rob banks of millions," *Tech Target,* April 8, 2015.

[511] Margaret Rouse, "distributed denial-of-service attack (DDoS)," *Tech Target*, March 31, 2015.

[512] The Open Systems Interconnection model defines seven conceptual layers in a communications network.

consume all of the network and server's available resources. These attacks cause traffic congestion and service disruption for legitimate users trying to gain access. Volumetric attacks are getting larger, more sophisticated and lasting for longer durations. Many of the large scale DDoS attacks, of nearly 400 Gbps, use reflection and amplification techniques through the Network Time Protocol (NTP) or Domain Name System (DNS).[513] Another example of an attack at the network layer is "Slowloris" that slowly delivers request headers, forcing the web server to keep connections open, without ever completing the requests. Whereas in an application layer attack, a web application vulnerability or feature is exploited when attacks that mimic legitimate user traffic overwhelm a server or database powering the application.[514] An illustration of an application database attack is "Abuse of Functions" where blasting bad password requests locks out legitimate users because of a restricted number of failed logins.[515]

Malicious Actors and their Motivation

A complex, rising audience exists that needs to be deterred, ranging from non-state actors, such as Anonymous, to increasingly aggressive largescale state actors. As of late 2016, more than 30 nation states, many hostile to Western values, are developing offensive cyber attack capabilities. The rampant proliferation of cyber capabilities will allow standoff and remote operations, especially in the initial phases of military operations in conflict. Cyber attacks against information networks and critical infrastructure can bypass traditional defenses, disrupt command and control, and undermine political will. Most concerning are state adversaries with

---

[513] Brandan Blevins, "Vendor reports largest-ever NTP reflection-driven DDoS attack," *Tech Target*, May 13, 2015.

[514] Imperva, "The Top 10 DDoS Attack Trends," White Paper, 2015: 1-13.

[515] Securosis, "Defending Against Application Denial of Service Attacks," White Paper, Version 1.6, December 20, 2013: 1-12.

sophisticated capabilities that could be prone to conduct preemptive attack and rapid escalation.[516] Non-state actors will exploit advanced technologies for nefarious purposes. For example, hacker groups will use cyber operations to advance their political or social cause while criminal organizations will use persistent capabilities for theft or extortion. Furthermore terrorist groups will use Internet-based technology to incite fear and facilitate operations.

A plethora of cyber incidents reveal that malicious actors employ attack vectors in a systematic, coordinated fashion in an attempt to achieve their objectives. Criminal organizations and terrorist groups are mostly *bad actors* with average to good skills, while nation states and hacker groups, are considered to be *wicked actors* that have exquisite skills, high threat enduring motivations, and the ability to organize to create deep harm. The globally unfettered structure of the cyber substrate offers asymmetric advantages in the scale, proximity, and precision of actor attacks. Actors can scale their attack organization from five to 5,000 other internet users, can operate at any proximity to their targets from five to 5,000 miles away, and can target with any level of precision from one entity, five individuals, or entire systems in most cases.[517] A clandestine black market provides malicious actors with powerful and easy-to-use sets of tools and services for all manner of theft, exploitation, disruption and destruction, in some cases with little or no technical skills required.[518]

Malicious actors have in house attack capabilities or can contract with hackers for hire. An example of an illicit Web site that traffics tools and talent is Darkode, a sophisticated English language Internet forum. Darkode offers exploit kits, botnets, ransomware programs and zero

---

[516] The Honorable James R. Clapper, et al., “Foreign Cyber Threats to the United States,” Joint Statement for the Record to the Senate Armed Services Committee, 5 January 2017: 4.

[517] Chris C. Demchak, “Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI),” *Journal of Comparative Policy Analysis: Research and Practice*, July 12, 2012: 263-265.

[518] Cyveillance, “Intelligence for Security,” White Paper, January 2015: 4.

day attack tools.[519] Even though Darkode was shut down by the FBI, in less than two weeks the forum was rebuilt with new security measures.[520] Bulletproof hosting services (BPHS) shield these sorts of malicious sites that sell or trade malware, security exploits, and also stolen personal and financial data. BPHS protect malicious sites by appearing as a legitimate service provider to avoid suspicion and by residing in countries with lax law enforcement jurisdiction if exposed.[521] These illicit, inherent and intrinsic advantages allow actors to operate with little risk of repercussion. To better understand the challenges in influencing malicious actor decisions to benefit from these advantages, the following section will investigate their motivation for employing doctrine and capabilities in actual cyber incidents.

Nation States

North Korea. According to a report by HP Security Research, Leader Kim Jong Un has "referred to cyber warfare capabilities as a 'magic weapon' in conjunction with nuclear weapons and missiles."[522] He has poured resources into the next generation of the weapons of warfare - skills in hacking and computer science.[523] Consequently the South Korean Defense Ministry has reported that North Korea has a 6,000 member Cyber Army.[524] Several of the Cyber Army

---

[519] Ellen Nakashima, "Major computer hacking forum shut down by 20 countries, U.S. announces," *The Washington Post*, July 15, 2015.

[520] Michael Heller, "Darkode criminal forum reborn less than two weeks after DOJ shutdown," *Tech Target*, July 31, 2015.

[521] Olivia Eckerson, "New Report sheds light on the growing threat of bulletproof hosting services," *Tech Target*, August 5, 2015.

[522] Brian Krebs, "FBI: North Korea to Blame for Sony Hack," krebsonsecurity.com, December 19, 2014.

[523] Charlie Osborne, "A glimpse into the world of North Korea's hacking elite," zdnet.com, December 5, 2014.

[524] Associated Press, "South Korea: North Korea Has 6,000 Member Cyber Army," *ABC News*, January 6, 2015.

divisions have been ordered to secure critical data on weapons development from nuclear armed states, particularly in nuclear warhead miniaturization and ballistic missile technology.[525] One of the Units, 121, of the General Bureau of Reconnaissance is suspected in particular by U.S. investigators of being behind the attack on Sony Pictures and by South Korea for staging a series of disruptive attacks in Seoul.[526] For North Korea, cyber warfare is considered to be the modern chapter of asymmetrical warfare, intended to offset aging and declining conventional capabilities.[527] For instance in June 2016, North Korean hackers stole wing designs for the F-15, a U.S. fighter jet, from a South Korean company, in a campaign that exfiltrated more than 40,000 documents related to the defense industry.[528] Cyber warfare capabilities are an important asset for North Korea in "the face of its perceived enemies, the U.S. and South Korea" who are both "heavily dependent upon technological infrastructure for social, economic and political stability."[529]

North Korea's cyber activity appears to follow a distinct pattern, either around the time of U.S. – South Korean joint military exercises, correlated with a significant date, or in response to political events. For instance, following the UN emergency meeting condemning the North Korean underground nuclear test in May 2009 and subsequent South Korean joining of the

---

[525] Jenny Jun, Scott LaFoy, and Ethan Sohn, "What Do We Know About Past North Korean Cyber Attacks and Their Capabilities?" Korea Chair Platform, Center for Strategic & International Studies, December 12, 2014: 1.

[526] Jeyup S. Kwaak, "Sony Hack Shines Light on North Korea's Cyber Attackers," *The Wall Street Journal,* December 17, 2014.

[527] HP Security Research, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," HP Security Briefing Episode 16, August 2014.

[528] Jack Kim, "North Korea mounts long-running hack of South Korean computers, says Seoul," *Reuters,* June 13, 2016, plus Alastair Gale and Kwanwoo Jun, "North Korean Hackers Stole F-15 Wing Designs, Seoul Says," *The Wall Street Journal,* June 13, 2016.

[529] HP Security Research, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," HP Security Briefing Episode 16, August 2014.

Proliferation Security Initiative, called an act of war by the North, a wave of attacks struck South Korean and U.S. government entities, coinciding with the 4th of July, the U.S. Independence Day. The distributed denial of service (DDoS) attacks saturated target websites, like the White House, Defense Department and New York Stock Exchange in the United States and the presidential Blue House, Defense Ministry and National Assembly in South Korea, with access requests for several hours.[530] In March 2011, after U.S. testimony on undeclared North Korean uranium enrichment facilities, almost 30 South Korean media, financial, and critical infrastructure targets suffered a DDoS and disk-wiping malware attack.[531] Next, the third example of this pattern, occurred in March 2013, after U.S. and South Korea began their annual joint military exercise near the North Korean Peninsula, with cyber attacks upon the South Korean Shinhan Bank and NongHyup Bank, and television media outlets, YTN, MBC, and KBS. The organizations were crippled as data was lost and machines were unable to reboot.[532] The pattern continued at the start of similar military drills in March 2016, when South Korea's National Intelligence Service accused Pyongyang of attempting hacks into government websites and smartphones.[533]

The North Korean pattern of behavior indicates state sponsored cyber actors launch attacks in response to a political trigger perceived to be a threat to the regime. The nation's official political ideology of *juche,* which emphasizes maintaining self-reliance and displaying one's strength, provides context for the regime's motivations. *Juche* places "the survival of the regime as its primary goal, and any perceived threat to the regime may be targeted."[534] The regime fears losing control of the populace to outside cultural and political influence, as shown

---

[530] "Governments hit by cyber attack," *BBC News*, July 8, 2009.

[531] "South Korea hit by cyber attacks," *BBC News*, March 4, 2011.

[532] Kelley Jackson Higgins, "Loud Data-Annihilation Cyberattacks Hit South Korean Banks, Media Outlets," *Dark Reading*, March 20, 2013.

[533] Alastair Gale, "South Korea Accuses North of Hacking as Tensions Escalate," *The Wall Street Journal*, March 7, 2016.

[534] HP Security Research, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," HP Security Briefing Episode 16, August 2014.

in its reaction to the film “The Interview” that portrayed their leader as sadistic. A statement by a spokesman for the Ministry of Foreign Affairs called the comedy film “an act of war that we will never tolerate” and vowed “a decisive and merciless countermeasure” if “the United States administration tacitly approves or supports the release of this film.”[535] Obviously the attack upon Sony Pictures five months later should not have come as a surprise. The leaders of the North Korean regime appear committed to demonstrate the illusion of a powerful entity through destructive and coercive cyber attacks at no matter what cost of irresponsible behavior.[536]

Iran. Similar to North Korea, cyber doctrine in Iran relies heavily on asymmetrical warfare tactics. However in contrast to the use of military units by North Korea, Iran leverages hacker crews as a force multiplier to make up for the lack of military capability.[537] In light of Iran’s long track record of employing proxies for terrorist acts, it is not inconceivable that Iran would use proxy groups for cyber attacks against its adversaries.[538] Several pro-Iran hacker groups share common traits in they view Western entities and Israel as enemies, are heavily influenced by Islamic principles, make their exploits public, and associate with one another. The most renowned vigilante groups are the Iranian Cyber Army, the Islamic Cyber Resistance Group, and the Ashiyane Digital Security Team who has apparent ties to Iran’s premier Sharif University.

Iranian hacker crews are used in reaction to political events. For example in August 2012, when the European Union decided to boycott Iranian oil exports, the Iranian activist group

---

[535] Choe Sang-Hun, “North Korea Warns U.S. Over Film Mocking Its Leader: Kim Jong-un Declares ‘War’ on ‘The Interview,’” *The New York Times*, June 25, 2014.

[536] Sung Kim, “The North Korean Threat: Nuclear, Missiles and Cyber,” Testimony before the House Foreign Affairs Committee, Washington, DC, January 13, 2015.

[537] HP Security Research, “Islamic Republic of Iran,” HP Security Briefing Episode 11, February 2014.

[538] Frank J. Cilluffo, “The Iranian Cyber Threat to the United States,” Statement before the House of Representatives Committee on Homeland Security, April 26, 2012: 4.

Cutting Sword of Justice took credit for attacking Saudi Aramco Oil Company with the Shamoon malware. Analysts suspect Iran may have commissioned the attack to exert influence after the Kingdom's oil minister pledged to boost production to compensate for the sanctions.[539] Then in September, a hacker group called Izz ad-Din al-Qassam Cyber Fighters took credit for denial of service attacks on six major American banks. Al-Qassam announced the attacks on Pastebin, criticizing Israel and the United States and citing the film Innocence of Muslims that mocks the Prophet Muhammad as motivation for the attacks. The group's Operation Ababil caused Internet blackouts and delays in online banking.[540] Three months later, the group Parastoo, linked to an Iranian Special Forces unit, hacked the computer servers of the International Atomic Energy Agency involved in the contentious inspections of Iranian facilities. Parastoo then published stolen sensitive diagrams, satellite photos, and other documents to expose and discredit the Agency.[541]

Similar to North Korea's cyber strategy but different again from their use of military units, Iranian hacker crews are also being used to position the nation to impact critical infrastructure on a global scale. An advanced malware campaign named Operation Cleaver waged against an array of targets indicates Iranian motivations to extract sensitive materials and establish beachheads for sabotage. The name Cleaver is a string of code found several times in custom software used in the attacks. An Iranian team dubbed Tarh Andishan has compromised more than 50 victims in 16 countries in the operation. Networks and systems have been targeted in critical industries, like energy, utilities, airlines and transportation, and companies, such as aerospace and telecommunications. For attribution, an IP (Internet Protocol) address in Iran was found to be used by one of the primary attackers to conduct SQL injections, control backdoors,

---

[539] Kelly Jackson Higgins, "Shamoon, Saudi Aramco, And Targeted Destruction," *Dark Reading*, August 22, 2012.

[540] Nicole Perlroth, "Attacks on 6 Banks Frustrate Customers," *The New York Times*, September 30, 2012.

[541] Eli Lake, "Did Iran's Cyber-Army Hack into the IAEA's computers?" *The Daily Beast,* December 5, 2012.

and exfiltrate information. Also, domains used in the campaign were registered in Iran and the infrastructure was hosted by an Iranian provider.[542] The state-sponsored campaign's objectives may be to use sensitive data taken from critical infrastructure companies to damage control systems. As the only nation to actually suffer a catastrophic cyber attack, namely Stuxnet blamed on the U.S. and Israel, Iran may have the will to intentionally conduct this sort of cyber mayhem, or the capability to inadvertently do so as well.[543]

China. The Chinese government's engagement in cyber espionage for commercial advantage was exposed in May 2014, when the U.S. Justice Department charged five People's Liberation Army (PLA) officers with hacking into five U.S. companies to steal trade secrets.[544] This type of espionage under dispute threatens business interests in key industries, especially if the Chinese government provides state-owned enterprises with extracted information to improve their competitive edge, cut research and development timetables, and reduce cost.[545] The PLA officers in the indictment work for Unit 61398, also known as APT1 (an advanced persistent threat group), which has penetrated the networks of at least 141 organizations in 15 countries.[546] Another global campaign run by another APT group from China that appears to steal information beneficial to Chinese companies is named NetTraveler.[547] This group doesn't use zero-day attacks but instead exploits two well-known vulnerabilities in Microsoft Office. Their attacks start with spear phishing emails using attachments rigged with the Office exploits. Their malware infected more than 350 victims in 40 countries, allowing theft of more than 22 gigabytes of

---

[542] Stuart McClure, Operation Cleaver, Cylance Report, December 2014.

[543] Patrick Tucker, "Can Iran Turn Off Your Lights?" *Defense One*, December 9, 2014.

[544] United States District Court, Indictment, Criminal No. 14-118, Filed May 1, 2014: 1-48.

[545] Larry M. Wortzel, "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology," Testimony before the House of Representatives, July 9, 2013: 7.

[546] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 27, 2013.

[547] Kaspersky Global Research and Analysis Team, "The NetTraveler (aka Travnet)," 2013: 1-25.

data.[548] The domains of interest the group hunted were space exploration, nanotechnology, energy production, nuclear power, lasers, medicine and communications.[549] These sorts of attacks lead the Director of the U.S. Defense Intelligence Agency to warn that America's technological edge over China is at risk.[550]

Compared to espionage in peacetime, Chinese military doctrine in wartime calls for computer network operations to "disrupt and damage the networks" of an adversary's infrastructure facilities, such as power and telecommunications systems.[551] The finding of an intrusion in a honeypot resembling the industrial control system of a water plant in the United States, attributed to Unit 61398 in July 2013, indicates ongoing intelligence collection on critical infrastructure.[552] Chinese military analysts have also established that logistics and power projection are likely weak points in modern warfare.[553] The cases described by U.S. Senate investigators of China breaking into computer networks of private transportation companies working for the U.S. military appear to be an attempt to prepare the digital battlefield for a

---

548 Kelly Jackson Higgins, "NetTraveler Cyberespionage Campaign Uncovered," *Dark Reading*, June 4, 2013.

549 GReAT, Kaspersky Lab Expert, "NetTraveler is Running! Red Star APT Attacks Compromise High-Profile Victims," Securelist, June 4, 2013.

550 Associated Press, "Intel Chief Warns US Tech Threatened by China Cybertheft," *The New York Times*, February 3, 2015.

551 Larry M. Wortzel, "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology," Testimony before the House of Representatives, July 9, 2013: 4.

552 Larry M. Wortzel, "China's Military Modernization and Cyber Activities," *Strategic Studies Quarterly*, Vol. 8, Issue 1 (Spring 2014): 12.

553 United States, Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," May 2013: 33.

potential conflict.[554] Chinese intrusions into the networks of US defense contractors and industries threaten military operations, equipment and readiness. In May 2013, the Washington Post described a classified report by the Defense Science Board, which lists more than 24 US weapon systems accessed by Chinese intruders, to include the Aegis ballistic missile defense system, the F/A-18 tactical fighter jet, the V-22 Osprey vertical takeoff aircraft and the multi-mission Littoral Combat Ship.[555] After Chinese hackers infiltrated Lockheed Martin's network, it is no wonder the new Chinese J-31 jet aircraft strikingly resembles the low observable features of the F-35 Joint Strike Fighter under production by the United States and its allies.[556]

Ongoing cyber operations by China mirror "its leadership's priorities of economic growth, domestic political stability and military preparedness" according to the U.S. Director of National Intelligence.[557] Ensuring the obtainment of these priorities through cyber activity supports the expansion of comprehensive national power which perpetuates Chinese Communist Party rule.[558] Maintaining economic growth involves industrial cyber espionage of U.S. and other foreign targets; domestic stability occurs through information control and propaganda; and preparing for military scenarios consists of military modernization and computer network operations. The actions of Chinese hackers appear consistent with these efforts to increase

---

[554] Danny Yadron, "Chinese Hacked U.S. Military Contractors, Senate Panel Says Hackers Broke Into Computer Networks 20 Times in a Year," *The Wall Street Journal*, September 18, 2014.

[555] Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Companies," *Washington Post*, May 27, 2013.

[556] Paul McLeary and David Francis, "Pentagon Says It is Moving To Protect Its Cyber Flanks," Foreign Policy, The Cable Blog, April 9, 2015.

[557] James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record, House Permanent Select Committee on Intelligence, February 4, 2014: 2.

[558] United States, Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," April 2015: 21.

national power and prestige.[559] Likewise foreign policy and military developments in the past few years show that cyber operations are a high priority for the Chinese government. China's most recent Defense White Paper noted that cyberspace is a "new domain of national security and area of strategic competition."[560] Therefore in the foreseeable future, Chinese behavior in cyberspace may not change in intentions unless major shifts occur in regional politics or incentives change the calculus of risk.[561]

Russia. Although China is the object of U.S. allegations of cyber spying, the U.S. Director of National Intelligence said "I worry a lot more about the Russians."[562] This avowal is partly because of the Russian government's ability to covertly team with business and criminal entities to generate cyber capabilities that threaten perceived opponents. Clues of this nexus emerged in April 2007 in the DDoS attack on Estonia during riots over the movement of a Soviet World War II memorial from the city center and in Georgia in August 2008 during armed conflict with the Russian Federation over South Ossetia. The assault against the Web pages of Estonian government ministries, financial institutions, and media outlets came from a botnet associated with a Russian cybercrime group operating from St. Petersburg, with links to the Russian Business Network.[563] The command and control servers used to issue attack commands on Georgian websites, after Russian ground troops engaged Georgian forces, were registered

---

[559] James A. Lewis, "Economic warfare and cyberspace," *China's cyberpower: International and domestic priorities*, Austrian Strategic Policy Institute, Special Report, November 2014: 3-5.

[560] United States, Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," April 2016: 64.

[561] Amy Chang, "Warring State: China's Cybersecurity Strategy," Center for a New American Security, December 2014: 7-8.

[562] Danny Yadron and Siobhan Gorman, "Hacking Trail Leads to Russia, Experts Say," *The Wall Street Journal*, October 28, 2014.

[563] Binoy Kampmark, "Cyber Warfare Between Estonia and Russia," Contemporary Review, Autumn 2007: 288-293, and, Iftach Ian Amit, "Cyber [Crime/War]: Linking State Governed Cyber Warfare with Online Criminal Groups," *Security and Innovation* (2010): 4.

through a bulletproof hosting service provider in Russia and the domains were hosted by a business front for cybercrime activities.[564] In both of these incidents, Russian-language Internet forums posted instructions, malware and targets for patriotic hackers to participate in the campaign.[565] Although in the 2014 Crimea incursion, Russian did not use the same playbook. First off the Nashi youth organization that participated in attacks in both Estonia and Georgia is no more, and second regarding forums recruiting volunteers, many Russian hackers support an independent Ukraine.[566] Instead, Russia relied on the nationalist hacking group CyberBerkut to run a disinformation campaign to stir unrest.[567] Throughout 2015, in the continued state conflict, CyberBerkut conducted DDoS attacks against multiple German and Ukrainian government websites and nationalist Ukrainian rivals.[568]

Russian actors have engaged in challenging international norms in cyberspace.[569] In the area of intelligence collection, the government has benefited from a campaign by a group known as APT28, or Fancy Bear.[570] This group, unlike Chinese actors, does not appear to conduct intellectual property theft for economic gain, but collects information on defense and geopolitical

---

[564] Jeff Carr, "Russia/Georgia Cyber War – Findings and Analysis," Project Grey Goose: Phase I Report, October 17, 2008, and, Iftach Ian Amit, "Cyber [Crime/War]: Linking State Governed Cyber Warfare with Online Criminal Groups," *Security and Innovation* (2010): 5.

[565] Eneken Tikk, Kadri Kaska, and Liis Vihul, "International Cyber Incidents: Legal Considerations" (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2009), 14–32 and 66-76.

[566] Jeffrey Carr, "Rival hackers fighting proxy war over Crimea," *CNN Special*, March 25, 2104.

[567] CrowdStrike, "Global Threat Intel Report," 2014: 25-27, John Bumgarner, "A Cyber History of the Ukraine Conflict," *Dark Reading*, March 27, 2014, and, Doug Bernard, "Russia-Ukraine Crisis Could Trigger Cyber War," *Voice of America*, April 20, 2014.

[568] CrowdStrike, "Global Threat Intel Report," 2015: 24-29.

[569] Ash Carter, Secretary of Defense, "2017 Defense Posture Statement: Taking the Long View, Investing for the Future," February 2016: 17.

[570] CrowdStrike, "Global Threat Intel Report," 2014: 58-59.

issues. FireEye reported in 2014 that APT28 has been engaged in espionage against targets in the Caucasus, Eastern Europe, and European security organizations. It uses spear phishing to target its victims with emails that mention specific topics or lures relevant to recipients, written in local languages. The group also registers domains that mimic those of legitimate news, politics or other websites of topics relevant to particular targets, from which to down load malware and gain backdoor system access for reconnaissance, monitoring and theft. APT28 attempts to obfuscate code,[571] implement counter-analysis techniques and encrypt stolen information during exfiltration.[572] Researchers made a connection to the Russian government because the malware was written during working hours in Russia's major cities, on computers with Russian language settings, and for targets aligned with Russian interests.[573] Apparently Fancy Bear continues to seek information on political matters for Russian intelligence, since the malware obfuscation techniques discovered in the Democratic National Committee hack in April 2016 have been attributed to the group.[574] The APT28 exposure of Russia's cyber espionage operations is not the first, as another spear phishing campaign known as Red October was unveiled in 2012 targeting diplomatic entities mainly in Eastern Europe and Central Asia.[575]

Although discovery of cyber espionage is disturbing enough, Russia appears to be preparing for computer network attacks against Western critical infrastructure. At least one

---

[571] Reza Hedayat and Lorenzo Cavallaro, "The Devil's Right Hand: An investigation on malware-oriented obfuscation techniques," Royal Holloway, August 2016: 1-10.

[572] FireEye, "APT28: A Window into Russia's Cyber Espionage Operations," Special Report, 2014: 1-28.

[573] Nicole Perlroth, "Online Security Experts Link More Breaches to Russian Government," *The New York Times*, October 29, 2014: B3.

[574] Teri Robinson, "Guccifer 2.0 out – Cozy Bear, Fancy Bear hacked DNC, Fidelis analysis shows," SC Magazine, June 21, 2016: http://www.scmagazine.com/guccifer-20-out---cozy-bear-fancy-bear-hacked-dnc-fidelis-analysis-shows/printarticle/504441/

[575] Kelly Jackson Higgins, "Red October Attacks: The New Face of Cyberespionage," *Dark Reading*, January 14, 2013.

government sponsored APT group, named Energetic Bear, alternatively known as Dragonfly, has infected industrial control systems of energy related companies.[576] Dragonfly began targeting US and European energy gird operators, electricity generation firms, and petroleum pipeline operators in early 2013 with three infection tactics. The earliest method was by spear phishing emails to selected executives containing a malicious PDF attachment, then the watering hole compromise of energy industry and control system related websites, and finally the infection of legitimate software packages available for download by three different Industrial Control System equipment providers. Dragonfly uses both custom built and underground market available malware to access and control compromised computers.[577] The group has not only provided its state sponsor with persistent access for spying, but also with sabotage capabilities that could cause disruption to energy supplies in the event of cybered conflict.

United States. After revelation that the United States pierced the networks of the Chinese telecommunications company Huawei to conduct surveillance,[578] a Huawei senior executive in the United States said "The irony is that exactly what they are doing to us is what they have always charged that the Chinese are doing through us."[579] This assertion prompted President Obama to tell Chinese President Xi at a meeting in The Hague that the United States, unlike China, does not use its technological powers to steal corporate data and give the data to its own companies, instead, its spying is solely for national security priorities.[580] Three other discoveries

---

576 Khatuna Mshvidobadze, "Creeping bear: the growing cyber threat from Russia," *Jane's Defense Weekly*, 17 December 2014: 20.

577 Symantec, "Dragonfly: Cyberespionage Attacks Against Energy Suppliers," Security Response, July 7, 2014.

578 "Targeting Huawei: NSA Spied on Chinese Government and Networking Firm," *Spiegel Online,* March 22, 2014.

579 David E. Sanger, "N.S.A. Breached Chinese Servers Seen as Security Threat," *The New York Times*, March 22, 2014.

580 David E. Sanger, "U.S. Tries Candor to Assure China on Cyberattacks," *The New York Times*, April 7, 2014.

support this spying contention based on the alleged implication of the United States to the Stuxnet intrusion upon Iranian nuclear enrichment facilities.[581] The first is the data mining *Flame* virus that shares portions of its code with the Stuxnet malware, for instance, exploiting vulnerabilities in the same printing routine. Flame was found to have infiltrated thousands of computers in Iran and the adjacent areas in 2012. The virus copied keyboard entries, sifted through emails and text messages, captured screen shots, and recorded microphone sounds.[582] Although Iranian leaders claimed the massive data loss caused by Flame to be tantamount to an attack, in defense of United States position on allowable surveillance if guilty, Flame should only be considered an act of digital espionage, not defined or prohibited in international law.[583]

Circumstantial evidence also associates the United States with the Gauss virus found in 2012 on some 2,500 computers, largely in Lebanon.[584] A notable security firm said they were confident the Gauss virus was written by the same programmers who created Flame, by extension linked to Stuxnet, because of significant similarities in code and architecture, to include C++ computer language and encryption methods.[585] The Gauss virus, so-called because of this name in its code, acquired logins for email as well as instant messaging, social accounts, and financial transactions. In this case the targeting of banking customers was likely American cyber espionage against the Syrian regime and the Hezbollah organization.[586] The last revelation

---

[581] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *The New York Times*, June 1, 2012.

[582] Jared Newman, "The Flame Virus: Your FAQs Answered," *PC World*, May 30, 2012.

[583] Jason Koebler, "World Powers Play Blame Game with Flame Virus," *US News and World Report,* May 30, 2012.

[584] Mathew J. Schwartz, "Gauss Espionage Malware: 7 Key Facts," *Information Week,* August 10, 2012.

[585] Kaspersky Lab Global Research and Analysis Team, "Gauss: Abnormal Distribution," 2012: 1-10.

[586] Nichole Perlroth, "Virus Seeking Bank Data is Tied to Attack on Iran," *The New York Times*, August 9, 2012.

is the Duqu virus infiltration, which is named for files used by its key logger to store collected data such as DQx.tmp.[587] Duqu was detected in 2011 to be mining data from Hungarian and Iranian computers. Commonalities in the drivers suggest the Duqu and Stuxnet programs were created by the same platform and that early versions of Duqu gathered intelligence for the Stuxnet operation.[588]

Although deductive reasoning suggests that the four computer viruses which surfaced in the Middle East in three years were state-sponsored because they share a common architectural platform, it is possible the code was made available underground and repurposed or reused by other actors. That possibility is refuted by Kaspersky researchers in an analysis and comparison of code for advanced hacking tools stolen from the National Security Agency in August 2016,[589] to malware code used by the Equation Group that Ars Technica has attributed to both Stuxnet and Flame. The fact the code is functionally identical and shares specific traits demonstrates that Equation Group had clear connections to the National Security Agency.[590] The hard reality that the four cyber incidents are affiliated with the United States actually lends credence to the White House press secretary's declaration that U.S. "intelligence programs serve a specific national security mission."[591]

[587] Kenneth Rapoza, "Duqu Virus Likely Handiwork of Sophisticated Government, Kaspersky Lab Says," *Forbes*, October 21, 2011.

[588] Robert Lemos, "Four Takeaways from the Stuxnet-Duqu Connection," *Information Week Reports*, February 2012: 7.

[589] Ellen Nakashima, "Powerful NSA hacking tools have been revealed online," *The Washington Post*, August 16, 2016.

[590] Dan Goodwin, "Confirmed: hacking tool leak came from "omnipotent" NSA-tied group," Ars Technica, Risk Assessment, Blog Post, August 16, 2016.

[591] Ashley Frantz and Paul Armstrong, "Beijing denounces U.S. hacking charges against Chinese Army Officers," *CNN News*, May 20, 2014.

Hacker Groups

SEA. The Syrian Electronic Army (SEA) supports a state government in a nebulous arrangement. Based in Syria since 2011, with accomplices in Germany,[592] they have hacked and defaced over 40 sites to voice political sentiments in support of the Assad regime. They gain access to blogging or social media accounts and use that medium to spread propaganda. SEA tactics include setting up fake Facebook and YouTube sites to collect login credentials and compromising websites with the automated SQL Injection exploit tool Havij.[593] In one defacement, SEA sent phishing emails to employees containing a link to a website that mimicked a news agency's external email login page. After gaining compromised accounts, the SEA targeted email distribution lists to obtain credentials of users with access to the company's Content Management System, from which SEA could deface news articles. The SEA also gained access to a marketing email account to reset the agency's Twitter password and send unauthorized Tweets.[594] One of their most famous attacks was the takeover of the Associated Press Twitter account via phishing in April 2013 and subsequent Tweet of a message that a bomb exploded in the White House injuring President Obama which temporarily plunged the Dow.[595] One Syrian hacker claims the state pays the Syrian Electronic Army to work for them.[596]

For Hire. A clearer example of a hacker group for hire, but in this case for the theft of research information and military secrets, is the Appin Security Group in India. This group of

---

592 Graham Cluley, "Syrian Electronic Army hacker pleads guilty after sending victim scan of his passport," Tripwire, The State of Security Blog, September 29, 2016.

593 HP Security Research, "Syrian Electronic Army," HPSR Threat Intelligence Briefing Episode 3, April 2013: 1-29.

594 Mandiant, "M Trends: Beyond the Breach," Alexandria, Virginia, April 2014: 5-6.

595 Max Fisher, "Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?" *The Washington Post*, April 23, 2013.

596 Seamus Mirodan, "Online Pirate Army Fights for Downfall of Assad," *The Irish Times*, December 19, 2012.

talented hackers is suspected of targeting organizations in Pakistan, China, Norway and the United States.[597] The attackers leveraged already-patched vulnerabilities in products like Microsoft Word and Oracle's Java and did not use malware that employs techniques to evade detection, such as obfuscation or encryption, indicating they saw no need to implement advanced techniques because simple ways worked.[598] On the other hand, an APT group named Hidden Lynx is a professional team with more advanced capabilities that appears to offer the Chinese government a "hackers for hire" operation, since much of their attack infrastructure and tools originate in China. Since 2011, this APT has used primarily watering hole and spear phishing attacks to target hundreds of commercial and government organizations worldwide in concurrent campaigns. The most heavily sought industry has been financial services, particularly investment banks and asset management agencies to gain competitive information, and also the defense industry in pursuit of confidential information.[599]

Anonymous. This hacker group is a self-proclaimed Internet movement with a decentralized structure that "operates on ideas rather than directives."[600] Their collective motivation to express dissent over perceived injustices was first revealed in Operation Payback in 2010. When PayPal, Visa and MasterCard stopped processing payments to WikiLeaks, which publishes leaked documents on its website, Anonymous called the actions an affront to Internet freedom and retaliated with DDoS attacks.[601] Average citizens, mostly from the United States, participated in a campaign to disable corporate websites, after downloading over 40,000 copies

---

[597] Ali Raza, "Espionage-for-hire Operation Hangover Unveils New Indian Cyber Threats," Posted at hacksurfer.com on August 7, 2013.

[598] Dan Kaplan, "Espionage hacking campaign "Operation Hangover" originates in India," *SC Magazine*, News Section, May 20, 2013.

[599] Stephen Doherty,Jozsef Gegeny, Branko Spasojevic, and Jonell Baltazar, "Hidden Lynx – Professional Hackers for Hire," Version 1.0, Symantec, September 17, 2013.

[600] "ANON OPS: A Press Release," Blog Posting, Wired.com, December 10, 2010.

[601] Charlie Savage, "F.B.I. Warrants Into Service Attacks by WikiLeaks Supporters," The New York Times, January 27, 2011.

of software designed to flood websites.[602] However Anonymous organizers realized the volunteer pool was insufficient and engaged two botnet masters to use their private collections of 75,000 and 50,000 compromised computers to create more damaging effects.[603] The subsequent arrest of 14 individuals alleged to have participated in the attacks on PayPal's website brought a stern warning from FBI director Steve Chabinsky that "We want to send a message that chaos on the Internet is unacceptable."[604] In response, the global hacking collective stated "Your threats to arrest us are meaningless to us as you cannot arrest an idea."[605]

In a further affirmation of how hard it is to deter all actors and activities in cyberspace, Anonymous has claimed to have "NO leader" and that "nothing is official" but to be everywhere "helping to give voices to the voiceless."[606] With very few barriers to expression, an example of an Anonymous effort to influence an entity can be found in Operation Pharisee in 2011. The collective conducted a 25 day online assault upon the Vatican to disrupt a visit by Pope Benedict XVI to Madrid as part of World Youth Day 2011.[607] The attack started with skilled hackers conducting reconnaissance of the Vatican website, looking for Web application vulnerabilities with freely available tools, including the Iranian-built automated SQL injection scanner named Hajiv. When no vulnerabilities were found to exploit, Anonymous turned to laypeople to conduct

---

[602] Oren Dorell, "Hackers multiply attacks on popular websites," *USA Today*, December 10, 2010.

[603] Parmy Olson, *We are anonymous: Inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency*, (Back Bay Books: Reprint Edition May 14, 2013).

[604] Tom Gjelten, "FBI Tries To Send Message With Hacker Arrests," NPR, National Security Section, July 20, 2011.

[605] Zach Epstein, "Anonymous hackers to FBI: There is nothing you can do to stop us," BGR, July 21, 2011.

[606] "AnonNews – Everything Anonymous," IRC Radio, Blog Posting, Creative Commons, February 26, 2011.

[607] Mathew J. Schwartz, "Anonymous Leaves Clues in Failed Vatican Attack," *Dark Reading*, February 29, 2012.

DDoS attacks, either by downloading software or by going to custom built websites, even with mobile device browsers.[608] The targets of Anonymous protests have continued to diversify to include Israeli websites in 2013 after their airstrikes in Gaza[609] and Islamic State supporters after the 2015 terror attacks in Paris.[610] In 2016, the hacker group even took on Republican Presidential frontrunner Donald Trump for his stance on Muslim immigrants, exposing his personal information on Pastebin.[611]

Criminal Organizations

The merge in criminal tactics and tools with state sponsored or state hired APT groups complicates analysis of actor objectives when interpreting technical behavior for the purposes of deterrence. For instance according to one U.S. official, differentiating between Russian criminal hackers and government hackers is difficult because they use cyber surveillance tools created by each other. The U.S. still has not figured out whether criminals or government hackers infiltrated a classified military system in 2008 because both employ the same cyber tool used in the incident.[612] Tactical overlap between malicious actor types exists in the use of spear phishing and interactive social engineering, the contacting of victims through popular social network data,

---

608 Imperva, "The Anatomy of an Anonymous Attack," Imperva's Hacker Intelligence Summary Report, 2012: 1-16.

609 Isabel Kershner, "Israel Says It Repelled Most Attacks on Its Web Sites by Pro-Palestinian Hackers," *The New York Times*, April 7, 2013.

610 Swati Khandelwal, "#Paris Attacks – Anonymous declares War on ISIS: 'We will hunt you down'," The Hacker News, November 16, 2015.

611 Bradley Barth, "Anonymous escalates offensive against Trump, declares total war," *SC Magazine*, News Section, March 15, 2016 and Teri Robinson, "Donald Trump doxed by Anonymous group, SSN revealed," *SC Magazine*, News Section, March 17, 2016.

612 Danny Yadron and Siobhan Gorman, "Hacking Trail Leads to Russia, Experts Say," *The Wall Street Journal*, October 28, 2014.

in addition to the use of publicly available toolkits and the creation of custom built malware.[613] Also, both actor types have found the attacking of a primary target through a secondary or tertiary service provider is one of the easiest avenues of compromise,[614] adding further systemic complexity to efforts in deterrence. For example, Eastern European hackers that stole 40 million credit card numbers from the retail giant Target creatively used a third party to get into the Target Corporation network to install their malware. The breach begun with an email phishing attack sent to employees at a heating, ventilation and air conditioning firm that did business with the nationwide retailer. The criminals broke in and stole credentials Target had issued to the firm for electronic billing, contract submission and project management to eventually access the corporate network that housed the card payment system.[615]

Whether based in Russia, China, Africa, the United States or anywhere else on the globe, organized criminal syndicates, armed with innovative technologies and techniques, outwit stalwart cyber defenses. Criminals move fast to exploit flaws as evidenced in a data breach at Home Depot. Senior executives at the Hardware giant assembled a task force in the weeks after the data theft at Target Corporation to draw up a plan to avoid becoming a victim of a similar attack. Although by the time Home Depot signed a contract to install new technology to fully encrypt payment card data, hackers had already cracked their payment system.[616] In September 2014, the company announced that criminals had used custom-built malware to put payment card information at risk for approximately 56 million payment cards. The company also released

---

[613] Mandiant, "M Trends 2015: A View From the Front Lines," Alexandria, Virginia, June 2015; 20-22.

[614] Institute for Critical Infrastructure Technology, "Handing Over the Keys to the Castle," July 2015: 19.

[615] Brian Krebs, "Email Attack on Vendor Set up Breach at Target," krebsonsecurity.com, February 12, 2014.

[616] Danny Yadron and Shelly Banjo, "Home Depot Upped Defenses, But Hacker Moved Faster," *The Wall Street Journal*, September 12, 2014.

initial estimates for the cost of the breach in staffing and services at $62 million.[617] Turns out similar to the Target breach, the hackers used a vendor's stolen log-on credentials to penetrate Home Depot's computer network and install malware on self-checkout registers. The use of stolen credentials from third parties is a continuing trend that has expanded to use of credentials from compromised outsourced IT service providers. Criminals can leverage the elevated privileges of the IT administrators to move throughout the victim's networks undetected.[618] By starting an attack inside the network, criminals bypass perimeter cyber defenses. The financial barrier for criminals to conduct cyber attacks continues to drop as underground forums offer sophisticated hacking and malware packages, including security software checking services for malware detection, at low costs, making extra problems for deterrence.[619]

Terrorist Groups

The U.S. Director of National Intelligence has told Congress that cyber attacks from groups like Anonymous pose a greater threat than terrorism.[620] Politically motivated cyber attacks come from a range of actors, to include extremists, but in reality only one terrorist organization,[621] namely the Islamic State, has exploited the internet for campaign gains and

---

[617] Stephen Holmes and Diane Dayhoff, "The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in All U.S. Stores," The Home Depot, Atlanta, September 18, 2014.

[618] Mandiant, "M-Trends 2016," Special Report, February 2016: 24-27.

[619] Michael Winter, "Home Depot hackers used vendor log-on to steal data, e-mails," *USA Today*, November 7, 2014.

[620] Nicole Arce, "Cyber Attack Bigger Threat Than ISIS, Say U.S. Spy Chief," techtimes.com, February 27, 2015, and, "U.S. spy chief James Clapper highlights cyber threats," *BBC News,* February 27, 2015.

[621] Most violent extremist groups, like al-Qa'ida and their Khorasan Group operatives, are too consumed with plotting transnational attacks to develop disruptive cyber capabilities. See

conducted low-level cyber attacks to attract the attention of the media. The Islamic State declared in June 2014 the establishment of an "Islamic Caliphate," extending from "Aleppo to Diyala," while calling on all Muslims to pledge allegiance to the Islamic State and denunciating Western society.[622] The Islamic State uses cruel acts of terrorism to create hate propaganda. Videos of militants humiliating or killing captured soldiers posted on social-media websites intimidate opposition.[623] Near-real time footage of victorious militants hoisting their black flags and patrolling newly conquered towns vanquishes foes through fear.[624] While displays of battlefield actions and military parades on YouTube and Twitter draw new recruits and funding, as Facebook requests garner private donations.[625] Theatrically produced videos of beheadings or executions by the terror group are intended to incite horror, change policy, or demand ransom,[626] or even worst indoctrinate child soldiers, like one of five young boys shooting five Kurdish prisoners in 2016, all before the physical demise of the Caliphate from coalition victories.[627]

Vincent R. Stewart, Director of Defense Intelligence Agency, "Worldwide Threat Assessment," February 3, 2015: 21-24.

[622] Charlie Caris, "The Islamic State Announces Caliphate," Institute for the Study of War, Blogspot, June 2014.

[623] Michael R. Crittenden and Sam Dagher, "Obama Cools Talk of Strikes Against Islamic State in Iraq or Syria: Extremists Killed Nearly 500 This Week in One Syrian Province, Opposition Activists Say," *The Wall Street Journal,* August 28, 2014.

[624] Tim Arango, 'Sunni Extremists in Iraq Seize 3 Towns from Kurds and Threaten Major Dam,' *The New York Times,* August 3, 2014.

[625] Maria Ari-Habib, "Jihadists Step Up Recruitment," *The Wall Street Journal*, June 27, 2014.

[626] *Hussein Ibish, "*The ISIS Theater Of Cruelty," *The New York Times,* February 19, 2015 and Alan Cowell and Austin Ramzy, "Video posted threatening Japanese hostages: Tokyo ordered to pay ransom of $200 million to Islamic State militants," *International New York Times*, January 21, 2015: 1.

[627] Susanna Capelouto and Lonzo Cook, "ISIS video shows boys executing prisoners," *CNN News*, August 27, 2016.

The Islamic State initially established a "Cyber Caliphate," with the aim of using jihadist developed encryption software to mount catastrophic hacking attacks on America and the West.[628] In January 2015, sympathizers of the Islamic State took control of the U.S. Central Command Twitter accounts, changing the profile photo to a black-and-white image of a fighter wearing a Keffiyeh, or scarf and posting at the top of the page "CyberCaliphate" and "i love you isis."[629] The hackers also posted tweets with phone numbers of officers, unclassified military scenarios, and threats against military members. Using the Command YouTube account, hackers also posted two videos, of attacks on U.S. troops and of fighters wielding weapons. Although the Pentagon labeled this incident as little more "than a cyberprank," a senior congressman called the intrusion a cyberattack and "severely disturbing."[630] The terrorist affiliate's cyber capabilities appear rudimentary, as they might have simply guessed at weak account passwords, but continued recruitment of experienced hackers, like their British born founder since identified,[631] will eventually yield cyber-enabled means to inflict destruction on infrastructure.

Systemic Consequences

Admiral Michael Rogers, the commander of U.S. Cyber Command stated "we expect state and unaffiliated cyber actors to become bolder and seek more capable means to affect us and our allies."[632] The *Islamic State* terrorist organization aims to affirm that statement with

---

[628] Jamie Dettmer, "Digital jihad: ISIS, Al Qaeda seek a cyber caliphate to launch attacks on US," *Fox News*, September 14, 2014.

[629] Jose Pagliery, Jamie Crawford and Ashley Killough, "CENTCOM Twitter account hacked, suspended," *CNN News*, January 12, 2015.

[630] Julian E. Barnes and Danny Yadron, "U.S. Probes Hacking of Military Twitter Accounts by Pro-Islamic State Group," *The Wall Street Journal,* January 12, 2015.

[631] Marc Hosenball, "British hacker linked to attack on Pentagon Twitter feed: sources," *Reuters,* January 13, 2015.

[632] Michael S. Rogers, Statement before the House Committee on Armed Services, March 4, 2015.

video threats of an all-out cyber crusade against the United States and Europe. Rogers worries that cyber could give the terrorist group offensive capabilities to wage attacks, by using the Internet as "a vehicle to inflict pain against the United States and others."[633] Likewise, Rogers believes China, along with one or two other countries, already has cyber capabilities that could shut down the electric grid in parts of the United States.[634] These statements of potential malevolent cyber activity point to increasing risk to socio-technical-economic systems making deterrence both more crucial and harder than ever.

Leadership at the U.S. National Protection and Programs Directorate assert that "malicious actors, including those at nation-state level, are motivated by a variety of reasons that include espionage, political and ideological beliefs, and financial gain."[635] For the Russian group, APT28, their motivations appear to be expanding from just espionage, pertaining to defense and geopolitical issues that would be useful to a government, to financial gain, according to an industry report that uncovered plans by the threat group to attack international financial institutions. Most likely APT28 would use a spear-phishing campaign, their attack vector of choice, with well-crafted emails containing either a malicious file or web hyperlink to what recipients believe is an actual, but compromised, website.[636]

The seriousness of cyber attacks is rising, causing significant harm to security and damage to the economies of major Western nations. Official government assessments parallel

---

[633] Cory Bennett and Elise Viebeck, "ISIS preps for cyber war," *The Hill*, May 17, 2015 and Billy Mitchell, Senators consider splitting NSA/CyberCom director position," *Fedscoop,* April 5, 2016.

[634] Catherine Herridge, "NSA Director: China can damage US power grid," *Fox News,* November 20, 2014.

[635] Suzanne Spaulding and Phyllis Schneck, Written testimony for a House Security Hearing, February 25, 2015.

[636] Eduard Kovacs, "Russian Cyber Espionage Group Planning to Hit Banks: Report," *Tech Target*, May 13, 2015.

industry threat predictions about the looming security concerns. Small nation states, like North Korea or Iran, are conducting cybered conflict by launching crippling distributed denial of service attacks or using malware to wipe computer master boot records. Long-term players, like China or Russia, are already using better methods to remain hidden on victim's networks. Similarly, sophisticated cyber criminals, like those from Eastern Europe, are adopting an advanced persistent threat approach to collect personal intelligence, looking and acting more like nation-state cyber espionage actors.[637] Even more troubling, renowned security expert Eugene Kaspersky, has stated he is "really afraid some terrorist group will pay cyber criminals to develop and deploy [devastating] weapons on their behalf."[638] Finally politically motivated attacks will continue as hacker groups like Anonymous take advantage of showcase events on the world stage to promote their malevolent ideas.[639] The collective judgement is that attacks and campaigns will only grow in frequency and sophistication, as malicious actors develop and use new "cyber attack vectors" in multiple stage attacks[640] to exploit vulnerabilities all across the socio-technical-economic systems of defending nations to illegally or coercively obtain for political, economic or military advantages. Deterrence is preferable to kinetic war as the losses through cyberspace grow. The difficulty is that current theories and tools of deterrence are over challenged by the magnitude of the near term.

---

[637] Ryan Sherstobitoff, "Cyber Espionage," McAfee Labs Threats Report, November 2014: 6.

[638] Warwick Ashford, "Terror groups likely to be first to unleash cyber weapons, says Eugene Kaspersky," *Computer Weekly*, October 6, 2016.

[639] Mandiant, "M Trends: Beyond the Breach," Alexandria, Virginia, April 2014: 1-7.

[640] James Andrew Lewis, "Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage," Center for Strategic and International Studies, March 13, 2014: 1-8.

CHAPTER III

Theoretical Foundations and History of Deterrence

The concept of deterrence is often the cornerstone of national security strategy in dealing with powerful and emerging threats. The national security strategy itself can signal resolve and readiness to deter potential adversaries.[641] That includes the deterrence of adversaries as way to secure national interests.[642] This chapter explores how the theories of *strategy* and *deterrence* underpin the creation of contemporary strategic deterrence options or an alternative option most likely to influence the behavior of malicious actors in cyberspace. It starts by describing how great thinkers have theorized about the role of deterrence in national strategy. It then uses national strategic choices made in three historical periods to illustrate the role that deterrence plays with respect to strategies, as a subset, a backup, an element of one or another choice. Specifically, the chapter examines three distinct uses of deterrence as strategy tools to reduce conflict: the use of coercive diplomacy and preemption before World War II, escalation dominance and countervailing strategy during the Cold War, and superiority in cyberspace and other domains or functional models in an era of Rising Cyber Power. In each of the three historical periods, the chapter explores how theories of deterrence found in these periods apply or not in the formulation and implementation of strategic cyber deterrence options. Finally in recognition of the intrinsic complexity found in various socio-economic-technical systems, the chapter concludes with an explanation of why a comprehensive approach enhances organizational interaction for the deterrence of malicious actors in cyberspace.

---

[641] Executive Office of the President, *National Security Strategy*, (Washington, DC: The White House, February 2015): 1.

[642] U.S. Department of Defense, *The National Military Strategy*, (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, June 2015): 5-7.

Theories of Strategy and Deterrence

Strategy can be defined as the “direction and use made of means by chosen ways in order to achieve desired ends.”[643] Strategy is subordinate to the more inclusive subject of security and in turn security is regarded as a field of politics. Thus at the level of national strategy, the functional means consist of any and all among the vital assets of a designated security community used for the purposes of policy as decided by politics. Another more specific view of national strategy is the use of “political, economic, and psychological powers of a nation, together with its armed forces, during peace and war, to secure a nation’s objectives.”[644] Here the distinction between the theory and practice of strategy is both objective and subjective. In practice the strategist must always balance political ends with available means, arranged in appropriate ways. However strategy is complicated in its many aspects and causes and effects are intrinsically difficult to separate. Ends, ways, and means have to be unarguably different in meaning from each other as they are interdependent. Yet in principle, the simple relationship of ends, ways, and means in a Trinitarian formula serves as a proven construct for managing the complexity, confusion, and chaos of disordered behaviors and events.[645]

Strategy can also be thought of as the link between political aims and the use of force, or its threat. Therefore another suitable version of strategy is the pursuit of political aims by the use or possession of military means. This link between policy at the highest level and the use of military force as its tools is postulated by Clausewitz in his narrow definition of strategy merely as ‘the use of engagements for the object of war,’ where war is ‘an act of force to compel our enemy to do our will.’ His seminal writings reason that the aim in war is the imposition of one’s

[643] Colin S. Gray, *The Strategy Bridge: Theory for Practice,* (Oxford University Press, 2010): 18.
[644] Arthur F. Lykke, Jr. “Toward an Understanding of Military Strategy,” *Guide to Strategy,* (Carlisle Barracks: US Army War College, 1983), February 2001): 179-185.
[645] Colin S. Gray, “The Whole House of Strategy,” *Joint Force Quarterly*, Issue 71, 4th Quarter, 2013: 58-62.

will upon the enemy, and to see all strategy as the pursuit of that aim, while taking into consideration the interaction of one's own side with the enemy.[646] According to this reasoning, a succinct and normative application of the Trinitarian formula for describing strategy would be "the art of the dialectics of wills that use force to resolve their conflict."[647] For in various forms of conflict, the use or threat of force for the purposes of policy has to overcome, or at least diminish, resistance manifested by human will.[648] Political will is usually based on the advancement and survival of national interests. As a manifestation of political will, strategic deterrence options convince adversaries not to take actions that threaten national interests.

Deterrence can be defined as "to prevent from action by fear of consequences."[649] Deterrence aims to convince adversaries not to take actions that threaten "vital interests by means of decisive influence over their decision making."[650] Decisive influence is achieved by "credibly threatening to deny benefits and/ or impose costs while ensuring restraint by convincing the actor that restraint will result in an acceptable outcome."[651] For deterrence to alter behavior, it must instill a belief in an adversary that a threat of retaliation actually exists, the intended action cannot succeed, or the costs outweigh the benefits of acting. Therefore effective deterrence requires capability (possess the means to influence behavior), credibility (that proposed actions may actually be employed), and communication (sending the intended message

---

[646] Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present*, (Cambridge University Press, 2010): 1-17.

[647] Edward N. Luttwak, *Strategy: The Logic of War and Peace*, (Cambridge and London: The Belknap Press of Harvard University Press, 1987): 241.

[648] B.H. Liddell Hart, "The Theory of Strategy," *Military Strategy: Theory and Application*, (Carlisle Barracks: US Army War College, 1983), 3-22 to 3-23.

[649] Thomas Schelling, *Arms and Influence*, (New Haven and London: Yale University Press, 1966): 71.

[650] U.S. Department of Defense, *Deterrence Operations Joint Operating Concept*, Version 2.0, (Washington, DC: US Strategic Command, December 2006), 8.

[651] Ibid.

to the desired audience).[652] Prevailing capability must be coupled with appropriate credibility and communication. If a state has all the capability required to response, but lacks the will to launch a credible reprisal or the reputation that it would, deterrence fails. Even if a state has the capability and credibility (will and reputation) to respond effectively, it must communicate its position. For unless others receive the message clearly, they will not fully understand the probable repercussions of potential actions and deterrence will breakdown. Finally, if credible capability is obtained, but credibility erodes, a greater response may be required to reintroduce the belief in an adversary that malicious actions will not be tolerated by the state.[653] In this work, strategy is defined as "direction and use made of means by chosen ways in order to achieve desired ends,"[654] and deterrence is defined as "to prevent from action by fear of consequences,"[655] and relates to strategy as the use of "means of decisive influence over [adversary] decision-making."[656] Contemporary deterrence strategies involve ways to credibly threaten to impose costs (retaliation), to credibly threaten to deny benefits (denial) and to encourage adversary restraint (entanglement).[657]

The Role of Deterrence

The great thinkers of our time have theorized about the purpose and role of deterrence in national security strategy. Patrick Morgan accurately observed that deterrence has been the

---

[652] U.S. Department of Defense, *Joint Operations,* Joint Publication 3-0, (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 17 January 2017): xxii.

[653] Peter Roberts and Andrew Hardie, "The Validity of Deterrence in the Twenty-First Century," Royal United Services Institute, Occasional Paper, August 2015: 5-9.

[654] Colin S. Gray, *The Strategy Bridge: Theory for Practice,* (Oxford University Press, 2010): 18.

[655] Thomas Schelling, *Arms and Influence*, (New Haven and London: Yale University Press, 1966): 71.

[656] U.S. Department of Defense, *Deterrence Operations Joint Operating Concept*, Version 2.0, (Washington, DC: US Strategic Command, December 2006), 8.

[657] Ibid, 24-28.

focus of “one of the more elaborate attempts at rigorous theory in the social sciences.”[658] Thus deterrence theory, according to Robert Jervis, is “probably the most influential school of thought in the American study of international relations.”[659] Although Morgan offered that deterrence is “an old practice in international politics and other areas of behavior.”[660] Lawrence Freedman concurred that deterrence is concerned with “deliberate attempts to manipulate the behaviour of others through conditional threats.”[661] In line with this view, Morgan stated the essence of deterrence is that “one party prevents another from doing something the first party does not want by threatening to harm the other party seriously if it does.”[662] With the advent of nuclear weapons, Bernard Brodie staked out deterrence as the dominant concept of nuclear strategy. He realized “thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them.”[663] For Brodie, the imperative question was “how to regulate the new weapons so as to minimize both the chances of their use and the levels of devastation that would result if they were used,”[664] which conveyed the need for ways that threaten to impose costs for, and deny benefit of, an attack. In questioning whether forces would tend toward first-strike capabilities, Brodie stated that if “neither side can hope to eliminate the retaliatory power of the other,” then restraint “becomes prudence,”[665] which spoke to the need for a way to persuade an actor that restraint will result in an acceptable outcome.

---

[658] Patrick M. Morgan, *Deterrence: A Conceptual Analysis*, (Beverly Hills, CA: Sage Publications, 1977): 25.

[659] Robert Jervis, “Deterrence Theory Revisited,” *World Politics*, Vol. 31, No. 2, Princeton University Press, January 1979: 289.

[660] Patrick M. Morgan, *Deterrence Now*, (Cambridge University Press, 2003): 1.

[661] Lawrence Freedman, *Deterrence*, (Cambridge: Polity Press, 2004): 6.

[662] Patrick M. Morgan, *Deterrence Now*, (Cambridge University Press, 2003): 1.

[663] Bernard Brodie, *The Absolute Weapon* (New York, 1946): 76.

[664] David MacIsaac, “Voices from the Central Blue: The Air Power Theorists,” *Makers of Modern Strategy*, (Princeton University Press, 1986): 640.

[665] Bernard Brodie, “Unlimited Weapons and Limited War,” *The Reporter*, November 18, 1954: 18.

Patrick Morgan reiterated that considerable speculation exists about the utility of deterrence since the end of the Cold War. After all, the theory and strategy were "conceived with individual governments as targets, not a collective actor."[666] The United States or the West "now has to confront opponents not easily deterred," to include fanatical movements, terrorists and rogue states. Morgan pointed out the "fear is that these opponents will be difficult to understand, inclined to be uncompromising, likely to take high risks and pay a high price in pursuit of their goals."[667] Lawrence Freedman asserted that since the Cold War "involved a bipolar relationship [it] allowed for deductive theorizing."[668] For multiple audiences, the situation is not stark and simple. Nevertheless, Ned Lebow argued "the theory and practice of deterrence cannot be separated from the Cold War, and the ways in which deterrence was conceived and practiced by the superpowers."[669] He contended the "superpowers sought to intimidate the other" through exaggerated claims or demonstrations on strategic capability.[670] Lebow explained intimidation through threat-based strategies is risky since they can provoke instead of prevent behavior, because restraint will be interpreted as weakness. In looking at an equation for threat-based strategies, Lebow stated that theorists have emphasized the ability to inflict punishment and all but ignored the ability to absorb cost.[671] Freedman opined that first principles determine whether "deterrence as a strategic option can be rescued from its cold war use and abuse."[672] He stated that "deterrence is a coercive strategy," which involves "the purposive use of overt threats of

---

[666] Patrick M. Morgan, *Deterrence Now*, (Cambridge University Press, 2003): xviii.

[667] Ibid, xvii.

[668] Lawrence Freedman, *Deterrence*, (Cambridge: Polity Press, 2004): 47.

[669] Richard Ned Lebow, "Deterrence: Then and Now," *Journal of Strategic Studies*, Vol. 28, No. 5, October 2005: 766.

[670] Ibid, 766-767.

[671] Ibid, 770.

[672] Lawrence Freedman, *Deterrence*, (Cambridge: Polity Press, 2004): 26.

force to influence another's strategic choices."[673] Whereas a controlling strategy restricts choices, by defending territory and a consensual strategy adjusts choices, with another without force.

To prevent unacceptable action, Patrick Morgan stated that a government "may issue a threat to attack or impose some other punishment."[674] His precept frames the strategic option of deterrence by retaliation, where threats of harm are woven into foreign policy. Morgan pointed out that deterrence is "one aspect of what is called coercive diplomacy in which a government uses force or threats to get what is wants."[675] Lawrence Freedman went on to say deterrence "is a sub-set of the study of coercion, which can also include threats designed to compel action from others."[676] With deterrence the objective is inaction, primarily obtained through the threat of retaliation. Freedman states "deterrence becomes a matter of strategy when A makes a direct attempt to influence B's behavior through warning about the consequences of certain acts that B might be contemplating."[677] Although for that warning, Thomas Schelling noted that "one must threaten that he *will* act, not that he *may* act, if the threat fails."[678] To say one *may* act, leaves the opponent guessing whether one will punish or pass. Also to say one *may* act, gives the threatener a clear choice to act or abstain. However, Schelling argued "the final decision is not altogether under the threatener's control."[679] The uncertain element is aptly termed "the threat that leaves something to chance." Chance can be for example a product of an accident, false alarm, mechanical failure, somebody's panic, madness or mischief. Schelling further explained

---

[673] Ibid.

[674] Patrick M. Morgan, *International Security: Problems and Solutions*, (Washington, DC: CQ Press, 2006): 77.

[675] Ibid.

[676] Lawrence Freedman, "Deterrence: A Reply," *The Journal of Strategic Studies*, Vol. 28, No. 5, October 2005: 789-790.

[677] Ibid.

[678] Thomas Schelling, *The Strategy of Conflict*, (Cambridge: Harvard University Press, 1960): 187.

[679] Ibid, 188.

that the decision to respond might be made in a sequence of decisions, some deliberate along a "graduated series of trips wires, each attached to a chance mechanism, with the daily *probability* of detonation increased as the enemy moves from wire to wire."[680]

In line with using a threat of retaliation prior to an enemy's aggressive move to deter it, Glenn Snyder stated that essentially deterrence "means discouraging the enemy from taking military action by posing for him a prospect of cost and risk outweighing his prospective gain."[681] Snyder distinguished the role of deterrence in contrast to defense, which "means reducing our own prospective costs and risks in the event deterrence fails."[682] Therefore deterrence works on intentions, whereas defense reduces capability to damage, which includes the capability for denial. In this regard, the defense resists the enemy's onslaught in order to minimize losses. Patrick Morgan remarked that "putting up a strong defense" prevents someone from attacking you because the other side decides not to attack.[683] Hence the potential for denial of benefit from the attack influences a rational decision to attack, in effect enacting the strategic option of deterrence by denial. Yet Robert Jervis asked the difficult question of "how rational do men have to be for deterrence theory to apply?" and surprisingly answered "much less than total rationality is needed for the main lines of the theory to be valid."[684] Jervis went on to say "rationality may be neither necessary nor sufficient for deterrence" and explained while irrationality could produce emotional impulsiveness to launch an attack; it could also lead to passive acquiescence, where on the contrary, rationality could lead to belligerence.[685] In a situation where the attacker and defender are neatly separated, Paul Kecskemeti pointed out

[680] Ibid, 192.

[681] Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton University Press: 1961): 3.

[682] Ibid.

[683] Patrick M. Morgan, *International Security: Problems and Solutions*, (Washington, DC: CQ Press, 2006): 78.

[684] Robert Jervis, "Deterrence Theory Revisited," *World Politics*, Vol. 31, No. 2, Princeton University Press, January 1979: 299.

[685] Ibid.

"only the attacker, not the defender, can always settle for the status quo, thereby avoiding the risks and costs of attack by abstaining."[686]

Glenn Snyder also suggested "the broad scope of the concept of deterrence" is not limited to military factors given "its fundamental affinity to the idea of political power."[687] Joe Nye advanced this suggestion by identifying the political mechanism of entanglement and norms as means of dissuasion. Nye specified that entanglement refers to "the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim."[688] Since benefits exist in the status quo and its continuation, the contention is the potential adversary may not attack, because it also has something valuable to lose. Nye also asserted that entanglement by deterrence is sometimes called "self-deterrence," in reference to an argument by Robert Jervis that "because actors can perceive things that are not there, they can be deterred by figments of their imagination – self-deterrence if you will."[689] However in not dismissing the importance of the strategic option of deterrence by entanglement, Nye countered that "perceptions that costs will exceed benefits may be accurate, and self-restraint may result from rational calculations of interest."[690] Furthermore, according to Nye, "normative considerations can deter actions by imposing reputational costs that can damage an actor's soft power beyond the value gained from an attack."[691] Patrick Morgan appeared to concur in saying "if norms of behavior are internalized, then behavior is self-directed," however,

---

[686] Ibid, 297.

[687] Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton University Press: 1961): 11.

[688] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol.41, No. 3, Winter 2016/2017: 58.

[689] Robert Jervis, "Deterrence and Perception," *International Security*, Vol.7, No. 3, Winter 1982/1983: 14.

[690] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol.41, No. 3, Winter 2016/2017: 59.

[691] Ibid, 60.

he noted only when “*fear of the consequences* of violating certain norms” is internalized “is deterrence at work.”[692] Accordingly, Lawrence Freedman questioned whether “certain norms – such as non-aggression - can be upheld without forms of collective enforcement.”[693]

Robert Jervis affirmed that “in the most elemental sense, deterrence depends on perceptions” and therefore “unless statesmen understand the ways in which their opposite numbers see the world, their deterrence policies are likely to misfire.”[694] Jervis postulated that for deterrence to work, an actor has to be convinced “that the expected value of a certain action is outweighed by the expected punishment.”[695] That value, or risk, calculation resides ultimately in the “eye of the beholder” – that is, “of the party being – it is hoped – deterred.”[696] Therefore a key requirement for successful deterrence is viewing it “through the eyes of the adversary, and not one’s own, including removing a Western perception of rationality from the risk calculation.”[697] An adversary’s intentions are too often viewed by decision makers from perceptual biases and organizational interests, rather than credible signals.[698] Thomas Schelling said deterrence is “aimed at the rational calculator in full control of his faculties and his forces.”[699] Furthermore, “the operation of the deterrence principle,” according to Max Lerner,

---

692 Patrick M. Morgan, “Taking the Long View of Deterrence,” *The Journal of Strategic Studies*,” Vol. 28, No. 5, October 2005: 751-752.

693 Lawrence Freedman, *Deterrence*, (Cambridge: Polity Press, 2004): 69.

694 Robert Jervis, Deterrence and Perception, *International Security*, Vol.7, No. 3, Winter 1982/1983: 3.

695 Ibid, 4.

696 Michael Mandelbaum, “It’s the Deterrence, Stupid,” *The American Interest*, July 30, 2015.

697 Peter Roberts and Andrew Hardie, “The Validity of Deterrence in the Twenty-First Century,” Royal United Services Institute, Occasional Paper, August 2015: 26.

698 Keren Yarhi-Milo, “In the Eye of the Beholder,” *International Security*, Vol.38, No. 1, Summer 2013: 9.

699 Thomas Schelling, *Arms and Influence*, (New Haven and London: Yale University Press, 1966): 229.

"depends upon an almost flawless rationality on both sides."[700] Although an understanding of what is the "rational value-maximizing mode of behavior of adversaries"[701] requires perceptions of risk from "the eye of the beholder." A conception in line with the conclusion by Schelling that each opponent's "best choice of action depends on what he expects the other to do."[702] Therefore, according to Lawrence Freedman, deterrence can be a state of mind, where "in all cases it is about setting boundaries for actions and establishing the risks associated with the crossing of those boundaries."[703]

Deterrence in Pre-World War II Conditions of Conflict

The political uses of force for deterrence dominated the eras before WWII, and the means were as varied and pervasive as the relations of states. In principle, any instrument of military power that can inflict damage upon an adversary may also affect his conduct, even if force is never used. The necessary condition for this effect is that the parties concerned perceive that the capabilities will be or are actually deployed, thus allowing those capabilities to affect their decisions. In peacetime the most versatile and extensive means for a deterrent influence was by sea power. Inherent mobility, tactical flexibility, and wide geographic reach render sea power particularly useful as an instrument of foreign policy. Land based forces, either ground or air, can be used to encourage friends or coerce enemies, but with more constraints and risks. Naval forces, by virtue of their perceived capabilities, their role as a symbol of national power, and their manifestation of political will provide formidable military options.[704] In theory, "deterrence is a coercive strategy" that involves "the purposive use of overt threats of force to influence

---

[700] Max Lerner, *The Age of Overkill*, (New York: Simon and Schuster, 1962): 27.

[701] Thomas Schelling, *The Strategy of Conflict*, (Cambridge: Harvard University Press, 1960): 15.

[702] Ibid.

[703] Lawrence Freedman, *Deterrence*, (Cambridge: Polity Press, 2004): 116.

[704] Edward N. Luttwark, *The Political Uses of Sea Power*, (Baltimore and London, The John Hopkins University Press, 1974): v-34.

another's strategic choices."[705] In the absence of hostilities, such as before World War II in Europe and Latin America, the indirect threat or use of limited naval force by the United Kingdom, Italy, Germany and the United States served as a form of coercive diplomacy. At the onset of hostilities, such as before World War II in the Pacific, the use of naval forces by Japan served as a means of preemption, after a failure of deterrence by the opposing forces prompted the Japanese to act quickly in the belief they were about to be attacked anyway.

Coercive Diplomacy

The strategy of coercion "includes deterrent as well as compellent intentions."[706] The deterrent component prevents undesirable actions by instilling a fear of consequences into a targeted actor. Yet the deterrent threat only changes the consequences if the act in question is taken. Whereas the compellent component offers the actor positive reinforcement for taking actions he otherwise would not. Compellence usually involves initiating an action that can cease but only if the opponent responds.[707] The general intent of coercive diplomacy "is to back a demand on an adversary with a threat of punishment for noncompliance."[708] This strategy was seen more than a century ago in the form of gunboat diplomacy, considered to be the threat of or use of "limited naval force, otherwise than as an act of war, in order to secure advantage or avert loss, either in the furtherance of an international dispute or else against foreign nationals within the territory or the jurisdiction of their own state."[709] Gunboat diplomacy can be by definitive, purposeful, or expressive force, which varies in the use of deterrent or compellent elements.[710] An example of definitive force occurred in February 1940, months before Germany invaded

---

[705] Ibid.
[706] Thomas Schelling, *Arms and Influence*, (New Haven and London: Yale University Press, 1966): 71.
[707] Ibid, 69-72.
[708] Alexander L. George and William E. Simon, *The Limits of Coercive Diplomacy* (Boulder, CO: Westview, 1994): 2.
[709] James Cable, *Gunboat Diplomacy 1919-1991*, (London: Palgrave Macmillan, 1994): 14.
[710] Ibid, 15-64.

France, when the German naval auxiliary *Altmark*, suspected of carrying British prisoners, gained shelter in the territorial waters of neutral Norway. The *HMS Cossack* with five other combatants intercepted the auxiliary under escort by Norwegian torpedo boats. Captain Vian of the *Cossack* was under direct orders from Winston Churchill to liberate the prisoners and if fired upon, to defend himself using no more force than is necessary. He was also told to suggest to the Norwegians "that honor is served by submitting to superior force."[711] Upon informing the torpedo boat commander of his intent to proceed with or without consent, Captain Vian boarded the *Altmark* and steamed out of the fjord with 299 British subjects, after in effect issuing a deterrent threat to the Norwegians if they acted. For in a deterrent threat "the objective is often communicated by the very preparations that make the threat credible."[712]

Compellent threats "tend to communicate only the general direction of compliance."[713] An example of their use in purposeful force was the landing of Italian troops on the Greek island of Corfu in August 1923, after Italian demands for financial and symbolic reparations for the massacre of their Military Mission in Greek territory.[714] While "the distinction between deterrence and compellence is not necessary sharp," the "main difference is the time pressure" and usually compellence is "associated with ultimatums,"[715] as seen in British policy advances in Latin America through gunboat diplomacy. For example in Argentina in 1875, when under pressure from British bankers, railway and ship owners to safeguard property during civil unrest, the British sailed a gunboat up the River Parana to threaten the port of Rosario to force a reverse liquidation of a British bank.[716] Likewise the United States used gunboat diplomacy by

---

[711] Sir P. Vian, *Action This Day,* (London: Fredrick Muller, 1960), passim.

[712] Thomas Schelling, *Arms and Influence*, (New Haven and London: Yale University Press, 1966): 73.

[713] Ibid.

[714] J. Barros, *The Corfu Incident of 1923* (Princeton University Press, 1965).

[715] Lawrence Freedman, *Deterrence,* (Cambridge: Polity Press, 2004): 111.

[716] Andrew Graham-Yooll, *Imperial Skirmishes: War and Gunboat Diplomacy in Latin America*, (Olive Branch Press, 2002): 90-157.

purposeful force in Latin America in the years before World War II. For instance, the presence of 400 U.S. Marines embarked on the *USS Pennsylvania* persuaded Panama in 1921 to conform to a U.S. decision regarding her border dispute with Costa Rica.[717] The United States also employed warships for expressive force to emphasize attitudes or to lend credibility to unconvincing statements. For example in 1936 President Roosevelt arrived at Buenos Aires in Argentina in the Cruiser *Indianapolis* escorted by the *USS Chester* to attend the first session of the Inter-American Conference for the Maintenance of Peace amidst U.S. reluctance to accept Argentinian doctrine prohibiting interference in other countries.[718] Expressive force can be a key to diplomatic success, as proclaimed by American Diplomat George Kennan that "you have no idea how much it contributes to the general politeness and pleasantness of diplomacy when you have a quiet little force in the background."[719]

Preemption and Prevention

The failure of deterrence efforts can make the strategy of preemption an attractive choice. An enemy belief that "we are about to attack anyway, not after he does but possibly before, merely raises his incentive to do what we wanted to deter and to do it more quickly."[720] The enemy "may attack in order to reduce its losses, even if it loses more than it gains."[721]

---

[717] Council on Foreign Relations, *American Relations in the Caribbean* (Yale University Press, 1929): Chapter 5.

[718] *Franklin D. Roosevelt and Foreign Affairs*, volume III (Harvard University Press, 1969).

[719] Stephan M. Walt, "Which Works Best: Force or Diplomacy?" *Foreign Policy*, August 21, 2013.

[720] Thomas Schelling, *Arms and Influence*, (New Haven and London: Yale University Press, 1966): 75.

[721] Peter Roberts and Andrew Hardie, "The Validity of Deterrence in the Twenty-First Century," Royal United Services Institute, Occasional Paper, August 2015: 8.

Preemption is defined as the anticipatory use of force in the face of an imminent attack.[722] For centuries international law has "recognized that nations need not suffer an attack before they can lawfully take action to defend themselves against forces that present an imminent danger of attack."[723] Provided the action taken, "at a point in time when the opportunity arises to eliminate the threat," is in proportion to the threat, and avoids excessive force.[724] Usually at this point a decision for war has been taken by the aggressor. The strategy of prevention differs both in its timing and motivation. While the preemptor has no choice than to conduct a first strike in a rapid manner, the preventer choses to launch military action because of fears for the future should it fail to act now. Preventive action for choice takes the form of a raid, not an invasion and occupation. Both strategies are about self-defense. The main difference is that in prevention, the proposition exists that the preventer is able to detect and to anticipate a deadly menace, or at least predict an intolerable major negative power shift. To preempt is "to act on the basis of certain, absolutely contemporary knowledge," while in contrast, to prevent is "to bereft of temporal discipline."[725] The Japanese in the first half of the twentieth century enacted both precepts, first at Port Arthur and second at Pearl Harbor.

In 1904, Russia was confident that its great prestige would deter Japan from going to war. The Japanese strike on the Russian Pacific fleet stationed at Port Arthur on the Chinese coast initiated the two year Russo – Japanese War. The cause of war on the Asian mainland was a matter of prevention of an emerging threat to national security. Russian aggression to challenge Japan's vital interests in Korea and home islands threatened its national existence. The answer

---

[722] James B. Steinberg, Michael E. O'Hanlon and Susan E. Rice, "The New National Security Strategy and Preemption," Policy Brief #113, Brookings Institution, December 2002: 1-6.

[723] President George W. Bush, "The National Security Strategy of the United States of America," The White House, September 2002: 15.

[724] Harry S. Laver, "Preemption and the Evolution of America's Strategic Defense," *Parameters,* Summer 2005: 116.

[725] Colin S. Gray, *The Implications of Preemptive and Preventive War Doctrines: A Reconsideration* (Carlisle, PA: Strategic Studies Institute, July 2007): 1-60.

on how to engage this formidable foe was the strategy of preemption. Japan needed to preclude the Russian naval forces from interfering with the transfer of its army to the Korean peninsula. Although the damaged Russian ships at Port Arthur were repaired, the fleet would never successfully emerge.[726] Nevertheless, the war continued as the Russians committed additional resources to the fight. Russia's Second Fleet passed through the straits of Korea to engage the Japanese Navy near the island of Tsushima in May 1905. After two days of battle, the Japanese warships captured or destroyed thirty-one Russian ships.[727] Preemption at Port Arthur had contributed to success at Tsushima by ensuring a clash of equal numbers, and to the peace that followed, which gave Japan control over Korea and thereby security from invasion.

In 1941 the United States "sought to stop Japan without a war, but ended up provoking war."[728] The Japanese attack on the American fleet at Pearl Harbor resulted in the U.S. declaration of war against Japan.[729] The cause of the preemptive raid was the threatened economic destruction of Japan by the United States. American attempts to deter Japanese expansion into the Southwestern Pacific through deployment of the U.S. Fleet to Pearl Harbor, economic sanctions that deprived Japan of 80 percent of its oil requirements, and dispatch of B-17 bombers to the Philippines all failed due to Japanese pride. America insisted that Japan leave conquered Indochina and China as a condition for restoration of trade, essentially abandoning its empire and submitting to the economic domination of the United States.[730] Given the scope of

---

[726] Matthew J. Flynn, *First Strike: Preemptive War in Modern History*, (New York and Oxon: Routledge, 2008): 55-66.

[727] Ronald H. Spector, *At War, At Sea: Sailors and Naval Combat in the Twentieth Century*, (New York: Viking Penguin Publishers, 2001): 1-21.

[728] Jeffrey Record, *Japan's Decision for War in 1941: Some Enduring Lessons* (Carlisle, PA Strategic Studies Institute, 2009): 41.

[729] Ronald H. Spector, *Eagle against the Sun: The American War with Japan*, (New York: The Free Press, 1985): 1-8.

[730] Jeffrey Record, *Japan's Decision for War in 1941: Some Enduring Lessons* (Carlisle, PA Strategic Studies Institute, 2009): 1-70.

Japan's imperial ambitions and alliance with Nazi Germany, Japanese leaders in September 1941 believed that war was inevitable, and prepared to attack in advance.[731] The longer Japan took to start a preventive war with the United States, the less its chance of success, given the oil embargo and declining military power. Japan needed to seize the Dutch East Indies to obtain a substitute for American oil. The naval strike on Pearl Harbor was to be just a flanking raid, not an occupation, in support of the conquest of Malaya, Singapore, the Indies, and the Philippines. However, Japan knew it stood to lose more than it gained, signaled by a prediction by Admiral Yamamoto that "It is obvious that a Japanese-American war will become a protracted one."[732] Tokyo's grand strategy was to fight the United States to a stalemate in an island-by-island battle and extract a political settlement that would preserve imperial interests. The strategy of preemption was meant to just buy time to construct a defense zone for negotiations.[733]

Cyber Deterrence Implications

The strategy of coercive diplomacy employed in Europe and Latin America in the examples above depended on the threat of or use of limited force through deterrent as well as compellent intentions. Coercive diplomacy is a "political-diplomatic strategy that aims to influence an adversary's will or incentive structure."[734] The strategy shows determination so an adversary under pressure concludes it must make concessions. The key contrast with classical diplomacy is that coercion, although limited, is not merely a remote contingency. The prospects for "successful coercive diplomacy depend on the costs of noncompliance that can be imposed

---

[731] Louis Morton, The War in the Pacific, United States Army in World War II Series, (Washington, D.C: U.S. Government Printing Office, 1978): 92-93.

[732] Sadao Asada, *From Mahan to Pearl Harbor: The Imperial Japanese Navy and the United States*, (Annapolis, Maryland, Naval Institute Press, 2006): 277.

[733] Tomoyuki Ishizu and Raymond Callahan, "The Rising Sun Strikes: The Japanese Invasions," Chapter 3, *The Pacific War* (Oxford: Osprey Publishing Ltd, 2010): 47-61.

[734] Jack S. Levy, "Deterrence and Coercive Diplomacy: The Contributions of Alexander George," *Political Psychology*, Vol. 29, No. 4, 2008: 539.

on the target state."[735] Costs can be imposed by economic sanctions as well as by military force. Economic sanctions are an increasingly prominent tool of statecraft. They are the threat by a government to disrupt economic exchange with the target state, unless the target acquiesces to an articulated demand. If the target complies, the sanctions are not imposed.[736] Although emerging, cyber power has yet to exert anywhere near the same level of political influence of sea power. For unlike naval forces, cyber capabilities do yet not reflect a symbol of national power and the manifestation of political will. To both deter and coerce an adversary in the absence of hostilities, an additional instrument of power besides cyber, like economic sanctions, should be considered in any strategy of coercive diplomacy.

The strategy of preemption, for preventative reasons, as seen in the Japanese attacks on Port Arthur and on Pearl Harbor, is difficult to implement in the cyber realm. The use of preemption depends on detecting moves early and averting attacks by moving first, the equivalent of a first-strike. The challenge of situational awareness in cyberspace hinders the understanding of adversary origins and intentions. Therefore a preemption strategy in cyberspace is susceptible to misattribution and overreactions or miscalculations.[737] However, international law does allow any nation to defend itself from threats, and the United States has perhaps applied that concept to conduct preventive, and prepare for preemptive, cyber related actions, to control dangers in its external security environment. The Stuxnet worm attack on Iranian nuclear facilities to destroy uranium enrichment centrifuges, although never acknowledged by the United States, could be considered a preventive cyber attack to forestall a nuclear attack. Furthermore, the United States created a plan for a cyberattack on Iran in case diplomatic efforts to constrain its nuclear program failed and Iran struck back at the United

---

[735] Bruce Jentleson, "Coercive Diplomacy: Scope and Limits in the Contemporary World," Policy Analysis Brief, The Stanley Foundation, December 2006: 3.

[736] Daniel W. Drezner, "The Hidden Hand of Economic Coercion," *International Organization*, Cambridge University Press, vol. 57, Issue 03, 2003: 643-659.

[737] Robert A. Miller, Daniel T. Kuehl, and Irving Lachow, "Cyber War: Issues in Attack and Defense," *Joint Force Quarterly*, Issue 61, 2nd Quarter 2011: 18-23.

States and allies in the region. American personnel placed "electronic implants in Iranian computer networks to prepare the battlefield" for preemptive strikes on Iranian air defenses, communications systems and power grid.[738] A secret legal review of America's use of cyber weapons concluded that the President has "the broad power to order a preemptive strike if the United States detects credible evidence of a major digital attack looming from abroad."[739] The preemptive strike would attack adversary computer networks by injecting them with destructive code. Yet officials have not revealed what exactly that threshold would be in order to sustain ambiguity in an adversary's mind, inducing an element of deterrence, the threat of retaliation.

Cold War Choices

In January 1954, Secretary of State Dulles announced that the United States intended in the future to deter aggression by depending "primarily upon a capacity to retaliate, instantly, by means and at places of our choosing."[740] The policy became known as massive retaliation and was interpreted as a threat to devastate Soviet economic and political centers in response to any aggression, no matter how limited. Meanwhile the Soviet Union was mounting a substantial threat against America's Allies, and it was not to be long before the continental United States was at risk from Soviet aircraft. Thus the adoption of this concept made the United States more reliant on the deterrent effect of nuclear weapons, and ultimately its credibility would depend on taking nuclear risks on its allies' behalf. With the Soviet Union in the lead on the development of intercontinental ballistic missiles, U.S. analysts introduced the concepts of first and second strike, the ability to absorb a first strike and inflict a devastating retaliation. The requirement for the second strike force was to be survivable. The placement of intercontinental missile forces in

---

[738] David E. Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *The New York Times*, February 16, 2016.

[739] David E. Sanger and Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes," *The New York Times*, February 3, 2013.

[740] John Foster Dulles, "The Evolution of Foreign Policy," Department of State Bulletin, vol. 30, January 25, 1954.

reinforced-concrete underground silos and also on nuclear-powered submarines by both sides eventually resulted in a condition of stability based on invulnerable retaliatory forces.[741] Although a global stalemate for nuclear war was attained, a pressing problem the United States still faced was how to extend nuclear deterrence over far away allies in a technically credible manner.

Ultimately for the United States, national strategy is about the expansion of American interests and the security of the American people. Yet in the Cold War, the perceived need to protect the European periphery against the Soviet Union drove the design and execution of an American strategy of onshore containment. For this strategy the United States had ample geopolitical and economic resources to extend protection over allies and friends confronting Soviet land power. However, since both the Soviet and NATO governments regarded nuclear weapons as useable weapons of war, the United States was left with no choice but to assume nuclear weapons were instruments of policy capable of functioning as means in the Trinitarian formula. Therefore the United States elevated nuclear weapons to a dominant position in national strategy. This decision was consistent with the American way of war that called for maximum violence for quick results.[742] The American policy to use nuclear weapons in a strategy of Soviet containment remained firm throughout the nearly thirty years of the Cold War, however, the strategic concepts or ways for their use changed as advances were made and realized in the destructive potential of the weapons or means of the policy.

Escalation Dominance

The strategy of escalation outlines promised responses to deter adversaries. During the Cold War, escalation was the basic concept around which attempts to develop a credible nuclear

---

[741] Lawrence Freedman, “The First Two Generations of Nuclear Strategists,” *Makers of Modern Strategy*, (Princeton University Press, 1986): 735-778.

[742] Colin S. Gray, “Strategy in the Nuclear Age: The United States, 1945-1991,” *The Making of Strategy*, (Cambridge University Press, 1994): 579-613.

strategy evolved. A ladder of escalation conceptualizes how activities in a given scenario maintain dominance at any particular level of escalation. Clearly set guidelines at ladder rungs integrate reactions and deterrence with policy decisions. Although since crossing of the nuclear threshold would produce unpredictable results, the most useful escalation dominance would start at the conventional level in a concept of flexible response. In 1961, the American government began to posit that a major nuclear war might not, and need not, be a simple contest in destructive fury. Secretary of Defense McNamara gave a speech in June 1962 on the idea that deterrence might operate even in wartime, where belligerents might out of self-interest limit the destructive nature of nuclear war. Each might feel that the destruction of enemy people and cities, as called for in massive retaliation, would serve no decisive military purpose but that a continued threat to destroy them might serve a purpose. McNamara said the United States has come to the conclusion that in general war "the destruction of the enemy's military forces, not of his civilian population" would give the opponent the "strongest imaginable incentive to refrain from striking our own cities."[743]

Less than six months after McNamara's expression of this conclusion, President Kennedy solemnly stated that any nuclear missile launched from Cuba on the United States would require a full retaliatory response upon the Soviet Union.[744] Leading up to that point in time, the Soviet Union had faced a widening window of vulnerability with the buildup of American strategic nuclear forces. For the Soviets, reducing the threat of a U.S. first strike would take several years. However the Soviets did possess a surplus of shorter range missiles that could not reach the United States from Soviet bases but could if based in Cuba. Faced with few options, the Soviets decided to move existing weapons to Cuba from which they could reach American targets. The United States discovery of Soviet ballistic weapons in Cuba in October 1962 instigated the thirteen day Cuban missile crisis. After previous deterrent threats to the Soviet government that

---

[743] Secretary of Defense Robert McNamara, Commencement Address, University of Michigan, June 16, 1962.

[744] Albert and Roberta Wohlstetter, "Controlling the Risks in Cuba, Adelphi Papers, 17 (London, Institute for Strategic Studies, 1965).

offensive weapons in Cuba would not be tolerated, the United States made the choice to respond with a compellant threat, specifically a naval blockade, called quarantine, coupled with a demand for withdrawal of the missiles. This form of value-maximizing escalation ended the crisis, with the Soviet removal of the missiles.[745] Fortunately the crisis did not escalate across a threshold that had been previously accepted by both sides.

With an acceptance of the growing American position to not use an automatic nuclear response to conventional Soviet aggression, NATO adopted in 1967 the concept of flexible response. In this strategic concept, attempts would be made to respond to conventional aggression by the Soviets with conventional means. If that failed NATO would move to tactical nuclear weapons, and if necessary, the final recourse would be the U.S. strategic nuclear arsenal. This progression effectively adhered to use of an escalation latter.[746] NATO appeared to be aiming for escalation dominance by deliberate progression. In 1974, the concept of escalation dominance emerged again in an announcement by Secretary of Defense Schlesinger that a range of nuclear options would reduce dependence on threats of assured destruction. Schlesinger made clear it was neither feasible nor desirable to develop a true first strike capability but in major conflict nuclear weapons would impede enemy advance and warn against continued aggression.[747] In a scenario of assured destruction a condition of stability is balanced if neither opponent in acting first gains the advantage of obliterating the other's ability to lash back. This stalemate guarantees deterrence since no rational actor could dare to choose a course of action

---

745 Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, Second Edition (New York: Addison Wesley Longman, 1999): 1-142.

746 Roger L. L. Facer, "Conventional Forces and the NATO Strategy of Flexible Response," R-3209-FF, (Santa Monica: The Rand Corporation, January 1985): 1-18.

747 Lawrence Freedman, "The First Two Generations of Nuclear Strategists," *Makers of Modern Strategy*, (Princeton University Press, 1986): 766-775.

equivalent to national suicide. This deduction assumes rational behavior generated by a conscious calculation of advantages based on an explicit value system.[748]

Countervailing Strategy

The danger in a strategy of escalation lies in its predictability. If an aggressor knows the steps of the ladder, then they can test the rules and assess resolve to climb the ladder. In 1980, US President Carter unveiled a countervailing strategy, by signing Presidential Directive 59 that brought it into force. The strategy implied should the Soviet Union move up the escalation ladder, the United States would be able to respond effectively to exchanges at each level. PD-59 sought a nuclear force posture that guaranteed a “high degree of flexibility, enduring survivability, and adequate performance in the face of enemy actions.” The strategy emphasized that “if deterrence fails initially, we must be capable of fighting successfully so that the adversary would not achieve his war aims and would suffer costs that are unacceptable, or in any event greater than his gains, from having initiated an attack.”[749] To make this feasible, PD-59 described targeting categories appropriate to implement a countervailing strategy that put the weight of the initial response on military and control targets. The rapid planning targets described in PD-59 covered nuclear forces, command and control, stationary and mobile forces, and industrial facilities that support the military, while pre-planned strike options according to PD-59 remained for attacks on the political control system or general industrial capacity.

A key component of PD-59 was to “use high-tech intelligence to find nuclear weapons targets” on the battlefield, strike those targets, and then assess the damage.[750] A “look-shoot-

---

[748] Thomas Schelling, *The Strategy of Conflict*, (Cambridge: Harvard University Press, 1960): 4 and 232.

[749] President Jimmy Carter, “Nuclear Weapons Employment Policy,” Presidential Directive/NSC-59 (Declassified), July 25, 1980.

[750] William Burr, “Jimmy Carter’s Controversial Nuclear Targeting Directive PD-59 Declassified,” National Security Archive, September 14, 2012.

look" capability would allow the president and his advisers to improvise targeting during the war.[751] This flexible targeting system was supposed to provide an adequate deterrent, along with rigid pre-planned strategic options.[752] Drafters of PD-59 believed they could control escalation of a rational actor making rational choices during a nuclear war, but gave up "victory" as an aim. Likewise, Soviet leadership did not think neither side could win a nuclear war.[753] PD-59 sought to create the forces and codify the will to retaliate, but to actually deter, the Soviet leadership had to be convinced the Americans would do so. U.S. Defense Secretary Brown publicly discussed the major precepts of the countervailing strategy during the SALT arms control hearings in 1970 and at a NATO Nuclear Planning Group in early 1980. The policy of PD-59 was dubbed the countervailing strategy because its fundamental feature is the proposition that deterrence over the full range of nuclear contingencies requires the United States to have forces and plans for their use that convince the Soviets that no plausible outcome of aggression would represent victory.[754]

Nonetheless by 1985 Soviet debate reached a consensus that nuclear war is so farfetched and dangerous that it has become an instrument of policy only in theory, and thus an instrument of policy that cannot be used. That year Marshal Ogarkov, the Soviet Chief of the General Staff, published a revised description of the modern theater operation, in which military action is conducted without resorting to nuclear weapons. In his book, Ogarkov wrote of a new U.S. capability to wage a protracted conventional war through the concept of Air-Land Battle. This development inspired a new revolution in Soviet military affairs that involved changes in Soviet doctrine generated by emerging technologies. The Soviets saw the need for precision conventional means with the same ranges as those of nuclear weapons. By 1986 they were fielding long-range cruise missiles such as the SS-NX-24 to pose a non-nuclear threat to U.S.

---

[751] Ibid.

[752] Ibid.

[753] William Burr, "How to Fight a Nuclear War," *Foreign Policy*, September 14, 2012.

[754] Walter Slocombe, "The Countervailing Strategy," *International Security*, 5, No. 4, Spring 1981: 21-22.

and Eurasian airfields and nuclear weapons.[755] Meanwhile the United States pursed their so called revolution in military affairs, developing communications, precision weapons, and intelligence systems for increased reach and awareness for deep Air-Land Battle engagements.[756] These revolutions persisted on both sides through the end of the Cold War in 1991.

Cyber Deterrence Implications

Theories of deterrence provided the basis for the American strategy of containment of the Soviet Union in the Cold War. The United States extended deterrence through the threat of nuclear use on behalf of its allies, in insisting that an attack on the territory of NATO may invoke a U.S. nuclear retaliatory strike plus physical capabilities. The United States eventually developed an invulnerable retaliatory capability in its strategic triad of intercontinental ballistic missiles in hardened silos, submarine launched ballistic missiles, and dispersed strategic bombers. There was really no defense against nuclear weapons delivery by these platforms, either by ballistic missile defense or by air defense, although admittedly bombers were the most vulnerable part of the triad. And even if defenses were available and robust, the damage that could be inflicted by surviving missiles or bombers would be viewed as an unacceptable loss. Therefore the Cold War deterrence framework relied heavily on the threat of punishment by punitive destruction.[757] Here offensive retaliation is not only costly to the aggressor, but also makes a first strike unsuccessful in its objective. This results in a denial of victory, or more precisely the denial of success by the attacker in achievement of military and political objectives. Therefore, deterrence by denial, in contrast to deterrence by punishment, stresses the role of

---

[755] Mary C. FitzGerald, “Marshal Ogarkov and the new Revolution in Soviet Military Affairs,” Research Memorandum, Center for Naval Analyses, January 1987: 1-25.

[756] William A. Owens, “The Once and Future Revolution in Military Affairs,” *Joint Force Quarterly*, Summer 2002: 55-61.

[757] Schuyler Forester, “Theoretical Foundations: Deterrence in the Nuclear Age,” in *American Defense Policy*, Schuyler Foerster and Edward Wright, eds., 6th ed. (Baltimore, MD: Johns Hopkins University Press, 1990): 42-51.

defense to limit the damage the defender will suffer. Damage limitation enables survival, denies attacker success, and enables retaliatory strikes to terminate the conflict on the defender's terms.

After the Cold War ended, U.S. government officials exhibited continued confidence in the nuclear deterrence framework based on the assumption that unified national actors would make decisions regarding the use of nuclear weapons in a reasonable and predictable fashion. However for a wider variety of malicious actors, confident predictions about deterrence should be viewed with skepticism because of the human element in deterrence, where a leader must agree to be deterred. Desperate or determined leaders that are intent on their selected course can be obvious or resistant to the promises or threats of their foes. Even the rationality of an opponent's decision making does not guarantee they will be receptive to strategies of deterrence, including very severe threats. As noted earlier, the rational decision maker choses a course of action that is calculated to be most suitable for achieving their preferred goal based on available information. Rationality does not mean the decision maker's goals and values are considered to be reasonable by others. Therefore rational decision making can underpin behavior deemed by observers to be insensible, shocking or even criminal. For example, rational leaders with radical ideological views may pursue goals that are sensible to them, but through behavior that appears unreasonable to observers based on their own moral set of values and standards.[758]

The Cold War deterrence framework was developed and practiced based on a particular context, not only a limited number of rational national actors, but also their capacity to deliver nuclear weapons. To assume that nuclear deterrence must fit well enough the circumstances for other attempts to deter in the twenty-first century would be a gross and avoidable error.[759] Nuclear deterrence is about one specific and highly lethal type of physical weapon. The capability of the weapon to produce destructive effects is clear and demonstrated. Yet the

[758] Keith B. Payne and C. Dale Walton, "Deterrence in the Post-Cold War World," *Strategy in the Contemporary World*, (Oxford University Press, 2002), 170-173.

[759] Colin S. Gray, *Perspectives on Strategy*, (Oxford University Press, 2013): 116-152.

success of nuclear deterrence relies on the weapon itself, which by design restricts usage.[760] The use of the weapon would be a rare occurrence and attribution for any attack, at least by ballistic missile or strategic bomber, is most certainly assured. Therefore the theory of nuclear deterrence relies primarily on retaliation or punishment for use of this particular type of weapon, in the form of nuclear counter strikes. All other efforts today to create a deterrent effect center on denial of access, by restricting the proliferation of information and materials to produce the weapons, or on norms, in the form of international agreements that limit the purchase and use of nuclear technologies, or by active defense, entitled more succinctly as ballistic missile defense.

Prominent defense officials have summed up the prevailing view that "traditional Cold War deterrence models of assured retaliation do not apply to cyberspace."[761] Their reasoning stems primarily from the difficulty in obtaining timely and accurate attribution of actions in cyberspace. Especially since the complexities associated with cyber attacks are compounded by the use of compromised servers and uncooperative countries.[762] Without attribution that connects the action to an individual or state actor with confidence and verifiability, policy-makers are constrained in making decisions on offensive retaliation.[763] Also, unlike nuclear attacks that produce only destructive effect, cyber attacks are being used for disruption or espionage, which causes challenges for policy makers in determining whether the action rises to the level of an armed attack that justifies retaliation. In the Cold War, the possession of nuclear weapons meant it was possible to deter by threating horrific retaliation "without maintaining any

---

[760] Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly*, Number 77, 2nd Quarter 2015: 8-12.

[761] William J. Lynn III, "Defending a New Domain," *Foreign Affairs,* Vol. 89, No. 5, September–October 2010: 97–108.

[762] Kevin G. Coleman, "US Cyber Defenses Outmatched by Hackers," *Defense Systems*, August 2011: 2.

[763] Major General Maurice H. Forsyth, USAF, "Cyberspace Operations," Air Force Doctrine Document 3-12, July 15, 2010: 10.

serious defenses."[764] In the cyber era, threatening harm on the attacker can also "be inflicted by a stout defense," either by "frustrating the attack or making it too costly."[765] This form of denial, of benefit, convinces the "opponent to reject undertaking even a seriously prepared attack."[766] Therefore for cyberspace, effective deterrence rests not only upon ensuring the capability to respond to hostile acts, but also upon the security of networks and systems.[767]

Rising Cyber Power

Over the past four decades, through the advancement of information and communication technology, the Internet have evolved into a global medium for collaboration and interaction between computers and individuals. Through the physical and digital manifestation of this medium, cyberspace has become a primary conduit for transactions vital to every facet of modern life and security. While society has benefited from connectivity and interoperability, technological advancements in cyberspace have provided means for the U.S. military, its allies, and partner nations to sustain advantage over adversaries. Although unfettered access to cyberspace also provides malicious actors the avenue to compromise the integrity of critical infrastructure in direct or indirect ways. Most critical infrastructure that empowers national economies, like financial systems, the power grid, and health systems, runs on networks connected to the Internet. Concern resides over what a set of systematic cyber attacks might do. For example, in thinking of real-life examples, such as an air traffic control system going down and disrupting flights, or blackouts that plunge cities into darkness.[768] Therefore a paradox exists

---

[764] Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," *Proceedings of a Workshop on Deterring Cyberattacks*, (Washington, D.C.: The National Academies Press, 2010). 55-56.

[765] Ibid.

[766] Ibid.

[767] US Department of Defense, *Cyberspace Policy Report*, November, 2011:7.

[768] President Barak Obama, "Remarks at the Cybersecurity and Consumer Protection Summit," Stanford University, Palo Alto, California, February 13, 2015.

within cyberspace, as while technological advancements have enhanced the prosperity and security of nations, the same advancements have led to increased vulnerabilities and dependence on cyberspace, for both society and the military.

This paradox has contributed to the rise of cyber power, broadly defined as the ability to "exploit cyberspace to create advantages and influence events."[769] As applied for these outcomes, many definitions of cyber power "emphasize how cyberspace can be used to fulfil the ends of strategy."[770] Accordingly cyber power can be considered as the "process of converting information into strategic effect."[771] This view considers the instrumentality of cyber power but neglects to discuss the process of using that power in the face of a willful and determined adversary. A more explicit definition of cyber power is "the national ability to disrupt [the] obscured bad actor somewhere in the digital globe, whether nonstate or state, in proportion to its motivations/ capabilities to attack with violent effects and yet be resilient against exposed or enhanced nasty surprises across all critical nationally sustaining systems."[772] This definition recognizes that cyber power is employed as a strategic instrument against a malicious actor that is attempting to use cyberspace for their own ends. The obtainment of stated effects, through systemic resilience and disruption capacities, can be part of an overall national strategy. The attraction of cyber power as a strategic instrument lies in the ability for global reach with a certain degree of desired anonymity. This characteristic can be useful in peace, conflict or war.

---

[769] E. Lincoln Bonner III, "Cyber Power for 21st- Century Joint Warfare," *Joint Force Quarterly*, Number 74, 3rd Quarter 2014: 102-109.

[770] John B. Sheldon, "The Rise of Cyberpower," in *Strategy in the Contemporary World*, John Baylis, James J. Wirtz, and Colin S. Gray, editors, 5th Edition (Oxford University Press, 2016): 285.

[771] Ibid.

[772] Chris Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*, (University of Georgia Press, September 2011): x.

Just as a state actor can create strategic effects against globally distributed targets through cyber power, so can malicious actors outside a state's immediate jurisdiction, "exercise power against the wishes of a state with little or no chance of being traced or interdicted by the state."[773] The reduction in time and space through instantaneous interactions increases the number of malicious actors that were previously constrained by temporal or physical separations.[774] Thus the domain is "marked by power diffusion,"[775] where large countries will share the domain with new actors and have trouble controlling their borders in the domain. Those new actors are vast, diverse, sometimes anonymous, and operate with an advantage in the offense over the defense. States and other actors will attempt to exercise cyber power to obtain preferred outcomes either within cyberspace or in other domains outside cyberspace. Both will use hard power through coercion and payment or use soft power through agenda framing, attraction or persuasion.[776] Forms of hard power can include denial of service attacks and insertion of malware to steal data within cyberspace or cyber attacks on industrial control systems that physically reside outside cyberspace. Examples of soft power would be setting standards for the security of software used in cyberspace or an online propaganda campaign to influence citizens outside of cyberspace. The diffusion of power complicates the development of state strategy to counter non-state actors with new found capacity to exercise both hard and soft power in cyberspace.

Strategy brings together lines of effort to manage challenges in the strategic environment. A pervasive property of the environment is complexity, which rises when a state faces a greater number of threats, a more diverse set of security actors, and a more interdependent and

---

[773] David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, (Routledge, 2011): 39.

[774] Ibid.

[775] Joseph S. Nye, Jr. "Cyber Power," Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010: 3.

[776] Ibid, 4-7.

networked environment.[777] Decision makers face uncertainty in the identity and capabilities of the threats and actors operating in the environment. A number of strategic choices exist to respond to uncertainty, a byproduct of complexity. One of these choices is the proactive strategy of shaping, where the "expectations and behaviors of others can be shaped through the power of ideas or superior capabilities."[778] Shaping embraces a wide range of options, to include the use of cyber power, to alter the strategic environment so that serious challenges do not emerge. The concept of 'Shape' is referred to as Phase Zero of the notional six-phase model of joint and multinational operations described in U.S. joint doctrine. This doctrine presents military operations leading to "war" as a natural progression of activities, from shaping, deterring, seizing initiative, dominating, stabilizing to enabling civil authority. The intent of 'Deter' in Phase One is to deter undesirable actor activities by demonstrating capabilities and resolve.[779]

In the military context, cyber power "is equivalent to military power in the physical domains,"[780] which are air, land, maritime, and outer space. Cyber power is enacted through cyberspace operations, which employ cyberspace capabilities "to achieve objectives in or through cyberspace."[781] A cyberspace capability is "a device, computer program, or technique designed to create an effect in or through cyberspace."[782] Cyberspace operations are conducted and synchronized across the range of military operations. The concept of cyberspace superiority is achieved when the degree of dominance in cyberspace by one force "permits the secure,

---

[777] Chris Demchak, Complex Machines: Modernization in the U.S. Armed Services, (Ithaca, NY: Cornell University Press, 1991).

[778] Emily O. Goldman, *Power in Uncertain Times,* (Stanford University Press, 2011): 1-21.

[779] U.S. Department of Defense, *Joint Operation Planning,* US Joint Publication 5-0, (Washington, DC: The Joint Staff, August, 11 2011), III-38 through III-44.

[780] Ragnhild Siedler, "Hard Power in Cyberspace: CNA as a Political Means," in *Proceedings 8th International Conference on Cyber Conflict* (Tallinn, Estonia: CCD COE, June 2016): 24.

[781] U.S. Department of Defense, *Cyberspace Operations,* Joint Publication 3-12 (R), (Washington, DC: The Joint Staff, 5 February 2013): v.

[782] Ibid. I-6.

reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary."[783] As seen in recent incidents, cyberspace operations serve as a component of warfare. Militaries can use cyber operations to disrupt command and control, delay force deployments, sever logistic pipelines, degrade weapons performance and produce political or psychological effects. Most cyber attacks will not produce destructive effects similar to kinetic weapons, but can disrupt data and services, damage networks and computers, and maybe destroy machinery.[784]

Other Domain or Functional Models

Cyberspace is often described as a global commons. Likeminded nations have labeled the global commons as shared spaces – cyber, space, air and oceans - which exist outside exclusive sovereign jurisdictions.[785] Access to these shared spaces is at risk due to increased competition and provocative behaviors. Therefore the United States and its allies are promoting rules for responsible behavior in shared spaces while creating capabilities to assure access.[786] While the U.S. military has removed cyberspace as one of the global commons in their concepts of operation,[787] the analogy at the strategic level has proven useful for resolving issues nations face in regard to domain security, and for guiding regulatory frameworks, such as those

[783] U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms,* (Washington, DC: The Joint Staff, As of February 2017): 60.

[784] James A. Lewis, "Cyber War: Definitions, Deterrence and Foreign Policy," Statement before the House Committee on Foreign Affairs, September 30, 2015.

[785] Major General Mark A. Barret, USAF, et al., "Assured Access to the Global Commons," (Norfolk, VA: Supreme Allied Command Transformation, April 3, 2011): 5.

[786] Executive Office of the President, *The National Security Strategy,* (Washington, DC: The White House, February 2015): 12.

[787] Dan Shinego, "Defining the Term: Global Commons," News & Notes on Multi-Service Collaboration to Address A2/AD, Volume 2, Issue 1, October 2015: 1.

envisioned in the theory of entanglement.[788] Deterrence by entanglement is a way to entrench potential adversaries in a shared network they would not attack because of mutual interests and unintended consequences.[789] For example, an attack on the commercial satellite infrastructure in outer space that facilitates military communications would have huge consequences on the wealth of globalized economies. Besides economic entanglement, nations also share a degree of technological entanglement (and potential economic loss) in space, like in applications of Global Positioning Systems (GPS) data.[790] Mechanisms to promote responsible behavior in space, like confidence building measures, can be adapted for cyberspace, due to similarities in the unique characteristics of the domains, such as the difficulty in attribution of attacks.[791]

Warfighting concepts found in other domains suggest a new strategy for securing cyberspace resides in technical combinations of offensive and defensive operations occurring simultaneously and in concert.[792] An operational perspective for countering air and missile threats indicates the relationship between offensive and defensive systems.[793] To confront the tyranny of the offense dominated environment of air and missile threats, offensive counterair

---

[788] Julie J. C. H. Ryan, Daniel J. Ryan, and Eneken Tikk, "Cybersecurity Regulation: Using Analogies to Develop Frameworks for Regulation," 76-99.

[789] Schulyer Forester, "Strategies of Deterrence," in *Conflict and Cooperation in the Global Commons,* Scott Jasper, editor (Washington, DC: Georgetown University Press, 2012): 55-67.

[790] Roger Harrison, Collins G. Shackelford and Deron R. Jackson, "Space Deterrence: The Delicate Balance of Risk," *Space and Defense,* Volume Three, Number One, Eisenhower Center for Space and Defense Studies, Summer 2009: 1-22.

[791] Marc J. Berkowitz, "Shaping the Outer Space and Cyberspace Environments," in *Conflict and Cooperation in the Global Commons*, Scott Jasper, editor (Washington, DC: Georgetown University Press, 2012): 190-213.

[792] Kamal T. Jabbour and E. Paul Ratazzi, "Deterrence in Cyberspace," *Thinking About Deterrence*, (Maxwell Air Force Base, Alabama: Air University Press, December 2013): 37-50.

[793] Leon Sloss, "The Strategist's Perspective," in *Ballistic Missile Defense,* Ashton B. Carter and David N. Schwartz, editors (Washington, DC: The Brookings Institute, 1984): 24-48.

operations prevent the launch of threats, while defensive counterair operations use active and passive measures to defeat threats attempting to penetrate through friendly airspace. Active measures include defensive weapons in an integrated defense-in-depth system. Passive measures include deception, dispersion, reconstitution, detection and warning systems, and protective construction.[794] An example of a defensive weapon is the Patriot surface-to-air missile system, which uses a radar system and interceptor missile to detect and shoot down hostile aircraft and missiles. The concept definition can be adapted to the cyber domain, where active cyber defense is taken to be direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats, while passive cyber defense is about all other measures to minimize their effectiveness.[795] These definitions allow the examination of various active and passive measures to see how they act or interact, simultaneously or in concert, against hostile cyber threats.

Cyber Deterrence Implications

In an era of Rising Cyber Power, a tailored deterrence approach can serve as a vital part of a cyber security strategy designed to prevent and reduce adversarial intrusions. One such approach recommended by notable academics emphasizes raising costs of, and reducing benefits from, cyber attacks, to include use of economic sanctions, mandatory standards for protection and resilience, international agreements, and active defense.[796] The U.S. government's approach on its cyber security strategy focuses on four key elements. The first to improve defenses to manage risk more effectively; the second to improve the ability to disrupt, respond to, and

---

[794] U.S. Department of Defense, Countering Air and Missile Threats, Joint Publication 3-01, (Washington, DC: The Joint Staff, 23 March 2012), I-2 to I-5.

[795] Dorothy E. Denning and Bradley J. Strawser, "Active Cyber Defense: Applying Air Defense to the Cyber Domain," *Cyber Analogies*, Technical Report, Naval Postgraduate School, 2014: 64-75.

[796] Franklin D. Kramer and Melanie J. Teplinsky, "Cybersecurity and Tailored Deterrence," Atlantic Council, December 2013: 1-10.

recover from cyber attacks; the third to enhance international cooperation to hold bad actors accountable; and the fourth to make cyberspace intrinsically more secure by building more resilient networks.[797] Effective resilience measures can convince malicious actors of the futility of commencing cyber attacks on networks. Therefore the U.S. Defense Department has incorporated the necessity to strengthen the overall resilience of their systems in its new cyber strategy.

The U.S. Defense strategy adds resilience as a factor in effective deterrence. Resilience is deemed necessary to withstand a potential attack if it penetrates defenses. The Defense Department intends to invest in resilient systems so they may continue "operations in the face of disruptive or destructive cyberattacks."[798] The DOD realizes it cannot foster resilience in organizations that fall outside its authority. Therefore for resilience measures to "succeed as a factor in effective deterrence," other agencies must work with critical infrastructure and key resource owners to develop resilient systems.[799] The vast majority of large-scale socio-economic-technical systems from electrical grids to manufacturing supply chains have become vulnerable to nasty surprises in cyberspace. The increasing complexity of these systems challenges efforts to increase resilience. Complexity rises as "the number, differentiation, and interdependence" of elements and nodes rises.[800] Therefore if a "surprise can cascade over enough nodes," it becomes a systemic event.[801] The challenge in accommodating surprise is to gain sufficient knowledge of threats and vulnerabilities. A proven mechanism is necessary to self-organize disparate organizations in their efforts to generate resilience.

---

[797] Lisa O. Monaco, "Strengthening our Nation's Cyber Defenses," Remarks as Prepared for Delivery, The Wilson Center, Washington, D.C., February 10, 2015.

[798] U.S. Department of Defense, *The DoD Cyber Strategy*, April 17, 2015: 11.

[799] Ibid.

[800] Chris C. Demchak, "Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)," *Journal of Comparative Policy Analysis: Research and Practice*, July 12, 2012: 254-258.

[801] Ibid.

Comprehensive Approach Applications

The comprehensive approach is a proven mechanism for coordinating efforts to respond to security challenges. Absent a precise definition, the phrase "mobilizing the resources of an entire society to succeed in modern missions" encapsulates the meaning.[802] The model builds on a whole-of-government approach, to include the additional capabilities of allies and partners, non-governmental and private voluntary organizations, international organizations, and the private sector.[803] Intended to enhance organizational interaction, the comprehensive approach or whole-of-nation response is a way of thinking or a method, instead of a mechanical process.[804] Although reaching consensus on the objectives of the approach can be elusive, any discussion requires identifying the underlying apparatus of this approach, which is cooperation among actors when feasible, and integration of capabilities when possible. Although acknowledging the complexities and challenges, employing a comprehensive approach may lessen distrust and hesitancy among the participants, boosting the number of organizations willing to accept responsibilities in modern missions.

The fundamentals of a comprehensive approach include interdependence in political, security, economic, and social systems; cooperation by constant communication, dialogue and negotiation; prioritization of multiple competing demands; nesting of short-term objectives into longer term goals; flexibility in sequenced or phased actions; and measurements of progress in

---

[802] James G. Stavridis, "The Comprehensive Approach in Afghanistan," *PRISM*, 2 no. 2, March, 2011: 65-76.

[803] Stephan J. Hadley and William J. Perry, *The QDR in Perspective: Meeting America's National Security Needs in the 21st Century*, (Washington, DC: US Institute of Peace, July 29, 2010): 31-32.

[804] Kristina Rintakoski and Mikko Autti, *Trends, Challenges and Possibilities for Cooperation in Crisis Prevention and Management*, (Helsinki, Finland: Crisis Management Initiative, June 17, 2008), 1-34.

translating goals into outcomes.[805] Just as important as understanding the fundamentals are the unified principles for planning and conducting operations with all relevant actors in an increasingly complex environment.[806] The four unified principles of the approach identified by the United Nations are: first, a shared vision of strategic objectives, and second, congruence of purpose, through unity of effort by all parties, not of command by a single governing body.[807] In this context, congruence is defined as agreeing or coinciding as a state of compatibility. Third, some level of coordination with all relevant actors that enhance effectiveness. Fourth, successful use of the comprehensive approach requires mutual awareness and deliberate consideration of the charters, interests, limitations, and perspectives of stakeholders. With a comprehensive approach, organizations are tasked to do things they do best. Proper application could yield efficiencies in allocating resources and reducing duplication of effort. The principles are not a panacea for all problems seen in a multidimensional environment, but even modest gains in facilitating cooperative interaction justify the effort.

The comprehensive approach uses cooperative interaction to advance the common interests of organizations. To be useful in deterring cyber attacks, the approach needs to overcome a clash of self-interests that prevent cooperation, where one party tries to sustain economic or military advantage. For instance the private sector is reluctant to share cyber threat data with the government because it does not believe the latter can protect the confidentiality of an attacked company, which may devalue stocks or compromise proprietary information to the

---

[805] United States Institute of Peace, "Fundamentals of a Comprehensive Approach," in *Guiding Principles for Stabilization and Reconstruction*, (Washington, DC: United States Institute of Peace Press, 2009): 5-30 to 5-32.

[806] Scott Jasper and Scott Moreland, "A Comprehensive Approach to Multidimensional Operations," *Journal of International Peacekeeping*, Vol. 19, (2015): 191-210.

[807] Michael Hallet and Oke Thorngren, "Attempting a Comprehensive Approach Definition and Its Implications for Reconceptualizing Capability Development," Chapter 3, *Capability Development in Support of Comprehensive Approaches*, (National Defense University, December 2011): 35-50.

advantage of competitors, and protect personally identifiable information (PII) which might be found in stolen data.[808] A state might not agree to cooperative action if binding rules constrain their preferred method of competition in cyberspace. Critical to gaining consensus for the comprehensive approach is the multilateral characteristic of diffuse reciprocity, whereby parties recognize their self-interests will be satisfied over the long term. Examination of models and precedents in other domains could identify principles and mechanisms that foster greater cooperation and transparency. Winston Beauchamp, the deputy undersecretary of the Air Force for space touts how space operators have the "equivalent of maritime rules of the sea about encounters and how to deal with them."[809] Many of the provisions of the emerging International Code of Conduct for Outer Space Activities can be translated for cyberspace, such as to avoid harmful interference with outer space activities, to prevent outer space from becoming an arena of conflict, and to reinforce international norms for responsible behavior in outer space.[810]

The comprehensive approach does not apply only to operations by friendly entities, for example a hybrid threat can "avail themselves of a comprehensive range of methods and weapons to accomplish their objectives – a comprehensive approach to goal obtainment."[811] Therefore to rapidly adapt to new threats, the Chairman of the U.S. Joint Chiefs of Staff states that "success will increasingly depend on how well our military instrument can support the other instruments of power and enable our network of allies and partners."[812] His comment openly

---

[808] Larry Clinton, "Cyber Security Social Contract," in *Conflict and Cooperation in the Global Commons*, Scott Jasper, editor (Washington, DC: Georgetown University Press, 2012): 185-198.

[809] Amber Corrin, "How DoD is re-writing the rules of space," *C4ISR&Networks*, April 28, 2016.

[810] European Union, "International Code of Conduct for Outer Space Activities," Version 31, March 2014: 1-13.

[811] Michael Aaronson, et al, "NATO Countering the Hybrid Threat," *PRISM,* Vol 2, No 4, September 2011: 111-124.

[812] Marcus Weisgerber, "Dempsey's Final Instruction to the Pentagon: Prepare for a Long War," *Defense One*, July 1, 2015.

acknowledges the role of the military in a contribution to a comprehensive approach for security. The term for the military component is "full spectrum operations," explained in doctrine as the "range of operations forces conduct in war and military operations other than war."[813] For preparation and response to cyber attacks, the Joint Staff proclaims success is dependent upon unity of effort enabled by collaboration among partners, to include the private sector.[814] This claim is consistent with an affirmation by the NATO Enhanced Cyber Defense Policy that 'strong partnerships play a key role in addressing cyber threats and risks." [815] NATO consequently intends to engage actively on cyber issues with relevant partner nations and international organizations plus intensify cooperation with industry. Private sector expertise and innovations are seen as crucial by NATO to achieve the objectives of the Enhanced Cyber Defense Policy. One of these is the strategic deterrence of cyber attacks.

---

[813] Russell W. Glenn, "Thoughts on Hybrid Conflict," *Small Wars Journal*, March 2, 2009: 1-8.

[814] US Department of Defense, *Unity of Effort Framework Solution Guide*, (Suffolk, Virginia: US Joint Staff J-7, August 31, 2014) Foreword.

[815] North Atlantic Treaty Organization, "Wales Summit Declaration", Paragraph 72, September 5, 2014.

Section Two:

Contemporary Deterrence Strategies

CHAPTER IV

Deterrence by Retaliation

The strategy of deterrence by retaliation is based upon the credibility of a threat to impose overwhelming costs for hostile acts, including in cyberspace. Nations reserve the right to respond by all necessary means, often in kind, to an attack on their interests where they are able.[816] Since deterrence is partially a function of perception, the strategic option of retaliation works by convincing a potential adversary that it will suffer unacceptable costs if it acts in an undesirable manner.[817] Deterrence by retaliation seeks to change the cost-benefit calculations of a malicious actor by proving that a response by the victim to an attack will occur at or in a chosen time, manner, and place. This influence occurs through not only the clear articulation of declaratory policy to use all necessary means in response, but also the overt display of effective response capabilities. The threat of or use of all necessary means and the potential for harm deters an actor from carrying out a course of action to attack, but only if the costs are viewed to outweigh the benefits. Thus successful deterrence requires not only the capabilities to harm the malicious actor, but also the communication of will to launch a reprisal coupled with the credible reputation to actually do so. Furthermore, the initiator of retaliation must have the resolve to accept any harm or pain that may be caused by a reprisal act in response to the original deterrent act.[818]

Yet in today's threat environment, cyber attacks seriously challenge the strategic option of deterrence by retaliation. Senator John McCain stoutly claimed that "our adversaries view our

---

[816] Executive Office of the President, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011): 14.

[817] Ash Carter, Secretary of Defense, "The DoD Cyber Strategy," April 17, 2015: 10-11.

[818] Peter Roberts and Andrew Hardie, "The Validity of Deterrence in the Twenty-First Century," Royal United Services Institute, Occasional Paper, August 2015: 5-9.

response to malicious cyber activity as timid and ineffectual," since we have not proven that the "consequences of continued cyberattacks against us outweigh the benefit."[819] Not only has retaliation failed because of choses to apply it poorly, it is not suited for cyberspace and cannot be effective. To date few malicious actors responsible for significant cyber attacks on critical infrastructure have faced criminal justice. The five members of the Chinese Military indicted in May 2014 on charges of computer fraud, damaging a computer, and aggravated identify theft are "no closer to seeing the inside of a federal courtroom" while "China's campaign of economic espionage against U.S. firms continues."[820] U.S. authorities did file charges ranging from securities fraud to money laundering on criminals in cases bearing some link to the massive cyber-attack on JP Morgan Chase Bank in 2014.[821] Yet it took eighteen months before prosecutors publicly and directly linked the suspects to the hack.[822] When asked do we need to go on the offensive in ways that we have not before, Admiral Michael Rogers, the head of the National Security Agency, responded "I think clearly we have got to change the current dynamic. To date, most nation states, most groups, most individuals, have come to the conclusion that there is little price to pay for the actions they're taken."[823] Uttering that the U.S. is at a tipping point, Admiral Rogers openly inquires, "how can we increase our capacity on the offensive side here to get to that point of deterrence."

---

[819] Greg Otto, "Clapper not optimistic on China cyber deal," *Fedscoop,* September 29, 2015.

[820] Elias Groll, "The U.S. Hoped Indicting 5 Chinese Hackers Would Deter Beijing's Cyberwarriors. It Hasn't Worked," *Foreign Policy,* September 2, 2015: 1-12.

[821] Joab Jackson, "5 arrested in JP Morgan hacking case," *Computer World,* July 22, 2015.

[822] Nicole Hong, "Charges Announced in J.P. Morgan Hacking Case," *Morningstar*, November 10, 2015.

[823] Dennis K. Berman, "Adm. Michael Rogers on the Prospect of a Digital Pearl Harbor," *The Wall Street Journal*, October 26, 2015.

Lawmakers in the United States have voiced frustration with the lack of an effective deterrent strategy for cyber attacks.[824] U.S. Deputy Secretary of Defense Robert Work told a congressional committee that a key objective of his Department's cyber strategy "is to develop cyber options to hold an aggressor at risk in cyberspace if required." Although Secretary Work admitted, that "in many instances non-cyber capabilities may provide a more appropriate or effective response."[825] Therefore the range of means to directly impose costs for hostile acts in cyberspace span military cyber operations, diplomatic engagements, law enforcement measures, economic sanctions, and even the use of kinetic capabilities. These means are reviewed for what is necessary to change an actor's perception. Or simply which means will work best to convince a malicious actor, whether from a nation state, hacker group, criminal organization or terrorist group, that the costs of conducting an attack outweigh any potential benefits. This chapter starts with an illustrative case that depicts an example of a justified and proportionate response by the United States government to a destructive and vindictive cyber attack by a nation state. It then examines the circumstances and concerns for employing the range of necessary means and to what extent will the threat of or use of them, often in kind, achieve deterrence by retaliation in response to hostile acts in cyberspace.

Illustrative Case of Muted Response

Deterrence by retaliation fails in principle in cybered conflict. The 2014 threat landscape saw an increasing frequency of cyber attacks, underscored by theft of data at retailers such as Target Corp., hardware store Home Depot Inc., luxury goods Neiman Marcus Group, craft chain Michaels Cos., and grocer Supervalu Inc,[826] and at banks like JP Morgan Chase. The most

---

[824] Joe Gould, "Constructing a Cyber Superpower," Focus US Cyber Command, *Defense News*, June 29, 2015.

[825] Robert O. Work, Deputy Secretary of Defense, "Cybersecurity Risks to DoD Networks and Infrastructure," Statement before the Senate Armed Services Committee, September 29, 2015.

[826] Rachel Feintzeig, Clint Boulton and Joann S. Lublin, "Fears Spread of Sony-Style Hack," *The Wall Street Journal*, December 7, 2014.

sensational act was the destructive and coercive cyber attack on Sony Pictures Entertainment. The attack was “a game changer because it wasn’t about profit,” but “a dictator trying to impose censorship and prevent the exercise of free expression.”[827] On November 24, 2014, images of a neon red skull appeared on computer screens at the entertainment giant Sony. An accompanying message by a group called ‘#GOP,’ standing for Guardians of Peace, threaten to release data secrets if undisclosed demands were not met. Sony initially downplayed the intimidating promise, still bruised from an attack months prior that forced their PlayStation network offline.[828] However, along with the vivid warning expressed to Sony Pictures employees, hackers launched a so called ‘wiper’ attack deleting files and disabling computers. They used malicious software similar to the virus seen in attacks on South Korean banks and media outlets the previous year in a campaign dubbed Dark Seoul.[829] Soon after, sensitive personal information regarding thousands of employees of Sony Pictures and confidential emails by executives were leaked online, along with five new or unreleased films.

On December 16, 2014, Guardians of Peace posted on the Pastebin web site another threat that people who see Sony’s movie “The Interview” would suffer a “bitter fate.”[830] The comedy portrays the leader of North Korea as a sadistically irrational tyrant. This menacing promise prompted Sony Pictures to cancel the Christmas release of the movie at the largest

---

[827] David E. Sanger, “Obama Administration Plans to Open Center to Fight Cyberattacks,” *The New York Times*, February 11, 2015.

[828] Richard Taylor, “Sony Pictures computer system hacked in online attack,” *BBC News*, Technology Section, November 25, 2014.

[829] Ellen Nakashima, Craig Timberg and Andrea Peterson, “Sony Pictures hack appears to be linked to North Korea, investigators say,” *The Washington Post*, December 5, 2014.

[830] David Goldman and Jose Pagliery, “Sony hackers threaten moviegoers with terrorist acts,” *CNN News*, Money Section, December 15, 2014.

multiplex theater chains in North America.[831] President Obama criticized the decision by Sony to cancel the release of the "Interview" as a bad precedent and stated "we will respond proportionately and we will respond in a place and time and manner we choose."[832] The FBI concluded the North Korean government is responsible for the incident at Sony Pictures based in part on analysis of data deletion malware similarities in lines of code and encryption algorithms previously developed by North Korean actors and the discovery that several Internet Protocol (IP) addresses used were associated with known North Korea infrastructure.[833] Although the evidence appeared circumstantial, technical malware analysis confirms the attack was not the work of suspected insiders or hacktivist.[834]

The FBI observed "the destructive nature of this attack, coupled with its coercive nature, sets it apart," as North Korea's actions were intended "to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves."[835] Yet even with confidence in attribution, U.S. policymakers did not have "an established menu of proportionate response options" for this low-intensity cyber attack.[836] Any military retaliation would be out of proportion and would risk escalation, no trade exists for sanctions, and any legal action in

---

[831] Drew Harwell and Ellen Nakashima, "Hackers' threats prompt Sony Pictures to shelve Christmas release of The Interview," *The Washington Post*, Economy Section, December 18, 2014.

[832] Devlin Barrett and Bryon Tau, "Obama Says Sony 'Made a Mistake' Canceling Film," *The Wall Street Journal*, Politics and Policy Section, December 19, 2014.

[833] FBI National Press Office, "Update on Sony Investigation," The Federal Bureau of Investigation, Washington, D.C. December 19, 2014.

[834] Noveta, "Operation Blockbuster: Unraveling the Long Threat of the Sony Attack," February 2016: 12-13.

[835] FBI National Press Office, "Update on Sony Investigation," The Federal Bureau of Investigation, Washington, D.C. December 19, 2014.

[836] Jenny Kim, Scott LaFoy, and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Responses," Center for Strategic & International Studies, December 2015: 7.

indictments would be pointless.[837] Nevertheless the United States did respond in a limited way, potentially covertly and definitely overtly. Perhaps a coincidence, soon after the President's pronouncement, the Internet in North Korea, available only to the elite, the military and the propaganda apparatus, went dark for nearly ten hours.[838] Days later, under an Executive Order signed by President Obama, the Treasury Department imposed financial measures on three North Korean organizations and ten officials. The legislative basis for the sanctions for "destructive, coercive cyber-related actions" was violation of four United Nations Security Council Resolutions and commission of serious human rights abuses.[839] The targets of the sanctions were the Reconnaissance General Bureau, which probably orchestrated the cyber operation, the Korea Mining Development Trading Corporation, their main arms dealer, and the Korean Tangun Trading Corporation, responsible for defense research and development, plus individuals operating out of Russia, Iran, Syria, China and Namiba with suspected connections to the North Korean government.[840]

The Sony attack was sophisticated enough that a prominent security company felt Sony could not have been fully prepared.[841] North Korean used "spear phishing" attacks in early September to steal "credentials" of a Sony systems administrator, which allowed the hackers to

[837] Danny Yadron, Devlin Barrett and Julian E. Barnes, "U.S. Struggles for Response to Hack," *The Wall Street Journal*, December 19, 2014.

[838] Nichole Perlroth and David E. Sanger, "North Korea Loses Its Link to the Internet," *The New York Times*, December 22, 2014.

[839] President Barak Obama, "Imposing Additional Sanctions with Respect to North Korea," Executive Order, The White House, January 2, 2015.

[840] Carol Morello and Greg Miller, "U.S. imposes sanction on N. Korea following attack on Sony," *The Washington Post,* January 2, 2015.

[841] Danny Yadron, "Cyberattack on Sony is Called Sophisticated," *The Wall Street Journal*, December 7, 2014.

roam freely inside Sony's systems.[842] Hackers spent two months collecting passwords and mapping the network before activating a virus named Destover that wiped data and crashed the system in a 10 minute time bomb. Available on the black market, Destover also functions as a back door to an affected network, allowing remote access without detection of intruders.[843] Destover contains configuration files created on systems using Korean language. Not only did analysis of Destover used by #GOP and the virus used in the Dark Seoul attack by the Whois Team reveal similarities in techniques and code, but also comparisons exist in the computer screen images used by the claimed perpetrators in warnings, threats and original skeletal artwork.[844] The cyber defenses at Sony had failed and the U.S. government resorted to retaliation against a nation state through an instrument of power, namely economic sanctions intended to inflict some new financial pain, particularly in exports of military goods and services.

Military Response Options

The United States chose not to use a military response, at least an overt one, to impose costs on North Korea in the Sony incident despite attribution by the FBI. The options for a military response include using cyber or kinetic capabilities. The attack on Sony, although cited by Admiral Rogers as an attack on critical infrastructure in U.S. territory,[845] did not cross the threshold for the use of forceful military means in retaliation. According to Michael Schmitt, "Pursuant to Article 51 of the UN Charter and customary international law, if the malicious

---

[842] David E. Sanger and Martin Fackler, "U.S. hacked North Korean before attack on Sony," *International New York Times*, January 18, 2015: 1 and 3.

[843] Pavel Alpeyev and Grace Huang, "Sony Hacker Snooped for Months, Then Planted 10-Minute Time Bomb," *Bloomberg News*, December 22, 2014.

[844] Kurt Baumgartner, "Sony/Destover: Mystery North Korean Actor's Destructive and Past Network Activity," *Securelist Blog Research*, December 4, 2014.

[845] Ian Kelly, "Cyber Attacks on Critical Infrastructure on the Rise," ID Experts Blog, August 24, 2016: https://www2.idexpertscorp.com/blog/single/cyber-attacks-on-critical-infrastructure-on-the-rise

cyber operation attack against Sony had constituted a 'use of force' rising to the level of an 'armed attack,' the United States would have been entitled to respond forcefully, whether by kinetic or cyber means."[846] The attack against Sony involved the release of sensitive information and the destruction of data. Although disruptive and costly, the effects were not at the level of an armed attack. Likewise the attack, although severe, would probably not be characterized as a use of force by the international community. However, the cyber attack against Sony, since attributed to the State of North Korea, was a violation of U.S. sovereignty. As such, under the law of State responsibility, the attack amounted to an "internationally wrongful act." The commission of an internationally wrongful act entitles an injured State to engage in countermeasures in order to persuade the responsible State to return to a state of lawfulness.[847] For which the United States might have done covertly, by crippling the Internet in North Korea for a brief period of time.

In the Sony case, the United States did make a determination on attribution one month after the attack. Attribution plays a key role in signaling, or proving, that a response by the victim to an attack will occur. Yet tracing cyber attacks back to their origin is difficult. Attackers evade detection by using hijacked systems as proxies or by changing [spoofing] the source field of IP data packets.[848] Attackers can also modify [spoof] the Media Access Control address of network devices to mask identify or poison a Domain Name System server to redirect users to a malicious website.[849] Technical attribution seeks to identify IP ownership or domain registration, but other indicators can help to attribute attacks, such as tradecraft tools, code styles,

---

[846] Michael Schmitt, "International Law and Cyber Attacks: Sony v. North Korea," *Just Security*, December 17, 2014: 1.

[847] Ibid, 2-5.

[848] Larry Greenemeier, "Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers," *Scientific American*, June 11, 2011:

[849] Mauno Pihelgas, "Back-Tracing and Anonymity in Cyberspace," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 31-60.

resource language, and time zone information such as malware build time or command and control check in times.[850] "Attribution is not impossible, it's just hard," according to General Michael Hayden, former Director of the Central Intelligence Agency, and "good attribution does not include up to the point of beyond all reasonable doubt," rather "this is about enabling governments to act in the face of continued doubt."[851] That entails acting without meeting some sort of judicial standard to protect national interest, and if necessary by military means. If a decision to maintain credibility by military means is made, then a plethora of considerations follow in this section for use of cyber or kinetic weapons in a proportional and justified response.

Response Thresholds

The threshold for use of military means in response to a cyber attack by a nation state is imprecise. Difficulties in reaching international consensus on what qualifies as the "use of force" rising to a level of an "an armed attack" in cyberspace impedes the application of international law to cyber operations, which are defined as "the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace."[852] The lack of a common understanding on these terms and conditions also restricts the ability to deter cyber attacks. In the Charter of the United Nations, Article 2 calls on all Members to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[853] The most serious and dangerous form of the use of force is aggression. Acts that qualify as aggression include invasion, blockade, bombardment, and other attacks by armed

---

[850] Dmitri Alperovitch, "The Art of Attribution: Identifying and Pursuing your Cyber Adversaries," RSA Conference, February 24-28, 2014: 13.

[851] General Michael V. Hayden, "HBO What to Do about Cyberattacks," Council on Foreign Relations Event Transcript, October 6, 2015: 28.

[852] U.S. Department of Defense, *Cyberspace Operations,* Joint Publication 3-12 (R), (Washington, DC: The Joint Staff, February 5, 2013): v.

[853] United Nations, Charter of the United Nations, Chapter VII, Article 2, San Francisco, CA, October 24, 1945.

forces of a state on the land, sea or air forces of another state.[854] The Russian occupation of Crimea qualified as aggression, since Russia exercised territorial control without the consent of the Ukrainian Government. However an act qualifying as a use of force need not be undertaken by state armed forces. For example an act would qualify if undertaken by state intelligence agencies or by a private contractor whose conduct is attributable to the state. Cyber operations may "in certain circumstances constitute a use of force within the meaning of Article 2 (4) of the UN Charter," if they cause effects that, if caused by traditional physical means, would be clearly regarded as a use of force.[855] For example, the United States would categorize cyber operations as a use of force if they: 1) "trigger a nuclear plant meltdown;" 2) "open a dam above a populated area, causing destruction;" or 3) "disable air traffic control services resulting in airplane crashes."[856]

The term "use of force" is not to be equated with the term "armed attack." Not every use of force rises to the level of an armed attack. Likewise the choice of means of attack is immaterial to the determination. For example, the Tallinn Manual 2.0 states "it is universally accepted that chemical, biological, and radiological attacks of the requisite scale and effects to constitute armed attacks trigger the right of self-defense."[857] Under identical reasoning, Rule 71 states that "whether a cyber operation constitutes an armed attack depends on its scale and effects." The parameters for scale and effects are "unsettled beyond the criteria they need to be grave." The International Group of Experts that wrote the Tallinn Manual 2.0 agreed that "a cyber operation that seriously injures or kills a number of persons or that causes damage to, or destruction of, property would satisfy the scale and effects requirement." They also agreed that

---

[854] United Nations, General Assembly, Resolution 3314 (XXIX), December 14, 1974.

[855] Harold Hongkin Koh, Legal Advisor, Department of State, "International Law in Cyberspace," Remarks at USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Maryland, September 18, 2012.

[856] Ibid.

[857] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 340.

"acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services do not qualify as armed attacks."[858] The United States view is similar on cyber operations that resemble traditional signal intelligence activities, in considering cyber intrusions to collect data for national security purposes as within the realm of international law.[859]

<u>Resort to Force</u>

The body of international law entitled *jus ad bellum* governs a state's resort to military force, including through cyber operations, as an instrument of its national policy. Certain criteria for *jus ad bellum* have been drawn from principles as part of Just War Tradition.[860] The principles start with a competent authority to order war for a just cause, such as self-defense. Article 51 of the Charter of the United Nations demarcates "the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations."[861] Traditionally, Article 51 has been characterized as applicable to armed attacks undertaken by one nation state against another, but recent practice establishes a right of self-defense in the face of armed attacks by non-state actors, such as terrorist or rebel groups.[862] Not all states accept the United Nations strict criteria on armed attack. For instance "the United States has long taken the position that the inherent right of self-defense potentially applies against any illegal use of

---

[858] Ibid, 339-41.

[859] Executive Office of the President, *Presidential Policy Directive on Signals Intelligence Activities*, PPD-28, (Washington, DC: The White House, January 17, 2014).

[860] Office of General Counsel, *Department of Defense Law of War Manual*, June 2015 (Updated December 2016): 38-42.

[861] United Nations, Charter of the United Nations, Chapter VII, Article 51, San Francisco, CA, October 24, 1945.

[862] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 345.

force."[863] Regardless of viewpoint, to constitute legitimate self-defense, the defending state's use of force must be necessary and proportionate, which limits the application of retaliation in cyber conflict because of constraints on the use of overwhelming force.

Necessity requires that "a use of force, including cyber operations that amount to a use of force, be needed to successfully repel an imminent armed attack or defeat one that is underway."[864] For example if passive cyber defenses like firewalls are "adequate to reliably and completely thwart a cyber armed attack, other measures, whether cyber or kinetic, at the level of a use of force are impermissible."[865] Likewise, other non-forceful measures, such as diplomacy, economic sanctions or law enforcement must be insufficient to address the situation. Proportionality addresses "how much force," including through cyber operations, "is permissible once force is deemed necessary;" the measures taken in self-defense must be proportionate in "scale, scope, duration and intensity" to the nature of the threat being addressed.[866] There is no requirement for the measures taken to be of that which constituted an armed attack, for instance "a cyber use of force may be resorted to in response to a kinetic armed attack, and vice versa."[867] For illustration the insertion of a logic bomb would qualify as "an imminent armed attack if the specified conditions for activation are likely to occur."[868] In the case of an ongoing pattern or campaign of cyber operations, proportionality can be assessed by what use of force is judiciously necessary to discourage future armed attacks or the threat thereof.

---

[863] Office of General Counsel, *Department of Defense Law of War Manual*, June 2015 (Updated December 2016): 47.

[864] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 348.

[865] Ibid, 349.

[866] Ibid.

[867] Ibid.

[868] Ibid, 352.

Justification for a resort to force for NATO resides in Article 5 of the North Atlantic Treaty, where "the Parties agree that an armed attack against one of more of them in Europe or North America shall be considered an attack against them all."[869] Consequently "they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense... will assist the Party or Parties so attacked."[870] This principle named collective defense binds members together, committing them to protect each other. Article 5 was invoked for the first time in its history after the 9/11 terrorist attacks against the United States. The North Atlantic Council Treaty Organization (NATO) Summit in Wales in 2014 affirmed "that cyber defense is part of the NATO's core task of collective defense."[871] Rule 74 of the Tallinn Manual 2.0 reiterates that "collective defense against a cyber operation amounting to an armed attack may only be exercised at the request of the victim state and within the scope of the request."[872] That State may, for instance, limit assistance to non-kinetic measures, consistent with NATO's emphasis on defense.

At the 2016 NATO Summit in Warsaw, the Heads of State and Government reaffirmed "NATO's defensive mandate," and recognized "cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea."[873] This declaration is intended to maintain freedom of action and support broader deterrence and defense, through integration of cyber defense into operations and missions. Even more so in following the principle of restraint, the Heads affirmed their "commitment to act in accordance

---

[869] North Atlantic Treaty Organization, "The North Atlantic Treaty," Article 5, Washington, D.C., April 4, 1949.

[870] Ibid.

[871] North Atlantic Treaty Organization, "Wales Summit Declaration", Paragraph 72, September 5, 2014.

[872] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 354.

[873] North Atlantic Treaty Organization, "Warsaw Summit Communique," Paragraph 70, July 9, 2016.

with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable."[874] The strengthening of cyber defensive capabilities will include the latest cutting edge technologies. Overall the Communique stays in line with NATO's Enhanced Policy on Cyber Defense, but any follow-on discussions or decisions on offensive capabilities will be important, since the lack of a well-articulated offensive cyber capability does affect NATO's ability to deter or defend against cyber attacks, although national capabilities are at different levels of maturity.[875] To that extent, the Polish think tank Kosciuszko Institute is already calling for NATO development of offensive cyber capabilities.[876]

In Armed Conflict

The body of international law entitled *jus in bello* regulates how hostilities may be conducted in cases of declared war or any armed conflict and protects those affected by them. Practically the term armed conflict has replaced the notion of war as an international legal concept. Rule 80 of the Tallinn Manual 2.0 states that "cyber operations executed in the context of an armed conflict are subject to the law of armed conflict."[877] This rule applies in both international (between two or more states countries) and non-international (between a state and an organized armed group) situations of armed conflict. For the first situation, the law of armed conflict did govern cyber operations that occurred during the armed conflict between Russia and Georgia in 2008 because they were undertaken in furtherance of that conflict.[878] For the latter situation, the International Committee of the Red Cross has characterized the protracted

---

[874] Ibid.

[875] James A. Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defense," A NATO CCD COE Publication on Strategic Cyber Security, Tallinn Paper No. 8, 2015: 2-10.

[876] Wieslaw Gozdziewicz, et. al, "NATO Road to Cybersecurity," The Kosciuszko Institute, August 25, 2016: 1-77.

[877] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 375.

[878] Ibid, 376.

hostilities in eastern Ukraine as a non-international armed conflict between the government of Ukraine and separatists from the cities of Donetsk and Luhansk. Although there is widespread belief that Moscow supports the separatists, Russia would have to actively participate or exercise overall control for the situation to be considered an international armed conflict.[879] By contrast, even though Estonia in 2007 was the target of persistent cyber operations targeting civilian infrastructure, the law of armed conflict did not apply because the situation did not rise to the level of armed conflict.[880]

Regardless of the situation, it is the policy of the U.S. Department of Defense that members will comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations.[881] Under *jus in bello* the law of war is also known as the law of armed conflict and international humanitarian law. According to the International Committee of the Red Cross, the means and methods of warfare which resort to cyber technology are subject to international humanitarian law.[882] Therefore the customary and fundamental principles of the law of war, specifically military necessity, distinction, proportionality, and humanity apply to the conduct of cyber operations.[883] The aforementioned law of war principles "work as interdependent and reinforcing parts of a coherent system."[884]

---

[879] Jan Stinissen, "A Legal Framework for Cyber Operations in Ukraine," *Cyber War in Perspective: Russian aggression against Ukraine*, Chapter 14, (Tallinn, Estonia, NATO Cooperative Cyber Defense Center of Excellence Publications, 2015): 123-134.

[880] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 376.

[881] U.S. Department of Defense, *Cyberspace Operations,* US Joint Publication 3-12 (R), (Washington, DC: The Joint Staff, February 5, 2013): III-10.

[882] Catherine Lotrionte, "Cyber War: Definitions, Deterrence and Foreign Policy," Statement before the House Committee on Foreign Affairs, September 30, 2015.

[883] Office of General Counsel, *Department of Defense Law of War Manual*, June 2015 (Updated December 2016): 1013.

[884] Ibid, 50-51.

Military necessity "justifies the use of all measures needed to defeat the enemy as quickly and efficiently as possible."[885] Distinction requires Parties to the conflict at all times to distinguish between the civilian population and combatants and between civilian objects and military objectives, and accordingly direct operations only against military objectives. Humanity, the prohibition of the causing of unnecessary suffering, forbids actions unnecessary to accomplish a legitimate military objective. Proportionality requires that justified actions not be unreasonable or excessive. This principle obliges persons to refrain from attacking where the expected harm incidental to attacks outweighs the military advantage anticipated to be gained.[886]

Cyber Capability Employment

Any examination of targeting for the employment of cyber capabilities starts with the principle of distinction which restricts operations against civilians and civilian objects that do not qualify as military objectives. Usually military attacks will only be directed at military targets. By their "nature, location, purpose, or use," military targets are those objects "whose total or partial destruction, capture, or neutralization" offers a direct and concrete military advantage.[887] For example, a command and control facility and cyber infrastructure for military tasks would qualify. Aside from military equipment, objects can qualify by the use criterion, like air traffic control or global positioning systems that serve both civilian and military systems, irrespective of the extent of civilian reliance on them.[888] Persons directly participating in hostilities qualify, such as those conducting a denial of service operation or building a botnet for enemy use. Otherwise it is only legal to conduct cyber operations against civilians and civilian objects so long as they are not harmed or injured. In this case, relevant factors that suggest a cyber operation is allowed are whether it causes only reversible or temporary effects, such as defacing

[885] Ibid, 52.

[886] Ibid, 58-65.

[887] Ibid, 210.

[888] Michael Peck, "The Pentagon is Worried about Hacked GPS," *The National Interest*, January 14, 2016.

a government webpage, a minor disruption of internet services, brief interference with communications, and dissemination of propaganda.[889]

The principle of distinction also prohibits use of indiscriminate means. Cyber weapons are indiscriminate if incapable of distinguishing between combatants and civilians or civilian objects and military objectives. A destructive computer virus that spreads and destroys "uncontrollably within civilian internet systems would be prohibited as an inherently indiscriminate weapon."[890] Consider for example malware introduced into a military system that spreads randomly into civilian networks, or malware placed on a website open to civilians and combatants, or innocuous email attachments sent to combatant's private account that could be forwarded to civilians.[891] Even for legal weapons, the risk of cascading and collateral effects is a pervasive feature of weaponry. Due to policy concerns, rules of engagement may limit cyber operations to those "that result in no or low levels of collateral effects."[892] Even if a proposed cyber operation is permissible after a collateral effects analysis, it must "also be permissible under a law of war proportionality analysis."[893] The principle of proportionality prohibits a cyber operation which may be expected to "cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof," that would be excessive in relation to the anticipated concrete and direct military advantage.[894] An example would be a cyber attack on the dual-use global positioning system, which although a lawful target, would most likely cause

[889] Office of General Counsel, *Department of Defense Law of War Manual*, June 2015 (Updated December 2016): 1022.

[890] Ibid, 1026.

[891] Michael N. Schmitt, "The Law of Cyber Targeting," A NATO CCD COE Publication on Strategic Cyber Security, Tallinn Paper No. 7, 2015: 7-19.

[892] U.S. Department of Defense, *Cyberspace Operations,* US Joint Publication 3-12 (R), (Washington, DC: The Joint Staff, February 5, 2013): IV-4.

[893] Ibid.

[894] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 470.

harm, for instance, to merchant vessels and civil aircraft, potentially excessive to military advantage.[895]

To avoid law of war prohibitions expect advanced cyber weapons used by states in armed conflict to exploit particular vulnerabilities in specific, closed systems. Take for instance the Stuxnet operation found in June 2010 to be infecting the Bushehr and Natanz nuclear facilities in Iran.[896] In light of the damage caused to nearly 1000 Iranian centrifuges,[897] some of the International Group of Experts that wrote the Tallinn Manual held the view that the Stuxnet operations reached the armed attack threshold.[898] Stuxnet "has been called a cyber weapon," according to the senior vice president of Integrity Global Security, because "the intent was to cause physical damage and maybe to kill people."[899] The malware was most likely delivered into the closed nuclear systems by an infected USB drive.[900] It exploited a total of four unpatched Microsoft vulnerabilities, of which two had yet to be disclosed or zero days.[901] Stuxnet was written to target specific frequency converter drives used to control the speed of a device. The malware does not sabotage any frequency converter, just drives made by the particular company Siemens, that run at high speeds, between 807Hz and 1210Hz like those used

---

[895] Ibid, 471-72.

[896] "Iran: Stuxnet Worm, Computer Terrorism," Press TV, October 13, 2010.

[897] IISS Strategic Comments, "Stuxnet: targeting Iran's nuclear programme," Volume 17, Comment 6, February 2011.

[898] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 342.

[899] William Jackson, "Stuxnet vulnerabilities in industrial controls," *Government Computer News*, October 1, 2010.

[900] Gregg Keizer, "Is Stuxnet the best malware ever?" *Computer World*, September 16, 2010.

[901] Nicolas Falliere, Liam O. Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response, Version 1.3, November 2010.

for uranium enrichment.[902] Accordingly, the malicious code adhered to the principles of distinction and proportionality because it targeted converters operating at unique speeds. Although the facilities may have been used for civilian purposes, they were reasonably assumed to have a military role and not merely a remote possibility, and therefore were legitimate targets.[903] The Stuxnet malware did demonstrate the risk of unintentional or unanticipated migration into civilian systems by escaping the Iranian nuclear enrichment plants. The malware was found on 100,000 infected hosts in more than 25 countries where it can be re-engineered.[904]

Kinetic Capability Choices

As evidenced through alleged involvement in the Stuxnet operation, United States policy is to conduct offensive cyber operations in a manner consistent with the policy principles and legal regimes for kinetic capabilities, including the law of armed conflict.[905] In some cases, the use of kinetic options in other domains strengthens legitimacy and credibility to respond to malicious cyber activity. For example when overmatched online by the Islamic State propaganda machine, the United States turned to lethal force against this terrorist group in an attempt to stop an avalanche of videos and statements. U.S. airstrikes in military operations against the Islamic State have terminated several high level media division operatives, including Junaid Hussain, a British born computer expert.[906] Hussain was killed by a drone strike while he was in a car in Raqqa, Syria. Hussain was viewed by U.S. officials as a top terrorist threat

---

[902] Kim Zetter, "Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage," *Wired*, November 15, 2010.

[903] John Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield," *Journal of Computer and Information Law* 29 (Fall 2011): 1–37.

[904] William Jackson, "Stuxnet Reveals Vulnerabilities in Industrial Controls," *Government Computer News*, October 1, 2010.

[905] U.S. Department of Defense, *Cyberspace Policy Report*, November, 2011: 5.

[906] Greg Miller and Souad Mekhennet, "Inside the surreal world of the Islamic State's propaganda machine," *The Washington Post*," November 20, 2015.

because he would post names, addresses and photos of U.S. troops on his Twitter feed and suggest followers find and kill the person. He also developed a Remote Access Trojan to hack into computers and was training other Islamic State members in how to use hacker techniques.[907] In the case of Hussain, his affiliation with the terrorist group Islamic State made him a member of an organized armed group, which made him a legitimate target in an armed conflict.[908]

Other Response Options

Lisa Monaco, the former Assistant to the U.S. President for Homeland Security and Counterterrorism, contended that "meeting cyber threats requires a whole-of-government approach that uses all the appropriate tools available."[909] The approach relies on unity of effort within the Federal Government and close coordination between public and private sectors to achieve optimal results based on shared interests.[910] Appropriate tools include global diplomacy, law enforcement expertise, economic clout, and when necessary military capability. Monaco stressed that those who would harm the United States should know that they can be found and will be held to account. A RAND Corporation study agrees with the intrinsic value of the first tool of global diplomacy in reaching the conclusion that the best means for deterring, for instance, Chinese behavior is by diplomatic action.[911] However holding a pragmatic nation state

[907] Margaret Coker, Danny Yadron, and Damian Paletta, "Hacker Killed by Drone Was Islamic State's Secret Weapon," *The Wall Street Journal,* August 27, 2015.
[908] Jeffrey Carr, "The Legal Rationale For Killing An Enemy Hacker (or Could You Be The Next Junaid Hussain)?" Blogspot, Digital Dao: Evolving Hostilities in the Global Cyber Commons, September 1, 2015.
[909] Lisa O. Monaco, "Strengthening our Nation's Cyber Defenses," Remarks as Prepared for Delivery, The Wilson Center, Washington, D.C., February 10, 2015.
[910] Executive Office of the President, *Presidential Policy Directive – United States Cyber Incident Coordination*, PPD-41, (Washington, DC: The White House, July 26, 2016).
[911] Abram N. Shulsky, *Deterrence Theory and Chinese Behavior*, (Santa Monica, California: RAND Corporation, 2014).

actor like China to account for activity it conducts or allows inside its borders requires not just global diplomacy, but also coercive diplomacy, which combines techniques of deterrence and compellence to elicit desired actions.[912] The law enforcement component of deterrence by retaliation attempts to prevent undesirable actions by instilling a fear of punishment into a targeted actor. Yet for actors outside state borders, the deterrent threat only works if there is interstate cooperation. For an uncooperative state, the element of compellence offers positive reinforcement for taking actions it otherwise would not take. To compel responsible state behavior, economic sanctions initiate harmful actions that can cease, but only if the uncooperative state responds favorably by ceasing its malicious activity or by cooperating in the punishment of malicious actors inside its territory.

Law Enforcement

State cooperation between law enforcement agencies is essential to hold malicious actors accountable for their crimes in cyberspace. The Budapest Convention on Cybercrime, the first such international treaty, outlines the widest possible means of cooperation to investigate crimes involving "computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[913] Over 35 nations, largely in Europe, in addition to Canada, Japan, South Africa, and the United States have acceded to the treaty, and many others are in various stages of ratifying it. The Convention provides arrangements "to stem cross border crimes while recognizing divergent interpretations of national sovereignty."[914] At the 10th anniversary meeting of the Council of Europe on adoption of the Convention, the Secretary General declared that "the treaty still represents the only accepted international text on how to protect against and

[912] Thomas Schelling, *Arms and Influence*, (New Haven and London: Yale University Press, 1966): 69-78.

[913] Council of Europe, "Convention on Cybercrime," Budapest, Hungary, November 23, 2001: 1–24.

[914] Scott Jasper, "Are US and Chinese Cyber Intrusions So Different?" *The Diplomat*, September 09, 2013.

control online crime while at the same time respecting human rights."[915] Since then the European Union and the Council of Europe initiated a three year joint project entitled Global Action on Cybercrime (GLACY) aimed at supporting countries worldwide in the implementation of the Budapest Convention on Cybercrime. GLACY held international conferences, courses, and workshops "to enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime." Results of the events were expected to garner progress in the areas of harmonization of legislation, judicial training, law enforcement capacities, international cooperation, and information sharing.[916]

Cooperation between State law enforcement agencies has resulted in arrest or extradition of criminals, terrorists and hackers operating in cyberspace. For example, in New York in July 2015, three Estonian men were sentenced to over three years in prison for their involvement in an Internet scheme that infected more than 4 million computers in over 100 countries. The U.S. District Judge said he wanted it to be known that those who breach the security of computers on a large scale will "face very substantial risks." The men were arrested in Estonia and served time in Estonia prisons before extraditions to the United States.[917] In another case in October 2015, Malaysian police detained Ardit Ferizi, a citizen of Kosovo, on a U.S. provisional arrest warrant. The U.S. Justice Department accused him of stealing the personal data of U.S. service members and passing it to Islamic State member Junaid Hussain. Ferizi had hacked into a server used by a U.S. online retail company and obtained data on about 100,000 people, from which he sent

---

[915] Speech by the Secretary General, "Budapest Convention on Cybercrime," 10th Anniversary meeting, Strasbourg, 23 November 2011.

[916] Council of Europe, "Global Action on Cybercrime," Capacity Building, located at http://www.coe.int/en/web/cybercrime/glacy, Accessed on January 7, 2017.

[917] Larry Neumeister, "3 Estonian men get over 3 years in prison for cyberfraud," *Daily Herald*, July 23, 2015.

details of 1,351 military and government personnel to the Islamic State.[918] Ferizi was extradited to the United States and charged with computer hacking, identify theft, and providing material support to a terrorist organization.[919] In June 2015, Ferizi pleaded guilty.[920] In March 2016, the U.S Justice Department charged three members of the Syrian Electronic Army that support President Assad with computer hacking conspiracies targeting government agencies and media companies. Though Dmitri Alperovitch, cofounder of CrowdStrike astutely observed "This is yet another law enforcement win that [shows] no one is above the law, but these are not major criminals that were posing a threat to the United States."[921]

Economic Sanctions

A successful example of sanctions changing the behavior of an uncooperative nation state was those imposed by the UN Security Council on Iran during 2010-2013 for lack of compliance with resolutions to ensure the peaceful nature of its nuclear program. The sanctions contributed to the acceptance by Iran in July 2015 of a comprehensive accord that exchanges constraints on its nuclear program for broad sanctions relief. The UN sanctions had caused Iran's crude oil exports to fall by over a million barrels per day and its economy to shrink by about 10%.[922] In January 2016, the International Atomic Energy Agency verified that Iran had met its commitments as set out in Annex V of the accord, and the United States initiated steps to meet its

---

[918] Ellen Nakashima, "U.S. accuses hacker of stealing military members' data and giving it to ISIS," *The Washington Post*, October 16, 2015.

[919] Aaron Boyd, "Hacker who outed feds' info charged with terrorism," *C4ISR &Networks*, January 28, 2016.

[920] Rachel Weiner and Ellen Nakashima, "Hacker admits he gave military member's data to the Islamic State," *The Washington Post*, June 15, 2016.

[921]Andrea Peterson and Ellen Nakashima, "U.S. charges three suspected Syrian Electronic Army Hackers," *The Washington Post*, March 22, 2016.

[922] Kenneth Katzman, "Iran Sanctions," Congressional Research Service, CRS Report RS20871, January 21, 2016.

obligations to lift sanctions.[923] Not all nations agreed with the accord, in particular Israeli Prime Minister Netanyahu told the U.S. Congress before acceptance that the deal would not block Iran's way to a bomb "but paves its way to a bomb."[924] Israel vowed to act alone if necessary to prevent Iran from obtaining a nuclear weapon, and could decide the deal is so bad that force is necessary. After all, the Israeli Air Force has already taken out nuclear reactors in Iraq and Syria, the latter with a cyber attack on air defenses.[925] Pro-Israel Lobbies also expressed concern that once the deal is done, and Iran becomes a nuclear threshold state, there would be no peaceful way to stop Iran from building a nuclear weapon, except to resort to force.[926] When asked whether the United States failed to use all of its leverage, including a credible threat of force, President Obama said "I think that criticism is misguided... we have cut off every pathway for Iran to develop a nuclear weapon" and "if we can in fact resolve some of these differences, without resort to force, that will be a lot better for us and the people of that region."[927]

The accord reached in Vienna to limit the Iranian nuclear program is the most detailed non-proliferation agreement ever devised, but only in years will the world know if it was a reasonable bet.[928] The White House obviously recognizes the value of combining diplomacy with sanctions, and the prospect of both for changing malicious cyber behavior. In April 2015,

---

[923] Dianne E. Rennack, "Iran: U.S. Economic Sanctions and the Authority to Lift Restrictions," Congressional Research Service, CRS Report R43311, January 22, 2016.

[924] Barak Ravid, "Netanyahu tells U.S. Congress: This Deal paves Iran's path to the Bomb," *Haaretz*, March 3, 2015.

[925] Jeremy Diamond, "Could military force still be used against Iran?" *CNN News*, Politics Section, April 2, 2015.

[926] The American Israel Public Affairs Committee, "Analysis: The Iran Nuclear Deal," July 28, 2015: 1-10.

[927] Thomas L. Friedman, "Obama makes his Case on Iran Nuclear Deal," *The New York Times*, July 14, 2015.

[928] Bruno Tertrais, "Iran: An Experiment in Strategic Risk-Taking," *Survival: Global Politics and Strategy*, Vol 57, Issue 5, October-November 2015: 67-73.

President Obama signed an Executive Order to try to deal with the threat of malicious cyber-enabled activities originating from or directed by persons located outside the United States. The Order blocks all property and interests of persons found to be "harming or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;" "causing a significant disruption to the availability of a computer or network of computers," including through a distributed denial of service attack; and "causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain."[929] It authorizes the Secretary of the Treasury to impose sanctions on those individuals and entities that are responsible for cyber-enabled activities that threaten "the national security, foreign policy, economic health, or financial stability of the United States."[930] By sanctioning these actors, their access to American financial systems, companies and territory is restricted, which basically harms their ability to commit malicious acts and to profit from them.[931] Michael Daniel, special assistant to President Obama, said the order will "enable us to have a new way of both deterring and imposing costs on malicious cyber actors, wherever they may be and across a range of threats."[932] Although in the "absence of satisfying policy options, we risk deploying sanctions that... disadvantage U.S. companies... and expose our economy to retribution."[933]

---

[929] President Barak Obama, "Blocking the Property of Certain Persons engaging in Significant Malicious Cyber-enabled Activities," Executive Order, The White House, April 1, 2015.

[930] Michael Daniel, "Our Latest Tool to Combat Cyber Attacks: What You Need to Know," Fact Sheet, The White House, April 1, 2015.

[931] Aaron Boyd, "Treasury finalizes rule for imposing cyber sanctions," *Federal Times*, January 4, 2016.

[932] Aaron Boyd, "Obama: Cyberattacks continue to be national emergency," *Federal Times*, March 10, 2016.

[933] William J. Burns and Jared Cohen, "The Rules of the Brave New Cyberworld," *Foreign Policy*, February 16, 2017.

Necessary Means Utility

U.S. Secretary of Defense Ashton Carter has stated “Adversaries should know that our preference for deterrence and our defensive posture don’t diminish our willingness to use cyber options if necessary.”[934] His communication of a willingness to take cyber enabled action in a deterrent posture is apparently backed by capability to do so, although the credibility to evoke military retaliation is suspect given few publicly known examples to date. Doing nothing signals to other nation states, other groups, and other actors that malicious behavior is okay and will not generate a response. Congressman Mac Thornberry, chairman of the House Armed Services Committee, adamantly stated “We have to figure out how to retaliate against an attack.”[935] The problem starts with identifying the attacker and ends with the uncertain consequences of deploying a cyber weapon if necessary. Attributing malicious activity in cyberspace to an actor with sufficient confidence and verifiability to hold them accountable is difficult. If attribution is certain enough to respond, the effects from escalation in counter attacks could reverberate across the Internet. A stockpile of cyber weapons is simply not good enough to deter malicious actors if the threat to use them is not credible enough to act when necessary.

The challenge is when to decisively act, especially if the circumstances of a cyber attack fall close to the threshold for military response. When does a cyber attack upon critical infrastructure, such as civilian financial systems, public utility sectors like power grids, or critical defense industries, justify a military counter strike? The Tallinn Manual says it depends on the scale and effects of the attack, yet the precise point at which the extent of death, injury, damage, destruction, or suffering qualifies as an armed attack is unclear. In the United States, the basic framework for the military to intervene in protecting non-military networks and take retaliatory action would be in the event of significant consequence typically reflecting loss of life. As to whether there is a clear threshold that would trigger military intervention, the Deputy

---

[934] Amber Corrin, “Cyber goes on the offense,” *C4ISR &Networks*, June 2015: 32.

[935] W. J. Hennigan and Brian Bennett, “Pentagon seeks cyberweapons strong enough to deter attacks,” *The LA Times*, July 31, 2015.

Commander of U.S. Cyber Command, Lieutenant General James McLaughlin has said "to be honest, it will never be black and white."[936] There is a structure in the government for a request to come forward for Cyber Command to take action. However given the range of domestic and international actors from the civilian, commercial, and governmental sectors involved in cyberspace, any cyber operation will have to consider complicated issues such as fratricide avoidance, role of noncombatants, proportional use of force, and rules of engagement.[937]

Even still an argument exists that the need for an appropriate response in real time to a cyber attack on critical infrastructure requires explicit policies to be in place.[938] Therefore Senator Mike Rounds has introduced legislation that would "require the executive branch to define which of these actions constitute a cyber act of war, which would allow our military to be better able to respond to cyber-attacks."[939] Although with the threshold defined to reach a decision for the military to return fire, can collateral damage be avoided if the intrusions were launched through thousands of hijacked computers in third-country or target nation sites? The containment of effects to the intended target set within a highly networked, potentially globally interconnected system is more difficult than against closed systems that may be only accessed locally. If effects cannot be meaningfully limited, controlled, or known, any cyber attack in retaliation, no matter how discretely intended, could have massive unintended consequences and pose significant political risk.[940] The inability to predict collateral damage and uncertainty over

---

[936] Zachary Fryer-Biggs, "21st century spy wars," Cyber Espionage Briefing, *Jane's Defense Weekly,* November 11, 2015: 26-30.

[937] Brett T. Williams, "Ten Propositions regarding Cyberspace Operations," *Joint Force Quarterly,* Issue 61, 2nd Quarter 2011: 11-16.

[938] Mike Rounds, "Defining a Cyber Act of War," *The Wall Street Journal,* May 8, 2016.

[939] Cyber/IT Blog, "Rounds Introduces Cyber War Definition Bill," *Defense Daily,* May 10, 2016.

[940] Maren Leed, "Offensive Cyber Capabilities at the Operational Level," Center for Strategic & International Studies, September 2013: 1-9.

political effect requires caution.[941] Especially since unintentional results could lead to escalation, which is an unplanned rise in the scope or intensity of a conflict, or cascade effects. Escalation is an interactive concept in which action by one party triggers a response. Inadvertent escalation occurs when one party takes actions that it does not believe are escalatory, but cross a threshold of the other party. Accidental escalation occurs when an operational action has direct effects that are unintended. Of concern is a chain reaction, in which actions feed off each other to raise the conflict to a level not initially contemplated by any party.[942]

Once a conflict evolves, termination of cyber activity is not trivial. With detection and attribution so difficult, will it be clear when one side has stopped attacking another? One should consider three termination paths: negotiation, tacit deescalation, and petering out.[943] A cease fire agreement in cyberspace presumes assurance that all parties are in control and will understand, monitor and adhere to the terms of the agreement. These conditions are strained by conceptual differences in terminology and technical limitations in verification. Each side could cheat by shifting from visible disruption to more subtle corruption attacks. Or they could use third parties, like hacker crews or patriotic hackers, outside the agreement to reap unilateral advantages from attacks. In mutual deescalation, formal adjudication of the original issues is not necessary, just both sides need to believe that neither would make much headway through further cyber attacks. Unfortunately, in tacit deescalation the same validation problems exist, except are worst since there would only be a rough consensus on what was and was not considered a violation. In the third path, hope exists that attacks peter out, if each side concludes that attacks are growing difficult to conduct and pointless for the retaliation effort, but hope is never a strategy to follow.

---

941 James Lewis, "Low-level cyberattacks are common but truly damaging ones are rare," *The Washington Post*, October 9, 2013.

942 Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, Vol. 6, Issue 3 (Fall 2012): 52-63.

943 Martin C. Libicki, *Cyberdeterrence and Cyberwar*, (Santa Monica, California: RAND Corporation, 2009): 135-137.

The use of means for retaliation other than cyber operations alleviates many intrinsic concerns. A prime example of the utility of a law enforcement attempt to impose cost is the indictment of three men that allegedly hacked JP Morgan in 2014. The indictment reveals a broad network of criminal activity with computer hacking at its center.[944] JP Morgan is actually listed as Victim 1 of twelve. The range of illicit activities run by the conspirators included Securities Market Manipulation, Unlawful Internet Gambling, Illicit Payment Processing, and an Unlawful Bitcoin Exchange. In the list of Statutory Allegations, the conspirators were charged with 23 criminal counts, including Computer Hacking, Wire Fraud, Securities Fraud, all under violations of Title 18, United States Code.[945] The indictment indicates existing laws are sufficient to cover a gambit of malicious cyber activities. The larger hurdle is finding the attribution to bring the criminals to justice in a timely manner to impose costs for their malicious behavior. The time from JP Morgan reporting the hack in the media to the indictments was about fifteen months. Maybe that time line is enough to communicate resolve to prosecute, but the charges need to hold in a conviction to produce credibility in legal action. However even filing the charges does signal the threat of retaliation through employment disqualifications and travel restrictions. A high profile Russian hacker found out justice is patient, for after being tracked for a decade by the U.S. Secret Service, he was apprehended on vacation in the Maldives, extradited and convicted in a federal court in 2016.[946]

As for the use of economic sanctions, the Executive Order imposing such on North Korea for the Sony attack was the first time the United States cited cyberattacks in sanctioning another nation state.[947] Yet the sanctions could be of dubious value since they have not worked in

[944] Nicole Hong, "Charges Announced in J.P. Morgan Hacking Case," *The Wall Street Journal*, November 10, 2015.

[945] United States District Court, Indictment, Criminal No. S1 15 Cr. 333 (LTS), Unsealed November 10, 2015: 1-68.

[946] Kate O'Keeffe and Jacob Gershman, "Russian Convicted in Hacking Case," *The Wall Street Journal*, August 26, 2016.

[947] Michael A. Memoli and Ryan Faughnder, "U.S. sanctions on North Korea suggest prospect of further retaliation," *Los Angeles Times*, January 2, 2015.

changing the isolated regime's behavior. Following a nuclear test by Pyongyang in 2013, the U.N. Security Council adopted sanctions to tightened financial restrictions on North Korea. Despite any pain imposed by these sanctions, North Korea successfully detonated a hydrogen bomb in January 2016, although probably still fission on a boasted design.[948] Concern resides in the international community that North Korea will succeed in the mating a nuclear weapon to an accurate missile.[949] The Chinese resisted broad new sanctions against Pyongyang following the nuclear test,[950] but did finally agreed after North Korea launched a long-range rocket in February 2016.[951] Still undeterred by sanctions, Pyongyang kept on launching missiles shortly after, starting with a submarine-launched ballistic missile in April 2016[952] and two Musudan intermediate-range road-mobile missiles in June 2016.[953] After the Security Council threatened "further significant measures,"[954] North Korea promptly responded with its fifth underground nuclear test that produced a more powerful explosive yield. [955] Despite calls for new punitive

---

[948] Alastair Gale and Kwanwoo Jun, "North Korea says it successfully conducted Hydrogen-Bomb Test," *The Wall Street Journal,* January 6, 2016.

[949] Steve Almasy and Euan McKirdy, "North Korea: Our nuclear warheads can fit on missiles," *CNN News*, March 9, 2016.

[950] Jane Perlez and David E. Sanger, "John Kerry Urges China to Curb North Korea's Nuclear Pursuits," *The New York Times*, January 27, 2016.

[951] Farnaz Fassihi, "U.S., China Agree to Sanction North Korea on Nuclear Program," *The Wall Street Journal*, February 25, 2016.

[952] Don Melvin, Jim Sciutto and Will Ripley, "North Korea launches missile from submarine," *CNN News*, April 24, 2016.

[953] Luis Martinez, "North Korea Launches 2 Intermediate-Range Missiles," *ABC News*, June 21, 2016.

[954] Edith M. Lederer, "UN Security Council Condemns North Korea Missile Tests," *Associated Press*, September 6, 2016.

[955] Choe Sang-Hun and Jane Perlez, "North Korea Tests a Mightier Nuclear Bomb, Raising Tension," *The New York Times*, September 8, 2016.

action, years of sanctions show the approach is ineffective.[956] For instance a loophole in the sanctions allows North Korea to sell coal if the proceeds are used for humanitarian purposes[957] and shipments on coal to China have far exceeded the U.N. Security Council ceiling that China helped pass.[958]

The Chinese Foreign Minister had adamantly stated "sanctions are not an end in themselves," in promoting the need to bring the nuclear issue on the Korean Peninsula back to the track of negotiation.[959] In this regard sanctions provide pressure for negotiations, such as in the historic Iran nuclear deal, but the pressure of sanctions cannot be relieved or forgone if other violations of international order occur. For example, Iran could have violated a United Nations Security Council resolution with its ballistic missile test in October 2015 during fulfillment of the nuclear accord.[960] Iran tested a long-range missile called the Emad which according to their Defense Minister was capable of precise control.[961] In response, regardless of the perceived good will garnered in the nuclear agreement, the U.S. Treasury Department sanctioned nearly a dozen Iranian-linked entities for their alleged role in Iran's ballistic missile program.[962]

---

[956] Alastair Gale, "Pyongyang Faces More-Punitive Sanctions," *The Wall Street Journal,* August 25, 2016.

[957] Jane Perlez, "China's Silence Reinforces Its North Korea Calculus," *The New York Times,* September 12, 2016.

[958] Chun Han Wong, "North Korea Coal Exports to China Breached U.N. Cap," *The Wall Street Journal*, February 23, 2017.

[959] Felicia Schwartz, "China, U.S. Divided on Response to North Korea's Nuclear Blast," *The Wall Street Journal,* January 28, 2016.

[960] Kenneth Katzman, "Iran, Gulf Security, and U.S. Policy," Congressional Research Service, CRS Report RL32048, January 14, 2016: 25.

[961] Aresu Eqbali and Asa Fitch, "Iran Test-Fires New Missile," *The Wall Street Journal,* October 12, 2015.

[962] Jay Solomon, "U.S. Sanctions 11 Iranian-Tied Entities for Role in Tehran's Ballistic Missile Program," *The Wall Street Journal,* January 17, 2016.

Likewise the sanctions relief from the nuclear deal has not relieved tensions in the maritime domain, where boats from the Islamic Revolutionary Guard Corps have increasingly harassed U.S. military vessels transiting the Straits of Hormuz through dangerous close-in maneuvers.[963] Finally in the cyber domain, Iran is only looking to enhance cyber capabilities for use as a tolerated form of behavior,[964] just like high speed boat approaches to foreign military ships.

An Insufficient Deterrence Option

The U.S. military is working to become more transparent about offensive planning in cyberspace, hoping that communication of such information will deter cyber attacks. For example, public media releases indicate contractors have been asked to compete for a nearly half-billion dollar military contract to develop and deploy if necessary lethal cyber weapons.[965] The use of these weapons as an instrument of deterrence also requires transparency in direct attribution, so an actor knows any threat of retaliation is credible.[966] The executive director of U.S. Cyber Command has said they are looking for loud offensive cyber "tools that can be definitely traced back to the United States military," to possibly deter future intrusions.[967] At the classified level, massive cyber weapon capability could exist to hold an adversary at significant risk. Powerful and authentic espionage tools created by hackers at the National Security Agency, to include several exploits and a number of implants, have been mysteriously leaked online. The

[963] Paul Sonne, "Iran Vessels Harassed U.S. Destroyer Near Persian Gulf, *The Wall Street Journal,* August 24, 2016, and Gordon Lubold, "In Common Occurrence, Iranian Boats Veer Close to U.S. Warship," *The Wall Street Journal,* July 11, 2016.

[964] Michael Eisenstadt, "Iran's Lengthening Cyber Shadow," Research Notes, The Washington Institute for Near East Policy, No. 34, July 2016: 1-20.

[965] Aliya Sternstein, "Pentagon Contractors Developing Lethal Cyber Weapons," *Nextgov*, November 4, 2015.

[966] United Kingdom Ministry of Defense, "Future Operating Environment 2035," First Edition, December 2015: 20.

[967] Chris Bing, "U.S. Cyber Command director: We want 'loud,' offensive cyber tools," *Fedscoop*, August 30, 2016.

software would be used to take over firewalls that are used "in the largest and most critical commercial, educational and government agencies around the world."[968] Therefore malicious actors should not take the lack of a cyber response as a lack of capability or an unwillingness to use it if deemed necessary.

The United States has used cyber operations against the terrorist group Islamic State, breaking into computers of fighters to implant malware that mines for intelligence and blocking their use of encrypted communications.[969] Yet, despite an ongoing process to build and demonstrate a cyber deterrent, according to Admiral Rogers, foreign countries and criminal hackers still believe there is "little price to pay" for breaching the U.S. government or U.S. companies.[970] Therefore without risk of punishment, cyber attacks continue unabated against federal agencies[971] and civilian companies.[972] Malicious actors appear to have developed a greater tolerance for risk and plan their attacks to avoid triggering credible military deterrent responses, staying below the implicit thresholds of "use of force" or "armed attack." Nevertheless the experience of sanctions and indictments do show there are viable alternatives to the threat and use of military force, especially for cyber espionage and crime.[973]

---

968 Ellen Nakashima, "Powerful NSA hacking tools have been revealed online," *The Washington Post*, August 16, 2016.

969 Shane Harris, "U.S. Ratchets Up Cyber Attacks on ISIS," *The Daily Beast,* April 17, 2016.

970 Damian Paletta, "NSA Chief Says Cyberattack at Pentagon Was Sophisticated, Persistent," *The Wall Street Journal*, September 8, 2015.

971 Riley Walters, "Continued Federal Cyber Breaches in 2015," *The Heritage Foundation,* Issue Brief, No. 4488, November 19, 2015.

972 Riley Walters, "Cyber Attacks on U.S. Companies in 2016," *The Heritage Foundation*, Issue Brief, No. 4636, December 2, 2016.

973 James A. Lewis, "Cyber War: Definitions, Deterrence and Foreign Policy," Statement before the House Committee on Foreign Affairs, September 30, 2015.

Despite the dropping of "cyber bombs" on the Islamic State, according to former Deputy Secretary Work,[974] loose groups of supportive hackers have joined forces to create a mega hacking unit named the United Cyber Caliphate to run defacement and doxing campaigns.[975] To dox is to "search for and publish private or identifying information about (a particular individual) on the internet, typically with malicious intent."[976] Contrary to this development, it turns out that legal action to indict five PLA officers in May 2014 did have an effect in China. In the months that followed the indictment, the Chinese military quietly begin to dismantle their economic espionage campaign apparatus. It initially appeared legal measures by the United States had altered the behavior of portions of the Chinese government, but in reality, the mission was just shifted to the Ministry of State Security. This Ministry is better suited anyway for economic espionage, with elite contract hackers that can better hide telltale digital trails, and with direct channels to state-owned enterprises.[977] Already active and productive, the Ministry is most likely behind the intrusions into Anthem Health Service in 2014[978] and the U.S. Office of Personnel Management in 2015.[979] If law enforcement is not sufficient, that leaves economic sanctions, which require a threshold of attribution lower than beyond reasonable doubt for legal action. Yet not just the threat of them is enough but actual imposition in a demonstration of credibility, to create a real effect on nation state sponsored cyber activity. The United States did not hesitate to impose sanctions on North Korea for the Sony attack. However the Executive

---

974 Amber Corrin, "U.S. goes to cyber war with ISIS," *C4ISR &Networks*, April 14, 2016.

975 Catalin Cimpanu, "ISIS Hackers Join Forces to Create Mega Hacking Unit," *Softpedia*, April 25, 2016.

976 Oxford Living Dictionaries: https://en.oxforddictionaries.com/definition/dox; accessed on July 1, 2017.

977 Ellen Nakashima, "Following U.S. Indictments, China shifts commercial hacking away from military to civilian agency," *The Washington Post*, November 30, 2015.

978 Michael A. Riley and Jordan Robertson, "Chinese State-Sponsored Hackers Suspected in Anthem Attack," *Bloomberg News*, February 5, 2015.

979 Kirstin Finklea, "Cyber Intrusion into U.S. Office of Personnel Management: In Brief," Congressional Research Service, CRS Report R44111, July 17, 2015.

Order, while expansive in legal breath, was weak in implementation, targeting three organizations already on the U.S. sanctions list and ten individuals not directly involved in cyber warfare.[980]

Overall today malicious actors are left guessing if costs can or will be imposed upon them for malicious cyber activities. The possession of capabilities and communication of consequences is not quite consistent. President-elect Donald Trump told a veterans group in October 2016, "As a deterrent against attacks on our critical resources, the United States must possess – and has to – the unquestioned capacity to launch crippling cyber counterattacks." Furthermore "America's dominance in the arena must be unquestioned. Today, it's totally questioned. People don't even know if we have the capability that we are supposed to have."[981] Although for retaliation by military means, maybe it is alright to keep adversaries like nation states and terrorist groups guessing on capability. For under the "idea of a threat that leaves something to chance,"[982] they will be kept guessing on what the punishment will be, not whether there will be punishment. In talking about advanced technologies, Deputy Secretary Work stated "We will reveal to deter and conceal for war-fighting advantage. I want our competitors to wonder what's behind the black curtain."[983]

Well-respected reporter David Sanger countered Secretary Work in saying "we are facing a shroud of secrecy, which is undermining the deterrent effect."[984] America could have a secret

---

980 Bruce Klingner, "The U.S. Needs to Respond to North Korea's Latest Cyber Attack," *The Heritage Foundation*, Issue Brief, No. 4367, March 20, 2015.

981 Aaron Boyd, "Trump administration promises more aggressive, less political cyber stance," *Federal Times*, November 9, 2016.

982 Thomas Schelling, *The Strategy of Conflict*, (Cambridge: Harvard University Press, 1960): 187-203.

983 Aaron Mehta, "Work outlines key steps in Third Offset tech development," *Defense News*, December 14, 2015.

984 David Sanger, Keynote Address, CyCon 2016, Tallinn, Estonia, June 3, 2016.

arsenal of the most powerful cyber weapons on Earth. Their development would be for use as a component of any future military campaign. How and when these capabilities will be used outside armed conflict is uncertain. Congressman Jim Himes, ranking member of the House Intelligence subcommittee on Cybersecurity, asked "What is the legitimate retaliation for an act of war?" and sums up the current predicament well in stating "In place of norms and definitions you've just got a series of endless question marks. That's a dangerous world because uncertainty in this world equals risk."[985] So it appears today, for at least the United States, in accordance with the principle of necessity, all peaceful alternatives must be exhausted before a resort to force.[986] This staunch policy most likely means attackers will continue to believe there is "little price to pay" for their malicious activity, and the strategy of deterrence by retaliation will remain an insufficient strategic cyber deterrence option. In sum, the shortcomings of deterrence by retaliation if used in cybered conflict have unconvincing means, limited real effects, and questionable resolve.

---

[985] Danny Vinik, "America's Secret Arsenal," *Politico*, The Agenda: The Cyber Issue, December 9, 2015.

[986] Office of General Counsel, *Department of Defense Law of War Manual*, June 2015 (Updated December 2016): 42.

CHAPTER V

Deterrence by Denial

The strategy of deterrence by denial of benefit from undesired activity seeks to convince any malicious actor that their undesired behavior will fail to achieve their desired outcome or simpler still, seeks to deny their success. The U.S. Defense Department Chief Information Officer tacitly endorsed this strategy in stating "one of the best ways to reduce the cyber threat is to make it harder and more costly for adversaries to initiate attacks."[987] He opines that innovative security measures along with strategic security planning and training could make launching attacks on Departmental resources time-consuming and futile. Since deterrence is partially a function of perception, the strategic option of denial works in the mind of the adversary by decreasing the likelihood that an intended attack will succeed. Deterrence by denial focuses on increasing capabilities to defend networks and systems from cyber attack by any actor, no matter whether that actor is a nation state, hacker group, criminal organization, or terrorist group. In their 2015 Cyber Strategy, the U.S. Defense Department recognizes the importance of working with other departments, agencies, international allies and partners, and also the private sector to strengthen deterrence by denial through improved cyber security.[988] In doing so, the development and implementation of effective protective measures deny any potential attacker the benefit of succeeding.

However in the current threat landscape, cyber attacks seriously challenge the strategic option of deterrence by denial. The incidents seen today range from basic criminal schemes to massive denial of service attacks to sophisticated (and sometimes destructive) intrusions into critical infrastructure networks and systems. Most of the headlines focus on data breeches in government and across the spectrum of industries, and rightfully so, as the number of identities

[987] John Edwards and Eve Keiser, "Raising the cost of cyberattacks," *C4ISR& NETWORKS,* July/August 2015: 12.

[988] Ash Carter, Secretary of Defense, "The DoD Cyber Strategy," April 17, 2015: 10-11.

that have been exposed through these breaches over the past three years alone surpasses one billion.[989] The economic impact can be immediate with the theft of money or long term with the loss of intellectual property. The success of malicious actors in cyberspace is partly due to the weakest link in defense, the behavior of users combined with the effectiveness of social engineering methods, such as reconnaissance based spear phishing which can lead to exploit execution or compromised passwords. The latter can be leveraged in second generation activity, such as in recent government breaches in the United States where illegally obtained valid credentials were acquired by social engineering methods.[990] Once the actor gets inside the organization, only 31 percent of victims discover the breach by internal means and for the rest alerts can come months later after stolen property is found in the wild.[991] Although encouraging news comes from a 2015 report by the Online Trust Alliance that contends 90 percent of recent breaches could have been prevented if organizations had implemented the most basic cyber security best practices.[992]

Protective measures to reduce risk and enhance security include the promulgation of security strategies, the implementation of security controls, and the sharing of cyber threat information. The strategy of deterrence by denial seeks to change the cost-benefit calculations of a malicious actor by credibly signaling, or proving, that an attack will fail.[993] Security strategies articulate proven models for the identification and deployment of defensive capabilities, such as security controls or best practices. The use of cyber security frameworks result in the selection of risk-informed investments in these security controls and associated security solution products,

[989] Adam Bromwich, Symantec, "Emerging Cyber Threats to the United States," Testimony before House Committee on Homeland Security, February 25, 2016.

[990] John Zarour, "How to avoid becoming the next OPM," *GCN Magazine,* August 2015: 12.

[991] Mandiant, "M Trends 2015: A View from the Front Lines," Threat Report, 2015: 2-3.

[992] Online Trust Alliance, "OTA Determines Over 90% of Data Breaches in 2014 Could Have Been Prevented," Press Releases, January 21, 2015.

[993] Peter Roberts and Andrew Hardie, "The Validity of Deterrence in the Twenty-First Century," Royal United Services Institute, Occasional Paper, August 2015: 20.

which are ideally enhanced by shared cyber threat information. Preferably these security controls and solutions are deployed to block, detect, and interrupt the actor at the various phases of the cyber kill chain. Through risk management, the strategic selection and positioning of credible capabilities along the attack process offers the fluid form of deterrence aptly named denial of benefit. This chapter starts with an illustrative case that depicts the unfortunate failure of deterrence by denial of benefit, or of success. It then examines an assortment of promising protective measures and by what degree through risk management they improve the security of networks and systems to deny malicious actors the benefit of attack.

Illustrative Case of Security Vulnerabilities

In June 2015, the U.S. Office of Personnel Management (OPM) revealed that based on incident detection and forensic investigation that a cyber intrusion affecting information technology systems and data may have compromised the personnel information of approximately 4 million former and current federal employees.[994] A month later, OPM reported a separate incident targeting databases housing background investigation records of 21.5 million individuals.[995] According to US-CERT, the first hack of OPM systems occurred in July 2012. The attacker stole manuals and IT architecture information. That breach was halted by OPM after almost two years and reported to Congress.[996] Then in May 2014, a second, most likely related, attacker established a foothold in the OPM network and moved to the security clearance database, which exposed Standard Form 86 data entries where applicants list contacts and relatives, mental illness, drug and alcohol abuse, past arrests, bankruptcies and more. That

[994] Office of Personnel Management, "OPM to Notify Employees of Cybersecurity Incident," News Release, June 4, 2015.

[995] Kirstin Finklea, "Cyber Intrusion into U.S. Office of Personnel Management: In Brief," Congressional Research Service, CRS Report R44111, July 17, 2015.

[996] Committee on Oversight and Government Reform, U.S. House of Representatives, 114th Congress, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," Timeline of Key Events, September 7, 2016: 5-13.

security data revealed the identities of almost everyone who has gotten a United States security clearance.[997] The second attacker then moved laterally to breach systems maintained at a Department of Interior shared data center in October 2014, which resulted in the loss of files for every federal employee, every federal retiree, and up to one million former federal employees. The hackers stole military records and veterans' status information, address, birth date, pay history, insurance and pension information, and age, gender and race data.[998] Then in March 2015, the second attacker stole the fingerprint data of 5.6 million federal employees. Collectively the personnel records provide a foreign government with the ability to blackmail or impersonate federal employees to gain access to classified information or computer networks.

Finally in April 2015, OPM reported to US-CERT an unknown Secure Sockets Layer (SSL) certificate beaconing to an unknown site and deployed first Cylance V and later Cylance Protect security solutions which identified malware used by the second attacker. A week later, a product demo by CyTech Services of a network forensics software package also found malware embedded on the network.[999] Further forensics indicated the second attacker stole access credentials from the contractor KeyPoint and used those credentials to break into OPM systems.[1000] This finding makes sense for according to an inspector general report outsiders entering the OPM system were not subjected to multifactor authentication, where for example a code would be sent to a cellphone to be entered before giving a user access to a system. A host of deficiencies left OPM open to attack, for instance it did not have an inventory of all computer servers and devices with access to its network nor did it regularly scan for vulnerabilities in the

---

[997] Ken Dilanian and Ted Bridis, "U.S. Officials: Second Hack Exposed Military and Intel Data," *Associated Press*, June 13, 2015.

[998] Ken Dilanian, "Union Says All Federal Workers Fell Victim to Hackers," *Associated Press,* June 12, 2015.

[999] Sean Gallagher, "Report: Hack of government employee records discovered by product demo," Arstechnica, Risk Assessment/ Security & Hacktivism Blog, June 11, 2015.

[1000] Charles Hall, "How OPM Could Have Avoided the Data Breach," CTOvision, CTO Blog, June 30, 2015.

system.[1001] Consequently in the first attack, it is possible that OPM was breached through an unpatched vulnerability. Overall OPM suffered from an antiquated cybersecurity infrastructure, abysmal security practices, and ill-equipped personnel. If OPM had implemented proper IT governance practices, used encryption and assigned least privilege user access, the organization could have pushed the attacker closer to a threshold where the cost of resources outweighed the benefit of the data.[1002]

The Director of National Intelligence said Chinese hackers are the leading suspect in the OPM intrusion. To which a spokesman for the Chinese Embassy in Washington responded "we hope relevant parties of the U.S. side can stop making unfounded and hypothetical accusations, and work constructively with China to address cybersecurity issues."[1003] Even though forensic evidence leaves little doubt that China was responsible, the Obama administration chose not to make any official assertion about attribution due to concern over exposing details of the United States "own espionage and cyber capabilities" and ongoing diplomatic engagements.[1004] Even more so, the response to penetrations targeting government held data have been restrained, in part because such breaches are regarded as within traditional parameters of espionage. Seen as fair game, the former head of the Central Intelligence Agency said "This is espionage" and "I don't blame the Chinese for this at all. If I [as head of the National Security Agency] could have done it, I would have done it in a heartbeat."[1005] Instead, President Obama vowed to bolster

[1001] David E. Sanger, Julie Hirschfeld Davis and Nicole Perlroth, "U.S. Was Warned of System Open to Cyberattacks," *The New York Times*, June 5, 2015.

[1002] The Institute for Critical Infrastructure Technology, "Handing Over the Keys to the Castle," Technical Report, July 2015.

[1003] Damian Paletta and Danny Yadron, "Over 21 Million Hit by Hack," *The Wall Street Journal*, July 10, 2015.

[1004] Ellen Nakashima, "U.S. Not Naming China in Data Hack," *The Washington Post*, July 22, 2015.

[1005] Ibid.

cyber defenses to deny benefit of attack, saying the United States has old computer systems with "significant vulnerabilities" and needs to be "much more aggressive" in stepping up defenses.[1006]

Cyber warfare author Jeffrey Carr agreed that the way to fix the administration's cybersecurity problem is not to retaliate against a foreign government since digital espionage is the new normal. Carr believes that "deterrence is possible" but "doesn't come from force or trying to instill fear," instead from "enabling security protocols that make sensitive or valuable data so hard to steal that the effort isn't worth the effort."[1007] That means a complete overhaul of how the government employs protective measures, ferreting out weaknesses in security and correcting them, or building new security by-design at greater costs. No one should have been surprised by the OPM hacks. The inspector general audit in 2014 had found serious flaws in the network and the way it was managed. OPM is a monolithic agency run by politically appointed leaders who lack the expertise to make informed decisions on protective measures. Leadership needs to understand and appreciate cyber risk so they can authorize their IT security department to develop and deploy defenses against cyber threats.[1008] At OPM, the director eventually resigned after political pressure from Congress during the fall out investigation.[1009] In retrospect, the national security consequences of a successful hack at OPM should not have been a surprise. The signs were all there for it to happen, as it had the vulnerabilities, no security focused leadership, and a capable and motivated malicious actor that was not convinced their attacks

---

1006 Jeff Mason and Mark Hosenball, "Obama Vows to Boost U.S. Cyber Defenses, Amid Signs of China Hacking," *Reuters*, June 8, 2015.

1007 Jeffrey Carr, "Cyber Attacks: Why Retaliating Against China Is the Wrong Reaction," *The Diplomat*, August 6, 2015.

1008 Adam Rice, "Warnings, Neglect and a Massive Breach," *Information Security Magazine*, September 2015: 24-28.

1009 Mark Hosenball and Roberta Rampton, "U.S. personnel agency chief resigns over massive data breach," *Reuters*, July 10, 2015.

would fail.[1010] After a House Committee investigation, Representative Jason Chaffetz noted "with some basic hygiene, some good tools, an awareness and some talent, they [OPM] really could have prevented this."[1011]

Security Strategies

The lessons of the OPM hack can be applied in a range of protective measures that attempt to reduce cyber risk. These start with the development of cyber security strategies for the placement of defensive capabilities. Traditionally organizations focus their defenses at the perimeter of the network in the belief that this strategy makes it difficult for an attacker to penetrate systems. Typical passive defenses at the perimeter, like Anti-Virus software, which detect known malware signatures, and Blacklists, which blocks known malicious websites, have become less effective as the volume and complexity of threats increases.[1012] Once the perimeter is breached, as often occurs, the attackers have free reign within the network. In a test by the security industry firm FireEye, network and email appliances were placed among 1,216 organizations in 63 countries across more than 20 industries from October 2013 to March 2014. Analysis of the data generated from the trial deployments of the appliances revealed that 97 percent of the organizations had been breached and more than 75 percent of the organizations had active command-and-control communications between their internal systems and outside servers, meaning that the attackers had control of the breached systems and were exfiltrating data from them.[1013] To compensate for the failure of one layer of the system, like at the perimeter, organizations use a multi-layer security strategy aptly named defense-in-depth.

[1010] Forrester Research, Inc, "Quick Take: 12 Lessons For Security & Risk Pros From the US OPM Breach," White Paper, June 8, 2015: 1-10.

[1011] Eric Tucker, "Report Details Missed Opportunities To Stop OPM Cyber Breach," *Associated Press*, September 7, 2016.

[1012] Lumension, "Redefining Defense-in-Depth," White Paper, March 2014: 1-6.

[1013] FireEye, Inc. "Cybersecurity's Maginot Line: A Real World Assessment of the Defense-in-Depth Model," Report, 2014: 1-10.

Defense-in-depth strategies emphasize multiple, overlapping, and mutually supportive defenses, such as security controls or best practices, to guard against single-point failures in any specific technology or protection method. Security controls are synonymous with safeguards and countermeasures, which may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.[1014] A defense-in-depth strategy also accentuates the continual deployment of defenses to protect multiple threat points, including network, endpoint, web, and email security.[1015] In designing a multi-layered security infrastructure, numerous security controls and best practices can be implemented by an organization. One way to consider implementing controls is by using preventive and detective categories at the data, application, host, network, and physical layers. The security industry firm Tripwire offers here some of the main controls and where to consider for implementation:[1016]

Preventive Security Controls

- Encryption (Data layer) = encrypt sensitive information whether at rest or in transit.
- User Access Control (Data, Host layers) = access rights reflect level users require.
- Software Patching (Application layer) = update with latest software patch releases.
- Malware Detection (Host layer) = install software to identify and prevent malware.
- System Hardening (Application, Host, Network layers) = remove default user accounts and passwords, remove unnecessary services, and adjust permissions.
- Network Access Control (Network layer) = isolate sensitive systems from main network into secure segments with strict access rules.
- Security Awareness Training (Physical layer) = train users to recognize threats.

[1014] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, Appendix B, (Washington, DC: US Department of Commerce, April 2013): B-20.

[1015] McAfee, “Counter Stealth Attacks,” Santa Clara, California, 2013: 1-3.

[1016] Tripwire, “Layered Security: Protecting Your Data in Today’s Threat Landscape,” White Paper, Brian Honan, 2014.

– Policies/Procedures (Physical layer) = publish user roles and penalties if ignored.

Detective Security Controls

– File Integrity Monitoring (Data, Application, Host Layers) = regularly monitor for replacements of or changes to critical system files.
– Vulnerability Management (Application, Host, Network layers) = regular testing to identify vulnerabilities in software, configurations or processes.
– Change Control (Application, Host, Network layers) = actively monitoring for unauthorized changes on key systems.
– Incident Alerting (Host, Network Layers) = Identify suspicious activity and be alerted to it by intrusion detection/prevention systems.
– Log Monitoring (Data, Application, Host, Network layers) = monitor log files for unusual entries or certain security events.
– Security Configuration Management (Network Layer) = secure new systems or applications that are added to the infrastructure.

It should be obvious there is no one solution in an increasingly sophisticated and complex threat landscape. The security strategy of defense-in-depth offers a multi-layered security approach in which a combination of integrated technologies attempt to provide protection and detection against known, unknown and advanced malware and threats.[1017] Defense-in-depth is widely accepted by industry and the military as a way to enhance cyber defensive capabilities through layered sensors and countermeasures.[1018] For example the U.S. Navy has released new

[1017] Kaspersky, "Future Risks: Be Prepared," Special Report, Kaspersky Lab, 2014: 1-11.

[1018] Vice Admiral Jan E. Tighe, USN, Commander, U.S. Fleet Cyber Command, "Cyber Operations: Improving the Military Cyber Security Posture in an Uncertain Threat Environment," Testimony before House Armed Services Committee, March 4, 2015.

cyber standards that specifically require a defense-in-depth approach.[1019] Ideally these defenses are configured by leveraging industry security products informed by cyber threat intelligence.

Cyber Threat Intelligence

To effectively defend against cyber attacks an organization needs access to synthesized information about specific threats to specific targets. The fused product called cyber threat intelligence consists of threat information on malicious actor tactics, techniques, and procedures plus suggested actions to counter an attack and also threat indicators that an attack is imminent, is underway or that compromise may have already occurred. Cyber threat intelligence provides the ability to recognize and act upon this information or indicators, of attack and compromise, in a timely manner. Indicators of attack represent early warning signs, such as code execution, persistence, command and control, or lateral movement. Indicators of compromise show the presence of malware, signatures, exploits, vulnerabilities, or IP addresses.[1020] To be effective cyber threat intelligence exhibits the characteristics of timely: delivered rapidly to provide opportunity for the recipient to anticipate the threat and prepare a suitable response; relevant: applicable to recipient operating environment to address likely threats; and actionable: identifies actions the recipient can take to counter the threat.

For security teams trying to implement and manage security controls to thwart cyber attacks, threat intelligence can make a difference in risk management. The addition of threat intelligence in a security program can provide information and indicators to prioritize and adjust security controls to stop the latest attacks.[1021] For example a Fortune 100 financial services organization that faces 250,000 threats a day recently incorporated a threat intelligence platform

---

[1019] Sydney J. Freedberg, Jr. "Navy issues new Cybersecurity Standards – with more to come," *Breaking Defense*, February 22, 2016.

[1020] Crowdstrike, "Indicators of Attack versus Indicators of Compromise," White Paper, 2015: 3.

[1021] Nick Lewis, "How Threat Intelligence Can Give Enterprise Security the Upper Hand," E-Guide, *Tech Target*, 2015: 2-5.

to aggregate threat data and integrate existing security tools.[1022] In a 2016 institute survey of Information Technology security practitioners in the United States involved in endpoint security in a variety of organizations, 77 percent say they have added or plan to adopt a threat intelligence component.[1023] However an organization needs not only access to timely, relevant, and actionable cyber threat intelligence but also the ability to act on that intelligence. Security vendors gather information about active threats and use that information to inform their industry security products. Many security solution products have been optimized to integrate or incorporate threat intelligence data feeds. For example the IBM X-Force research team develops threat intelligence and countermeasure technologies for IBM products.

The IBM X-Force team monitors global threats around the clock to understand the latest vulnerabilities and exploit techniques. They use fully automated web crawlers to inspect millions of web sites every day to build a URL reputation data base. They also leverage intelligence to categorize IP addresses into threat categories, including malware hosts, spam sources, dynamic IPs, anonymous proxies, botnet command and control servers, and scanning IPs, with reputation scores that assist in traffic blocking decisions. In addition, the team categorizes web applications by threat origination and tracks security vulnerabilities. Other organizations can leverage the latest X-Force research through the IBM X-Force Exchange, launched in 2015 to share evidence and discoveries.[1024] Or organizations can view on-demand webcasts by the threat research team on topics such as trends and findings in volume of attacks, affected industries, prevalent types of attacks, and the key factors enabling them.[1025] Products within the IBM Security portfolio have been optimized to integrate or incorporate X-Force capabilities, such as the IBM Security Network Intrusion Prevention System uses X-Force feeds for URL filtering, IP source blocking,

---

[1022] Threat Connect, “A Financial Giant’s Threat Intel Success Story,” Case Study, August 2016.

[1023] Ponemon Institute, “2016 State of Endpoint Report,” April 2016: 15.

[1024] IBM Corporation, “Combat the latest security attacks with global threat intelligence,” White Paper, 2016: 1-10.

[1025] Nick Bradley and Michelle Alvarez, “IBM X-Force 2016 Cyber Security Intelligence Index Webcast,” IBM Security, August 5, 2016.

application action control, and virtual patch shielding of observed vulnerabilities.[1026] It is no surprise that in a 2015 SANS institute survey of organizations, 54 percent of them use intrusion monitoring platforms to accept and consolidate cyber threat intelligence feeds.[1027] The challenge for deterrence by denial is the percent of organizations that do not use these feeds.

Cyber Kill Chain

Layering controls informed by cyber threat intelligence provide reinforcing protections that attempt to halt attacks in progress. Yet before an organization can hope to thwart its adversaries and convince them that their efforts are futile, the organization must understand the adversary's attack methods. One of the most popular models of the methods used in the cyber attack process is the "intrusion kill chain" first popularized in a 2011 paper by Lockheed Martin researchers.[1028] A kill chain is a systematic process to target and engage an adversary to create a desired outcome. The integrated, end-to-end process is described as a "chain" because any one interuption will break the entire process. The intrusion or simply cyber kill chain is identified in seven phases, specifically consisting of reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. The phases describe the sequence of activities used by malicious actors, with specific tools and techniques within each phase, to obtain essential objectives required to proceed to the next phase in a cyber attack.[1029] Definitions for the kill chain phases are stated as:

[1026] IBM Corporation, "Security Network Intrusion Prevention System," Data Sheet, 2013: 1-6.

[1027] Dave Shackleford, "Who's Using Cyberthreat Intelligence and How?" A SANS Survey, February 2015: 10.

[1028] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, March 2011: 4.

[1029] Markus Maybaum, "Technical Methods, Techniques, Tools and Effects of Cyber Operations," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 103-131.

Cyber Kill Chain

1. Reconnaissance = harvesting email addresses, social relationships, and information on specific technologies.
2. Weaponization = coupling an exploit with a Remote Access Trojan into a deliverable payload.
3. Delivery = transmission of the weapon to the victim via email, web, usb, or mobile device.
4. Exploitation = of application or operating system vulnerability or an operating system feature to execute code.
5. Installation = of malware on the asset to maintain persistence.
6. Command and Control = for remote manipulation of victim's system.
7. Action on Objectives = intruders use hands on access inside the target environment to accomplish their goal. [1030]

The cyber kill chain becomes a model for defense when defenders align defensive capabilities, such as security controls or best practices, to the specific processes that a malicious actor undertakes to target and engage the victim's system. A defensive actions matrix can be constructed to identify and inject solutions and procedures that can impact an attacker's progress at various phases of the kill chain. For example, the use of Software Patching denies the Exploitation phase and Malware Detection products stop the Installation phase. Security firms will analyze real world attacks and offer suggestions on where their industry products or practices could detect, deny, disrupt, or contain an attack at each phase of the cyber kill chain. For example, Dell SecureWorks has examined the 2013 attack on Target Corporation to provide recommendations for securing Point-of-Sale (POS) systems. The Dell suggestions are similar to

[1030] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, March 2011: 4-5.

the preventive and detective security controls listed above, but also include an assortment of solutions and procedures at the particular kill chain phase stated as:

Defensive Actions Matrix (2013 Target Breach)

- Database Security (Reconnaissance) = manage and audit database accounts.
- Threat Intelligence (Weaponization) = leverage external and internal sources to gain visibility into specific types of attacks and indicators to detect these attacks.
- Application Whitelisting (Delivery) = limit sets of software that can be run on system.
- Endpoint Malware Protection (Exploitation) = antivirus and host intrusion prevention system identify and block malicious malware.
- Two-factor Authentication (Installation) = reduce effectiveness of password stealing and cracking attempts.
- Network Intrusion Detection System (Command and Control) = identify traffic patterns matching scanning, malware C2 communication and data exfiltration.
- Data Loss Prevention (Actions on Objective) = use information tagging, packet inspection, and network monitoring to identify movement of sensitive data. [1031]

However the trouble with using a patchwork of legacy solutions, called "best of breed" from multiple vendors, is they take manual intervention once a breach occurs. The use of point products also makes it difficult to coordinate and share intelligence among various devices. For example, if a sandbox device, which isolates and runs suspicious code, detects an unknown threat, it might not automatically share indicators with an Intrusion Prevention System, which detects malware. Therefore prominent leaders in the cyber security industry recommend use of their integrated and automated products to act across the cyber kill chain. For example, Palo Alto Networks presents its Next-Generation Security Platform as a multi-layered defense solution that integrates next-generation firewalls, cloud-based threat intelligence and advanced endpoint

[1031] Dell SecureWorks, "Inside a Targeted Point-of-Sale Data Breach", White Paper, January 24, 2014: 1-18.

protection. The Next-Generation platform inspects all network traffic and offers many security features designed to prevent and detect at every phase of the cyber kill chain wherever the organization's data may reside: in the cloud, on premise, in the network and on the endpoint.[1032] The WildFire intelligence cloud, a custom-built evasion-resistant virtual environment that uses hundreds of behavioral characteristics, static indicators and machine learning, inspects all files passing through the platform in order to prevent and detect known and unknown malware and exploits.[1033] The Palo Alto Networks platform integrates the process of prevention and detection down the kill chain so that network defenders do not have to do it themselves. It does that by establishing a system-of-systems that communicate with each other within the platform and integrates a host of third party tools behind the scenes in an effort to reduce the workload of all network defenders.[1034]

Solutions like the Palo Alto Networks Platform attempt to deny the benefit of an attack. In a cyber intrusion the real benefit to the attacker is the exfiltration of data at last stage in the kill chain. Critics of the cyber kill chain philosophy argue that too much emphasis is on the early stages which take relatively little time, whereas the final steps by the attacker can take months.[1035] In support of that notion, Black Hat 2016 attendees were told the popular cyber kill chain “doesn’t focus enough on what to do after adversaries break into networks successfully, which they inevitable will do.”[1036] Another prevalent counter point is the list of attack vectors is longer than those covered by the chain model, like the insider threat. Admittedly the kill chain is more suited to preventing intrusion and a highly determined and skilled attacker will find a way into the system. Therefore focusing on detecting ongoing attacks in the final stages of Command and Control and also Actions on Objectives is imperative before the damage is done. This

[1032] Palo Alto Networks, “Firewall Overview,” Data Sheet, 2016: 1-6.

[1033] Palo Alto Networks, “WildFire,” Data Sheet, 2017: 1-3.

[1034] Palo Alto Networks, “Breaking the Cyber Attack Lifecycle,” White Paper, March 2015: 1-6.

[1035] Giora Engel, “Deconstructing the Cyber Kill Chain,” Dark Reading, November 18, 2014.

[1036] Tim Greene, “Why the ‘cyber kill chain’ needs an upgrade,” *Computer World*, August 8, 2016.

requires detective security controls that automatically detect and analyze subtle changes in user and computer behavior, like File Integrity Monitoring, Change Control and Log Monitoring.

Security Controls

Guidance for the identification and application of protective measures in the form of security controls are contained in a variety of security frameworks. Security controls are safeguards or countermeasure "prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information."[1037] Security controls can be found in the National Institute of Standards and Technology (NIST) Special Publication 800-53. In many cases the controls identify industry best practices, also informally promulgated by leading security firms in annual reports. For example, Symantec Corporation publishes Best Practice Guidelines for Businesses and for Consumers. In the first category suggestions include use encryption to protect sensitive data, implement a removable media policy, be aggressive in updating and patching, enforce an effective password policy, and restrict email attachments. For the latter, recommendations include think before you click, guard your personal data, protect yourself and update regularly. In reviewing a number of good external best practice guidelines, Symantec specifically endorses the Critical Security Controls maintained by the Center for Internet Security and also the Cybersecurity Framework produced by NIST.[1038]

<u>Critical Security Controls</u>

The Critical Security Controls (CSC) is a framework that offers safeguards for computer security based on the combined knowledge of actual attacks and effective defenses.[1039] Twenty

---

[1037] National Institute of Standards and Technology, "Glossary of Key Information Security Terms," NISTIR 7298 Revision 2, May 2013: 176.

[1038] Symantec Corporation, "Internet Security Threat Report 2014," Volume 19, 2014: 86-93.

[1039] Center for Internet Security, "The CIS Critical Security Controls for Effective Cyber Defense," Version 6.1, August 31, 2016.

sets of safeguards are suggested to detect, prevent, and mitigate damage from the most common attacks. The goal of the CSCs is to protect critical assets and information by strengthening an organization's defensive posture through continuous, automated protection and monitoring of information technology infrastructure. Thus the controls attempt to deny benefit of attack by monitoring networks and systems, detecting attack attempts, identifying compromised machines, and interrupting infiltration. An organization implements, automates, and measures the effectiveness of each CSC through the application of sub-Controls that are categorized as either "Foundational" or "Advanced" as an aid to prioritization and planning.[1040] The CSCs also identify applicable commercial tools to detect, track, control, prevent, and correct weaknesses or misuse at threat points.[1041] Suggested security tools listed by control range from Network Access Control, Vulnerability Assessment, Application Whitelisting, and Intrusion Prevention Systems to Web Application Firewalls, Patch Management, Data Loss Prevention and Encryption.[1042] Many security solution firms map their products against the CSCs to illustrate how their features and capabilities meet safeguard requirements.[1043]

The first four CSCs (#1-4) alone are seen as especially very valuable by organizations such as the National Security Agency that rates them 'very high' in mitigation capability and 'high' in technical maturity. They directly address risk management, starting with Device (#1) and Software (#2) Inventory, Secure Configurations (#3), and Continuous Vulnerability Assessment and Remediation (#4), across a large number of systems in an enterprise. An organization could reduce the impact of cyber threats on the confidentiality, integrity and

---

1040 Robin Regnier, "Announcing Version 6.1 of the Critical Security Controls," Center for Internet Security, CIS Controls Adopter Communications, September 23, 2016.

1041 John Pescatore and Tony Sager, "Critical Security Controls Survey: Moving From Awareness to Action," A SANS Whitepaper, June 2013.

1042 SANS Institute, "Critical Security Controls Solution Providers and Critical Security Controls for Effective Cyber Defense," Poster – 31st Edition, Fall 2014.

1043 Tripwire, "The CIS Critical Security Controls and Tripwire Solutions," Solution Brief, 2017: 1-4, and McAfee, "Conquer the Top 20 Critical Security Controls," White Paper, 2104: 1-9.

availability of information through proper project planning, resource allocation and prioritization based on CSCs #1-4. This assertion can be affirmed in analyzing data breaches of four major U.S. technology firms, namely Twitter, Facebook, Apple and Microsoft, in February 2013 resulting from vulnerabilities in the Java application. In each situation the attacker following the pattern of the intrusion kill chain; discovering software weakness (reconnaissance), writing exploit code (weaponization), posting the code on a "watering hole" website (delivery), luring victims to the site (exploitation), downloading attack code (installation), compromising the victim's computers (command & control), and getting what they wanted (actions on objective). CSCs #1-4 could have prevented attack success at various points of the kill chain, through baseline device control, application version updating, forbidding code execution from untrusted websites, noting configuration changes, and scanning systems for vulnerable applications in outdated versions of Java.[1044]

Application of best practices like patch management, contained in CSC #4 for Continuous Vulnerability Assessment and Remediation, can only prevent attacks if used, as evidenced in the compromise of computers in the NetTraveler cyber espionage campaign. The malware infected more than 350 victims in 40 countries from 2005 through 2013.[1045] NetTraveler exploits two well-known vulnerabilities in Microsoft office, a Windows Common Controls bug (CVE-2012-0158) and flaws in MS Word (CVE-2010-3333), both patched for these errors years ago. All the victims had to do was patch their systems to prevent exploitation. Instead, the advanced persistent threat group using NetTraveler stole more than 22 gigabytes of data from their victims.[1046] Likewise, application of the best practice of removable media policy implementation, contained in CSC#8 for Malware Defenses, could have prevented an attack like

---

[1044] SANS Analyst Program, "Reducing Risk Through Prevention: Implementing Critical Security Controls 1-4," White Paper, James Tarala, June 2013: 1-12.

[1045] Kaspersky Global Research and Analysis Team, "The NetTraveler (aka Travnet)," 2013: 1-25.

[1046] Kelly Jackson Higgins, "NetTraveler Cyberespionage Campaign Uncovered," *Dark Reading*, June 4, 2013.

Stuxnet, where the virus was delivered by thumb drives used by contractors working at the Iranian nuclear enrichment facility. The Critical Security Controls were crafted to answer the question: "Where should I start to improve my cyber defenses?"[1047] Their implementation in order could deny attack benefit as they prioritize and focus on a small number of actionable controls with a high potential payoff. The first five alone provide effective defense against 80 percent of attacks.[1048] The 2016 NTT Group provides further guidance for practical application of security controls to the cyber kill chain.[1049] The challenge for deterrence by denial is the number of organizations that do not use the controls.

Cybersecurity Framework

In 2013, President Obama declared that the cyber threat to critical infrastructure represents one of the most serious challenges to national security. Therefore to enhance the security and resilience of National infrastructure, he signed Executive Order 13636 for "Improving Critical Infrastructure Cybersecurity." The Order directs the development of a "Cybersecurity Framework" to reduce cyber risks to critical infrastructure. A Framework can provide direction, focus and guidance to not just reduce risk, but also reduce downtime.[1050] The Order mandates that the Framework shall include a set of standards and procedures that align policy, business, and technological ways to address cyber risks. To help identify, assess, and manage cyber risk, the Framework is intended to provide a prioritized, performance-based, and cost-effective approach, including information security measures and controls. It will provide technology neutral guidance so users benefit from a competitive market for products and

[1047] Center for Internet Security, "Practical Guidance for Implementing the CIS Critical Security Controls (V6)," Version 6.1, September 23, 2016: 1.

[1048] Ibid, 3.

[1049] Solutionary, "Global Threat Intelligence Report," 2016 NTT Group, 21-46.

[1050] James Michael Stewart, "Cybersecurity Frameworks to Consider for Organization-wide Integration, *Global Knowledge*, 2016: 1-8.

services.[1051] The inaugural Cybersecurity Framework was released one year later in February 2014 by the National Institute of Standards and Technology (NIST). It is constructed around a Framework Core containing a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. The Framework incorporates international voluntary consensus standards and industry best practices to accomplish activities under the functions. The Critical Security Controls are part of the Framework's informative references.[1052]

Leading companies attest that the Framework has enhanced their ability to set security priorities, develop capital and operational expenditure budgets and deploy security solutions.[1053] Their endorsement stems from use of the Framework Profile "characterized as the alignment of standards and practices to the Framework Core in a particular implementation scenario."[1054] The Profile enables organizations to establish a roadmap that is aligned with business objectives, regulatory requirements, and risk management priorities. An organization first creates an "as is" Current Profile by reviewing all the Categories and Subcategories in the Core, and after assessing emerging cyber threats, develops a "to be" Target Profile. The organization then compares the Current and Target Profile to determine gaps in Security Controls. Next after a cost/benefit analysis of risk tolerance and available resources, they develop and implement an Action Plan to fix gaps.[1055] The risk tolerance is based on an acceptable level of risk for

---

[1051] President Barak Obama, "Improving Critical Infrastructure Cybersecurity," Executive Order 13636, February 12, 2013.

[1052] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, February 12, 2014.

[1053] Intel Corporation, "The Cybersecurity Framework in Action: An Intel Use Case," Solution Brief, 2015: 1-9.

[1054] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, February 12, 2014: 5.

[1055] Ibid, 13-14.

acquisition of products and delivery of services. The former Deputy Homeland Security Secretary, Alejandro Mayorkas, has touted the Framework as a document that has lifted cyber security awareness in private companies. In remarks at the Billington International Cybersecurity Summit, he implored a roomful of global experts to use it as a model for their home governments.[1056]

Information Sharing

Organizations in the same critical infrastructure or industry sector often face malicious actors that use common tactics, techniques and procedures that target the same types of systems and information. One organization's detection of a cyber attack can become another's prevention. When cyber threat information and indicators are exchanged within sharing communities, recipient organizations are able to deploy effective countermeasures that block or detect similar intrusions. For example an organization can use shared knowledge of indicators to disrupt the cyber kill chain. Through identifying indicators and determining where in the chain these indicators occur, defensive strategies and techniques can be applied within the kill chain process. For instance, security controls or solutions can be deployed to disrupt a malicious actor before achieving exploit phase execution. If the actor has already reached the installation phase, then the organization's defensive strategy shifts to detect actor presence on the network or system and craft an effective response. At each phase of the kill chain, shared threat information or indicators help to anticipate actor behavior and deploy defenses. Thus, by the sharing of cyber threat information and indicators, an organization benefits from the collective experience, resources, and capabilities of its peers.[1057]

[1056] Greg Otto, "U.S. officials: World needs to follow our lead on cyber norms," *Fedscoop,* April 5, 2016.

[1057] National Institute of Standards and Technology, *Guide to Cyber Threat Information Sharing,* Special Publication 800-150, (Washington, DC: US Department of Commerce, October 2016): 1-26.

Threat Intelligence Sources

Information alone does not equal intelligence. Intelligence is gained when context is applied to information – giving it meaning and operational significance.[1058] In a survey of over 378 organizations, 57 percent of respondents say the cyber intelligence currently available to their organization is often too stale to enable them to grasp the strategies, motivations, tactics, and location of attackers.[1059] Many lack current intelligence in the form of reports on latest hacker techniques or indicators of compromise that can spot and mitigate threats. So where does current threat intelligence come from? Sources of threat intelligence are found in a variety of places both internal and external to an organization. Internally an organization can create a threat intelligence program using their IDS/IPS, SIEM and AV products and investing in a team of researchers and analysts to process and correlate collected data. This team can review local data logs for malware, incident data, or IP addresses; perform forensic analysis on infected hard drives looking for attack patterns; and analyze login attempts or swipe access into server rooms.[1060] Since internally performing analysis on this magnitude of data is no small task, organizations can subscribe to external threat intelligence services provided by security vendors.[1061] An organization can also take a third option to participate in a sector or an industry specific sharing community and leverage CERT and central government warnings and threat sharing.

In the threat intelligence service option, some commercial providers provide data feeds in standard file formats that can be used in a variety of security platforms from different manufacturers. While other vendors offer levels of service that build upon one another, with the

---

[1058] Core Security, "Attack & Intelligence: Why It Matters," White Paper, 2014: 2.

[1059] Cyveillance, "Intelligence for Security," White Paper, 2015: 12.

[1060] Dan Waddell, "Where to find actionable threat intelligence," GCN Magazine, April 2015: 19.

[1061] Bob Gourley, *The Cyber Threat,* (Create Space Independent Publishing Platform, September 23, 2014): Appendix 2 - 79-85.

base service being a data feed subscription that requires the use of proprietary security appliances, such as FireEye Threat Intelligence. The basic option enhances the value of FireEye Threat Prevention platforms by providing ongoing updates of technical indicators. The most advanced FireEye Intelligence capability provides dossiers on advanced threat groups as well as profiles of targeted industries.[1062] In some cases, a third party security provider will use external feeds to support automated actions, like Hexis Cyber Solutions did in their HawkEye G integrated active cyber defense platform. Key criteria exist for evaluating which threat intelligence service providers are the best fit for an organization's needs. Evaluation points to use in research and comparison include for data feeds – what is the number, focus, format, and source; for equipment – what type, existing or proprietary, can accept the feeds; for alerts/reports – are there real time alerts and industry-specific reports; for price – are subscriptions tiered based on number of users; and for service support – is it timely 24/7/365 telephone access to engineers? The cost of data feed subscriptions is in the range of $1,500 to $10,000 per month depending on number of feeds.[1063]

Sharing Arrangements

Threat information and indicator sharing can and should be an important element in efforts to ensure defenders stay ahead of the threat. In a sharing community arrangement, an enterprise can join, for instance, an Information Sharing and Analysis Center (ISAC) to improve the quantity and quality of available threat information. The concept of the ISAC was introduced and promulgated pursuant to Presidential Decision Directive (PDD)-63 signed on May 22, 1998. In PDD-63 the federal government asked each critical infrastructure sector to establish sector specific information sharing organizations to share information about threats and vulnerabilities

[1062] FireEye, "FireEye Threat Intelligence: Get the Intelligence and Context You Need to Help Identify, Block and Respond to Advanced Attacks," Data Sheet, 2016: 1-3

[1063] Ed Tittel, "Five criteria for purchasing threat intelligence services," *Tech Target*, August 7, 2015.

within each sector.[1064] For example the Financial Services (FS) ISAC is a 501(c) 6 nonprofit self-funded organization which has grown to more than 5000 members from various commercial banks, credit unions, brokerage firms, insurance companies, payment centers and trade associations. FS-ISAC sharing activities include the delivery of timely, relevant and actionable cyber and physical email alerts, and also "an anonymous online submission capability to facilitate member sharing of threat, vulnerability and incident information."[1065] The National Cybersecurity and Communications Integration Center coordinates with the ISACs for the federal government on the sharing of information related to cybersecurity risks and incidents.

Substantial barriers to optimal sharing of cyber threat information by private sector entities exist. Their concerns reside in legal liability, antitrust violations, potential misuse, and risks of disclosure, especially of trade secrets and other proprietary information. They often "complain that the federal government does not share its information," in particular classified information and there is "little reciprocity or other incentives" for them "to share with government."[1066] Legislative proposals try to address these common concerns. In 2015 a total of six bills were introduced and reviewed in the U.S. Congress with varying provisions aimed at facilitating sharing of information among private-sector entities and providing protections from liability that might arise from sharing.[1067] Finally on December 18, 2015, President Obama

---

[1064] Executive Office of the President, *Presidential Policy Directive on Critical Infrastructure Protection*, PPD-63, (Washington, DC: The White House, February 12, 2013).

[1065] Gregory T. Garcia, Financial Services Sector Coordinating Council, Testimony before House Committee on Homeland Security, March 4, 2015.

[1066] Sara Sorcher, "Security Pros: Cyberthreat Info-Sharing Won't Be as Effective as Congress Thinks," Christian Science Monitor, June 12, 2015.

[1067] Eric A. Fisher and Stephanie M. Logan, "Cybersecurity and Information Sharing: Comparison of Legislative Proposals in the 114th Congress," Congressional Research Service, Report R44069, June 18, 2015.

signed the Cybersecurity Act of 2015 over the objections of civil liberties groups.[1068] Title 1 of the Act gives antitrust exemptions and liability immunity to companies that send the government cyber threat indicators or defensive measures. The Act states that data will be gathered in a manner that removes "personal information of a specific individual or information that identifies a specific individual not directly related to a cybersecurity threat."[1069] Still industry concerns linger over the bill, mostly on trusting the government on the use or security of the data.[1070] For the government to truly facilitate private sector sharing, it must not just implement privacy safeguards, but also establish viable controls on use, define limitations on liability, and create a value proposition, in regard to cost and risk, or fail to address industry interests and needs.[1071]

Risk Management

Despite ever-improving defenses, the vast array of attack methods will hold networks and systems at risk for years to come. According to the former Director of National Intelligence, "the cyber threat cannot be eliminated; rather, cyber risk must be managed."[1072] The Director is concerned that some private sector entities do not account for foreign cyber threats or the systemic interdependencies between critical infrastructure sectors in their risk calculus. Through

---

[1068] Tai Kopan, "Obama to sign cybersecurity bill as privacy advocates fume," *CNN*, December 18, 2015, and Chris Velazco, "Budget bill heads to President Obama's desk with CISA intact," engadget.com, December 18, 2015.

[1069] U.S. Congress, "Consolidated Appropriations Act, 2016," Division N- Cybersecurity Act of 2015, December 15, 2015: 1728-1770.

[1070] Mike O. Villegas, "How will the Cybersecurity Information Sharing Act affect enterprises?" *Tech Target*, October 21, 2015, and Jason Koebler,. "Lawmakers have snuck CISA into a Bill that is guaranteed to become law," motherboard.com, December 16, 2015.

[1071] Mary Ellen Callahan, "Industry Perspectives on the President's Cybersecurity Information Sharing Proposal," Testimony before House Committee on Homeland Security, March 4, 2015.

[1072] James R. Clapper, "Worldwide Cyber Threats," Statement for the Record for the House Permanent Select Committee on Intelligence, September 10, 2015: 2.

the process of risk management, leaders consider risk to national interests from malicious actors using cyberspace to their advantage. Risk is defined as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of ...adverse impacts... and the likelihood of occurrence."[1073] Risk management is a comprehensive process that requires organizations to "frame risk, assess risk, respond to risk, and monitor risk."[1074] The first component of frame risk or establish a risk context requires an organization to identify assumptions, constraints, tolerance, and priorities or tradeoffs. The purpose of the assess risk component is to identify threats to the organization, internal and external vulnerabilities, the harm that may occur from threats and vulnerabilities in the form of consequences or impacts, and the likelihood that harm will occur.[1075] The purpose of the third component of risk response is to develop, evaluate, determine and implement courses of action for responding to risk. The fourth component addresses how organizations monitor risk over time.

An important factor in deterrence by denial is determining risk tolerance in the risk frame component. Risk tolerance is "the level of risk or degree of uncertainty that is acceptable to organizations."[1076] Risk tolerant organizations may worry about threats experienced by peer organizations and not try to defeat all actors and attack vectors. Whereas less tolerant organizations worry about all threats that are theoretically possible across their attack surface. In regard to risk response, less tolerant organizations most likely prefer mature safeguards and

---

[1073] National Institute of Standards and Technology, "Glossary of Key Information Security Terms," NISTIR 7298 Revision 2, May 2013: 162.

[1074] National Institute of Standards and Technology, *Managing Information Security Risk*, Special Publication 800-39, (Washington, DC: US Department of Commerce, March 2011): 6-43.

[1075] National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, Special Publication 800-30, (Washington, DC: US Department of Commerce, September 2012): 5-13.

[1076] National Institute of Standards and Technology, *Managing Information Security Risk*, Special Publication 800-39, (Washington, DC: US Department of Commerce, March 2011): 14.

countermeasures that have a proven track record. Such organizations may decide to employ multiple safeguards and countermeasures from multiple sources or vendors in a “best of breed” defensive actions matrix. Hence risk tolerance plays a significant role in security solution investment strategies. The strategic investments required to address the risk from high volume bad actors, like volunteer hacktivists or less-skill nation states, are different than the investments needed to address the risk from wicked actors, like advanced persistent threat groups. To address less sophisticated threats, organizations can invest in proven security controls to address known vulnerabilities, whereas for advanced persistent threats, organizations will have to invest in cutting edge technologies over the course of several years.

Risk based decisions manage the potential impact of threats on the confidentiality, integrity, or availability of information that is being processed, stored, or transmitted by information systems. More risk tolerant organizations may concentrate on making investments that provide mission or business gains at the expense of malicious actors gaining benefit from compromising information systems. The massive breaches at Yahoo in 2013 and 2014 affecting 1.5 billion user accounts are an example of “a consistent lack of interest in security”[1077] given “a low priority to defense against hacker threat.”[1078] On the contrary, less tolerant organizations will attempt to deny all benefit of cyber attack, even at the expense of achieving some mission or business goals. For organizations that handle critical or sensitive information the emphasis is on preventing unauthorized disclosure or the loss of confidentiality. In contrast for organizations where the nature of operations or business depends on their functionality, the emphasis will be on maintaining the availability of information while protecting its integrity. Risk response “identifies, evaluates, decides on, and implements appropriate courses of action to accept, avoid,

[1077] Michael Heller, “Yet another Yahoo breach compromises more than 1 billion accounts,” *Tech Target*, December 15, 2016.

[1078] Nichole Perlroth and Vindu Goel, “Yahoo gave hacking threat low priority,” *International New York Times*, September 30, 2016.

mitigate, share or transfer risk."[1079] Courses of action for risk response are evaluated in terms of impact on organization mission or business needs and functions. To avoid risk, an organization might eliminate networked connections and employ an "air gap" between two domains. Risk mitigation can include use of security controls informed by threat intelligence, and of organizational policies, like restricting mobile device or removable media usage.

Risk sharing or transfer is the shifting of risk liability and responsibility to another organization.[1080] An example of risk sharing would be the purchasing of commercial vendor services to protect against volumetric DDoS attacks. In this arrangement, inbound malicious traffic is shifted to commercial servers that can accommodate high bandwidth packet requests. For example, the Akamai network defeats attacks measured in tens, or even hundreds, of Gbps. The Akamai Kona Site Defender deflects DDoS traffic targeted at the network layer. It defines and enforces IP whitelists and blacklists to protect the website. Defender also incorporates a highly scalable Web Application Firewall to absorb DDoS traffic target at the application layer, such as HTTP floods that issue erroneous requests. Over 210,000 edge servers distributed around the world are used to compare application requests to known attack profiles.[1081] The Kona Rule set protects against recent threats, such by Low Orbit Ion Cannon, used by Anonymous, or the Havij SQL injection tool, used by Iranian hacker groups.[1082] The Akamai cloud-based network, used on any given day for 80 percent of U.S. government web traffic, provides another layer of defense-in-depth protection.[1083]

[1079] National Institute of Standards and Technology, *Managing Information Security Risk*, Special Publication 800-39, (Washington, DC: US Department of Commerce, March 2011): 41.

[1080] Ibid, 43.

[1081] Akamai, "Cloud Security Solutions," White Paper, 2015: 1-13.

[1082] Akamai, "Kona Site Defender," Product Brief, 2015: 1-2.

[1083] Tom Ruff, "Nothing Beats Experience," Government Computer Networks, Sponsored Report, May 2016: 5.

An example of risk transfer is the purchase of cyber security insurance. Brokers and underwriters generally consider how companies manage cyber risk when assessing qualifications for coverage. They pay particular attention to company adoption, implementation, and enforcement of cyber security practices and procedures.[1084] If qualified the various elements of a protection policy can include "liability for a security or privacy breach... costs of notifying customers of a breach... losses from business interruption... costs for restoring or replacing lost or damaged data... liability for directors or officer of a company targeted by an attack... and costs associated with settling cyber extortion threats."[1085] Given an ongoing lack of actuarial data, this wide range of factors in writing policies can result in insurance coverage that does not adequately address actual risk, particularly for reputation damage and security remediation associated with large breaches experienced today. For instance the cost related to the theft of 56 million sets of credit and debit card data at Home Depot in 2014 is expected to reach into the billions, with only $100 million covered by insurance.[1086]

Protective Measure Utility

Organizational risk tolerance dictates the selection of risk response courses of action. Protective measures to reduce risk, which include the promulgation of security strategies, the implementation of security controls, and the sharing of cyber threat information, deny to some extent the benefit of attack. However organizations need to have resources and processes in place to implement these protective measures if they are to improve the security of their networks and systems. The data breaches at the Office of Personnel Management illustrate the result of blatant neglect of security strategies. Subsequent recognition of systemic failures at

---

[1084] Thomas Michael Finan, "The Role of Cyber Insurance in Risk Management," Statement of House Committee on Homeland Security, March 22, 2016: 1-11.

[1085] Bipartisan Policy Center, "Cyber Insurance: A Guide for Policymakers," Insurance Task Force, March 2016: 2.

[1086] Gregg Otto, "DHS pushes on towards cyber risk management, insurance," *Fedscoop*, October 2, 2015.

other U.S. government agencies spurred White House declaration of a “30-day Cybersecurity Sprint” to shore up protective measures. As part of the effort, the Federal Chief Information Officer instructed Federal agencies to patch critical vulnerabilities without delay, accelerate implementation of multi-factor authentication, tighten policies for privileged users, and immediately deploy indicators provided by the Department of Homeland Security regarding malicious actor techniques, tactics, and procedures.[1087] The last mandate reiterates that organizations need to know their attackers and the techniques they use to exfiltrate valuable data or conduct denial of service attacks. Federal respondents to an industry survey agree in principle that using threat intelligence is essential to a strong security posture, but nearly a third report their organizations are not able to collect and use it effectively.[1088]

To change the cost-benefit calculations of attackers, security leaders need to think like attackers in the implementation of security controls.[1089] The Critical Security Controls (CSCs) are built on the guiding principle that “offense informs defense,” which means knowledge of actual attacks provide the foundation to build practical defenses. In constructing the CSCs, top experts combined their knowledge of actual cyber attacks and created a consensus list of the most effective techniques to stop them. The CSCs are not limited to blocking compromises, but also can detect, prevent or disrupt attacker’s follow-on actions. It is no wonder the Critical Security Controls figure prominently in the NIST produced “Cybersecurity Framework.” The U.S. Chamber of Commerce believes the Framework is a success. Critical infrastructure sectors and important industry elements are keenly aware of, supportive of, or using the framework or

[1087] Tony Scott, “Enhancing and Strengthening the Federal Government’s Cybersecurity,” Fact Sheet, The White House, June 17, 2015.

[1088] Billy Mitchell, “White House renews push to pass CISA,” *Fedscoop*, October 6, 2015.

[1089] Mike O. Villegas, “Can thinking like cyberattackers improve organizations’ security?” *Tech Target*, September 10, 2015.

similar risk management tools.[1090] The former Senior Director for cybersecurity at the White House says that support for the framework has "exceeded expectations."[1091] Still greater resources are required to grow awareness of the framework and risk based solutions so decisions on investments are made based on risk tolerance for adversary behavior. In a survey of nearly two thousand IT security practitioners in 42 countries, 46 percent say their budgets have increased, to on average $9.14 million annually.[1092] However since the cost of a Remote Access Trojan (RAT Malware) on the underground hacker market ranges from only $5-$10 and an entire Angler Exploit Kit goes for $100-$135[1093] it appears that attackers are winning the cost ratio battle.

The creating of sufficient defense capacities through implementation of security controls in an "offensive informs defense" model requires defenders to learn from each other faster than attackers learn from each other. When considered collectively, the twenty individual ISACs provide shared cyber threat information through systemic outreach and connectivity to approximately 85 percent of U.S. critical infrastructure.[1094] However if private sector recipients find this information to be of little benefit, they are less likely to participate in sharing communities. Cyber threat information needs to be actionable in that it identifies or evokes a response useful for mitigating risk. Shared information may not be useful if it is delayed or provided without context or in the wrong format. It needs to be relevant for use in appropriate

---

[1090] Matthew J. Eggers, U.S. Chamber of Commerce, "Industry Perspectives on the President's Cybersecurity Information-Sharing Proposal," Testimony before the House Homeland Security Committee," March 4, 2015.

[1091] "At eight-month mark, industry praises framework and eyes next steps," *Inside Cybersecurity*, October 6, 2014.

[1092] Ponemon Institute, "2015 Global Study on IT Security Spending & Investments," Report, May 2015: 1-10.

[1093] Dell SecureWorks, "Underground Hacker Markets", Annual Report, April 2016: 4.

[1094] ISAC Council, "The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection," January 2009: 4.

security controls and associated security products to break the cyber kill chain. The usefulness of shared information rests on the nature of threat itself. For example for malware signatures to be useful, there has to be enough time for the signatures to be collected, shared, and inserted into defensive systems of potential future victims before they are attacked. This assumes an attack group will generate a consistent set of signatures that recur in multiple attacks, which likelihood is reduced by polymorphic malware, combined with shifting IP addresses. Many times attack groups evolve to use a new set of exploits and attack vectors with brand new signatures.[1095]

An Insufficient Deterrence Option

Evidence indicates deterrence by denial is not a sufficient strategy to convince malicious actors not to conduct cyber attacks. Current security mechanisms and practices are simply inadequate to achieve deterrence and likely will always be. U.S. Deputy Secretary of Defense Robert Work told a congressional committee that "Cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting government and business activity, and imposing significant costs to the U.S. economy."[1096] Although great strides have been made in Department of Defense cyber security through "the layering of our defenses," so that only about "0.001 percent" of millions of attacks per day are successful,[1097] highly publicized data breaches at Sony Pictures, JP Morgan Chase, Anthem Health Service, and the Office of Personnel Management expose a failure of cyber defenses at civilian companies and government agencies of all sizes. In a 2014 survey of U.S. companies, nearly half experienced a data breach involving the theft of more than 1,000 records,

---

[1095] Martin C. Libicki, "Sharing Information about Threats is not a Cybersecurity Panacea," Testimony before House Homeland Security Committee, RAND Corporation, March 2015: 1-6.
[1096] Robert O. Work, Deputy Secretary of Defense, "Cybersecurity Risks to DoD Networks and Infrastructure," Statement before the Senate Armed Services Committee, September 29, 2015.
[1097] Sandra I. Erwin, "Defense CIO: Cybersecurity Improving But Innovation Lags," *National Defense*, August 8, 2016.

up more than 10 percent from the previous year.[1098] Part of the problem is the utility of protective measures, primarily security strategies, security controls, and information sharing, is diminished by sophisticated attacks that are advanced, targeted, stealthy and persistent. Cyber attacks today unfold in multiple coordinated stages across the cyber kill chain, with calculated steps to get in, establish a foothold, surveil the victim's network and steal data. Malicious actors use a variety of stealthy tactics to evade detection and maintain control of compromised systems.

In response deterrence by denial counts on a defense-in-depth strategy that proposes the layering of multiple technologies combined with best practices, where in theory each layer blocks a different aspect of multi-pronged cyber attacks. For example, at the Delivery phase, device control blocks infected USB devices; at the Exploitation phase, patch and configuration management fixes known vulnerabilities; and at the Installation phase, application control stops unapproved executables.[1099] These defenses are intended to impose cost on the attacker by shutting off their attack vectors. For instance, issue of emergency patches for zero-day vulnerabilities in Flash Player closed off exploitation by the China-based threat group APT3[1100] and by a Russian APT group in Operation Pawn Storm, a spear phishing campaign against political targets in NATO and the United States.[1101] Yet this threat will most likely reconstitute as APT3 has a history of introducing new browser-based, zero day exploits, and the Pawn Storm group has been actively introducing new infrastructure and strategies for eight years.[1102] Consequently, in their yearly observation of cyber attack trends, the security firm Mandiant

---

[1098] Ponemon Institute, "Is your Company ready for a Big Data Breach?" September 2014: 1.

[1099] Lumension, "Preventing Weaponized Malware Payloads in Advanced Persistent Threats," Scottsdale, Arizona, February 2013: 1-4.

[1100] Michael Heller, "Adobe releases emergency Flash zero-day patch," *Tech Target*, June 23, 2015.

[1101] Michael Heller, "Adobe patches Flash zero-day used in foreign ministry attacks," *Tech Target*, October 19, 2015.

[1102] Trend Micro Labs Security, "Operation Pawn Storm Ramps Up it Activities: Targets NATO, White House, Trend Labs Security Intelligence Blog, April 16, 2015.

reaffirms the need for a defense-in-depth strategy in stating that "it is more critical to focus on all aspects of your security posture (people, processes and technologies) than ever before."[1103]

In the wake of the OPM hacks, in October 2015, the White House's Office of Management and Budget released their Cybersecurity Strategy and Implementation Plan (CSIP), which builds off the 30-day Cybersecurity Sprint. The CSIP directs actions to "improve capabilities for identifying and detecting vulnerabilities and threats, enhance protections of assets and information, and further develop robust response and recovery capabilities."[1104] The CSIP emphasizes "the need for a defense-in-depth approach that relies on the layering of people, processes, technologies and operations."[1105] Suggestions in CSIP include to improve security practices and controls around agency high value assets, implement tools to identify risks to systems and networks, advance information sharing on critical vulnerabilities and threats, and acquire innovative commercially available cyber security products and services.[1106] While the initiatives in the Cybersecurity Strategy and Implementation Plan appear promising, Representative Jason Chaffetz reminded Federal Chief Information Officers, in a Letter from the Chairman of the House Committee investigation of the OPM data breach, that "a single vulnerability is all a sophisticated actor needs to steal information, identities, and profoundly damage our national security."[1107]

Consequently it is no surprise that forensic evidence indicates malicious actors are not convinced defenses will deny their success. For instance, the Fortinet Cyber Threat Assessment

---

1103 Mandiant, "M-Trends 2016," Special Report, February 2016: 5.

1104 Shaun Donovan and Tony Scott, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government, Office of Management and Budget, October 30, 2015: 5.

1105 Ibid, 6.

1106 Ibid, 8-20

1107 Committee on Oversight and Government Reform, U.S. House of Representatives, 114th Congress, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," A Letter from the Chairman, September 7, 2016: ii.

Program recorded over 185 million threat events in the period from April 1 to June 30, 2016, meaning many of the events succeeded in getting past traditional security defenses onto the internal network where Fortinet assessment devices were located.[1108] Furthermore, Verizon reports that in 60 percent of cyber incidents, attackers are able to compromise an organization within minutes, while their detection takes months.[1109] These statistics mean threat groups can bypass conventional defenses at will and wander unimpeded to obtain their objectives on the target. The hard reality that attackers can compromise an organization quickly and persist undetected for long durations indicates that the strategy of deterrence by denial will remain an insufficient strategic cyber deterrence option. In sum, then, the shortcomings of deterrence by denial if applied to cybered conflict are in adversary ingenuity, defensive asymmetry, and undervalued risk tolerance.

[1108] Fortinet, "Threat Landscape Report," October 2016: 2.

[1109] Verizon, "2015 Data Breach Investigations Report," June 2015: 6.

CHAPTER VI

Deterrence by Entanglement

The strategy of deterrence by entanglement presumes strengthening state cooperation on mutual interests encourages restraint to avoid incurring unintended consequences and antagonizing third parties. Nations share political, economic, commercial, and strategic interdependence in cyberspace as well as some degree of vulnerability. Soft power theorist Joseph Nye claims that "entanglement refers to the existence of various independencies that make a successful attack simultaneously impose serious costs on the attacker, as well as the victim."[1110] Deterrence by entanglement encourages responsible state behavior by raising the perceived value of maintaining and not endangering the returns from government to government cooperation. The strategy uses a range of cooperative measures to restrain state behavior in conducting, endorsing or allowing malicious cyber activity by itself, or its authorities, or by hacker groups, criminal organizations, and terrorist groups originating from territory under their jurisdiction. Since deterrence is partially a function of perception, the strategic option of entanglement stems from a state actor's belief that the costs outweigh the benefits of acting in an irresponsible manner. Deterrence by entanglement seeks to change the cost-benefit calculations of a state actor by communicating the ramifications of their irresponsible behavior. For a deterrence strategy to be successful, the deterrer has to maintain not just the capability, will, and knowledge to restrict behavior as necessary, but also the credible reputation to do so.[1111] Therefore effective signaling of clear expectations is fundamental to the achievement of meaningful cooperation between states. Otherwise an uncooperative state will not believe the deterrer will not tolerate infractions and therefore not participate in cooperative measures to secure cyberspace for the good of all parties.

[1110] Joseph S. Nye, Jr. "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17): 58.

[1111] Peter Roberts and Andrew Hardie, "The Validity of Deterrence in the Twenty-First Century," Royal United Services Institute, Occasional Paper, August 2015: 8-9.

However in today's global environment, a clash of competing state interests seriously impairs the strategic option of deterrence by entanglement. For instance the United States is a strong proponent of a free and open Internet as shown in ongoing trade negotiations and decisions on net neutrality. But some nations, such as China and Russia, are pursuing a different vision. Theirs is "predicated on absolute government control of the Internet" and anti-access policies that restrict "publishing and distributing online content."[1112] In addition state-sponsored cyber theft and cyber espionage indicate differing views exist on the protection and use of intellectual property, partially based on a cultural divide. The use of state-sponsored or privately contracted APTs allows for plausible deniability of state involvement in a cyber attack. While the state feints anonymity, the operators themselves are not put at personal risk in any way. The situation is quite simple; if states do not share and adhere to the same underlying objectives and values then state cooperation to reduce risks and enhance security is futile. Yearning to counter that hurdle, the United Nations Government Group of Experts 2013 report contends that "further progress in cooperation at the international level will require actions to promote a peaceful, secure, resilient, and open Information and Communication Technologies environment."[1113]

For space deterrence, notable scholars have suggested a layered approach that considers entanglement based on interdependence and international norms as distinct elements.[1114] However in practical application, norms are a mechanism to implement the strategy of entanglement. Norms, rules and principles of responsible state behavior, along with confidence-

---

[1112] Ash Carter, U.S. Secretary of Defense, "Securing the Oceans, the Internet, and Space," Speech to Commonwealth Club, Silicon Valley, March 1 2016: 1-15.

[1113] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, 24 June 2013: 2.

[1114] Roger Harrison, Collins G. Shackelford and Deron R. Jackson, "Space Deterrence: The Delicate Balance of Risk," *Space and Defense,* Volume Three, Number One, Eisenhower Center for Space and Defense Studies, Summer 2009:17-22.

building and capacity-building measures form the range of cooperative measures that attempt to enhance international peace and security. However unlike binding treaty agreements that are essential to sustaining international order, adherence to and participation in cooperative measures remains voluntary. Therefore despite diplomatic overtures for increased involvement in cooperative measures, state cooperation for responsible behavior in cyberspace remains elusive. If countries behaved responsibly and cooperated the magnitude of the cyber problem would diminish. Likeminded nations need to "persuade or compel those countries who take action against us in cyberspace to stop."[1115] Or be incentivized to rein in non-state actors conducting proscribed activities.[1116] In some cases in order to elicit desired actions from uncooperative states, coercive diplomacy, which combines techniques of deterrence and compellence, is necessary. Unlike the former that waits for the attacker to act before fulfilling a threat, the latter involves initiating an overt action that can become harmless only if the opponent complies.[1117] This chapter starts with an illustrative case that depicts the use of coercive diplomacy by the United States government to reach an unprecedented cyber arms agreement with China. Then after assessing legal principles for establishing responsible state behavior in cyberspace, the chapter examines the range of cooperative measures and to what level they restrain state behavior in conducting, endorsing or allowing malicious cyber activity originating in their territory.

Illustrative Case of Coercive Diplomacy

Ahead of his first official state visit to the United States in September 2015, Chinese President Xi Jinping stated in a written transcript that "The Chinese government does not engage

---

[1115] James A. Lewis, "Cyber War: Definitions, Deterrence and Foreign Policy," Statement before the House Committee on Foreign Affairs, September 30, 2015.

[1116] Robert Litwak and Meg King, "Arms Control in Cyberspace?" *Wilson Center*, October 2015: 1-8.

[1117] Thomas Schelling, *Arms and Influence*, (New Haven and London: Yale University Press, 1966): 69-78.

in theft of commercial secrets in any form, not does it encourage or support Chinese companies to engage in such practices in any way."[1118] Contrary to this pronouncement, U.S. officials have repeatedly alleged state-sponsored Chinese hackers have stolen sensitive corporate data. For example, in May 2014, the U.S. Attorney General accused a group of five Chinese hackers affiliated with Unit 61398 of the People's Liberation Army of carrying out a hacking campaign against American businesses to include U.S. Steel and Westinghouse Electric. Nevertheless nearly a year and a half after that 48 page indictment, cybersecurity experts said China has only altered the methods used by its hackers and that its campaign against U.S. firms remains active.[1119] This difference in state position prompted U.S. officials to suggest they would use the state visit to confront China on the matter. In recognizing that the United States and China have boosted cooperation in many areas, the U.S. National Security Advisor said President Obama "would make clear that China must change its practices in other, more sensitive areas, particularly state sponsored, cyber-enabled economic espionage." In seeking this change, the Advisor stated the United States would continue to "urge China to join us in promoting responsible norms of state behavior in cyberspace."[1120]

Just a day before the arrival of President Xi in Washington, the Office of Personnel Management revealed hackers who stole security dossiers from the agency also got the fingerprints of 5.6 million federal employees. Although the administration has never publicly blamed China for the theft of the personnel files, American intelligence agencies have attributed the hack to China. Although stealing government records from another country is a common part of espionage, the episode intensified pressure on Mr. Obama to act on the more serious theft of corporate data. Weeks prior to the visit, his administration developed a package of economic

---

[1118] Written Answers, "Full Transcript: Interview with Chinese President Xi Jimping," *The Wall Street Journal*, September 22, 2015.

[1119] Elias Groll, "The U.S. Hoped Indicting 5 Chinese Hackers Would Deter Beijing's Cyberwarriors. It Hasn't Worked." *Foreign Policy*, September 2, 2015.

[1120] Damian Paletta, "Obama to Press Chinese President Xi Jimping on Cyberattacks, Human Rights, Advisor Says," *The Wall Street Journal*, September 21, 2015.

sanctions, considered to be “an increasingly important tool is our coercive diplomacy toolkit,”[1121] for use against Chinese companies and individuals who benefit from the cyber-enabled theft of U.S. trade secrets by the government.[1122] The sanctions would be the first use of an Executive Order signed by President Obama in April 2015 that established the authority to freeze financial and property assets of individuals and entities overseas who engage in not only destructive attacks on critical infrastructure but also commercial espionage for competitive advantage in cyberspace.[1123] The intent or threat of the sanctions, along with indictments, is to impose costs for malicious cyber-enabled activities.

Nonetheless the Obama administration held off on imposing the sanctions in hopes of resolving this issue with Mr. Xi during the state visit.[1124] Turns out for weeks before the state visit the United States and China had conducted negotiations with urgency hoping for a cyber arms agreement for the Presidents to sign. A high level Communist Party envoy came to Washington to meet with the National Security Advisor and Director of the FBI. The result of deliberations appeared initially to be a bilateral agreement that would be a generic embrace of the code of conduct adopted by the Government Group of Experts at the United Nations in July.[1125] Yet on the last day of the state visit, the White House released only a Fact Sheet that stated the two Presidents agreed to work together to manage differences and deepen cooperation in a number of areas, to include cybersecurity. The two countries agree that “neither country’s

---

[1121] William J. Burns and Jared Cohen, “The Rules of the Brave New Cyberworld,” *Foreign Policy*, February 16, 2017.

[1122] Ellen Nakashima, “U.S. developing sanctions against China over cyberthefts,” *The Washington Post*, August 30, 2015.

[1123] President Barak Obama, “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,” Executive Order, April 1, 2015.

[1124] Carol E. Lee and Jeremy Page, “Obama’s Ties to China Leader Face Test,” *The Wall Street Journal*, September 21, 2015.

[1125] David E. Sanger, “U.S. and China Seek Arms Deal for Cyberspace,” *The New York Times*, September 19, 2015.

government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[1126] Later President Obama said he told Mr. Xi "The question now is...are words followed by actions?" and indicated the United State "will apply [sanctions] and whatever tools to go after cybercriminals either retrospectively or prospectively."[1127]

U.S. Congressional reaction to the cyber deal was guarded. "I remain skeptical that China will deliver on this promise," said Representative Adam Schiff, "But if curbing cyber theft is a journey of a thousand miles, perhaps China has taken a first step."[1128] Although it was unclear how the agreement would be enforced, it could reflect an inflection point, according to Dmitri Alperovitch, cofounder of CrowdStrike a prominent cyber security company, where the Chinese "are now obligated to respond to evidence presented by the United States."[1129] Consequently only three weeks later China fulfilled that obligation with the arrest of a number of hackers at the request of the U.S. government showing it was serious about punishing hackers.[1130] However the unprecedented move by China could have been more a reaction to threats of economic sanctions. For despite the pledge by China's president, according to a

---

[1126] Office of the Press Secretary, "FACT SHEET: President Xi Jinping's State Visit to the United States," The White House, September 25, 2015.

[1127] Dan Roberts, "US and China back off internet arms race but Obama leaves sanctions on the table," *The Guardian*, September 25, 2015.

[1128] Sheera Frenkel, "Nobody thinks the U.S. and China's New Cyber Arms Pact will fix much of anything," *BuzzFeed*, September 23, 2015.

[1129] Damian Paletta, "Cyberattack Deal Seen as First Step, *The Wall Street Journal*, September 26, 2015.

[1130] Michael Heller, "Chinese Hackers arrested at the request of the US," *Tech Target*, October 13, 2015.

CrowdStrike report,[1131] hackers linked to the Chinese government attempted to gain access to U.S. tech and pharmaceutical companies in the same three weeks since President Xi left Washington. One year after the deal, according to a FireEye report, the number of network compromises by China-based hacking groups appears to have dropped. Yet "absence of evidence is not the same thing as evidence of absence" as China may just be more stealthy and sophisticated in their attacks, signifying a failure of the much heralded agreement to achieve deterrence by entanglement.[1132]

Norms of Responsible State Behavior

A central premise for responsible state behavior in cyberspace is that global interdependence requires it. Critical components of modern life such as food, water, health, finance, energy, manufacturing, and transportation are entrenched with Information and Communications Technologies. For society in every state, the security of the online infrastructure in these sectors is important. Yet as new cyber-related vulnerabilities are discovered the risk of systemic disruption increases in parallel with rising connectivity. Accordingly a Chatham House report recognizes that dependencies in cyber-enabled critical infrastructure "spread across national boundaries and become global."[1133] This newfound global interdependence challenges state sovereignty (defined by the Oxford dictionaries as "the authority of a state to govern itself") for maintaining security and prosperity in cyberspace. It also questions the limits of responsible state behavior in not endangering the same for other nations by conducting, endorsing or allowing malicious cyber activity originating from their territory. Rightfully so, the U.S. National Security Strategy eloquently states in 2015 that the

---

[1131] Ellen Nakashima, "China still trying to hack U.S. firms despite Xi's vow to refrain, analysts say," *The Washington Post*, 19 October, 2015.

[1132] Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later," *Net Politics*, September 28, 2016.

[1133] Dave Clemente, "Cyber Security and Global Interdependence: What is Critical?" Chatham House, February 2013: v-x.

"increasing interdependence of the global economy and rapid pace of technological change" are linking governments in unprecedented ways, while creating "shared vulnerabilities, as interconnected systems and sectors are susceptible" to the threats of malicious cyber activities.[1134] For example, according to Joseph Nye, in a scenario that envisages a Chinese attack on the U.S. power grid that results in costs on the U.S. economy, the economic interdependence of the two countries would mean costly damage to China as well.[1135] This phenomenon should hypothetically incentivize and enable new forms of cooperation based on mutual interests.

The bilateral agreement between China and the United States represents a form of cooperation for responsible state behavior in cyberspace. Any effort to further codify norms, rules, and principles of responsible behavior by states starts with an understanding of how international law is applicable to cyberspace. International law is made by states and comes from various sources, to include treaties and conventions, that are legally binding documents among states; customary international law, which is created by consensus of states over a long period of time; general principles of law, that are recognized among civilization; and the writing and teaching of scholars.[1136] In particular, general principles can be of contractual nature (in good faith) and procedural character (for advisory opinions) or of common heritage of mankind (for common spaces) or sustainable development (for the environment). In regard to international peace and security, a common core of general principles consist of: the sovereign equality of states, including the right to self-preservation, independence, jurisdiction, non-intervention, and duty not to harm the rights of other states; the maintenance of international peace and security,

---

[1134] Executive Office of the President, *National Security Strategy*, (Washington, DC: The White House, February 2015): 4.

[1135] Joseph S. Nye, Jr. "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17): 58.

[1136] Catherine Lotrionte and Eneken Tikk, rapporteurs, Summary for Panel 3: Applicability of International Law to Cyberspace & Characterization of Cyber Incidents, Cyber Norms Workshop 2.0, 2012.

including the obligation to refrain from threat or use of force and peaceful settlement of disputes; and duty to international cooperation in solving international relations.[1137] These principles serve as a "normative source of law, which governs situations not regulated by formulated norms." They can also serve as a "guide or framework for interpretation of conventional and customary international law." And they can serve as the "basis for the development of new rights and obligations."[1138] Most importantly, the aforementioned core of principles pertaining to international peace and security apply in some manner in cyberspace.

The topic of sovereignty opens the Tallinn Manual 2.0 in Rule 1, in delineating "The principle of State sovereignty applies in cyberspace."[1139] Therefore a State is "free to adopt any measure it considers necessary or appropriate with regard to cyber infrastructure, persons engaged in cyber activities, or cyber activities themselves within its territory," unless prevented by international law, such as those for international human rights.[1140] At the same time, sovereignty entails "a duty to protect within the territory, the rights of other states, in particular their right to integrity and inviolability in peace and in war."[1141] Based on the principle of territoriality, "states are able to legislate with regard to activities and to prosecute offences committed on their territory."[1142] Typical examples of offenses that are likely to be considered a violation of state territory or integrity include cyber-enabled political influence, economic

---

[1137] Katharina Ziolkowski, "General Principles of International Law as Applicable in Cyberspace," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 143-144.

[1138] Ibid, 154-155.

[1139] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 11.

[1140] Ibid, 13.

[1141] Benedikt Pierker, "Territorial Sovereignty and Integrity and the Challenge of Cyberspace," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 191.

[1142] Ibid, 196.

espionage, crime, terrorism, and sabotage. However there is no clear consensus in the international community on whether acts that cause no physical damage qualify as a violation. Hence it is “imperative to examine to what extent states are obliged to control and regulate cyberspace within the reach of their sovereign powers, in order to avoid being responsible”[1143] for these offenses, caused by acts which originate from their territory, by the state itself, or its authorities, or by private parties under its jurisdiction.

The duty to protect the rights of other states invokes the obligation of states to take preventive measures in cases where the state has actual as well as constructive or presumptive knowledge. A state may have detected a cyber-enabled activity; it may be told by the victim state; or it can be presumed to know about the activity. The prevention principle obliges states to conduct a risk assessment and tell other states of risk of harm. This obligation in effect requires the State to notice malicious cyber activity, create investigative cyber capabilities to identify the source, and establish an organizational and legal framework to enable the prevention or discontinuation of such activity originating on the state’s territory.[1144] In addition, states are also responsible for their “internationally wrongful acts” to those whom they have injured. Such acts are composed of a both a breach of an international obligation and attribution of the act to the responsible state.[1145] The conduct of “state organs”’ of government, such as military, intelligence, and security agencies,[1146] or a person or group of persons “acting on the instructions

---

[1143] Ibid, 203.

[1144] Katharina Ziolkowski, “General Principles of International Law as Applicable in Cyberspace,” *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 165-186.

[1145] United Nations, “Responsibility of States for Internationally Wrongful Acts,” General Assembly resolution 56/83, December 12, 2001: Article 2.

[1146] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 87.

of, or under the direction or control of, that state in carrying out the conduct,”[1147] is attributable to the state. With regard to the wrongfulness thereof, an example is cyber operations that violate the prohibition on the use of force. Those cyber operations which cause injury or death of persons, or damage or destruction of property violate the prohibition, as resident in customary law, and codified in Article 2(4) of the UN Charter.[1148] The latter was affirmed to be applicable to state conduct in cyberspace by the Group of Twenty (G-20) at their 2015 Summit in Turkey.[1149]

International law principles echo the basic values of international society that are intrinsic to international order. The United States considers a rules-based international order that promotes peace, security and opportunity to be an enduring national interest.[1150] For cyberspace, one prevailing scholarly view is that international order is inevitable due to the dynamics of power and competition, particularly competition over issues of sovereignty. Inevitability is deduced from the reality that states are always negotiating over the framework of competition. Therefore as “the international system moves from a unipolar format to a multipolar one, great powers will have no choice” but to cooperate, to “soften the harsh effects of multipolarity and oligopolistic competition.”[1151] A counter view is that while correct increased competition may create incentives for cooperation on rules for cyberspace, the history of norm evolution for other emerging-technology weapons, such as chemical and biological weapons, strategic bombing

[1147] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 95.

[1148] Michael N. Schmitt & Liis Vihul, “Proxy Wars in Cyberspace: The Evolving International Law of Attribution,” *Fletcher Security Review*, Vol I, Issue II, Spring 2014: 57-67.

[1149] Cody M. Poplin, “Cyber Sections of the Latest G20 Leaders’ Communique,” *Lawfare*, Cybersecurity: Crime and Espionage Blog, November 17, 2015.

[1150] Executive Office of the President, *National Security Strategy*, (Washington, DC: The White House, February 2015): 2.

[1151] Christopher Whyte, “On the Future of Order in Cyberspace,” *Strategic Studies Quarterly*, Vol. 9, Issue 2 (Summer 2015): 69-77.

platforms, and nuclear weapons, indicates otherwise. In each of these historic cases, the primary reason for developing norms was the "perception among powerful or relevant states that such norms are in their national self-interest."[1152] The counter view contends that an analysis of the cyber doctrines of China, Russia, and the United States for certain categories, indicates that their calculations of self-interest might not converge in favor of robust constraining cyber norms,[1153] signifying another intractable impediment to achievement of deterrence by entanglement.

Formal Binding Obligations

The start point for reaching concurrence between countries on rules or norms, and also confidence-building and capacity-building measures, is the recognition that a cyber treaty for international peace and security is simply not possible and therefore other means are necessary to achieve peace and security. According to cyber expert James Lewis, there is no real alternative to using these forms of cooperative measures as "legally binding commitments have serious drawbacks." [1154] Uncooperative states will most likely just ignore treaties regarding cybersecurity, as they face definitional, compatibility, compliance and verification problems in implementation. The first issue for an arms control type treaty is what defines a cyber weapon. One cyber security industry insight into common characteristics of a cyber weapon includes both an attacker with "intimate knowledge of the workings of the targeted system" and a special "code that can bypass protective cybersecurity technology."[1155] However those characteristics are also common to penetration tests, described in the Center for Internet Security Critical Security Control 20 as to test the strength of an organization's defenses "by simulating the objectives and

---

[1152] Brian M. Mazanec, "Why International Order in Cyberspace Is Not Inevitable," *Strategic Studies Quarterly*, Vol. 9, Issue 2 (Summer 2015): 78-84.

[1153] Ibid. 85-95.

[1154] James A. Lewis, "US International strategy for Cybersecurity," Testimony to Senate Foreign Relations Committee, March 12, 2015: 3-4.

[1155] Clay Wilson, "4 defining characteristics of cyber weapons," *Government Computer News*, July 2015: 15.

actions of an attacker."[1156] A more precise version of the definition is found in Rule 103 of the Tallinn Manual 2.0, where cyber weapons are considered to be "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects."[1157] Even Thomas Rid agreed that cyber weapons are "instruments of harm" where computer code causes these same effects.[1158] Although without pervasive consensus on the definition of a cyber weapon,[1159] there is no basis for cyber arms control treaties.

Past arms control arrangements between states such as the Outer Space Treaty of 1967, the Non-Proliferation Treaty of 1970, the Conventional Forces in Europe Treaty of 1992, the Comprehensive Test Ban Treaty in 1996, and the Anti-Ballistic Missile Treaty of 1972 offer policy makers extensive experience in governing armaments and their deployment or use.[1160] However the technical properties of cyber weapons are not compatible with the rationale used in these arms control treaties. For example unlike nuclear weapons affordable only to states, malware is easy to use and relatively inexpensive. And unlike other kinetic weapons, malware can be reproduced and distributed at minimal cost. In addition, the rapid pace of development of malware makes any listing of prohibited weapons impossible. Even if prohibitions were possible, dual use software, like that for intelligence collection can be repurposed for malicious

---

[1156] Center for Internet Security, "The CIS Critical Security Controls for Effective Cyber Defense," Version 6.0, October 15, 2015: 68-70.

[1157] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 452.

[1158] Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal*, Vol. 157, No. 1, February/March 2012: 6-13.

[1159] U.S. Department of Defense, "Cyberspace Policy Report," November 2011: 2.

[1160] Paul Meyer, "Cyber-Security through Arms Control," *RUSI Journal*, Vol. 156, No. 2, April/May 2011: 22-27.

action.[1161] The success of the aforesaid arms control treaties has been dependent on compliance and verification regimes. Yet no state would likely agree to verification measures which would require the scanning of their computers and devices, including those in classified systems.[1162] Therefore rather than ban cyber weapons, some scholars contend that binding agreements should stipulate acceptable types, which adhere to attributability and reversibility. For the first quality, a responsible country would make their attacks clear in origin, by using digital signatures in attack code. And for the second, nations would use attack methods that are repairable.[1163] Even though this approach seems to just encourage the use of cyber arms, while under some form of control.

All complications aside, China and Russia did sign in May 2015 a bilateral agreement dubbed a "nonaggression pact" for cyberspace that demonstrated their values diverge from Western society. The treaty broadly defines cyber threats to include the transmission of information that could endanger "societal-political and social-economic systems," seemingly counter to the free flow of information, and calls for the creation of "a multilateral, democratic and transparent management system" for the Internet, implying a predominant state voice in governance versus a multi-stakeholder model. Besides detailing pledges of cooperation, such as in international legal norms and on joint scientific projects, one particular provision in the treaty pledges the parties to refrain from "computer attacks" against each other. Specifically Article 4 provides that "Each Party has an equal right to the protection of the information resources of

---

[1161] Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations," in *Proceedings 4th International Conference on Cyber Conflict* (Tallinn, Estonia: CCD COE, June 2012): 91-101.

[1162] Dorothy Denning, "Obstacles and Options for Cyber Arms Controls, Heinrich Boll Foundation Conference, Berlin, Germany, June 29-30, 2001:3.

[1163] Neil C. Rowe, Simson L. Garfinkel, Robert Beverly, and Pannayotis Yannakogeorgos, "Challenges in Monitoring Cyberarms Compliance," *International Journal of Cyber Warfare & Terrorism*, Vol 1. No. 1, January-March 2011: 1-14.

their state against misuse and unsanctioned interference."[1164] Still the language is vague and could be interpreted differently, highlighting the difficulty of implementing the precise provision, the essence of the treaty. Efforts to limit the cyber arms race are confronted by a nations desire to maintain advantage in the domain for their own benefit. One public analysis of intrinsic challenges simply concludes that "cybersecurity treaties may be nice, but it's really every country for itself."[1165] Undoubtedly any hope for that assertion to be false resides in cooperative measures found in the strategy of deterrence by entanglement.

Cooperative Measure Selection

A broad range of cooperative measures attempts to restrain state activity, or state sponsored or endorsed activity, of a malicious manner in cyberspace. International forum discussions indicate that cyber related norms of behavior are the best means to guide state behavior in cyberspace. The main objectives for agreeing on norms appear to be "increased predictability, trust and stability in the use of ICTs, hopefully steering states clear of possible conflict due to misunderstandings."[1166] State acceptance of a prescribed norm can constrain and regulate their behavior, under the pretense that other states will sanction violations of the norm.[1167] The incentive for states to adopt norms stems from a common interest in sustaining cyberspace, in particular the Internet, for the benefit of all states. Therefore the United Nations has taken the lead on the development of norms for responsible behavior by states in cyberspace.

[1164] Elaine Korzak, "Russia and China Have a Cyber Nonaggression Pact," *Defense One*, August 20, 2015.

[1165] Robert Litwak and Meg King, "The Great Debate," *Reuters*, November 11, 2015.

[1166] Anna-Maria Osula and Henry Roigas, "International Norms Limiting State Activities in Cyberspace," *International Cyber Norms: Legal, Policy & Industry Perspectives*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016): 11-22.

[1167] Roger Hurwitz, "A New Normal? The Cultivation of Global Norms as Part of a Cybersecurity Strategy," *Conflict and Cooperation in Cyberspace*," (Taylor & Francis Group, 2014): 233-264.

Another cooperative measure choice resides in voluntary politically binding confidence-building measures (CBM) designed to prevent the outbreak of conflict. The Organization for Security and Co-operation in Europe (OSCE) has made progress in advancing cyber-related CBMs. Finally, the last category of cooperative measures is contained in capacity-building measures. They are intended to help secure ICTs and their use.

Norms, Rules and Principles

A norm can be defined as a "standard of appropriate behavior for actors with a given identity."[1168] Voluntary, and hence non-binding, norms of responsible state behavior are intended to reduce risks to international peace and security. They reflect international community expectations and standards for responsible state behavior. Normative regimes are beginning to influence the development of state policy embodied in their national cyber strategies and the position on related matters of intergovernmental bodies such as the United Nations.[1169] Although some state views and initiatives regarding norms, rules and principles substantially differs from international congruence based on their own interpretations of international order. For instance from China's perspective, international order reflects the relative balance of power and resides currently in the interest of hegemons, which makes it inconsistent and unfair. China would favor an international order that contributes to the maintenance of national sovereignty and political systems. Their foundational principles for international order specify "equality of the sovereign nations, non-interference in each other's internal affairs, and peaceful coexistence of different political systems."[1170]

[1168] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization,* 52, 4, Autumn 1998: 887-917.

[1169] Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," *International Cyber Norms: Legal, Policy & Industry Perspectives*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016): 23-47.

[1170] Shinji Yamaguchi, "China's perspective on international order," National Institute for Defense Studies (NIDS) Commentary, No. 46, May 15, 2015: 2.

Therefore China teamed with Russia, Tajikistan and Uzbekistan in September 2011 to submit to the United Nations their version of an international code of conduct for information security. Their letter recognizes that a "global culture of cybersecurity" needs to be implemented pursuant to a previous General Assembly resolution."[1171] The letter highlights "the importance of the security, continuity and stability of the Internet" and reaffirms "that policy authority for Internet-related public issues is the sovereign right of States."[1172] One purpose of the proposed code of conduct is to promote responsible behaviors of states in information space. Although adherence is voluntary, each state subscribing would pledge: to comply with universal norms governing "sovereignty, territorial integrity, and political independence of all States;" not to use information and communication technologies "to carry out hostile activities or acts of aggression;" and to reaffirm the rights of "States to protect... their information space and critical infrastructure from threats, disturbances, attack and sabotage."[1173] The draft code of conduct submission was revised in January 2015 to add that each State subscribing would also pledge: not to use information and communication technologies "to interfere in the internal affairs of other States" and not to "undermine States' right to independent control of information and communication technology goods and services,"[1174] in effect advocating government control of the Internet.

The code of conduct submission by China, Russia and most of the Central Asian States is not the only regionally endorsed proposal. In June 2014, the Member States of the African

---

[1171] United Nations General Assembly, "Creation of a global culture of cybersecurity and taking stock of national efforts to protect information infrastructures," Resolution 64/211, December 21, 2009: 1-5. .

[1172] United Nations General Assembly, "International code of conduct for information security," Document 66/359, September 14, 2011: 3.

[1173] Ibid. 4.

[1174] United Nations General Assembly, "International code of conduct for information security," Document 69/723, January 13, 2015: 5.

Union released a Convention on Cyber Security and Personal Data Protection. It establishes a normative framework that aims to strengthen existing legislations on Information and Communication Technologies. The provisions of the Convention are not to be interpreted in a way that is not consistent with the principles of international law, to include customary law. Actions that collect, process, transmit, store or use personal data by the state or a person are subject to the Convention.[1175] Each Member State is supposed to develop and adopt a national cyber security policy that acknowledges the significance of Critical Information Infrastructure. Suggested strategies to implement this policy include international cooperation, especially on the exchange of information on cyber threats and vulnerabilities, and legislative reform. For the latter, by mandating that each state shall take legislative or regulatory measures to make attempts to gain unauthorized access, remain fraudulently, hinder functioning, enter data deceptively, or damage data in a computer system a criminal offense.[1176] The Convention establishes a de facto baseline for norms of expected behavior by Member States, which also applies to individuals in their territory. Although critics of the Convention say serious concerns exist over its human rights implications, particularly provisions that restrict fee speech, limit freedom of association, and broaden judicial powers.[1177]

Also, eight months before the 2011 code of conduct submission, the UN General Assembly adopted a resolution, sponsored by the United States and Russia that notes "the dissemination and use of information technologies and means affect the interests of the entire international community" and expresses "concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining

---

[1175] Assembly of the Union, "African Union Convention on Cyber Security and Personal Data Protection," 23rd Ordinary Session, Malabo, June 27, 2014: 1-18

[1176] Ibid. 26-30.

[1177] Mailyn Fidler and Fadzai Madzingira, "The African Union Cybersecurity Convention: A Missed Human Rights Opportunity," *Council on Foreign Relations*, June 22, 2015.

international stability and security."[1178] Consequently the resolution requests the Secretary General to establish another Group of Governmental Experts, with an equitable geographical composition, to "study existing and potential threats in the sphere of information security and possible cooperative measures to address them."[1179] In 2013, the subsequent Group, comprised of representatives from China, Russia, the United States and twelve other nations, reached consensus on their report. They agreed that international law, and the Charter of the United Nations, is applicable and essential to promoting a peaceful ICT environment. Hence in regard to specific recommendations on norms, rule and principles of responsible state behavior, the 2013 Group of Governmental Experts concluded that:

> a. States must meet their international obligations regarding internationally wrongful acts attributable to them.
> b. States must not use proxies to commit internationally wrongful acts.
> c. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs.[1180]

These particular norms codify Group determination that the principles that flow from sovereignty apply to state conduct and jurisdiction over ICT-related activities or infrastructure respectively.

While regional and organizational initiatives advance, the broader international community has not sat idle on discussing norms for responsible behavior in cyberspace. As of 2017, a total of four Global Conferences on Cyberspace have been held with representatives

---

[1178] United Nations General Assembly, "Developments in the field of information and telecommunications in the context of international security," Resolution 65/41, January 11, 2011: 1-2.

[1179] Ibid. 3.

[1180] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, 24 June 2013: 8.

from governments, private sector and civil society. The first in London in November 2011, called the London process, asked this succinct question under the topic of international security: "How do we develop and apply appropriate principles of behavior?"[1181] In response all delegates agreed that immediate steps should be to create shared understanding and agree on common approaches. Some delegates noted the draft Code of Conduct being circulated at the United Nations. None wanted to expend effort on legally-binding international agreements. By the next iteration in Budapest in October 2012, very little progress had been made, and if anything, various actors dug in on their resistive positions. The Chinese indicated their preference for a cyberspace arms control treaty and the Russians rejected the Budapest Convention on Cybercrime because it serves their national interest.[1182] Although in a progressive manner, the United Kingdom asked for consensus on rules of the road and the Republic of Korea urged exploration on norms of behavior to avoid conflict between states.[1183] Real progress on areas of common ground was made at the Seoul Conference in October 2013, and reflected in the *Seoul Framework for and Commitment to Open and Secure Cyberspace*. The document identified elements for an open and secure cyberspace to include under the category of international security many verbatim conclusions from the 2013 UN Group of Government Experts report.[1184] The fourth Global Conference held in The Hague in April 2015, sought to build on the *Seoul Framework.* The Hague Conference "reaffirmed the applicability of existing international law to State behavior in cyberspace, as well as its commitment to exploring the development of

[1181] Foreign & Commonwealth Office, "London Conference on Cyberspace: Chair's statement," Full Text, November 2, 2011.

[1182] Cherian Samuel, "Some takeaways from the Budapest Conference on Cyberspace," Institute for Defense Studies and Analyses, October 11, 2012: 1-2.

[1183] Janos Martonyi, "Budapest Conference on Cyberspace: Summary by the Chairman," October 4-5, 2012.

[1184] H.E. Yun Byung-Se, "Seoul Conference on Cyberspace: Statement by the Conference Chair," October 17-18, 2013.

voluntary, non-legally-binding norms for responsible State behavior in cyberspace during peacetime."[1185]

Three months later, in July 2015, the Group of Governmental Experts released another report that distinctly expanded the discussion of norms. In the Foreword, the Secretary-General pronounced that "All States have a stake in making cyberspace more secure."[1186] Thus to better represent the international community in this quest, the 2015 Group was enlarged to 20 States. Their comprehensive exchange of views on norms, rules and principles of responsible State behavior resulted in consensus on the following additional recommendations:

a. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure.
b. States should take appropriate measures to protect their critical infrastructure from ICT threats.
c. States should respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts.
d. States should not conduct or knowingly support activity to the harm the information systems of the authorized emergency response teams.[1187]

These particular norms could be considered a breakthrough for U.S. diplomats pushing for an alternative to formal treaties. By delineating norms regarding critical infrastructure, the United States and other states reached "a consensus on the appropriate boundaries for state activities in

---

[1185] Bert Koenders, "Global Conference on Cyberspace 2015: Chair's Statement," The Hague, April 16-17, 2015.
[1186] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, 22 July 2015: 4.
[1187] Ibid. 8.

cyberspace in order to avoid wide-spread, potentially devastating, damage in cyberspace."[1188] Although in the spirit of concession, the United States did not reach consensus on their proposal to spell out the implications of the 2013 Group's agreement "that international law applies to cyberspace just as it does on land or at sea."[1189] A bloc of nations rebuffed the proposal to prevent their interpretation of an attempt to establish U.S. hegemony in cyberspace.

Not just states have "a stake in making cyberspace more secure," so do international corporations. More representative of the multi-stakeholder model is the Microsoft Corporation version of proposed Cyber Security Norms to limit potential conflict in cyberspace. The premise of their norms is that governments which are investing in offensive cyber capabilities have a responsibility to guide their use. Therefore norms can better define what type of government behavior is unacceptable so that incidents do not escalate to conflict. In order to be effective, Microsoft believes norms also have to drive behavior change that is observable. Their proposed norms are meant to reduce the possibility that states will use, abuse, or exploit ICT products and services as part of offensive operations that result in conflict. Therefore the six norms proposed by Microsoft focus mostly on protecting global trust in technology, per the following abbreviated recommendations that states should:

- Not target ICT companies to insert vulnerabilities that undermine public trust.
- Have a policy for handling product and service vulnerabilities that reflect a mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
- Ensure that any developed cyber weapons are limited, precise and not reusable.
- Commit to nonproliferation activities that pertain to cyber weapons.
- Limit offensive cyber operations in order to avoid creating mass events.

[1188] Catherine Lotrionte, "A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence," *Georgetown Journal of International Affairs*," December 23, 2013: 75.

[1189] Joseph Marks, "U.N. body agrees to U.S. norms in cyberspace," *Politico*, July 9, 2015.

– Assist the private sector to detect, contain, respond and recover from cyber incidents.[1190]

Microsoft recognizes that norms are not an objective by themselves, but can drive demonstrable changes in state behavior if implemented, assessed for accountability, and, if appropriate, evolved. Microsoft did just that in forwarding in June 2016 a new three-part organizing model of offensive, defensive, and industry norms. Offensive norms require restraint to not choose actions that violate boundaries of responsible state behavior. Defensive norms are meant to enable risk management through improved defenses and incident response. While the first two categories are consistent with the above 2014 list for states, industry norms are new in addressing their role in mitigating risks, for example, global ICT providers should not permit backdoors in their products, traffic in cyber vulnerabilities, or withhold patches from any party.[1191] Scott Charney, Corporate Vice President of Microsoft, described the relationship among the categories in stating "as governments commit increasing resources into offensive cyber capabilities, the global ICT industry must…take active steps to prevent user exploitation" and "raise the bar in our defensive capabilities to deter nation-states from targeting technology users."[1192]

Confidence-Building Measures

The 2015 Group of Governmental Experts proclaimed that confidence-building measures strengthen international peace and security. In their report, they assert these types of measures

[1190] Angela McKay, et al., Microsoft Corporation, "International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World," December 2014.

[1191] Scott Charney, et al., Microsoft Corporation, "From Articulation to Implementation: Enabling progress on cybersecurity norms," June 2016: 1-8.

[1192] Scott Charney, Microsoft Corporation, "Cybersecurity norms for nation-states and the global ICT industry," Microsoft on the Issues, Posted June 23, 2016.

"can increase interstate cooperation, transparency, predictability and stability."[1193] Confidence-building measures are used as an instrument of international politics, in attempts to prevent or reduce the risk of conflict by removing sources of mistrust, misunderstanding and miscalculation between states. They achieve this result by establishing practical means and processes for crisis management.[1194] For example, confidence-building measures have been developed and suggested for outer space activities to address state-owned threats to their sustainability and security.[1195] The world's growing dependence on vulnerable space-based platforms, technologies and information is no different than global interdependence in cyberspace. Likewise neither is the risk of conflict from the militarization of outer space and also cyberspace. The acceleration of an arms race in both domains only increases the risk of escalation and conflict. Confidence-building measures attempt to reach an adequate level of predictability of state behavior and prevent the loss of control over a perilous situation.

In 2013, the United States and the Russian Federation attempted a new field of cooperation in confidence-building. Both parties recognized not only the increasing interdependence of the world on Information and Communication Technologies, but also the political-military, criminal and terrorist threats to or in the use of them. Thus in demonstrating "commitment to promoting international peace and security," they completed so called "landmark steps designed to strengthen relations, increase transparency, and build confidence" between their nations, to include:

[1193] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, 22 July 2015: 9.

[1194] Katharina Ziolkowski, "Confidence Building Measures for Cyberspace – Legal Implications," (Tallinn, Estonia, NATO Cooperative Cyber Defense Center of Excellence, 2013): 1-13.

[1195] United Nations General Assembly, "Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities," A/68/189, 29 July 2013: 1-4.

- A mechanism and arrangements for information sharing between computer emergency response teams to better protect critical information systems.
- Authority to use the direct communications link between Nuclear Risk Reduction Centers for this purpose.
- A link between high-level officials to manage dangerous situations related to security threats to or in the use of Information and Communication Technologies.[1196]

These confidence-building measures are designed to "reduce the possibly that a misunderstood cyber incident could create instability or a crisis" between the two nations.[1197] Although not as formal, the United States and China do pursue a model of risk reduction under the rubric of "constructive management of differences." President Xi Jimping has labeled cooperation in this manner to be "of vital importance to the global community."[1198] The model applies not just to cyber security, but also to maritime disputes, as urged by the Chinese Chief of General Staff Fang Fenghui for the two sides to "manage their differences in a constructive way" in regard to South China Sea tensions, which has resulted in protests against U.S. tests of maritime claims instead of conflict.[1199]

On a more global scale, the U.S. Department of State has advanced the development of practical cyber confidence-building measures to reduce risk.[1200] This has occurred through

---

[1196] Executive Office of the President, "Joint Statement by the Presidents of the United States and the Russian Federation on a New Field of Cooperation in Confidence Building" (Washington: The White House, June 17, 2013).

[1197] Executive Office of the President, "Fact Sheet: US–Russian Cooperation on Information and Communications Technology Security" (Washington: The White House, June 17, 2013).

[1198] Lesley Wroughton and Michael Martina, "China, U.S. say committed to managing differences," *Reuters*, 9 July 2014.

[1199] John Ruwitch, "China, U.S. Should Manage South China Sea Differences Constructively – Chinese General," *Reuters*, 12 May 2016.

[1200] U.S. Department of State, "International Cyberspace Policy Strategy," March 2016: 4.

agreement in the ASEAN Regional Forum in 2015 on a work plan for such, and in the Organization for Security and Cooperation in Europe in 2016 on implementation of an initial set of voluntary confidence-building measures, which include:

- Provide national views on threats to and in use of ICTs.
- Facilitate co-operation among national bodies and exchange information.
- Hold consultations in order to reduce risks of misperceptions.
- Share information on measures taken to ensure a secure and reliable Internet.
- Have in place national legislation to facilitate bilateral co-operation.
- Share information on their national organization, strategy, policies and programs.[1201]

The development of confidence-building measures provides tools to manage expectations of responsible state behavior in cyberspace. For example, measures for communication, exchange and cooperation during transnational investigations facilitate norms for states to not allow malicious activity originating from their territory.[1202]

Capacity-Building Measures

The 2015 Group of Governmental Experts commented that some states may lack sufficient capacity to protect ICTs and prevent a haven for malicious actors. Consequently they endorsed the 2013 Group's findings that some states may require assistance "in their efforts to improve the security of critical ICT infrastructure; develop technical skill and appropriate

---

[1201] Organization for Security and Co-operation in Europe, "Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communications Technologies," PC.DEC/1106, 3 December 2013:

[1202] Patryk Pawlak, "Confidence Building Measures in Cyberspace: Current Debates and Trends," *International Cyber Norms: Legal, Policy & Industry Perspectives*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016): 129-132.

legislation, strategies and regulatory frameworks to fulfil their responsibilities."[1203] The 2015 Global Conference on Cyberspace held in The Hague not only reached the same deduction but also took action. The founding partners of the event announced the launch of the Global Forum on Cyber Expertise, described as a global platform for cyber capacity-building. The primary objectives of the Global Forum are to share expertise, experience, and best practices on thematic cyber issues; identify gaps in global cyber capacity and find solutions; and contribute to efforts to build global cyber capacity.[1204] The Framework Document for the Global Forum delineates that participation is voluntary, and does not impose any legal obligation. Members are to take on new initiatives or enhance and expand existing ones to improve capacity in cyber.[1205] In 2016, the Global Forum consisted of fifty organizations and states working together on four focus areas of strengthening cybersecurity, fighting cybercrime, protecting online data and supporting e-governance.[1206] The Global Forum continues today with over sixty organizations and states working together on practical initiatives.

Cooperative Measure Utility

As a leader of the international community, the United States has remained eager to pursue cooperative measures to restrain state behavior based not only on mutual interests, but also on mutual trust. After success in collaboration with Russia on ICT security measures, the United States elected to pursue comparable confidence-building measures to promote trust and

---

[1203] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, 24 June 2013: 10.

[1204] Launch of the Global Forum on Cyber Expertise, "The Hague Declaration on the GFCE," 16 April 2015: 1-2.

[1205] Launch of the Global Forum on Cyber Expertise, "Framework Document," 16 April 2015: 1-4.

[1206] See for example, News Item, "12-13 April: West Africa Cybersecurity Meeting," posted 21 March 2016, at www.thegfce.com.

assurance with China. An exchange on national policies for cyberspace was deemed the appropriate measure to head off the chance of fast escalating cyber attacks between the two nations. Therefore prior to the U.S. Defense Secretary visit to Beijing, in April 2014 the Obama administration quietly briefed Chinese military leadership on the Pentagon's emerging doctrine for defending against cyber attacks against the United States and for using its cyber technology against adversaries, including the Chinese. The intent was to allay Chinese concerns about plans to triple American cyber warriors in new teams for cyber operations, and the hope was to prompt the Chinese to give Washington a similar briefing about People's Liberation Army units believed to be behind cyber attacks on government and corporate networks in the United States.[1207] Without any guarantee of reciprocation, the briefing turned out to be a one way exchange. Although the United States hoped for the same openness, under the semblance of mutual transparency China gained access to sensitive U.S. defense information while offering very little in return. The reality is that "a collaborative and transparent relationship would run counter to the Chinese government priorities."[1208] Ultimately the United States had no choice but to turn to other measures, in particular coercive diplomacy to gain cooperation on mutual interests.

The result was President Xi's pledge during his State visit to Washington in September 2015 that China would not conduct cyber-enabled economic espionage. Up to that point, the Chinese government had never even acknowledged such activity. Remarkably at the 2015 Group of Twenty Summit, President Xi repeated that commitment to the heads of state. In response, the G-20 Leaders "affirmed that international law applies to state conduct in cyberspace and committed that all states should abide by norms of responsible state behavior in cyberspace."[1209] They also "affirmed that no country should conduct or support cyber-

---

[1207] David E. Sanger, "U.S. Tries Candor to Assure China on Cyberattacks," *New York Times*, April 6, 2014.

[1208] Amy Chang, "Warring State: China's Cybersecurity Strategy," Center for a New American Security, December 2014: 7-8.

[1209] Office of the Press Secretary, "FACT SHEET: The 2015 G-20 Summit in Antalya, Turkey," The White House, November 16, 2015.

enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors."[1210] A month later, China announced the arrest of hackers it says breached the OPM database. However U.S. officials are not sure if the arrests were of the guilty parties.[1211] FireEye and ISight Partners had attributed the attack to a Chinese state sponsored APT group referred to as Deep Panda, also responsible for the Anthem breach.[1212] It seems hard to believe the Chinese government would give up the Deep Panda operation that routinely steals Personally Identifiable Information from U.S. commercial and government networks. A combination of delivered indictments and threatened sanctions may have altered malicious Chinese behavior in cyberspace, shown in the OPM arrests. A year after the U.S.-China Cyber Agreement, although FireEye Chief Technology Officer Grady Summers reported the cyber firm is now conducting about 10 investigations of Chinese cyber espionage a month compared to a prior average of 35 per month for different corporate clients,[1213] according to Brad Bussie at STEALTHbits Technologies, "nothing has changed. Attacks and the origin of the attacks have simply become harder to detect."[1214]

The reality is that fundamental challenges in agreeing on and adhering to norms exists in competing views, particularly on use of the Internet. For instance, the 2015 UN Government Group of experts did not accept proposed norms related to intellectual property theft. For the Chinese, as a member of the UN Group, economic espionage in cyberspace is now part of normal business practice. China has no tradition of protecting intellectual property, evidenced

---

[1210] Ibid.

[1211] Ellen Nakashima, "Chinese government has arrested hackers it says breached OPM database," *The Washington Post*, December 2, 2015.

[1212] The Institute for Critical Infrastructure Technology, "Handing Over the Keys to the Castle," Technical Report, July 2015: 3.

[1213] Joseph Marks, "Obama's Cyber Legacy: He Did Almost Everything Right and It Still Turned Out Wrong," *NEXTGOV*, January 17, 2017.

[1214] Doug Olenick, "U.S.-China Cyber Agreement: Flawed, but a step in the right direction," *SC Magazine*, January 24, 2017.

by more than thirty years of licit and illicit acquisition of western technology.[1215] A cultural divide exists, where the Chinese believe that intellectual property is to be rightfully copied or obtained. Confucianism holds that imitation is the greatest form of flattery and emphasizes the significance of sharing intellectual products with society, even to the extent that it would be dishonorable if a scholar makes money by selling his book to others.[1216] In addition, communism discourages individual property.[1217] These fundamental precepts produce the prevailing Chinese view that copying is a form of compliment rather than disrespect, and thus justly acceptable.[1218] This view permeates Chinese thought to the extent that the obtainment of intellectual property for imitation is a moral duty. For illustration, after a Chinese national admitted to conspiring to hack into the computer systems of major U.S. defense contractors to steal military hardware secrets on Beijing's behalf,[1219] the state-run Global Times said that if he had done so, "we are willing to show our gratitude and respect for his service to our country."[1220]

On the contrary, the United States recognizes acts of cyber-enabled intellectual property theft as unlawful and impermissible. Assistant Attorney General John Carlin called the sentencing of the aforementioned Chinese national as "just punishment" for his role in a

[1215] James A. Lewis, "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology," Testimony to House Committee on Energy and Commerce, July 9, 2013: 1-2.

[1216] Guan H. Tang, *Copyright and the Public Interest in China*, (Northampton, MA: Edward Elgar Publishing, Inc, 2011): 16.

[1217] John, H. D'Antico, "A Quick Primer on Chinese Patent Law," I.P. insider, Spring 2003: 1-2.

[1218] Sisir Botta and Christopher Tsai, "Globalization is a Catalyst for Change in Intellectual Property Systems: Case Studies in India and China," *i-Manager's Journal on Management* 1, no. 1, 2006: 90-96.

[1219] Warwick Ashford, "Chinese man admits conspiring to hack US military secrets," *Computer Weekly*, March 24, 2016.

[1220] Ben Dooley, "Chinese Media Laud Hacker for U.S. Spying," *Agence France-Presse*, March 25, 2016.

conspiracy “to illegally access and steal sensitive U.S. military information.”[1221] Therefore to establish an environment of common expectations, the United States seeks to consolidate regional and international consensus on key cyberspace activities. Although consensus is difficult to achieve when not just values, but basic rights diverge. For example, the U. S. International Strategy for Cyberspace opines that “states should not have to choose between the free flow of information and the security of their networks.” The reason is because the best cybersecurity solution tools secure systems “without crippling innovation, suppressing freedom of expression or association, or impeding global interoperability.”[1222] In contrast, some totalitarian states call for national-level filters and firewalls that increase sovereign control over Internet access and content. At the 2015 World Internet Conference, Chinese President Xi called for governments to cooperate in regulating Internet use, stepping up attempts to promote controls. The human rights group Amnesty International scorned this assault on Internet freedom to make censorship and surveillance the norm everywhere under the guise of security. For already in China, the Communist Party tries to prevent Internet users from seeing news outlets, the Google search engine, and social media such as Facebook.[1223] In November 2016, China adopted a controversial cyber security law where elements, such as “criminalizing the use of the Internet to damage national unity, would further restrict online freedom.[1224]

According to Christopher Painter, the U.S. Coordinator for Cyber Issues, the area of Internet governance is where authoritarian governments are “pushing to shift from the long-standing and successful multi-stakeholder model...to an intergovernmental and exclusive system

---

[1221] Robert Abel, “Chinese businessman sentenced for cyberespionage targeting U.S. defense contractors,” *SC Magazine*, July 14, 2016.

[1222] Executive Office of the President, *International Strategy for Cyberspace*, (Washington, DC: The White House, May 2011): 5-9.

[1223] Joe McDonald, “China’s Xi Calls For Cooperation on Internet Regulation,” *Associated Press*, December 16, 2015.

[1224] Sue-Lin Wong and Michael Martina, “China Adopts Cybersecurity Law in Face of Overseas Opposition,” *Reuters*, November 7, 2016.

that could fundamentally undermine the future growth and potential of the Internet."[1225] The United States counters this movement by working to support and enhance the multi-stakeholder model, as evidenced by the Commerce Department announcement in 2014 of intent to transfer its stewardship of key Internet domain name functions to the global Internet community.[1226] In keeping this promise, the United States transferred the Domain Naming System to ICANN (the Internet Corporation for Assigned Names and Numbers) on 1st October 2016, even over the objections of several U.S politicians that the transfer increases "the power of foreign governments over the internet."[1227] Those objections continued in 2017 when Senator Ted Cruz insisted in the appointment of a new National Telecommunications and Information Administrator on the assembly of a "panel of experts to investigate options for unwinding" the transfer, which Cruz referred to as an "internet giveaway".[1228] Whereas in a show of contrasting views on multi-stakeholder governance, China and Russia have advocated for a new global cybercrime treaty that controls free speech and undermines human rights, while disregarding the long standing Budapest Convention on Cyber Crime from 2001 that has already been ratified by 46 countries.[1229] From the 2015 Global Conference on Cyberspace, the Chair's Statement reiterates the need to ensure that fundamental human rights are protected online. The Chair also notes commitment at the Conference to a multi-stakeholder approach for Internet governance that includes "civil society, the technical community, business and governments across the

[1225] Christopher M. E. Painter, "Cybersecurity: Setting the Rules for Responsible Global Behavior," Testimony to Senate Foreign Relations Committee, March 12, 2015: 2.

[1226] INTA Bulletin, "U.S. Department of Commerce Announces Intent to Transition Key Internet Domain Name Functions," Vol. 69, No. 9, May 1, 2014.

[1227] Dave Lee, "US ready to 'hand over' the internet's naming system," *BBC News*, Technology Section, August 18, 2016.

[1228] Joe Kane and Milton Mueller, "U.S. government should not reverse course on internet governance transition," *Brookings*, TechTank Blog, February 7, 2017.

[1229] Greg Masters, "Global cybercrime treaty rejected at U.N." *SC Magazine*, April 23, 2010.

globe."[1230] While the next Global Conference in The Hague called upon all stakeholders to strength the evolution of the multi-stakeholder model to achieve a free and open Internet, some countries would prefer to stake out borders in cyberspace, in a form of "balkanization of the Internet."[1231]

An Insufficient Deterrence Option

Part of the problem in achieving cooperation for restraint in cyberspace is that states are not going to agree on what they do not know is acceptable; instead they will wait to see what the international community will not tolerate. For instance China operates at a peer level and will do what it wants, inside the precise language of what is allowed, based on an assessment of its own national interests in any given situation.[1232] Take for example the Chinese military buildup in the South China Sea on disputed islands. As President Obama hosted Southeast Asia allies at a summit in California in February 2016, China stationed a modern surface-to-air weapons system, the HQ-9 on Woody Island in the Paracel chain, controlled by China but claimed by Vietnam and Taiwan.[1233] Then a month later, China not only deployed anti-ship cruise missiles, the YJ-62, to the island,[1234] but test fired the coastal battery.[1235] The placement of these advanced

---

[1230] Bert Koenders, "Global Conference on Cyberspace 2015, Chair's Statement," April 17, 2015: 1-8.

[1231] Nicholas Dynon, "The Future of Cyber Conflict: Beijing Rewrites Internet Sovereignty along Territorial Lines," Jamestown Organization, China Brief Volume 15, Issue 17, September 4, 2015.

[1232] Katherine Morton, "China and the future of international norms," Australian Strategic Policy Institute, Strategic Policy Forum, June 22, 2011: 1-13.

[1233] The Editorial Board, "China's missile gambit," *The Washington Post*, February 21, 2016.

[1234] Ankit Panda, "South China Sea: China Has Deployed Anti-Ship Missiles on Woody Island," *The Diplomat*, March 26, 2016.

[1235] Sam LaGrone, "China Defends Deployment of Anti-Ship Missiles to South China Sea Island," *U.S. Naval Institute*, News, March 30, 2016.

weapons not only challenges U.S. policy to sail anywhere in the world that international law allows, but also imposes China's unilateral resolution on island claims that the United States has insisted to be settled through negotiations. Russia also pushes international law and order to the edge, then recasts language to their terms. Although NATO called the Russian annexation of Crimea in March 2014 a violation of international law, Russia defended its actions as the lawful protection of the Russian speaking minority in Crimea. However there were really no indications that native Russians were in any danger, and even if so, that pretense could only have justified their evacuation, not the occupation of the entire peninsula. Without an invitation by the Ukrainian authorities to intervene in their country, the annexation by Russia was simply an illegal violation of the territorial integrity of Ukraine.[1236]

In addition, States use proxies, groups that act as a substitute for another, to allow for 'plausible deniability.' By the time the Russian Parliament approved the deployment of troops into Ukraine, Russian military forces disguised as 'little green men' were already present in Crimea. According to President Putin, these armed men were "members of 'self-defense groups' organized by locals who bought all their uniforms and hardware in a shop."[1237] Likewise in the 'Donetsk People's Republic,' Russian Special Forces troops reportedly reinforced local 'separatists.'[1238] This use of 'volunteers' allowed the Russian government to deny any involvement in Ukraine for months. Even more so, Russian use of proxies in the conflict in Ukraine extended beyond the physical domain into cyberspace. Here the most prominent proxy actors have been hacktivist groups, to include pro-Moscow Anonymous Ukraine and CyberBerkut. Their activities range from DDoS attacks and web defacements to the leaking of government files. While Ukrainian government officials blame the Russian government for

---

[1236] Jan Stinissen, "A Legal Framework for Cyber Operations in Ukraine," *Cyber War in Perspective: Russian aggression against Ukraine*, Chapter 6, (Tallinn, Estonia, NATO Cooperative Cyber Defense Center of Excellence Publications, 2015): 123-127.

[1237] Vitaly Shevchenko, "Little green men or Russian invaders?" *BBC News*, March 11, 2014.

[1238] Geraint Hughes, "Ukraine: Europe's New Proxy War?" *Fletcher Security Review*, Vol I, Issue II, Spring 2014: 106-118.

indirectly orchestrating these operations, the latter denies accusations that it has any influence over the groups.[1239] Yet the accusations are consistent with Russian government reliance on criminals and hacker groups to hide their attempts to break into computer systems. Admiral Rogers, the head of U.S. Cyber Command, testifies that this relationship "theoretically makes it more difficult to go to country X and say we see this activity going on, you are doing it, this is unacceptable," when they have the ability "to say it's not us, it's criminal groups."[1240]

Ultimately to attribute an attack to states, or to their proxies, to hold them accountable for irresponsible behavior is a political decision, which varies depending on the target and nature of the attack. In the OPM hack, even though forensic evidence leaves little doubt that China was responsible, the Obama administration chose not to make any official assertion.[1241] Likewise in hacks into unclassified networks at the State Department and White House, although investigators traced the malicious activity to hackers associated with the Russian government, U.S. officials refrained from going public with that allegation against Moscow.[1242] Like these political decisions, norms of responsible behavior are just political agreements, not binding arms control treaties, to be enforced by signature parties, or binding laws and rules, that hold parties accountable. At the very best norms can develop into shared daily practice by states and then eventually become customary international laws. Diplomatic statements, press releases, military manuals, national court decisions, legal advisor opinions, international tribunal rulings and

---

[1239] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," *Cyber War in Perspective: Russian aggression against Ukraine*, Chapter 9, (Tallinn, Estonia: NATO Cooperative Cyber Defense Center of Excellence Publications, 2015): 79-85.

[1240] Ian Duncan, "Cyber Command chief: Foreign governments use criminals to hack U.S. systems," *The Baltimore Sun*, March 16, 2016.

[1241] Jeff Mason and Mark Hosenball, "Obama Vows to Boost U.S. Cyber Defenses, Amid Signs of China Hacking," *Reuters*, June 8, 2015.

[1242] Ellen Nakashima, "U.S. Not Naming China in Data Hack," *The Washington Post*, July 22, 2015.

executive orders "can all serve to develop international law."[1243] Like minded nations must actively work together to develop those customary principles if they are eventually to be seen as the law in cyberspace.

The capability to create norms of responsible behavior and other forms of cooperative measures exists, but to be credible, uncooperative nations have to believe that their interests are also at stake. Admiral Rogers has publicly communicated that point, in saying "To my Chinese counterparts, I would remind them, increasingly you are as vulnerable as any other major industrialized nation state. The idea that you can somehow exist outside the broader global cyber challenges I don't think is workable."[1244] Nonetheless strategic advisor Patrick Cronin pointed out that "China apparently does not want to buy into a post-World War II international system that it did not play a role in creating."[1245] Cronin believes that finding a meaningful partnership with China will require some adjustments to the international order. Then in that new order, nations will determine through international relations what is considered to be irresponsible or unacceptable behavior. Take for example espionage, which by its terms violates state sovereignty, but since states do it to each other, over time espionage has become part of customary international law established by state practice. The blurry line between cyber-enabled espionage and intellectual property theft complicates state interpretation of what are realistic and consistent norms for responsible behavior in cyberspace. For the latter activity, despite claims by the United States of massive economic damage, without actual physical damage, there is no clear consensus if cyber-enabled economic espionage even qualifies as a violation of territorial sovereignty. Until underlying state objectives and values converge to remove conflicting interests regarding cyberspace, the strategy of deterrence by entanglement will remain an

[1243] Catherine Lotrionte, "Cyber War: Definitions, Deterrence and Foreign Policy," Statement before the House Committee on Foreign Affairs, September 30, 2015.

[1244] Andrew Clevenger, "China 'Vulnerable' in Cyberspace, US Cyber Chief Warns," *Defense News*, November 21, 2015.

[1245] Patrick Cronin, "China's Problem with Rules: Managing a Reluctant Stakeholder," *War on the Rocks*, June 26, 2014: 3.

insufficient strategic cyber deterrence option. In sum, then, the shortcomings of deterrence by entanglement, and the primary mechanism of norms, if applied to cybered conflict are competing state interests, self-serving technical and legal interpretations, and plausible deniability of wrongful acts.

Section Three:

A New Strategic Option

CHAPTER VII

Active Cyber Defense

The strategy of active cyber defense is based upon the real-time detection and analysis of network security breaches seeks to create a comprehensive, automated and thereby unavoidable response to neutralize and reinforce the effects automatically through associated auto trigger of legal simultaneous countermeasures inside and beyond network and state territorial boundaries.[1246] Active cyber defense in the near term combines internal systemic resilience to defeat malicious cyber activity after a network intrusion and tailored disruption capacities to punish the attacker. It serves as a comprehensive combination of strategic capabilities available now and able to compensate for the shortcomings of denial and retaliation in contemporary deterrence approaches while more comprehensive structures combining all three contemporary approaches are being evolved. The strategy encourages adversary restraint by shaping malicious actor experiences and thereby perceptions of the costs and benefits of any given cyber attack automatically and at scale large enough to handle the multiplicity of malicious actors in cyberspace. Since intrusions may not always be stopped at the perimeter, active cyber defense operates at cyber relevant speed before malicious activity can affect networks and systems.[1247] Active cyber defense is different from static activities, which harden networks and systems through preventive controls. Active cyber defense uses reactive activities, which stop or limit damage through detective controls and remediation actions, seamlessly automated in a common framework of integration. According to the Defense Information Systems Agency deputy Chief Technology Officer, we need "cyber capabilities integrated with each other and automatically

[1246] Robert S. Dewar, "The Triptych of Cyber Security: A Classification of Active Cyber Defense," in *Proceedings 6th International Conference on Cyber Conflict* (Tallinn, Estonia: CCD COE, June 2014): 7-21.

[1247] U.S. Department of Defense, *Strategy for Operating in Cyberspace*, July, 2011: 7.

defending against things."[1248] That means using not just a defense-in-depth strategy to layer various methods of cyber defense, but to include the more flexible tools and capabilities to be included in the strategy of active cyber defense.

Admiral Michael Rogers, the head of the National Security Agency, warned the audience at the London Stock Exchange that "it is not about if you will be penetrated, but when."[1249] If true that cyber defenses cannot block an attack, then organizations have to close the time from compromise to discovery before an actor achieves their objectives. Yet in 2015, the time from evidence of compromise to discovery of compromise, or the median time that threat groups are present on a network before detection, was 146 days.[1250] Active cyber defense seeks to close that gap by using synchronized, real-time capabilities not only to discover and detect the breach, but also to analyze and mitigate the threat and vulnerabilities. The difficult question to ask is whether these improved defenses are adequate enough to stop malicious actors inside the network or if an appropriate response is necessary outside the network to disrupt their activities. The use of proportionate countermeasures is allowed to some extent under international or customary law but constrained under national law, depending upon the party invoking their rights. Therefore the scope or use of active cyber defense depends on authorities to act inside or outside of the network. It is worth noting that while the rights of an injured state to resort to countermeasures in response to an internationally wrongful act or omission are explicitly articulated by international law, an argument can be made that licensed private companies in the United States should have the right to hack back in self-defense or in defense of property. Private actor hack back could turn "the tables on the attacker," thwarting or stopping a crime, or

---

[1248] Amber Corrin, "A defense-in-depth strategy: DISA's evolving fight to defend DoD networks," *C4ISR& NETWORKS, DISA Vision and Contract Guide 2016: A10.*

[1249] Danny Palmer, "It is not about if you will be penetrated, but when, warns NSA Chief," *Computing News*, July 16, 2015.

[1250] Mandiant, "M-Trends 2016," Special Report, February 2016: 4.

even stealing back what was taken.[1251] However, it is not required for a robust active cyber defense strategy.

The promise of active cyber defense is to deny benefits through systemic resilience and impose costs through tailored disruption in a rapid, more comprehensive and practical manner than what the three contemporary deterrence approaches can currently offer. Certain aspects of the strategy are agnostic to the origins and motivations of the malicious actor unlike contemporary deterrence by retaliation. Specifically active cyber defense capabilities deny actor objectives and raise actor costs by obstructing or interfering actively with their progress in the cyber kill chain inside the network and thereby signaling failure and likely future failures rapidly and directly. Regardless of who is the actor, even state intelligence agencies, their malware or techniques are detected, diverted, blocked or terminated. In recognition that a perfect defense against intrusion is impossible, active cyber defense also offers remedies outside the network. Either way, inside or outside the network, the strategy seeks to convince malicious actors that it is no longer worth making the attack. The strategic option of active cyber defense possesses the three necessary conditions to achieve deterrence, specifically the capability to deliver an appropriate cyber response, the communications to signal intentions, and the credibility to not tolerate malicious activity.[1252] This chapter starts with an illustrative case that depicts the virtues of active cyber defense capabilities applied across before, during and after the cyber kill chain is initiated. It then examines the opportunities and issues for use of active cyber defense inside and outside the network a new strategy to achieve deterrence within the cyber arena, one that critically reinforces and compensates for – rather than replaces – the other three contemporary deterrence strategies.

[1251] Melissa Riofrio, "Hacking Back: Digital Revenge is Sweet but Risky," *PC World*, May 9, 2013.

[1252] Emilio Iasiello, "Hacking Back: Not the Right Solution," *Parameters*, Vol. 44, No. 3, Autumn 2014: 107.

Illustrative Case of Active Cyber Defense Virtues

The massive theft of data at the mega retailers Target Corporation in 2013 and Home Depot in 2014 exhibited many similarities. In both incidents, attackers were able to upload malicious software to point-of-sale machines and collect unencrypted credit and debit card data for exfiltration. The Reedum malware, nearly identical to BlackPOS sold on cybercrime forums, used in the Target breach,[1253] was the basis for the tool used against Home Depot.[1254] The initial intrusion into the Target system was traced to network credentials stolen from a third party refrigeration, heating and air conditioning vendor.[1255] Likewise, an investigation revealed that criminals used a third-party vendor's user name and password to enter into Home Depot's network.[1256] After authenticated access to the networks, attackers moved laterally to eventually compromise the point-of-sale systems at checkout counters. In both high profile breaches, personal and financial information of millions of customers was exposed for criminal uses. This exposure was not deterred but could have been prevented by active cyber defense. Its exceptionally rapid and comprehensive detection, verification, and remediation of malicious behavior in the cyber kill chain, could have stopped harm or damage before the breach occurred.

Most organizations do not have reliable visibility of malicious activity in their networks. The most common approach is to look for indicators of compromise, such as virus signatures. This approach tends to produce high amounts of false positives, which can desensitize security teams to notifications. In the Target breach, the FireEye malware intrusion detection system

---

[1253] Brian Krebs, "A First Look at the Target Intrusion, Malware," Krebs on Security, January 15, 2014.

[1254] Danny Yadron and Shelly Banjo, "Home Depot Upped Defenses, But Hacker Moved Faster," *The Wall Street Journal*, September 12, 2014.

[1255] Brian Krebs, "Target Hackers Broke in Via HVAC Company," Krebs on Security, February 14, 2014.

[1256] Stephen Holmes and Diane Dayhoff, "The Home Depot Reports Findings in Payment Data Breach Investigation," The Home Depot, Atlanta, November 6, 2014.

used by the retailer actually detected the data exfiltration malware used in the attack, but reportedly the security team ignored the urgent alerts and did not allow the FireEye software to delete the malware.[1257] They claimed to receive hundreds of alerts each day and had difficulty determining which were malicious.[1258] This situation portrays a need for an approach that accurately and automatically prioritizes alerts. For example the previously described HawkEve G advanced threat detection and response platform provides that approach in using a threat feed that combines network and host sensors in order to detect and perform correlation on sophisticated and emerging threats. In addition, the platform collects a baseline of historical data across the network and hosts to determine anomalous behavior and activities. The vendor adamantly claims that "several months prior to the cyber attacks on Target and Home Depot, the HawkEye G threat feed had already blacklisted the source and could have helped both retailers detect and prevent these attacks."[1259] This claim supports the notion that the use of behavioral analytics with threat intelligence to detect and investigate threats in real time can optimize efforts of security teams.

In both the Target and Home Depot breaches, the starting point for detection was well inside the cyber kill chain due to attacker use of valid vendor credentials. Verizon consultants hired to probe the Target networks days after the breach found "no controls limiting their access

[1257] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," *Bloomberg Businessweek,* March 13, 2014.

[1258] Cybereason, "The Seven Struggles of Detection & Response," White Paper, 2015: 1-5.

[1259] Hexis Cyber Solutions, "How to Automate Cyber Threat Removal," A HawkEye G Technical White Paper, October 2015: 5, and John Breeden III, "Network World Gives HawkEye G 4.875 out of 5," *Network World,* December 8, 2014. Independent analysis of HawkEye G finds the endpoint detection and response system automatically catches malware, stops running processes, and quarantines malicious files.

to any system."[1260] Instead they discovered systems and services with either weak or default passwords and either outdated or missing security patches. These discoveries meant once inside Target's network, there was nothing to stop the attackers from moving across the cyber kill chain, as depicted by phases in the chapter on deterrence by denial (on page 234). The first opportunity for Target to disrupt the breach was at the Delivery phase, by requiring two-factor authentication for its vendors which means besides the stolen credentials, a second step is included such as a token or phone code or security question. At the Exploitation phase, Target could have paid attention to the FireEye software alerts or allowed malware deletion. At the Installation phase, it is suspected that the attacker exploited a default account name in a software management system, which Target could have altered. In the Command and Control phase, the method used by the attackers is unclear and Target's protective options were limited to Firewalls. Finally, at the Actions on Objectives phase, Target could have white listed[1261] - created listings of pre-approved - File Transfer Protocols (FTP), which is "a standard internet protocol for transmitting files between computers on the internet,"[1262] designated servers for uploading data, thereby blocking transmissions to outside servers, at least one found later to be located in Russia. Outside the network, Target's FireEye software did decode the destination of the servers on which stolen credit card data was stored for days at a time,[1263] opening an opportunity to disrupt the files on those servers.

Although the opportunities for breaking the kill chain appear limited in the Target breach, an analysis of the actions of the attacker and placement of resources to address capability gaps

[1260] Brian Krebs, "Inside Target Corp., Days after 2013 Breach," Krebs on Security, September 21, 2015.

[1261] Ajay Kumar, "Whitelisting: Filtering for advanced malware prevention," Tech Target, April 14, 2014.

[1262] Margaret Rouse, "File Transfer Protocol (FTP) Definition," July 13, 2015.

[1263] Committee on Commerce, Science, and Transportation, "A "Kill Chain" Analysis of the 2013 Target Data Breach," Majority Staff Report for Chairman Rockefeller, March 26, 2014: 7-11.

"raises the costs an adversary must expend to achieve their objectives."[1264] A number of technologies and processes can be identified and applied to detect, deny, disrupt or recover at each phase of the kill chain.[1265] For example the LightCyber Magna platform combines many of these technologies and processes across the kill chain for network and endpoint behavioral detection. Magna uses a next generation firewall at the Delivery phase, an intrusion detection system at the Exploitation phase, and endpoint detection and response at the Installation phase. Magna embraces the industry-wide megatrend toward automated removal of advanced threats. For instance one requirement in the trend is the ability to detect data flows, which might include outbound traffic from an internal server.[1266] Magna profiles the pattern and rate/volume of data sent to outside entities by domain and destination. It detects a change or anomaly in rate/volume of data sent. In the Target breach, the malware sent stolen data to an external FTP server via another compromised Target server used to collect the credit and debit card data. Over a period of two weeks, the attackers collected and transmitted 11 GB of stolen information.[1267] Not only does Magna have the capability to detect anomalously large uploads to external servers via FTP, Magna also includes a significant concentration of algorithms designed to detect the internal communications/movement of data to/from a compromised server. Magna almost certainly would have alerted on this activity (and the control of the compromised server) before the data exfiltration phase, preventing the exposure of customer financial data.

1264 Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, March 2011: 3.

1265 Looking Glass, "Addressing the Cyber Kill Chain: Full Gartner Research Report and Looking Glass Perspectives," Research Note, Table 1, 2016: 9.

1266 Bob Gourley and Roger Hockenberry, "Automating Removal of Advanced Threats/Malware," White Paper, CTOlabs.com, June 2014: 1-7.

1267 Aviv Raff, "POS Malware Targeted Target," Seculert Blog Post, January 16, 2014.

Today organizations like Target do not have to rely on manual analysis and adjustments. Automated active defense solutions, inside the network, provide distinct advantages over the attacker and warrant further consideration as a way to change the cost and benefit paradigm.

Inside Defender's Network

Although preventive controls have improved, so too have the techniques used by malicious actors to penetrate cyber defenses. They morph, encrypt and disguise existing malware so it cannot be detected by signature based defenses; develop custom malware for zero day targeted attacks before signature distribution; and create evasive malware that hides from sandboxes (virtual test environments) that attempt to capture and evaluate malware intent and capabilities.[1268] Even if security teams can find an initial threat indicator, it often takes days or weeks to trace the attack, analyze the threat, quarantine compromised systems, and implement remediation actions. The longer that process takes, the longer the malicious actor has to achieve objectives inside the network. Active cyber defense compensates for the shortcomings of deterrence by denial through reactive capabilities predicated on automated and integrated technologies. To break the cyber kill chain, active cyber defense synchronizes "the real-time detection, analysis, and mitigation of threats to critical networks and systems."[1269] Active cyber defense creates internal systemic resilience, wherein networks and systems can withstand a potential attack. Hence, the U.S. Defense Department has stated its intention to invest in resilient systems to continue operations in the face of disruptive or destructive cyber attacks. Documented as a form of deterrence, the U.S. Defense Department asserts that "effective resilience measures can help convince potential adversaries of the futility of commencing cyber attacks."[1270] Furthermore "in order for resilience to succeed as a factor in effective deterrence" in organizations that "fall outside its authority," the Defense Department counts on other

[1268] FireEye, "Debunking the Myth of Sandbox Security, White Paper, 2015.

[1269] National Security Agency Information Assurance Directorate, "Active Cyber Defense (ACD)," Fact Sheet, October 22, 2015: 1-2.

[1270] U.S. Department of Defense, "The DoD Cyber Strategy," April 2015: 10-11.

government agencies to “work with critical infrastructure owners and operators and the private sector to develop resilient and redundant systems” through a comprehensive cyber deterrence strategy.[1271]

Typical Proactive Activities

Common active cyber defense approaches have achieved resilience by placing emphasis on proactive methods to engage or deceive the adversary before or during a cyber incident. An organization might respond to an attack using as many as three active defense concepts: detection, deception, and termination.[1272] For the first concept, a variety of techniques can detect an attack, but the most prominent to attract attackers and look for their patterns of behavior are the use of honeypots and sinkholes per below:

Honeypots: are computer systems set up to act as a decoy to lure attackers away from assets of real value. They can be isolated or placed inside a production network to detect, deflect or study attempts to gain unauthorized access.[1273] Honeypots elicit exploitation by attackers by the use of real or simulated vulnerabilities or by configuration weakness, like easily guessed passwords.[1274] Legal issues confound the use of honeypots, in particular concerning privacy rights and entrapment accusations. Privacy concerns stem from honeypot recording and monitoring of all activity occurring on the device without consent. Entrapment concerns stem from inducement or encouragement of a person to commit a crime.[1275] Yet neither privacy nor

---

[1271] Ibid, 11.

[1272] Irving Lachow, “Active Cyber Defense: A Framework for Policy Makers,” Center for a New American Security, February 2013: 1-7.

[1273] Margaret Rouse, “honeypot (honey pot),” Tech Target, April 11, 2016.

[1274] Anand Sastry, “Honeypots for network security: How to track attackers’ activity,” Tech Target, November 16, 2010.

[1275] Jerome Radcliffe, “CyberLaw 101: A primer on US laws related to honeypot deployments,” SANS Institute, 2007: 1-14.

entrapment would be considered as a serious legal defense, for after all, the attacker committed the intrusion in the first place without authorization. The real issue is that organizations that deploy honeypots have to watch for their misuse, for if a malicious actor uses the honeypot as a launch point to attack other systems, then the organization could be held liable for any damages.[1276]

Sinkholes: are a system under the control of a defender used to intercept and receive traffic redirected from infected machines, like a botnet. The can provide intelligence to craft appropriate defenses, identify infection targets or geographically locate attackers.[1277] Organizations can set up an internal sinkhole where only traffic bound for an external malicious IP from victim machines in the organization is manipulated. Or they can set up an external sinkhole by registering known malicious domains as they expire or if not registered at all. Legal issues confound the use of external sinkholes in that victim machines that do not belong to your organization are now contacting a server you control, which is a criminal act in most jurisdictions. Another issue is that victims have a right to be notified if their machines are infected, which requires a reporting mechanism to do so.[1278]

While honeypots and sinkholes also deceive the attacker, other methods in a deception campaign include allowing the attacker "to steal documents that contain false or misleading information."[1279] While this method is intended to protect intellectual property or trade secrets, there could be harm if the misleading information is accidently leaked to the public and results in damage to the organization's credibility or reputation. The final concept of termination stops the

---

[1276] Ed Skoudis, "What security risks do enterprise honeypots pose?" Tech Target, January 4, 2008.

[1277] David Sancho and Rainer Link, "Sinkholing Botnets," A Trend Micro Technical Paper, March 30, 2011: 1-6.

[1278] John Bambenek, "Principles of Malware Sinkholing," *Dark Reading*, April 6, 2015.

[1279] Irving Lachow, "Active Cyber Defense: A Framework for Policy Makers," Center for a New American Security, February 2013: 6.

attack while it is occurring. In order to prevent information from leaving the network, the idea is to sever connections with the infected computer, although that might not work if the attacker has already moved laterally in the network. Each of the three options have merit but as rudimentary singular methods they have inherent limitations. Therefore today's approach for active cyber defense focuses on the advanced automation and integration of multiple services and mechanisms to execute detection, verification and remediation in cyber-relevant time.

New Reactive Approaches

Automation has become a key component of network protection strategies. As stated by the Chief Technology Officer at network management and discovery tools developer Solar Winds, "automating network security can help to quickly pinpoint a breach, identify the root cause and often help to resolve the issue quicker than manually checking every endpoint and connection."[1280] A corollary to automation is security event correlation, which can produce suitable remediation decisions. Those decisions can also be automated, like to revise user authorization privileges, place systems into protected zones, or redirect network flows. Once automated processes replace human operators, networks become more responsive to attacks. Humans are being overloaded with data, especially false positive alerts (errors in evaluations) from security information and event management (SIEM) systems. Automation systems can extract insights from data sets and device logs in real time. For example, Carbon Black technologies automate the continual recording of critical data before the moment of compromise, so after a breach is discovered, Carbon Black can highlight activity to better understand the cause and scope of the intrusion.[1281]

[1280] John Edwards and Eve Keiser, "Automating Security," *C4ISR& NETWORKS,* October 2016: 16.

[1281] Carbon Black, "Disrupting the Threat: Identify, Respond, Contain & Recover in Seconds," White Paper, 2014: 1-12.

The Carbon Black capability to continuously monitor connections and devices while correlating logs and data of user activity turns security automation into a reactive tool to deny malicious actors the benefit of their attack. Automation empowers security teams to act more quickly and aggressively to stop data breaches before they can threaten an organization. Today security teams lack the speed and agility to respond to a suspected data breach. Not only do teams lack the personnel and tools to identify anomalous behavior across endpoints and the network, they are not authorized to actually shut it down.[1282] Given the consequences of a data breach, organizations can no longer rely on manual procedures. They have to reduce the time to query through data, detect the breach and get to the decision point on remediation. Automation enables 24 hour security operations, with policy changes in remediation decisions if humans are or are not in the loop. At the same time, automation allows organizations to reduce manpower and save costs, by shifting basic and mundane tasks to machines. This benefit is important given ominous projections of shortfalls of more than 1.5 million information security professionals in the global cyber security workforce by 2019. According to Brett Helm, Chairman and CEO of DB Networks, "Intelligent IT security automation through machine learning and behavioral analysis is faster, more accurate, and frees up skilled professionals to focus on more critical issues."[1283]

Besides the advantages of automation, the integration of a diverse set of capabilities improves an organization's ability to respond to a cyber attack. Take for example the integration of endpoint detection and response solutions with third party devices or services. An endpoint is an Internet-capable computer hardware device, such as a desktop computer, laptop, smart phone, printer or other specialized hardware such as a point-of-sale terminal or smart meter.[1284]

[1282] John Kindervag and Stephanie Balaouras, "Rules of Engagement: A Call to Action to Automate Breach Response," Forrester Research, Inc., December 2, 2014: 1-11.

[1283] Steve Morgan, "Cybersecurity job market to suffer severe workforce shortage," Cybersecurity Business Report, July 28, 2015: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

[1284] Margaret Rouse, "endpoint device," WhatIs.com, July 2013.

Endpoint detection and response solutions monitor a range of actions on these devices. For example, they track registry entries created, edited and deleted; files created, opened, modified and deleted; changes in process tables; and network connections to other systems on the network or to unknown servers on the Internet.[1285] The advantage of these types of detection and response solutions is the ability to find and react to the activities of malware that may have evaded preventive controls. Yet to be effective, the endpoint detection and response solutions have to integrate easily with other devices, for example to automatically send unknown files to a sand box for analysis, or with other services, for example to get up-to-date threat intelligence based on the actor techniques. Therefore, the actuation of active cyber defense inside the network requires combinations of capabilities to collect security data, detect advanced malware, apply threat intelligence, conduct forensic analysis, and implement remediation actions.

Single Integrated Platforms

Active cyber defense strives to provide real-time defense inside the network through automation and integration of cyber defense services and capabilities. These synchronized services and capabilities are used to discover and detect a breach, and interdict, isolate or remove the threat. The benefits of new active defense solutions include:[1286]

- Detection of known, unknown, and zero-day threats missed by most anti-virus products.
- Coupling of enhanced threat intelligence and behavioral analytics on endpoint activity.
- Integration with the most effective commercial security solutions on the market.
- Threat response by policy-based automated or machine-guided remediation actions.
- Integration to SIEM systems, big data analytics, and real-time dashboards.

[1285] Dell SecureWorks, "Eliminating the Blind Spot: Rapidly detect and respond to the advanced and evasive threat", White Paper, 2015: 1-6.

[1286] Hexis Cyber Solutions, "Active Cyber Defense: Integrated, Automated, Effective," December 11, 2015: 3.

The need for continuous threat detection and response is becoming obvious and a number of endpoint security solutions achieve the benefits of automated investigation and removal. For example, one option is HawkEye G, acquired by WatchGuard Technologies,[1287] which provides automated detection, verification, and remediation capabilities in a single integrated endpoint detection and response platform.[1288]

HawkEye G received a score of 4.875 out of 5 in testing of ability to identify, block and remove threats in an independent evaluation.[1289] Hexis has described the ability of the Hawkeye G platform to remove advanced threats at machine speed before they can steal data, compromise intellectual property or cause process disruption.[1290] The platform provides visibility of threat actor activity on the endpoint through host and network sensors. The host sensor uses heuristics that analyze files, processes and registry events as they are created, modified, or executed. 175 different heuristics are calculated individually and then combined to give an initial threat score that is enhanced by cloud-based malware verification service. Network sensors utilize deep packet inspection technology to detect application usage by threat actors. The inspection module looks for outbound communication from infected endpoints, specifically for command and control traffic and downloading of exploits and remote access toolkits. The HawkEye G threat feed that covers malware data, phishing URLs, and controller information, is aggregated from multiple sources, to include integrated third party devices such as Palo Alto Networks Wildfire and FireEye Network Security. After the threat is verified and assigned a unified score, a range of network and host-based countermeasures are deployed to remediate the threat. Machine

---

[1287] Chris Warfield, "WatchGuard Acquires Hexis HawkEye G to Deliver Holistic Network Security from the Network to the Endpoint, WatchGuard Technologies, June 7, 2016.

[1288] Hexis Cyber Solutions, "HawkEye G: Endpoint Detection & Response," Products, August 27, 2016: https://www.hexiscyber.com/products/hawkeye-g

[1289] John Breeden III, "Network World Gives HawkEye G 4.875 out of 5," *Network World*, December 8, 2014.

[1290] Hexis Cyber Solutions, "How to Automate Cyber Threat Removal," A HawkEye G Technical White Paper, October 2015: 3.

guided actions for the host include to kill an executing process, quarantine a file, remove a registry value hijacked by malware, or whitelist a process and for the network include block access to controller URLs and divert traffic to/from an external server to a Bot Trap. Countermeasures can be executed manually or through automated policies based on multiple configurations that consider targets, scores and actions.[1291]

Another previously discussed platform is LightCyber Magna, acquired by Palo Alto Networks,[1292] that combines automated investigation and integrated remediation to reduce attacker dwell time and minimize damage.[1293] Like Hawkeye G, it was developed in response to a current lack of ability to detect active attacks. The difference is Magna detects attackers through the anomalies their activity introduces. The platform profiles normal user and device behavior then uses attack detectors to find behavior that registers as anomalies against those profiles. Magna has hundreds of detectors across all phases of the cyber kill chain, from reconnaissance, lateral movement, command & control, and data exfiltration. Magna embraces criticism of the kill chain expressed at Black Hat 2016 that the steps to be addressed should be internal, under a presumption of breach.[1294] A pertinent example is at the internal reconnaissance phase after intrusion, where the attacker is attempting to find out what servers and services are accessible or what vulnerabilities are available, Magna uses profiles of patterns of internal connections to find attack detectors, such as changes in connections, rates of connections and use of ports and protocols.[1295] Magna then enhances anomalous process findings with threat intelligence and malware analysis. Upon confirmation of an active attack, Magna provides one-click remediation through integration with third party security tools. Supported capabilities

---

[1291] Hexis Cyber Solutions, “HawkEye G Technical White Paper,” Release 3.1, October 2015: 3.

[1292] LightCyber, “Palo Alto Networks Completes Acquisition of LightCyber,” Press Release, February 28, 2017.

[1293] LightCyber, “Closing the Breach Detection Gap,” Data Sheet, 2015: 1-3.

[1294] Tim Greene, “Why the ‘cyber kill chain’ needs an upgrade,” *Computer World*, August 8, 2016.

[1295] LightCyber, “Magna Detection Technology,” White Paper, November 2015: 1-6.

include the ability to revoke user credentials or force a password reset with Microsoft Active Directory, or quarantine breached endpoints and malicious IPs or URL domains with Palo Alto Networks next generation firewall.[1296]

Outside Victim's Network

For the state the aggressive use of countermeasures beyond network and state territorial boundaries is governed by international law. Proportionate countermeasures are allowed in response to harm originating from a state.[1297] In the cyber context, countermeasures represent disruption capacities tailored to the circumstances of the harm. For private companies, not acting on behalf of the state, a number of legal issues confront the use of these forward deployment techniques. However, U.S. common law does admit "certain rights of self-defense and the defense of property in preventing the commission of a crime against an individual or a corporation."[1298] The defense of property is more limited in range of allowable actions, roughly comparable to what is allowed for non-lethal self-defense. For private companies the relevant concept will most always be defense of property, although that right does not allow for vigilantism. An argument exists that private companies have no choice but to resort to self-help, as the government is doing too little to protect them.[1299] Without policy or guidance, victims might already be taking self-help actions based on their own judgements and perceptions, which

---

[1296] LightCyber, "The New Defense against Targeted Attacks," White Paper, March 2015: 7.

[1297] Catherine Lotrionte, "State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights," *Emory International Law Review*, Vol. 26, May 28, 2013: 904.

[1298] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington D.C.: The National Academies Press, 2009). 204-205.

[1299] Sean L. Harrington, "Cyber Security Active Defense: Playing with Fire or Sound Risk Management," *Richmond Journal of Law & Technology*, Volume XX, Issue 4, September 17, 2014: 33.

could have substantial consequences. A Black Hat survey in 2012 found that thirty-six percent of attendees when asked "Have you ever engaged in retaliatory hacking?" said either "once" or "frequently".[1300] The question of whether private companies should be licensed to act on the government's behalf persists in the face of debilitating cyber attacks.

Permissive Conditions

In the Tallinn Manual 2.0, Rule 20 delineates that "A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that is owed by another State."[1301] The Rule is derived primarily from the *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, developed by the International Law Commission. Although not a binding treaty, the Draft Articles are authoritative and reflect and constitute customary international law, as extensively cited by legal bodies for fifteen years and commended to governments by the UN General Assembly.[1302] They define countermeasures as "measures which would otherwise be contrary to the international obligations of [an] injured state *vis-à-vis* the responsible state if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation."[1303] Regarding what constitutes an internationally wrongful act, the responsible state would for example have violated a treaty or customary law obligation. Prominent among

---

[1300] Shelley Boose, "Black Hat Survey: 36% of Information Security Professionals Have Engaged in Retaliatory Hacking," Business Wire, July 26, 2012: http://www.businesswire.com/news/home/20120726006045/en/Black-Hat-Survey-36-Information-Security-Professionals

[1301] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second Edition (Cambridge University Press, 2017): 111.

[1302] United Nations, "Responsibility of States for Internationally Wrongful Acts," General Assembly Resolution 56/83, December 12, 2001: Annex.

[1303] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, fifty-third session, 2001: Chapter II, Commentary, Para. 1.

treaty obligations is the prohibition on the use of force contained in Article 2 of the Charter of the United Nations.[1304] Rule 69 of the Tallinn Manual 2.0 affirms that a cyber operation "constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[1305] Prominent among customary law is the principle of sovereignty, which protects cyber infrastructure located on the territory of a state. Therefore cyber operations against that infrastructure that qualifies as a use of force would amount to a violation of that state's sovereignty. International law experts have taken the position that sovereignty can be violated even when no damage or injury results, such as in the case of the emplacement of malware or destruction of data.[1306]

The purpose of countermeasures is to persuade the responsible state to adhere to its legal obligations or to remedy existing harms. They are not allowed for other purposes, such as retribution or punishment. If the target state resumes its obligations of cessation and reparation, the measures are to be discontinued.[1307] Therefore, a state cannot be motivated by punitive considerations to use countermeasures, especially if the other state's breach of international law has ended. In general, countermeasures are allowed only after the injured state has asked the state in question to cease its internationally wrongful act. However this requirement is not absolute if urgent measures without notification are deemed necessary for the injured state to "preserve its rights and avoid further injury."[1308] In the cyber context, countermeasures "often represent an effective means of self-help by allowing the injured state to take urgent action that would otherwise be unavailable to it, such as 'hacking back,' to compel the responsible state to

---

[1304] United Nations, Charter of the United Nations, Chapter VII, Article 2, San Francisco, CA, October 24, 1945.

[1305] Tallinn Manual 2.0, 330.

[1306] Michael N. Schmitt, ""Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law*, Vol. 54:3, 2014: 704-705.

[1307] Responsibility of States, Article 49 (1 and 2).

[1308] Tallinn Manual 2.0, 120.

cease its internationally wrongful cyber operations."[1309] In their application, countermeasures must be "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act."[1310] This can be interpreted as proportionate to the breach of obligations. This restriction is intended to avoid the risk of escalation, where states respond interactively with acts of increased scope and duration. Also, countermeasures must not themselves violate the prohibition on the use of force.[1311] They should to the extent feasible be taken in such a way that permits the resumption of performance of the breached obligations in question. All of this means countermeasures should consist of temporary measures that produce as far as possible reversible effects[1312] and may only occur during an attack because "countermeasures must be suspended when the internationally wrongful act has ceased"[1313] – a currently nearly impossible requirement for any but the active cyber defense strategic option.

Countermeasures are allowed to be used when the breach of obligation is attributable to the responsible state.[1314] The clearest case of being attributable is when acts are conducted by state organs, like military or intelligence agencies. Acts committed by persons or entities that are empowered to exercise government authority, such as by a private company under contract from the state are equally attributable.[1315] Additionally, the conduct of a person or group of persons shall be considered an act of a state if "acting on the instructions of, or under the direction or

---

[1309] Michael N. Schmitt & Liis Vihul, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution," *Fletcher Security Review*, Vol I, Issue II, Spring 2014: 59.

[1310] Responsibility of States, Article 51.

[1311] Responsibility of States, Article 50 (1a).

[1312] Tallinn Manual 2.0, 119.

[1313] Michael N. Schmitt, ""Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law*, Vol. 54:3, 2014: 716.

[1314] Responsibility of States, Article 2 (a).

[1315] Below the Threshold, 669.

control of, that state in carrying out that conduct."[1316] For instance, although the Iranian activist group Cutting Sword of Justice immediately took credit for attacking Saudi Aramco Oil Company with the Shamoon malware in 2012,[1317] eventually the attack and group were attributed to the government of Iran by U.S. authorities.[1318] However, incidental or peripheral association does not qualify as attribution. For instance, the patriotic hacker operations conducted against Estonia in 2007 and Georgia in 2008 were not sufficiently determined to be under the control of Russia to justify attribution, and therefore the use of countermeasures. Likewise, although the hacktivist organization calling itself the Syrian Electronic Army has hacked and defaced over 40 sites, mostly global media outlets and notable universities, to voice political sentiments in support of the Assad regime since 2011,[1319] in the absence of proven instructions, direction, or control by Syria, the use of countermeasures is not an available response option for the injured state.

The limitation on use of countermeasures to acts by or attributable to states is significant since today the majority of harmful cyber operations are conducted by non-state actors. In observation of these constraints, the plea of necessity may offer relief to "states facing harmful non-state cyber operations" under certain conditions.[1320] A state may invoke necessity as a ground for precluding the wrongfulness of an act if it is the "only way for the State to safeguard an essential interest against a grave and imminent peril."[1321] An essential interest is "one that is

---

[1316] Responsibility of States, Article 8.

[1317] Kelly Jackson Higgins, "Shamoon, Saudi Aramco, And Targeted Destruction," *Dark Reading*, August 22, 2012.

[1318] Siobhan Gorman and Julian E. Barnes, "U.S. Says Iranian Hackers Are Behind Electronic Assaults on U.S. Banks, Foreign Energy," *The Wall Street Journal*, October 12, 2012.

[1319] HP Security Research, "Syrian Electronic Army," HPSR Threat Intelligence Briefing Episode 3, April 2013: 22-24.

[1320] Michael Schmitt, "In Defense of Due Diligence in Cyberspace," *Yale Law Journal Forum*, Vol. 125, No. 68, June 22, 2015: 77.

[1321] Responsibility of States, Article 25 (1a and b).

of fundamental and great importance to the State concerned."[1322] The peril is grave "when the threat is especially severe."[1323] Examples of when essential interests are gravely and imminently threatened would be in cyber operations that debilitate the state's banking system, ground flights nationwide, halt all rail traffic, alter national health records or shut down a large electrical grid.[1324] In certain cases where the exact nature or origin of a cyber attack is not clear, a state may justify cyber measures on the basis of the plea of necessity. For example in an emergency situation, a state could decide to shut off its own cyber infrastructure, as the only way to protect itself, even if doing so affects other state's cyber systems. In this instance the state's action is "directed against the danger itself, and not directed against another state or aggressor."[1325] Similarly, if significant cyber operations of unknown origin target its critical infrastructure, the Tallinn Manual 2.0 contends that "the plea of necessity could justify a State's resort to counter-hacking."[1326] Therefore, the plea of necessity provides a failsafe for a state facing severe cyber operations when they cannot be attributed to another state. For that matter, "factual and legal attribution is not a precondition to action," only that the state "locate the technological source of the harmful operation and assess the consequences of its own response."[1327] Therefore the plea can be resorted to whether the malicious actor is governmental or private.

Disruption Choices

"Only an injured state may engage in countermeasures" in response to an internationally wrongful act, or engage in counter-hacking under the plea of necessity, to disrupt a cyber

---

[1322] Tallinn Manual 2.0, 135.

[1323] Ibid, 136.

[1324] Ibid.

[1325] Benedikt Pierker, "Territorial Sovereignty and Integrity and the Challenge of Cyberspace," *Peacetime Regime for State Activities in Cyberspace*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): 214.

[1326] Tallinn Manual 2.0, 138.

[1327] In Defense of Due Diligence, 78.

operation in progress.[1328] The more controversial term hack back usually applies when a private organization responds with a counterattack. The difference between countermeasures and hack back is accessing a computer, network or information systems without authorization. An organization may be motivated to hack back against an attacker "to recover or wipe stolen data or intellectual property."[1329] An organization may also be motivated to enact revenge by "disrupting or damaging the malicious actor's system" or "degrading their capability to conduct future attacks."[1330] The cyber security firm Symbiot has placed methods of hack back into three categories: 1) invasive techniques to obtain access and then purse a "strategy of disabling, destroying, or seizing control over attacking assets," 2) symmetric counterstrikes which proportionally exploit "vulnerabilities on the attacker's system," and 3) asymmetric counterstrikes which constitute "retaliation... far in excess of the attack."[1331]

Countermeasures and hack back are similar in that an entity, whether a state or a private company, returns fire or sends data back at the attacker in some manner to stop the attack. Thus the range of tailored disruption choices for the two is blurred by motivation and authority. The range of countermeasures represents a sliding scale of aggressive actions that may include:

- Allow attackers to steal bogus files or embed beacons that reveal his location[1332]

[1328] Tallinn Manual 2.0, 130.

[1329] Peter Sullivan, Hacking back: A viable strategy or a major risk?" Tech Target, May 2, 2016: http://searchsecurity.techtarget.com/tip/Hacking-back-A-viable-strategy-or-a-major-risk

[1330] Ibid.

[1331] Bruce P. Smith, "Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help," *The Journal of Law, Economics & Policy*, Vol 1, Issue 1.2, 2005: 177-178.

[1332] Sean L. Harrington, "Cyber Security Active Defense: Playing with Fire or Sound Risk Management," *Richmond Journal of Law & Technology*, Volume XX, Issue 4, September 17, 2014: 11-13.

- Bait files with malware to photograph the malicious actor using his webcam[1333]
- Infiltrate malicious actor networks to retrieve, alter or delete stolen data
- Implant malware to damage or ransomware to lock down actor computers[1334]
- Insert logic bombs into files before stolen to damage computers when opened
- Use Denial of Service attacks to interfere with malicious activity

These methods are usually enabled by a combination of intrusion detection system technology to detect the intrusion and advanced traceback technology to ensure accurate targeting of the hacker.[1335] Primary IP traceback schemes or techniques are link testing, packet marking, ICMP (Internet Control Message Protocol) traceback, and log-based traceback.[1336] Analysis of logs (firewall, router, server and endpoint operating system) that extend from the network to the endpoint could reveal and correlate inbound and outbound attack patterns for route determination. Other methods for traceback include use of the Google Alerts function to search for stolen files, recognition of actor tactics, techniques and procedures (TTP), and inspection of industry threat intelligence. Some form of the disruptive responses above have been occurring for the past decade, by both government agencies and private companies, and software packages designed to execute them have been made commercially available to private companies.

[1333] Sam Cook, "Georgia outs Russian hacker, takes photo with his own webcam," *Geek News*, October 31, 2012, and Ministry of Justice of Georgia, "Cyber Espionage Against Georgian Government, CERT-Georgia, March 2011: 22.

[1334] Kaspersky Lab, "Ransomware: All Locked Up and No Place to Go," White Paper, 2016: 1-16.

[1335] Jay P. Kesan and Carol M. Hayes, "Thinking Through Active Defense in Cyberspace," *Proceedings of a Workshop on Deterring Cyberattacks*, (Washington, D.C.: The National Academies Press, 2010): 328-331.

[1336] Vijayalakshmi Murugesan, "A Brief Survey of IP Traceback Methodologies," Acta Polytechnica Hungaria, Vol 11, No. 9, 2014: 197-216.

Employment Options

Private Companies. Since only an injured state may use countermeasures or counter-hacking, there is no basis under international law for a private company, such as an Information Technology service or security firm, to act on its own initiative in response to malicious cyber activity.[1337] Private companies conducting methods of hack back would be subject to national criminal law for any violations of legal statute and be held criminally liable for unintended consequences. For example in the United States, a company that decides to hack back might face criminal and civil liability under the Computer Fraud and Abuse Act (CFAA).[1338] Specifically the CFAA stature 1030(a)(5) prohibits and punishes the following offenses for whoever "knowingly causes the transmission of a program, information code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer" and "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage."[1339] The paragraph establishes "crimes of dual intent - the intent to knowingly or intentionally intrude and intent to damage."[1340] Damage is defined as "any impairment to the integrity or availability of data, a program, a system, or information."[1341] Computer damage is a crime under the paragraph only if it involves a protected computer, which includes those used by the government, financial institutions, or in interstate or foreign commerce or communications.[1342] Under U.S. law, the punishment for a violation of the

[1337] Tallinn Manual 2.0, 130.

[1338] Cybersecurity Unit, "Best Practices for Victim Response and Reporting of Cyber Incidents," Computer Crime & Intellectual Property Section, U.S. Department of Justice, Version 1.0, April 2015: 12.

[1339] 18 U.S.C. 1030(a)(5)

[1340] Charles Doyle, "Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws," Congressional Research Service Report 97-1025, October 15, 2014: 31.

[1341] 18 U.S.C. 1030(e)(8)

[1342] 18 U.S.C. 1030(e)(2)

paragraph (summed up as knowingly causing a transmission that intentionally causes damage) depends on the severity of damage or loss, but could be imprisonment for 1 to 20 years, or even life, and fines up to $500,000.[1343]

Arguments do exist to allow a company to exercise its rights to self-defense and defense of property. As a general principle, one has the right to defend one's self and one's property by reasonable force.[1344] Hack back could be warranted if traditional law enforcement schemes are inadequate in response, which are hampered by the speed by which cyber attacks create damage and the multiple jurisdictions with varying laws and procedures often used to stage the attack. Other criteria for determining if hack back is an optimal solution include whether the likelihood of striking the attacker is higher than innocent third parties and whether damage to the victim outweighs potential damage to third parties.[1345] Although the CFAA appears to be clear on the matter, ambiguities do exist that could allow a company to exercise the principle of self-help. In particular debate exists on the meaning of the term "authorization." For example even though there is no exemption in the CFAA for a private party, "does a hacker nonetheless implicitly grant authorization to a hack back when that person infiltrates a victim's systems and exfiltrates digital assets? Is authorization a binary concept, for which permission is or is not granted?"[1346] If authorization is interpreted in a manner desirable to those who would engage in such activities, hack back by private companies could serve as a deterrent and supplement law enforcement. For

[1343] Congressional Research Service Report 97-1025, 35-37.

[1344] Kenneth W. Simons, "Self-Defense: Reasonable Beliefs or Reasonable Self Control," *New Criminal Law Review*, Volume 11, Number 1, Winter 2008: 51-90.

[1345] Jay P. Kesan and Ruperto Majuca, "Optimal Hackback," *Chicago-Kent Law Review*, Vol. 84, Issue 3, Article 10, (June 2009): 834-838.

[1346] Kim Peretti and Todd McClelland, "Legal Issues with Emerging Active Defense Security Technologies," Cyber Alert, Alston & Bird, LLP, January 2013: 1-4.

if a malicious actor knows that a particular company will strike back, they might be inclined to not attack the company in the first place.[1347]

Licensed Privateers. The Tallinn Manual 2.0 specifically states "There is no prohibition against injured States turning to a private firm, including foreign companies, to conduct cyber countermeasures on their behalf against responsible states."[1348] The injured state would be held responsible for the company's actions on their behalf, although the company would be subject to all applicable restrictions and conditions on the use of countermeasures.[1349] For overseas firms not under the national laws of the injured state, this responsibility prevents denial of culpability by the state if undesired consequences occur. For this reason, a more viable approach to avoid liability would be for the state to deputize or license a private company under its own jurisdiction to act on its behalf. Historical precedence for the use of cyber privateers exists for centuries in the issue of letters of marque and reprisal for naval privateers, starting as early as 1205 by England and as late as 1941 by the United States, for a civilian dirigible to hunt enemy submarines.[1350] Letters of marque and reprisal are basically "a license authorizing a private citizen to engage in reprisals against citizens or vessels of another nation."[1351] They were originally used by governments in time of war to grant private parties the authority to operate and use armed ships to attack and capture enemy merchant ships. The letters were written with enough specificity to ensure the private party did not surpass the intent of the government. Therefore conceptually the letters or licenses could be used by the government to specify the

---

[1347] Zach West, "Young Fella, If you're looking for Trouble I'll accommodate you: Deputizing Private Companies for the use of Hackback," *Syracuse Law Review*, Volume 63, November 2012: 133.

[1348] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 131.

[1349] Below the Threshold, 727-728.

[1350] John Rolland, "Letters of Marque and Reprisal," Constitution Society, Blog Site, December 28, 2007.

[1351] Black's Law Dictionary, 9th edition, 2009: 910.

circumstances under which "hack back" may be performed by a private company for the defense of property.[1352]

Article 1, Section 8 of the U.S. Constitution signed in 1787 states "the Congress shall have Power to…grant Letters of Marque and Reprisal." The U.S. Congress invoked that power during the War of 1812 with Britain. Later in 1856, the Paris Declaration Respecting Maritime Law adopted a solemn Declaration that "Privateering is, and remains, abolished."[1353] Notwithstanding, letters of marque have been used to counter piracy or to allow for self-defense. For instance the British Parliament authorized private ships to attack and capture pirates after the Declaration of Paris. More recently, for all practical matters, armed private companies that protect merchant ships off Somalia from piracy serve as a form of naval privateers. Hence there is "at least a colorful argument to be made that the Paris Declaration did not render unlawful the issuance of letters of marque for purposes of self-defense in countering piracy."[1354] Furthermore, one could compare cyber criminals, hackers, or hacktivist to modern day pirates that roam not the seas, but cyberspace, threatening the activities and interests of nation states.[1355] From this point, a tentative conclusion could be reached "that letters of marque for cyber privateers might, likewise, be lawful under international law to counter cyber pirates."[1356]

The United States never ratified the Paris Declaration. Whether bound by the Declaration or not, if any conclusion through broad interpretation that letters of marque are lawful holds ground, undoubtedly private companies will rise to the opportunity. This assertion is backed by the appearance in 2004 of Symbiot Security, Inc., which said its new "Intelligent Security

---

[1352] Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, 208.

[1353] Paris Declaration Respecting Maritime Law, 1856.

[1354] Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures," *Stanford Journal of International Law*, May 27, 2013: 10.

[1355] Joseph Roger Clark, "Arghh…Cyber-Pirates," Security Studies Blog Posts," May 28, 2013.

[1356] International Law and Private Actor Active Cyber Defensive Measures, 10.

Infrastructure Management Systems not only defends networks but lets them fight back."[1357] While most of the platform consists of traditional defensive measures, like blocking or deflecting malicious traffic, it can also escalate the response and return fire. The exact extent of aggressive measures was not made clear by the company, but executives professed in a position paper that based on the lawful military doctrine of necessity and proportionality, the private sector has the right to counterstrike hostile intent with the subsequence use of force in self-defense.[1358] Supposedly the controversial platform was deployed on several enterprise, government and military networks. It is not obvious how long Symbiot maintained this stance and product, since they were acquired by Chaotic Moon Studios in 2012 for their development over the last decade of proven technologies in quantifying network risks, not for their attack response platform.[1359]

Government Agencies. In the United States, the Department of Defense, in concert with other agencies, is responsible for "defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace."[1360] Therefore the Department of Defense has been given a primary mission to "help defend the nation against cyberattacks from abroad, especially if they would cause loss of life, property destruction, or significant foreign policy and economic consequences."[1361] In doing so, the DOD conducts Defensive Cyberspace Operations (DCO) to "preserve the ability to use friendly cyberspace capabilities and protect data, networks...and other designated systems."[1362] DCO may be conducted in response to an attack,

---

1357 Raksha Shetty, "Networks Lash Back At Cyber Hacks," CBS News, June 18, 2004.

1358 Dana Epps, "On the Rules of Engagement for Information Warfare," Web Blog, March 10, 2014: http://silverstr.ufies.org/blog/archives/000547.html.

1359 Chaotic Moon Studios, "Chaotic Moon Acquires Symbiot Security," PR News Wire, April 26, 2012.

1360 The DoD Cyber Strategy, 2.

1361 Secretary of Defense Ash Carter, "Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity," Drell Lecture at Stanford University, Palo Alto, CA, April 23, 2015.

1362 U.S. Department of Defense, *Cyberspace Operations,* US Joint Publication 3-12 (R), exploitation or intrusion on assets that the DOD is directed to defend. The DCO mission is accomplished "using a layered, adaptive, defense-in-depth approach," with equally supporting components for digital and physical protection. A key characteristic of the DCO approach is the "construct of active cyberspace defense."[1363] DCO activities can occur inside the network in the form of Internal Defensive Measures (IDM) or can occur outside the network through Response Actions (RA).

The ultimate goal of DCO is to "change the current paradigm where the attacker enjoys significant advantage."[1364] They strive to accomplish this goal through passive and active cyberspace defense activities that outmaneuver an attacker. DCO provides the capability to discover, detect, analyze and mitigate cyber threats. These operations taken for defensive purposes involve both DCO subcategories of Internal Defensive Measures and Response Actions. The primary tasks for IDM are hunting on networks for threats that evade security and directing authorized internal responses. RA is "about going after the shooter" with aggressive countermeasures to stop the attack in accordance with all legal and policy guidelines for operations outside the network.[1365] Any cyber operation that equates to the use of force requires authority that resides at the Presidential level, which would clash with a comfort level to stay inside the network.

Restriction Relief

Countermeasures provide a proportionate response for an injured State in cases where a cyber incident falls below the threshold of an armed attack. Because malicious activity in this

(Washington, DC: The Joint Staff, February 5, 2013): II-2.

[1363] Ibid.

[1364] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Number 73, 2nd Quarter 2014: 15.

[1365] Ibid, 16.

category can still have disruptive and threatening effects, States will want to react quickly.[1366] Yet there are various restrictions placed on the taking of countermeasures. For instance when a state is injured by an internationally wrongful act, it may only resort to proportionate countermeasures aimed at the responsible state, or persons or entities attributable to the state, violating its legal obligations. Execution of that right can be a problem since it is difficult to attribute malicious cyber activity to a particular state or actor with absolute certainty. Likewise, the difficulty in establishing the connection between the state and an actor is a further obstacle in the use of countermeasures. The Commentary in the Articles on State Responsibility, in the citing of the Iran-United States Claims Tribunal, affirms that "in order to attribute an act to the state, it is necessary to identify with reasonable certainty the actors and their association with the state."[1367] While that association might not be possible, the determination of reasonable certainty may be possible regarding the location from where the malicious activity was launched. Under the principle of due diligence, even in situations where the state is not behind the harm to an injured state, international law does allow for countermeasures in response to harm from cyber operations originating from the state.

In essence the principle of due diligence is based on a state's legal responsibilities "when cyber infrastructure located on its territory is used by another state, or by non-state actors, such as hacker groups, individual hacktivists, organized armed groups, or terrorists, to mount the operations."[1368] Rule 6 in the Tallinn Manual 2.0 provides that "a State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its government control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for other States."[1369] This Rule expresses "the obligation of states to take

---

[1366] Katharine C. Hinkle, "Countermeasures in the Cyber Context: One More Thing to Worry About," *The Yale Journal of International Law Online*, Vol. 37, Fall 2011: 12.

[1367] Responsibility of States, Chapter II.

[1368] In Defense of Due Diligence, 68.

[1369] Tallinn Manual 2.0, 30.

measures to ensure their territories are not used to the detriment of other states."[1370] The UN Government Group of Experts framed the principle of due diligence in hortatory, rather than obligatory terms, in stating that "States should seek to ensure that their territories are not used by non-state actors for unlawful use of ICTs."[1371] However if a state is "unwilling to terminate harmful cyber operations encompassed by the due diligence principle as opposed to unable to do so, the injured state may be entitled to resort to countermeasures based on the territorial state's failure to comply with this Rule [6]."[1372] This ruling gives the injured state another option when faced with harmful cyber operations conducted by non-state actors.

However the principle of due diligence only indisputably applies to a cyber operation that results in 'serious adverse consequences' in another country, not one that causes "inconvenience, minor disruption, or negligible expense."[1373] Serious adverse consequences could involve "interference with the operation of critical infrastructure or a major impact on the economy."[1374] Additionally, the obligation of due diligence attaches to a state only after the offending cyber activity comes to the attention of the state. If the state does not possess the resources to investigate the cyber operations originating from its territory, the victim state may be obligated to offer assistance to the responsible state before any forcible countermeasures would be justified. If the responsible state accepts the offer of assistance, the injured state may lose the right to use countermeasures since the responsible state would have resumed its international obligation to ensure its territories are not used to the detriment of other states. If, however, the offer of assistance is rejected and the responsible state still fails to stop a non-state cyber operation conducted from its territory, the injured state has the right to take proportionate

---

[1370] In Defense of Due Diligence, 69.

[1371] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, 24 June 2013: 23.

[1372] Tallinn Manual 2.0, 50.

[1373] Ibid, 36-37.

[1374] Ibid, 38.

countermeasures against it.[1375] Moreover in response to this breach of due diligence obligation, the injured state could launch cyber operations targeting the non-state actors. This is an important allowance given that the high thresholds in invoking the plea of necessity, namely a grave threat to an essential interest, limit its utility against non-state actors.

In regard to thresholds, the U.S. – China Economic and Security Review Commission asserts that international law has not kept pace with developments in cyber warfare, namely cyber espionage where stolen trade secrets are turned over to government-owned companies. Clearly malicious activity not in the category of serious adverse consequences or a grave threat to an essential interest. Therefore in June 2015 the Commission held hearings on "the possibility of U.S. corporations mounting retaliatory cyber strikes against Chinese companies." Although the Commission noted that today "U.S. companies cannot retaliate or "hack back" without violating current U.S. law."[1376] As a result the Commission recommended lawmakers should "look at whether U.S. based companies be allowed to 'hack back' to recover or wipe stolen data."[1377] Scholars at the Atlantic Council propose the development of a tailored deterrence approach to reduce adversarial intrusions into U.S. private, commercial, and government networks that result in intellectual property theft or destructive effects on critical infrastructure. They assert that an important element of tailored deterrence would be "a new legal framework authorizing *certified* private sector cybersecurity providers to take limited, but meaningful steps under proper supervision."[1378] The framework would describe requirements for certification and prescribe that providers register with the government. To ensure sufficient oversight,

[1375] State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights, 904-905.

[1376] U.S. – China Economic and Security Review Commission, "2015 Report to Congress," November 2015: 205-207.

[1377] Matthew Pennington, "U.S. Advised to examine "Hack Back" Options against China," Associated Press, November 17, 2015.

[1378] Franklin D. Kramer and Melanie J. Teplinsky, "Cybersecurity and Tailored Deterrence," Atlantic Council, December 2013: 1-6.

transparency, and accountability, the framework would require certified providers to articulate in advance and report on certain aggressive activities to law enforcement.

The creation of a new legal framework to use some form of cyber privateers could alleviate many of the concerns associated with private company hack back. At a Cyber Security Summit in October 2015, Admiral Rogers stated that "It's not without historical precedence that when a nation lacks capacity, it historically turned to the private sector," citing America's reliance on privateers before the Navy was established. Although while not unheard of, Rogers quantified he is "very leery" of moving in that direction. "I still believe that the nation state is best posed to apply force," Rogers said, "And I worry about what the implications are if we turn that over to the private sector."[1379] Some of those implications could be the intrinsic temptation to use resident hack back capability for other than sanctioned actions. For instance the use of hack back for revenge would turn the cyber privateers into nothing more than cyber vigilantes. Licensed privateers could prove difficult not only to trust, but also to manage without direct and persistent oversight. As Rogers opined "It's the Wild West in some ways already – we don't need more gunslingers out in the street."[1380]

An Alternative Strategy

Following his remarks that the "state of security of most companies is worse than ever," Dmitri Alperovitch, the Chief Technological Officer of the security firm CrowdStrike, asked the question "whether we should continue trying the same old tactics over and over again expecting a different result, or whether the time has come to fundamentally change our security strategy."[1381] Alperovitch noted that the U.S. Department of Defense has "proclaimed that it is changing its strategy to employ an active cyber defense capability" and "it is time for the private

[1379] Aaron Boyd, "Rogers: We don't need cyber privateers," Federal Times, October 29, 2015.
[1380] Ibid.
[1381] Dmitri Alperovitch, "Active Defense: Time for a New Security Strategy," Crowdstrike Blog, February 26, 2013.

sector to adopt the same strategy which focuses on raising costs and risks to adversaries in an attempt to deter their activities."[1382] Alperovitch said that his version of active defense is not about hack back, retaliation, or vigilantism, which could be counterproductive, or even illegal. Instead he believes an effective active defense strategy should focus on four key elements: real-time detection, attribution of threat actors, flexibility of response actions, and intelligence dissemination. His remarks were made during the launch of CrowdStrike Falcon, a big data active defense platform that embodies these elements. The platform promises to enable organizations to move beyond passive defenses by leveraging the kill chain model to obtain real time detection of what the attacker is doing and actually taking action against them.[1383]

In the CrowdStrike an approach that focuses more on the attacker than the exploit, several of the harshest critics of the company argue that "CrowdStrike will inevitably test legal and ethical boundaries in fighting hackers; the implication is that CrowdStrike offers offensive capabilities, known as hack back," which the Chief Executive Officer, Georg Kurtz emphatically denied.[1384] Thus with stated, suspected or denied capabilities, the CrowdStrike platform represents a private sector implementation of active cyber defense in the broadest sense. Inside the network, active cyber defense uses synchronized capabilities to discover the breach, isolate the threat and remediate the intrusion in real time. These capabilities operate inside the cyber kill chain to provide internal systemic resilience to withstand an attack. Outside the network, active cyber defense uses tailored disruption capacities to stop an attack. The conditions for use of countermeasures by an injured state against responsible states are well articulated by international and customary law. Delegation by the injured state to private companies to conduct cyber countermeasures on their behalf is allowed, but the private sector cannot go it alone under the concept of hack back. Besides lack of legal authority or precedence, the use of hack back

---

[1382] Ibid.

[1383] CrowdStrike, "CrowdStrike Launches Big Data Active Defense Platform," PRNewswire, June 18, 2013.

[1384] Fritz Nelson, "Why CrowdStrike's focus on attackers and active defense polarizes InfoSec pros," Pardo, July 17, 2013.

brings a plethora of concerns that undermine the credibility of active defense. Foremost among them is the motivation of the organization, misattribution of the attacker, third party collateral damage, and potential escalation out of control. A new novel legal framework proposed by Anthony Glosson at the Mercatus Center authorizes active defenses subject to third party liability and could temper excessive retribution and reduce societal risk.[1385]

The imposition of any new legal framework in the United States for authorized, certified, or licensed private company response would communicate the government's willingness to increase capability to deter malicious actors. While this initiative could work well at the criminal level for theft of data, the credibility of such a move is somewhat suspect in convincing state based or sponsored actors their attacks will not succeed. For in a direct contest, "despite the bluster of some in the high-tech community, private citizens are no match for the Russian mafia, the Russian Federal Security Service, or the People's Liberation Army in China."[1386] If this contest cannot be won by American companies, then the U.S. Government has no choice but to step in and U.S. Cyber Command is well positioned with the capability to do so. The Command has designated Cyber Protection Teams to conduct the Internal Defensive Measures mission and tasked National Mission Teams with the Response Action mission.[1387] In testimony, the Deputy Commander of U.S. Cyber Command, Lieutenant General James McLaughlin avowed that the Defense Department will defend "the U.S. homeland and interests from attacks of significant consequence that may occur in cyberspace."[1388] Public declarations on the use of active cyber defense by licensed private companies to defend against cyber attacks below that threshold have

---

[1385] Anthony D. Glosson, "Active Defense: An Overview of the Debate and a Way Forward," Mercatus Center, August 2015: 23-28.

[1386] James Andrew Lewis, "Private Retaliation in Cyberspace," Commentary, Center for Strategic and International Studies, May 22, 2013.

[1387] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Number 73, 2nd Quarter 2014: 16.

[1388] Thomas Atkin, James K. McLaughlin and Charles L. Moore, "Statement Before the House Armed Services Committee," June 22, 2016.

the potential to broaden beyond law enforcement "the range of punishments against which adversaries would have to calculate."[1389] Through open communication of intentions to deliver a credible response outside the network, coupled with emergence of automated capability to stop attacks inside the network, active cyber defense is well postured to serve as an alternative strategy to achieve deterrence within the cyber arena.

[1389] Steve Weber and Betsy Cooper, "Cybersecurity Policy Ideas for a New Presidency," Center for Long-Term Cybersecurity, November 2016: 1.

Conclusion

For the deterrence of malicious actors in cyberspace, the strategies of retaliation, denial and entanglement have made little progress in imposing costs for, denying benefit of, and encouraging restraint in malicious activity. Former FBI Director James Comey said in 2016 that "certain actions the federal government is taking to deter cyber threats to the country are working, at least in part."[1390] He claimed indictments of Chinese military and Iranian hackers "send an important and chilly wind through them," and he saw "early indications of efforts to cooperate" on norms for nation states to not engage in theft for commercial purposes. However, his recognition that "state sponsored cyber attackers are getting more aggressive" and "criminal organizations are getting more specialized" amplifies the reality that current strategies are insufficient to deter the number and type of actors engaged in cyber attack campaigns. Michael Daniel, the former White House cybersecurity coordinator, said in 2016 that "the cyber threat continues to outpace our current efforts."[1391]

In response, the Obama administration proposed for 2017 over $19 billion for federal cyber security efforts, with nearly $3.1 billion to retire, replace and modernize legacy IT systems.[1392] In addition the Justice Department asked in 2016 to increase its cyber security related funding by 23 percent to improve their capabilities to identify, disrupt, and apprehend malicious cyber actors.[1393] These cost intensive measures to improve defensive capabilities and punish actors arrive as cyber threats become more frequent and more serious, partly because of the availability of low cost and effective hacker toolkits. Technically proficient actors are

---

[1390] Calvin Biesecker, "Comey Says Deterrence Against Cyber Threats Showing Results," *Defense Daily,* August 30, 2016.

[1391] Calvin Biesecker, "White House Proposing Major Increase in Federal Cyber Security Spending," *Defense Daily*, February 9, 2016.

[1392] The White House, "The President's Fiscal Year 2017 Budget," Fact Sheet, February 9, 2016.

[1393] The White House, "Cybersecurity National Action Plan," Fact Sheet, February 9, 2016.

spending just over a thousand dollars for specialized toolkits to execute an attack that could impose losses in the many millions of dollars.[1394]

Asymmetric advantages for the malicious actor continue to shape their perceptions of the costs and benefits of a cyber attack. A reoccurring cyber security industry revelation is that "Defenders must block all attacks; to win; attackers need to succeed at only one."[1395] An ever expanding list of attack vectors and techniques, such as MITRE describes for lateral movement,[1396] allows an actor to execute the cyber kill chain with ease, despite attempts to install security controls for denial.[1397] Many tools and services are available on the open market from dark sources and overlap in their common use by nation states, proxies, patriots, sympathizers and criminals makes it hard to distinguish the source to impose costs. Even worst, nation state use of all these actors under some form of direction, control or incitement for plausible deniability makes concentration on just the nation state for deterrence impractical. The unrelenting motivations of the wide range of malicious actors to achieve political objectives, national pride, personal satisfaction or monetary gain exceed international efforts to restrain behavior, especially when actors know they can operate with little risk of repercussion. Optimism for the future appears bleak, as evident in a defense report that 62 percent of respondents expected their organizations to be compromised by a cyber attack in 2016, up from only 39 percent two years ago.[1398] These statistics indicate that a new way to alter malicious actor behavior in cyberspace is necessary.

[1394] Larry Ponemon, "Flipping the Economics of Attacks," ISACA Now Blog, January 26, 2016.

[1395] G. Mark Hardy, "Beyond Continuous Monitoring: Threat Modeling for Real-Time Response," A SANS Whitepaper, October 2012: 1.

[1396] MITRE Corporation, "Adversarial Tactics, Techniques & Common Knowledge: Lateral Movement," June 27, 2016: https://attack.mitre.org/wiki/Lateral_Movement

[1397] Solutionary, "Global Threat Intelligence Report: Practical Application of Security Controls to the Cyber Kill Chain," 2016 NTT Group, 21-46.

[1398] CyberEdge Group, "2016 Cyberthreat Defense Report," Executive Summary, 2016: 1-2.

This final chapter starts with how asymmetric advantages and system vulnerabilities create potential for systemic sector consequences from disruptive or destructive cyber attacks. Next, in consideration of threats that "exploit the increased complexity and connectivity of critical infrastructure systems,"[1399] the chapter presents an assessment at the strategic level of the impact of contemporary deterrence strategies on attacks (volume of noise across social, technical and economic systems), time (in mitigation of systemic security losses), and costs (in order of magnitude of gross domestic products). Given insurmountable gaps in the comprehensiveness of contemporary strategies, the chapter then examines whether the strategy of active cyber defense as a new approach to fill these gaps has been sufficiently shown to be technically capable and legally viable inside and outside the network for use in deterring the wide variety of malicious actors. Next an illustrative case of an alleged Russian multifaceted cyber campaign designed to interfere in the 2016 US Presidential Election process[1400] depicts why active cyber defense could be a strategic option for cyber deterrence. The chapter finishes with how the empirically grounded midrange theory of active cyber defense, comprised of the concepts of systemic resilience and disruption capacities, meets the conditions of capability, credibility and communication[1401] to be selected as an alternative strategy to achieve deterrence within the cyber arena, capable of compensating for the shortcomings of the contemporary three deterrence strategies.

Systemic Sector Consequences

The globally unconstrained structure of cyberspace offers asymmetric advantages in the scale, proximity, and precision of malicious actor attacks. Attackers can cause a significant and

---

[1399] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Draft Version 1.1, January 10, 2017: 1.

[1400] Shane Harris and Paul Sonne, "Intelligence Chief Defends Finding Russia Meddled in Election," *The Wall Street Journal*, January 6, 2017.

[1401] Department of Defense. *Joint Operations.* Joint Publication 3-0. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 17 January 2017): xxii.

disproportionate amount of damage without large resources or technical sophistication.[1402] A vibrant underground hacker market provides them with tools and services to increase the scale of their cyber attacks. Countries are becoming aware of "the asymmetric offensive opportunities presented by systemic and persistent vulnerabilities in key infrastructure sectors including health care, energy, finance, telecommunications, transportation, and water."[1403] Admiral Rogers, head of the National Security Agency, said he is watching "nation states, groups within some of that infrastructure" for now focused on reconnaissance.[1404] An example is the Iranian hacker breach of the Bowman Avenue Dam outside of New York City in 2013. The intrusion was a test by the hackers to see what they could access. They could have controlled the flood gates if not offline for maintenance. The breach illustrates that "overseas hackers can easily get into pieces of old critical infrastructure running on retro-fitted software that is connected to the Internet."[1405] Likewise attackers used remote cyber intrusions in the attack on the three power companies in Ukraine in 2015.[1406] The attackers ran a phishing campaign to get into the corporate network and hijack worker credentials. Eventually they took over control center computers to open breakers and take substations offline. Then the hackers wiped files from operator stations with KillDisk malware.[1407] Ukraine blamed Russian hackers for the power outage.[1408] It appears the

---

[1402] Mandiant, "M-Trends 2016," Special Report, February 2016: 9.

[1403] James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record for the Senate Armed Services Committee, February 9, 2016: 1-4.

[1404] Dennis K. Berman, "Adm. Michael Rogers on the Prospect of a Digital Pearl Harbor," *The Wall Street Journal*, October 26, 2015.

[1405] Shimon Prokupecz, Tal Kopan and Sonia Moghe, "Former official: Iranians hacked into New York dam," *CNN Politics*, December 22, 2015.

[1406] Michael Assante, "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," SANS Industrial Control Systems Security Blog, January 9, 2016.

[1407] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016.

[1408] Pavel Polityuk, "Ukraine sees Russian hand in cyber attack on Power Grid," *Reuters*, February 12, 2016.

attacks were part of a multi-stage campaign against the Ukrainian industrial network, also targeting a major mining company and a large railway operator.[1409]

While the above attacks on water, energy and transportation sector infrastructure a disconcerting demonstration, they were not necessarily destructive. Yet a few confirmed cases do exist in which a digital attack caused physical destruction. The first being a series of attacks against the Maroochy Shire Council sewerage control system in Australia in 2000 that caused raw sewage spills,[1410] and the second being the 2010 Stuxnet attack on Iranian nuclear facilities. The third occurred in late 2014 at an unnamed steel mill in Germany. A malicious advanced persistent threat actor used a spear phishing email, one of the most common attack vectors, to gain access to the mill's corporate network and then move, most likely through trusted connections, into its production network. The final stage of the attack produced "an accumulation of breakdowns of individual components of the control system."[1411] As a result, the plant was "unable to shut down a blast furnace in a regulated manner" which caused "massive damage to the system."[1412] It is "unclear if the attackers intended to cause the physical destruction or if that was simply collateral damage."[1413] The incident accentuates that not all intrusions into critical infrastructure will be as careful as the Stuxnet worm that destroyed only targeted uranium enrichment centrifuges.[1414] The German steel mill attack was an isolated, not

---

[1409] Warwick Ashford, "Ukraine cyber attacks extend beyond power companies, says Trend Micro," *Computer Weekly*, February 12, 2016.

[1410] Marshall Abrams and Joe Weiss, "Malicious Control System Cyber Security Attack Case Study– Maroochy Water Services, Australia," The MITRE Corporation, August 2008.

[1411] Robert M. Lee, Michael J. Assante and Tim Conway, "German Still Mill Cyber Attack," SANS Industrial Control Systems, December 30, 2014: 1-15.

[1412] Kim Zetter, "A cyberattack has caused confirmed physical damage for the second time ever," *Wired*, January 8, 2015.

[1413] Ibid.

[1414] Ibid.

systemic attack on an industry sector, but still concern resides of the impact of destructive attacks on critical infrastructure.

In the wake of the Ukraine incident, Admiral Rogers said at the 2016 RSA Conference that he worries over an infrastructure attack in the United States that causes significant damage. He also expressed fear over attacks that would manipulate data for the purpose of crippling financial institutions. Rogers asked the audience "What are we going to do as a society when you go to your bank account, and the numbers don't match what you think they should be?" or "What do you do if your business does financial transactions, and they don't reflect what you are seeing?"[1415] Those dreadful scenarios would cause systemic failure of the financial sector, and consequently cascading effects across the economy and society. Many banks have experienced denial of service attacks upon the availability of information, and intrusion attacks upon the confidentiality of information, but this new paradigm would affect the integrity of the information system. Disruption or manipulation of stock trading operations would cause a systemic global impact, as seen in January 2016 when the Chinese stock market crashed over the devaluation of its currency, driving a tumble in the Dow Jones industrial average of nearly 400 points.[1416]

The chief of strategy in the U.S. Defense Strategic Capabilities office remarked that we see "cyber being increasingly used as a first strike weapon by peer competitors" and "non-military assets are increasingly the targets."[1417] Those targets could include nuclear facilities,

---

1415 Greg Otto, "U.S. power grid cyberattack: When, not if, says NSA chief," *FedScoop*, March 1, 2016.

1416 Shanghai Business and Finance, "China's stockmarket crashes – again," *The Economist*, January 4, 2016; Chris Matthews, "Why China's Stock Market Crash Could Spark a Trade War," *Fortune*, January 7, 2016; and also Corrie Driebusch and Riva Gold, "Dow Tumbles Nearly 400 Points on China Worries," *The Wall Street Journal*, January 8, 2016.

1417 Sean Lyngaas, "U.S. official: Russian cyberwarfare getting more sophisticated," *Federal Computer Weekly*, February 2016: 8.

like in Stuxnet. A study of twenty nations with significant atomic stockpiles or nuclear power plants reveals the lesson of Stuxnet seems lost, as "too many states require virtually no effective security measures at nuclear facilities to address the threat posed by hackers."[1418] A similar report affirms a paucity of regulatory standards for civil nuclear facilities, coupled with insufficient spending on cyber security.[1419] Yet regardless of the catastrophic risk of a release of ionizing radiation, most of the hype over cyber intrusions has been over the relentless theft of personal, corporate or government information. For example, the German report of a destructive cyber incident got lost in the noise of the widely publicized Sony hack in late 2014. Although the method to deliver a hostile payload, like a social engineering attack seen in Sony, can be the same for all types of business networks, including those connected to production networks in industrial control systems.

Deterrence Strategy Shortfalls

At the strategic level, the deterrence option of entanglement attempts to reduce the volume of noise across social, technical and economic systems through cooperative measures that restrain state behavior. Although the impact of the primary mechanism of norms depends on "whether they are implemented faithfully and whether violators are held accountable."[1420] An example is the U.S. – China agreement not to conduct or support cyber-enabled theft of intellectual property. Here diminishment of state sponsored attacks is a matter of trust, and for China in other domains that trust is lacking. For instance China appears to have built "significant point-defense capabilities, in the form of large anti-aircraft guns and probable close-

---

[1418] David E. Sanger, "Nuclear Facilities in 20 Countries May Be Easy Targets for Cyberattacks," *The New York Times*, January 14, 2016.

[1419] Caroline Baylon with Roger Brunt and David Livingstone, "Cyber Security at Civil Nuclear Facilities," Chatham House Report, September 2015: i-x.

[1420] Scott Charney, et al., Microsoft Corporation, "From Articulation to Implementation: Enabling progress on cybersecurity norms," June 2016: 9.

in weapons systems (CIWS), at each of its outposts in the Spratly Islands,"[1421] despite President Xi Jimping's September 2015 pledge not to militarize the islands in the South China Sea.[1422] After all, the U.S.-China cyber deal was produced through coercive measures in the threat of sanctions, which came after criminal indictments of five members of the Chinese military.[1423] Public attribution of attacks is part of a U.S. strategy shift to "name and shame" countries, as the FBI did in naming North Korea as responsible for the Sony Pictures attack.[1424] Likewise, the Obama administration publicly blamed Iran for the 2013 New York dam cyber breach and attempted accountability through charges against seven hackers working as contractors for the Iranian government. The indictment brought attention to another uncooperative state actor, to include the hacker's roles in denial of service attacks on U.S. banks starting in 2011.[1425] In this case Iran is the belligerent actor that test-fired several ballistic missiles in February 2016 despite fresh sanctions imposed on their weapon's program.[1426]

The U.S. Senate unanimously approved legislation in December 2016 that reauthorized sanctions against Iran's ballistic missile development and weapons program for the next decade.[1427] Extension of the sanctions that were not covered by the landmark nuclear agreement

---

[1421] Asia Maritime Transparency Initiative, "China's New Spratly Island Defenses," December 13, 2016.

[1422] Jeremy Page, "China's Weapons Stoke Sea Dispute," *The Wall Street Journal*, December 16, 2016.

[1423] United States District Court, Indictment, Criminal No. 14-118, Filed May 1, 2014: 1-48.

[1424] FBI National Press Office, "Update on Sony Investigation," The Federal Bureau of Investigation, Washington, D.C. December 19, 2014.

[1425] Christopher M. Matthews, "U.S. Charges Seven Iranians in Hacking Attacks," *The Wall Street Journal*, March 24, 2016.

[1426] Asa Fitch, "Iran Launches Ballistic Missiles in Military Exercise," *The Wall Street Journal*, February 9, 2016.

[1427] Kristina Peterson, Carol E. Lee, and Jay Solomon, "Senate Approves Extending Sanctions," *The Wall Street Journal*, December 2, 2016.

indicates a lack of trust in improved behavior by Iran, as hoped for given related sanctions relief. In fact Iran's government has conducted nearly a dozen ballistic-missile tests in the year since the deal was implemented.[1428] In regard to China, the United States still trusts they will abide by the Obama-Xi cyber agreement. As mentioned previously, the Chinese government did arrest a handful of hackers it says were connected to the OPM breach, which could mark the first measure of accountability. Notwithstanding that the identities of the suspects remain unclear. U.S. government officials said "they suspected the involvement of the Chinese government, particularly the civilian Ministry of State Security."[1429] Whereas FireEye, iSight Partners and other firms attribute the OPM attack to a Chinese state sponsored APT group referred to as Deep Panda.[1430] A major challenge in attribution according to the U.S.-China Economic and Security Review Commission is that "distinguishing between the operations of official and other Chinese cyber actors is often difficult, as is determining how these groups interact with each other."[1431] The U.S-China cyber agreement to curb cyber-enabled theft of intellectual property should work regardless of what type of actor if the state enforces it. However more than a year after the agreement, the testimony of Director Clapper that "Beijing continues to conduct cyber espionage against the U.S. Government, our allies, and U.S. companies,"[1432] although at reduced levels, signals the continued insufficiency of deterrence by entanglement.

[1428] Jay Solomon, "Iran Missile Launch Detected, a Possible Violation of U.N. Resolution," *The Wall Street Journal*, January 30, 2017.

[1429] Ellen Nakashima, "Chinese government has arrested hackers it says breached OPM database," *The Washington Post*, December 2, 2015.

[1430] Institute for Critical Infrastructure Technology, "Handing Over the Keys to the Castle," July 2015: 3.

[1431] U.S.-China Economic and Security Review Commission, "2016 Report to Congress," November 2016: 293.

[1432] The Honorable James R. Clapper, et al., "Foreign Cyber Threats to the United States," Joint Statement for the Record to the Senate Armed Services Committee, 5 January 2017: 4.

The deterrence option of denial attempts to lessen the time in mitigation of systemic security losses through both preventive and detective security controls that deny attack success. For instance in the aftermath of the Ukraine power distribution attack, the U.S. Industrial Control System – Computer Emergency Response Team (ICS-CERT) released an alert that not only depicted the attack but also listed mitigation strategies for organizations across all sectors to review and employ. It suggested asset owners take defensive measures by leveraging best practices to minimize the risk from similar malicious cyber activity. Suggested practices included use of Multi-Factor Authentication to limit remote access and Application Whitelisting to prevent attempted execution of malware.[1433] ICS-CERT also recognizes that the increased integration of external, business, and control system networks to enhance productivity and reduce costs leads to vulnerabilities. The same protocols and standards that increase interoperability in the control systems community are the same technologies that have been exploited on the corporate networking domains. Open system architecture vulnerabilities that could migrate to control system domains include network reconnaissance, unauthorized intrusions and escalation of privileges. Therefore multiple countermeasures are needed to disseminate risk over layers of protection.[1434] However as asset owners move to implement defense-in-depth frameworks, informed by cyber threat intelligence, malicious actors continue to penetrate defenses, and the proportion of breaches discovered within days still falls well below that of time to compromise, usually in minutes or less.[1435]

The confounding question for the 22 million federal employees and others whose personally identifiable information was stolen in the OPM breach more than a year ago is "are

[1433] U.S. Industrial Control System - Computer Emergency Response Team (ICS CERT), Department of Homeland Security, "Cyber-Attack Against Ukrainian Critical Infrastructure," Alert (IR-Alert-H-16-056-01), February 25, 2016.

[1434] National Cyber Security Division, Department of Homeland Security, "Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies," October 2009: 1-34.

[1435] Verizon, "2016 Data Breach Investigations Report," May 2016: 10.

you safer now?" The acting director, Beth Cobert, "thinks so."[1436] She has outlined a long list of actions that OPM has taken to strengthen cybersecurity, including the deployment of two factor strong authentication, the limitation of remote access, and the implementation of data loss prevention systems, in addition to establishing an agency-wide IT security workforce and enhancing cybersecurity awareness training.[1437] These actions are all hallmarks of a defense-in-depth posture based on the primary elements of people, technology and operations.[1438] It is true these security controls might have even prevented the OPM breach, for example the second attacker utilized a single factor network credential stolen from a KeyPoint contractor for the "initial vector of infection."[1439] However the office of the agency's inspector general continues to believe that there is "a very high risk that the project will fail to meet its stated objectives of delivering a more secure environment at a lower cost." Part of the reason for this assessment is "potentially wasteful spending" in creating a new security environment before "it was clear that it was the best solution."[1440] Security spending on the right solutions is always a challenge, but spending will invariably rise as "organizations realize they need to protect against phishing, ransomware and the growing variety of threats they face."[1441] However since attackers receive "an estimated 1,425 percent return on investment for exploit kit and ransomware schemes

---

[1436] Joe Davidson, "One year after OPM cybertheft hit 22 million: Are you safer now?" *The Washington Post,* June 8, 2016.

[1437] Ibid.

[1438] National Security Agency, "Defense in Depth," Information Assurance Directorate Library, March 12, 2010: 1-5.

[1439] Committee on Oversight and Government Reform, U.S. House of Representatives, 114th Congress, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," Captain America: The First Indicator that Led to the 2015 Discovery of the Background Investigation Data Breach, September 7, 2016: 88.

[1440] Eric Yoder, "More questions raised about OPM's response to breaches of background, personnel records," *The Washington Post,* May 26, 2016.

[1441] Osterman Research, "Best Practices for Dealing with Phishing and Ransomware," White Paper, September 2016: 1.

($84,100 net revenue for each $5,900 investment),"[1442] the cost ratio imbalance forecasts the continued insufficiency of deterrence by denial.

The deterrence option of retaliation attempts to diminish the costs of systemic security losses by the credible threat to impose overwhelming costs for hostile acts. However the global economy is bearing the costs from cybercrime and cyberespionage, estimated to be annually around $455 billion. The estimate accounts for the loss of intellectual property and the theft of financial assets and sensitive business information, plus additional costs for securing networks and recovering from attacks, including reputational damage. For nations, those costs measured in order of magnitude of gross domestic products (GDP) are staggering. Costs in high-income countries are 0.9% of GDP on average.[1443] In the United States the loss is 0.64% of GDP which for a 2015 GDP figure of $18 trillion equals $115.2 billion a year. The threat of retaliation through use of all necessary means strives to shift costs to the malicious actors. For instance since the raid by Russian authorities in November 2015 of offices used in a financial hacking operation, a password stealing software program known as Dyre, responsible for tens of millions of dollars in losses at financial institutions including Bank of America and JP Morgan Chase, has not been deployed.[1444] Criminal prosecutions are intended to change the calculus of costs, yet many require slowly evolving international cooperation.[1445] In cases where overseas actors are unlikely to be held accountable, economic sanctions are an effort to prevent malicious actors from reaping rewards for their intrusions. However the building of a case to use these means requires letting federal investigators examine the forensic evidence left by the intruders. That is

---

[1442] Ibid, 2.

[1443] McAfee, "Net Losses: Estimating the Global Cost of Cybercrime," with Center for Strategic and International Studies, June 2014: 1-23.

[1444] Joseph Menn, "Top cybercrime ring disrupted as authorities raid Moscow offices," *Reuters*, February 6, 2016.

[1445] Joseph Menn and Eric Beech, "U.S., China reach agreement on guidelines for requesting assistance fighting cyber crime," *Reuters*, December 3, 2015.

futile as companies are wary of cooperating in government investigations for fear of exposure to regulatory actions, privacy suits or other civil litigation.[1446]

Malicious actors seem to act without impunity as if there is no deterrence strategy in place. Senator Dan Sullivan asked the witness at a recent Congressional Hearing "why the U.S. has not hit back against adversaries in a significant manner out of the public eye?"[1447] Under Secretary of Defense for Intelligence Marcel Lettre said "I think you're getting right at the question of what do we mean by a proportional response," while Director Clapper replied that "When we do choose to act, we need to model the rules we want others to follow since our actions set precedents." Both of their comments cumulatively speak to underlying legal and procedural constraints on the imposition of overwhelming costs. Director Clapper went on to say "there's always that issue of counter-retaliate, ergo my brief mention that it's in my view to consider all instruments of national power." Yet the apparent lack of a retaliatory response, by any instrument of power, against China for the OPM hack has made the United States appear to look weak on the world stage. That look continued in a crisis with China in 2016 over their seizure of a U.S. Navy underwater drone in waters near the Philippines. The day prior, the Commander of U.S. Pacific Command, Admiral Harry Harris told diplomats in Sydney that "capability times resolve times signaling equals deterrence." The host for his speech at the Lowy Institute, Director Euan Graham, remarked after the maritime incident that "the weak link is the resolve, and the Chinese are testing that." The muted U.S. response, outside a demand by the Obama administration to return the drone, carries well into other domains. The embolden act by China that fell short of provoking conflict and suffered few consequences, quite similar to the OPM hack, indicates the continued insufficiency of deterrence by retaliation.

[1446] Ellen Nakashima, "Hacked U.S. companies have more options, departing cybersecurity official says," *The Washington Post*, March 2, 2016.

[1447] Mark Pomerleau, "U.S. intelligence director questioned in Senate over responses to cyberattacks," *C4ISRNET*, January 6, 2017.

The aim of deterrence is to "decisively influence the adversary's decision making calculus."[1448] Thus deterrence is a "state of mind brought about by an adversary's perception of three factors: being denied the expected benefits of his action; having excessive costs imposed for taking the action; and that restraint is an acceptable alternative."[1449] The deterrence strategies of denial, retaliation and entanglement seek to convince adversaries not to take malicious actions by changing their perceptions.[1450] They concentrate primarily on means to deny benefits, impose costs, or encourage restraint. An adversary chooses "not to act for fear of failure, risk, or consequences."[1451] These strategic options are not mutually exclusive and U.S. doctrine, for instance, uses a mixed methodology, especially across diplomatic, legal, economic and military dimensions. The cumulative effect of these strategies is gained from a synchronized and coordinated use of all instruments of national power in a comprehensive approach. Regrettably evidence indicates that contemporary deterrence strategies, even if applied together, are insufficient to deter the wide range of malicious actors conducting cyber attacks.[1452] Critics of the U.S. approach to "name and shame" foreign cyber threat actors believe it's just "yapping in the wind." While nation states stand at the top of the FBI stack of threat actors, followed by criminal syndicates, hacktivists, and terrorists, former Director Comey admits that "all cyber attackers are becoming more sophisticated."[1453] Therefore without a doubt, an alternative and

---

[1448] U.S. Department of Defense, *Deterrence Operations Joint Operating Concept*, Version 2.0, (Washington, DC: US Strategic Command, December 2006), 23.

[1449] US Department of Defense, *Joint Operation Planning,* US Joint Publication 5-0, (Washington, DC: The Joint Staff, August, 11 2011), E-2.

[1450] U.S. Department of Defense, *The DOD Cyber Strategy*, April 2015: 11.

[1451] Department of Defense. *Joint Operations.* Joint Publication 3-0. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 17 January 2017: VI-4.

[1452] Joseph Marks, "Obama's Cyber Legacy: He Did Almost Everything Right And It Still Turned Out Wrong," *NEXTGOV*, January 17, 2017.

[1453] Calvin Biesecker, "Comey Says Deterrence Against Cyber Threats Showing Results," *Defense Daily*, August 30, 2016.

compensating strategy is necessary that encourages adversary restraint, by shaping perceptions of the costs and benefits of a cyber attack in a different way.

A Sufficient Alternative

An alternative strategy of active cyber defense combines internal systemic resilience to halt malicious cyber activity after an intrusion with tailored disruption capacities to thwart malicious actor objectives and compensate for gaps in – but does not replace – existing deterrence strategies. The question of whether a strategy of active cyber defense is *technically capable and legally viable* to deny benefits through systemic resilience and impose costs through tailored disruption was publicly examined in 2013 by the Commission on the Theft of American Intellectual Property (IP Commission). Outside the victim's network, the IP Commission noted that "while not permitted under U.S. laws, there are increasing calls for creating a more permissive environment for active network defense that allows companies not only to stabilize a situation but to take further steps... within an unauthorized network."[1454] Inside the defender's network, the IP Commission recommended that besides vulnerability mitigation measures such as firewalls and password protection systems, companies and governments should also "install active systems that monitor activity on the network, detect anomalous behavior, and trigger intrusion alarms that initiate both network and physical actions immediately."[1455] These suggestions tacitly endorse the use of automated active cyber defense type capabilities to provide internal systemic resilience through legally acceptable means as long as actions stay inside organizational boundaries.

[1454] The National Bureau of Asian Research, "The Report of the Commission on the Theft of American Intellectual Property," May 2013: 81.

[1455] Ibid, 80.

Inside the Defender's Network

Industry solutions are actually getting better in monitoring activity and detecting malicious behavior. The security firm Mandiant reported in 2012 that the median days an organization was compromised before the breach was discovered was 416 days. That number dropped in their reports, in 2014 to 205 days and then to 146 days in 2015.[1456] For companies that detected a breach on their own, which is less than 20 percent,[1457] the median number was 46 days compromised before discovery. This decline in days over the past few years most likely indicates the wide spread installation of not just preventive, but also detective security controls on organizational systems. In an 2016 institute survey of Information Technology security practitioners in the United States involved in endpoint security in a variety of organizations, 95 percent said their organizations will evolve toward a more "detect and respond" orientation from one that is focused on prevention.[1458] Organizations could adopt a single integrated platform, like LightCyber Magna considered to be a single real-time detection platform,[1459] or they can opt to select an endpoint detection and response solution, like one used in Magna, which comprises many active cyber defense type capabilities, empowered by actionable cyber threat intelligence.

In cyber incidents, penetration often occurs via endpoints, for instance when malware is downloaded from a spear-phishing email to the victim's desktop or laptop, or through known vulnerabilities in older point-of-sale terminals, or by a USB stick used between the home and the office.[1460] After penetrating an endpoint, the malware establishes command and control for an attacker to conduct reconnaissance and lateral movement inside the network. The identification

---

[1456] M-Trends 2016, 4.

[1457] Verizon, "2016 Data Breach Investigations Report," May 2016: 11.

[1458] Ponemon Institute, "2016 State of Endpoint Report," April 2016: 16.

[1459] Steve Schick, "LightCyber Unveils Second Generation Magna Platform," LightCyber Press Releases, July 30, 2014: http://lightcyber.com/lightcyber-unveils-second-generation-magna-platform/

[1460] Carbon Black, "Breach Detection: What you need to know," eBook, 2016: 1-18.

of actions originating from the compromised endpoint provides an opportunity to break the cyber kill chain. This opportunity is the reason for a rise in commercial endpoint detection and response solutions. A worthwhile vendor solution must be able to detect, contain, investigate and remediate the incident at the endpoint. Capable solutions inventory and manage system configurations to establish a normal baseline. Then the same solution monitors configuration changes to detect unusual behavior. Such changes can be in new software or files, the registry, account information, user privileges, new processes and open ports or communications activity.[1461] The solution may contain a process or traffic then investigate through threat intelligence exchanges. Upon confirmation of malicious behavior, the solution remedies the situation through routine repairs, software de-installations or further blocks of IP addresses.[1462] Ideally to stop or limit damage, configurations will be automatically compared to indicators of compromise for quick detection and remediation actions will be automatically run for real time response.

In order to better understand possible indicators of compromise, most endpoint detection and response solutions are integrated with multiple independent threat intelligence services and feeds. They will consume these sources constantly and filter information on malware, URL domains, email sources, IP addresses, etc. on a massive scale for organizational relevance.[1463] The solutions will then compare configuration changes to relevant indicators of compromise for threat detection. As necessary a suspect change or file will be sent to a third party threat intelligence service, like to the cloud-based virtual malware analysis WildFire environment, "built for high fidelity hardware emulation" to analyze "suspicious samples as they execute."[1464] The solution can also use a log event analysis service to identify odd behavior on systems and

---

[1461] Ed Tittel and Gajraj Singh, "Endpoint Detection and Response for Dummies," Tripwire Special Edition, (Hoboken, NJ; John Wiley & Sons, 2016): 11-16.

[1462] Ibid, 22-24.

[1463] Anomali, "Operationalizing Threat Intelligence Data: The Problems of Relevance and Scale," White Paper, 2016: 1-4.

[1464] Palo Alto Networks, "WildFire Data Sheet," 2015: 1-4.

the time of occurrence, such as by LogRhythm labs which “collect and process all of an organization’s log, flow, event and other machine data, as well as endpoint, server and network forensic data” to identify activities and automatically prioritize incidents.[1465] In this fashion cyber threat intelligence “has gone from a niche product to a general-use tool.”[1466]
Yet to be valuable for endpoint detection and response solutions, it still has to be accurate, relevant and timely for use across each phase of the cyber kill chain.[1467] That means a threat intelligence platform should also execute automated processes to provide seamless integration with endpoint detection and response solutions, such as sending a block action on an indicator.[1468]

The demand for next generation endpoint security solutions is high. In a 2016 survey of enterprises across all industries, a whopping 86 percent of respondent organizations report they are not satisfied with their current endpoint protection software.[1469] In response to this demand, a number of capabilities are available starting with Magna and also HawkEye G technologies integrated into a new Threat Detection and Response (TDR) platform delivered as part of a Total Security Suite. The WatchGuard FireBox appliance T30 model that delivers the Total Security Suite won Gold in the “Best Security Products and Solutions for Medium Enterprises” category at the 13th Annual Global Excellence Awards held by Info Security Products Guide.[1470] The new TDR platform employs a host sensor to detect security events using heuristics and behavioral

---

[1465] LogRhythm, “LogRhythm Threat Intelligence Ecosystem,” Product Overview, 2015: 1-2.

[1466] Armor, “Threat Intelligence,” ebook: An SC Magazine publication, 2016: 1-7.

[1467] Solutionary, “Global Threat Intelligence Report: The Role of the Cyber Kill Chain in Threat Intelligence,” 2016 NTT Group, 52-55.

[1468] Threat Connect, “Threat Intelligence Platforms,” Report, 2015: 30.

[1469] CyberEdge Group, “2016 Cyberthreat Defense Report,” Section 4: Future Plans, 2016: 31.

[1470] See Editor, “WatchGuard Honored At This Year’s Info Security Products Guide Global Excellence Awards,” Secplicity Security Simplified, March 2, 2017: https://www.secplicity.org/2017/03/02/watchguard-honored-years-infosecurity-products-guide-global-excellence-awards/

analytics.[1471] Data on these events is then sent to a cloud-based threat intelligence correlation and scoring engine to generate a threat score and rank based on severity. Based on score, threats can be quickly remediated through one-click response options or through policies that enable automated responses including quarantine the file, kill the process or delete the registry value.[1472]

Other emerging capabilities include the Cb Response platform that visualizes the complete kill chain to find the root cause and see lateral movements to accelerate investigations. The Carbon Black Platform is the winner of the SANS "Best of 2016 Award" for "Endpoint Detection/Response."[1473] Cb Response attempts to stop attacks in progress by isolating infected systems, terminating processes and banning hashes (numerical text strings) across an enterprise. It also retains historical data for review of any attack.[1474] Another new Enterprise type endpoint defense solution is contained in an integrated suite for real-time detection, analysis and response. The Tripwire Enterprise is the winner of the Bronze award for Endpoint Security Solution Innovations in the Information Technology and Security Innovations - Best Product or Service of the Year category at the Golden Bridge Awards for 2016.[1475] This capability monitors and compares files changes in endpoints against baseline configurations, then automatically uploads and detonates suspicious files in a sandbox provided by an advanced malware detection system. The Lastline advanced malware detection system was deemed to be the most effective in a NSS Labs Test.[1476] The Enterprise solution also monitors and correlates state changes with system

---

[1471] WatchGuard, "Host Sensor," Data Sheet, 2017: 1-2.

[1472] WatchGuard, "Threat Detection & Response," Data Sheet, 2017: 1-4.

[1473] See SANS Press, "SANS Announces 2016 Best of Award Winners," March 27, 2017: https://www.sans.org/press/announcement/2017/03/27/1

[1474] Carbon Black, "Cb Response," Data Sheet, 2017: 1-2.

[1475] See "Tripwire Wins Two 2016 Golden Bridge Awards," September 14, 2016: https://www.tripwire.com/company/press-releases/2016/09/tripwire-wins-two-2016-golden-bridge-awards/

[1476] See "NSS Labs Test: Lastline Most Effective in Advanced Malware Detection," 2017: https://go.lastline.com/rs/373-AVL-445/images/Lastline_NSS_DS.pdf events and application logs. Upon solution prediction of risk, a security analyst manually defends assets through protective controls.[1477]

Another new capability for Endpoint Protection is claimed to integrate "innovative security technologies to protect against all stages of an attack."[1478] Sophos Endpoint received an overall Security Effectiveness rating of 94.7% by NSS Labs.[1479] Although whitepapers by vendors seem to just herald their capabilities, independent testing of endpoint security solutions often shows they actually work. For example in a test of HawkEye G for malware installed on a protected system, the solution caught the malware trying to contact its botnet handler and automatically routed traffic to a Bot Trap. HawkEye G automatically stopped the process from running on the host computer, and then encrypted and quarantined the malicious file for operator review.[1480] Customers trust these solutions as evidenced by the deployment of the Enterprise endpoint defense solution in over a million business-critical systems. In regard to the legality of deployment of endpoint defense solutions, the Cybersecurity Act of 2015 Section 104 stated "notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, to monitor an information system of such private entity" and "operate a defensive measure that is applied to an information system of such private entity in order to protect the rights or property of the private entity."[1481] Therefore given the proven qualities of endpoint security solutions

---

[1477] TripWire, "Solutions for Endpoint Detection and Response," Solution Brief, 2015: 1-5.

[1478] Sophos, "Next-Generation Endpoint Protection Explained," White Paper, April 2016: 1-8.

[1479] See NSS Labs, "Advanced Endpoint Protection Comparative Report," February 14, 2017: https://pages.cylance.com/rs/524-DOM-989/images/NSS%20Labs%20Advanced%20Endpoint%20Protection_Comparative%20Report_Security%20Value%20....pdf.

[1480] John Breeden III, "Network World Gives HawkEye G 4.875 out of 5," *Network World*, December 8, 2014.

[1481] U.S. Congress, "Consolidated Appropriations Act, 2016," Division N- Cybersecurity Act of 2015, December 15, 2015: 1728-1770.
1742-43.

available for installation today, for the category of inside the defender's network, the strategy of active cyber defense seems to be both *technically capable and legally viable* through automated and integrated capabilities that act only inside organizational boundaries.

<u>Outside the Victim's Network</u>

Yet even with promising advances in security solutions, the IP Commission contended that the best security systems cannot be depended upon for protection one hundred percent of the time against the most highly skilled hackers. Therefore they felt new ways are necessary to reverse "the time, opportunity, and resource advantage of the targeted attacker by reducing his incentives and raising his costs."[1482] The IP Commission appeared to support ways to identify and render inoperable stolen intellectual property through cyber means, such as marking electronic files with beacons and writing software that renders files inaccessible to unauthorized persons. Yet the IP Commission did not recommend specific revised laws to recover a stolen file or to degrade or damage the computer system of a hacker under present circumstances.[1483] The specific reasons that the IP Commission was not ready to endorse the idea of Congress authorizing aggressive cyber actions for the purpose of self-defense, were the dangers of misuse of legal hacking authorities and the potential for collateral damage.[1484]

The primary motivation for the private sector to hack back against an attacker would probably be to recover or delete stolen data, intellectual property or trade secrets on an attacker's computers or servers. Yet private organizations could be enticed to hack back for retaliatory reasons to obtain justice for any perceived harm and induced inconvenience, including to disrupt or damage the attacker's systems, and even more so, to degrade their ability to carry out future

[1482] Report of the Commission, 80.

[1483] Ibid, 81.

[1484] Ibid, 83.

attacks.[1485] Also, the choice to hack back could produce unintended collateral damage to an innocent bystander's system. Attackers often use compromised home or office computers as bots in a botnet for distributed denial of service attacks or to distribute spam in illicit schemes. They also route attack traffic through compromised computers without the owner's knowledge to hide their tracks. For the latter, just imagine for instance the impact of a destructive hack back on an emergency service provider, a school, or even worse, a hospital system and the associated punitive and civil damages.[1486]

Despite the apparent risks of hack back, one could argue that private companies will aggressively act covertly anyway, partly due to their frustration with government inability to act in a timely and effective manner by other means, such as by legal indictments or economic sanctions. In the aforementioned 2016 institute survey of Information Technology security practitioners involved in endpoint security, 64 percent said their organizations are pursuing now or planning to pursue an offensive security capability, described as to discover who is behind an attack and then to counterattack.[1487] Furthermore, the Black Hat USA 2016 conference even offered a technical course in "Active Defense, Offensive Countermeasures and Hacking Back" to learn "how to force an attacker to take more moves to attack your network...to detect them" and "how to gain better attribution" and "how to get access to a bad guy's system."[1488] While the Black Hat site claims this could be done legally, the last objective neglects the reality that often the source of the attack is a compromised computer of an unwitting third party and any aggressive action after unauthorized access could result in undesired collateral damage.

[1485] Peter Sullivan, "Hacking back: A viable strategy or a major risk?" Tech Target, June 27, 2016.

[1486] Sean L. Harrington, "Cyber Security Active Defense: Playing with Fire or Sound Risk Management," Richmond Journal of Law & Technology, Volume XX, Issue 4, September 17, 2014: 27.

[1487] Ponemon Institute, "2016 State of Endpoint Report," April 2016: 16.

[1488] Black Hat USA 2016, "Active Defense, Offensive Countermeasures and Hacking Back," SANS – John Strand, Registration Site, July 30-August 2, 2016.

The potential for collateral damage to an innocent third party highlights the importance of attribution. However the determination of "absolute attribution can be difficult if not near impossible."[1489] Therefore if absolute identification is unrealistic, could a legal framework prevent mistakes and consequences from the employment of hack back in case of misattribution? One way, suggested by Anthony Glosson, to protect against the dangers of misattribution and other associated risks, would be for Congress to accommodate hack back by "adding a qualified active defense right to the CFAA. The right would balance the active defense privilege with misattribution concerns by imposing strict liability for harm caused during misdirected active defense efforts."[1490] Glosson believes "firms will use active defense tactics only when they have an appropriate degree of confidence in the identity of their targets."[1491] Under certain conditions, those tactics could include disruptive options to disable an attacker's system or destructive measures to destroy stolen trade secrets. Even still, a lingering concern if counterattacks were somehow made legal is that too many of the techniques would cause severe and irreparable harm to not just innocent third parties from misattribution, but also to the attacker's systems that could result in escalation. If the attacker perceives the hack back as disproportionate to the initial attack, it could invite a stronger counterattack against more valuable systems.[1492]

Taking all considerations into account, the IP Commission determined that only the Department of Homeland Security, the Department of Defense, and Law Enforcement Agencies should have the legal authority to use countermeasures against targeted attackers for

---

[1489] Shane McGee, Randy V. Sabett, and Anand Shah, "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense," *Journal of Business & Technology Law*, Volume 8, Issue 1, Article 3, 2013: 5-7.

[1490] Anthony D. Glosson, "Active Defense: An Overview of the Debate and a Way Forward," Mercatus Center, August 2015: 23.

[1491] Ibid, 24-26.

[1492] Emilio Iasiello, "Hacking Back: Not the Right Solution," *Parameters*, Vol. 44, No. 3, Autumn 2014: 110.

unauthorized intrusions into national security and critical infrastructure networks.[1493] This legal authority already exists in international law for state use of countermeasures, as previously described in three distinct forms with associated conditions and restrictions:

- *Injured State*: has the right to resort to proportionate countermeasures against a responsible State for an internationally wrongful act to include a violation of a treaty or customary law obligation.
- *Plea of Necessity*: may be invoked to justify a state's resort to cyber measures when faced with a grave and imminent threat to an essential interest to include in certain cases where the exact nature or origin of a cyber attack is not clear.
- *Due Diligence*: principle allows a state to resort to countermeasures if a responsible state fails to meet its obligation to not allow cyber infrastructure located on its territory to be used to mount a cyber operation that results in serious adverse consequences in another country.

The three categories of allowable state responses represent sovereign privileges granted to nations. If the United States or its allies disrespect the law by sanctioning private hack back, others will most likely cite use as precedent. A myriad of complications would follow that would weaken efforts to sustain customary law and create international norms. For instance, would China or Russia even know that a damaging attack by a private company is not an official cyber attack signaling state response? Also, would Iran or North Korea adopt a similar retaliatory policy through use of hacker groups not under state control or direction?[1494]

The IP Commission determination on authority for only government use of countermeasures appears valid given the risks of private sector hack back. Thus the use of tailored disruption capacities is probably best left to government agencies, especially for disruptive activities outside victim's network, such as taking control of remote computers or

[1493] Report of the Commission, 80-83.

[1494] James Andrew Lewis, "Private Retaliation in Cyberspace," Commentary, Center for Strategic & International Studies, May 22, 2013.

launching denial of service attacks. However the difficulty with this determination lies in the question of whether the government really has the capacity to defend the private sector? Or even the willingness to do so, given the high thresholds for response delineated in international law and reiterated in national strategy. For instance in the United States, the Department of Defense mission to defend the nation and its interests applies to "cyberattacks of significant consequence" which may include "loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States."[1495] The magnitude of these consequences would not apply to many of the cyber attacks seen today. Likewise, many of the organizations experiencing cyber attacks do not fall into the category of "national security and critical infrastructure" delineated by the IP Commission. If the government were to respond to more common incidents for more common organizations, then a new precedence would be set below the current threshold of government response.

The Department of Defense Cyber Strategy recognizes that the "private sector owns and operates over ninety percent of all the networks and infrastructures of cyberspace and is thus the first line of defense."[1496] Not a surprising statement since the talent, tools, and technical capacity reside primarily in the private sector. What is surprising is that the private sector has already publicly used hack back with proven success in multiple incidents, as documented by Anthony Glosson. In his first example, Google mounted an active defense campaign in response to Chinese hacker intrusions into private Gmail accounts in 2009. Google gained access to a computer in Taiwan used by the hackers to see evidence of the attack. The evidence revealed the breaches of the so called Operation Aurora were not only at Google, but also at 33 other companies, including Adobe Systems and Northrop Grumman. Google shared the evidence with American intelligence and law enforcement officials and cooperated with them to determine the origin of the attack was on the Chinese mainland.[1497] In a second instance, Facebook used

---

[1495] U.S. Department of Defense, "The DoD Cyber Strategy," April 2015: 4-5.

[1496] Ibid.

[1497] David E. Sanger and John Markoff, "After Google's Stand on China, U.S. Treads Lightly," *The New York Times*, January 14, 2010.

active defense tactics in response to the compromise of Facebook servers by the “Koobface” gang in 2011. Koobface installed a virus on user devices to draft their computer into a botnet, hijack Web searches to deliver clicks to unscrupulous marketers, and trick the user into paying for fake antivirus software.[1498] Facebook Security performed a technical takedown of the gang’ command and control server to exfiltrate evidence and disable it. Facebook then shared its intelligence with the online security community and law enforcement agencies to rid the Web of the Koobface virus.[1499]

For legal use of tailored disruption capacities outside the victim’s network, after taking the factors of willingness, capacity, and benefits into account, a better option than relying only on the government could be closely regulated use by licensed private companies under limited circumstances. The concept of licensed privateers to augment government capability has a strong historical basis in the maritime environment. By applying this logic to the cyber domain, a reasonable contention is that “a limited number of entities certified by the government and working with the government could add to the government’s capabilities to address extensive cyber intrusions through the application of active defense.”[1500] To ordain this contention, revised laws might not even be necessary, as a new legal framework could capitalize on clauses in existing laws. Section 1030(f) of the CFAA’s unauthorized access ban “does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.”[1501] In essence, Section 1030(f) is “an explicit exception from the CFAA for

---

[1498] Riva Richmond, “Web Gang Operating in the Open,” *The New York Times*, January 16, 2012.

[1499] Facebook Security Team, “Facebook’s Continued Fight Against Koobface,” January 17, 2012: https://www.facebook.com/notes/facebook-security/facebooks-continued-fight-against-koobface/10150474399670766/

[1500] Franklin D. Kramer and Melanie J. Teplinsky, “Cybersecurity and Tailored Deterrence,” Atlantic Council, December 2013: 6.

[1501] 18 U.S.C. &1030 (f).

law enforcement agencies" which allows them "to undertake normally prohibited cyberattacks."[1502] Since there is "no explicit provision exempting private companies from the CFAA," an approach proposed by Zach West is to "deputize U.S. companies under Section 1030(f)."[1503]

The Active Cyber Defense Task Force Project Report released in October 2016 agrees that "there is a need for government to partner with the private sector in developing and implementing a framework for active defense. Such a framework would allow forward-leaning and technologically advanced private entities to effectively defend their assets in cyberspace, while at the same time ensuring that such actions are embedded in a framework that confirms government oversight."[1504] The pertinent question is what delineations or limitations should be made for the type of malicious actor and the type of disruptive action to be used against them by licensed private companies in various scenarios outside the network? In consideration of risk, a sliding scale of aggressive actions could be applied in "limited circumstances in cooperation with or under delegated authority of a national government:"[1505]

- *Nation States*: the use of countermeasures against state organs, namely military or intelligence agencies has potential to cause escalation. Therefore aggressive actions, such as denial of service or damage to their computers should only be undertaken by government agencies. Countermeasures against persons or groups acting on the instructions of, or under the direction or control of a State, could be conducted by licensed private companies but limited to bogus files or embed beacons, traceback property and delete stolen data. The Task Force Report

---

[1502] Zach West, "Young Fella, If you're looking for Trouble I'll accommodate you: Deputizing Private Companies for the use of Hackback," Syracuse Law Review, Volume 63, 2012: 139-140.

[1503] Ibid.

[1504] Center for Cyber & Homeland Security, "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," Project Report, The George Washington University, October 2016: v.

[1505] Ibid, 9.

argues that retrieval attempts are not likely to succeed because an advanced adversary would replicate, hide or back up stolen data.[1506] Thus the data should be wiped in route on a third party server before local business hours of the adversary.

- *Hacker Groups*: the use of countermeasures against loosely state affiliated “hackers for hire” groups would be to deny their objective of stealing competitive or confidential information. For commercial victims, this activity would most likely fall below the current threshold of government response. Therefore countermeasures could be conducted by licensed private companies but mostly limited to bogus files or embed beacons, traceback property and delete stolen data per above. The insertion of logic bombs into files before stolen to damage computers when opened is risky but would prevent initial access to files before replication and dispersion. The use of countermeasures against movements like Anonymous would be to halt their hacktivist campaign. The challenge is the difficulty of interfering with tens of thousands of enthused citizens using their computers for typical denial of service attacks or worst collateral damage to compromised computers in botnets. Countermeasures against the verified source of an intrusion, like by a skilled hacker attempting SQL injection, could be conducted by licensed private companies in order to achieve disruptive signaling, to include denial of service or implanting malware to damage the hacker’s computer.

- *Criminal Organizations*: the use of countermeasures against criminal syndicates would be to halt the theft of financial assets and sensitive information. For commercial victims, this activity would most certainly fall below the current threshold of government response. Therefore countermeasures could be conducted by licensed private companies to not just delete stolen data but bait files with malware to photograph the actor for evidence for prosecution. An alternative is to implant ransomware to lock down the computer to impose proportionate costs.

- *Terrorist Groups*: the use of countermeasures against an organized armed group like the Islamic State would fall under the category of armed conflict and is best left to the military.

[1506] Ibid, 12.

Granted the Zach West framework for use of deputized U.S. companies adopted here is slightly different than the one suggested in the Task Force Report. Yet given the proven utility of hack back by the private sector, for the category of outside the victim's network, the strategy of active cyber defense could be *technically capable and legally viable* for use in deterring the wide variety of malicious actors. However only by licensed private companies under the supervision and approval of proper authorities, such as by the Department of Justice under CFAA Section 1030(f) exceptions, in certain authorized scenarios.

Illustrative Case of Deterrence Strategy Failure

The 2016 hack into the Democratic National Committee (DNC) network outlined in the Introduction provides an illustrative case for final analysis of the sufficiency of contemporary deterrence strategies or the alternative strategy of active cyber defense. The Obama administration hesitated to publicly named Russia as behind the hack into the DNC, and also into other Democratic Party accounts as the campaign was revealed to be wider than first thought.[1507] Some prominent figures, such as U.S. House Democratic Leader Nancy Pelosi, bluntly said "It is the Russians."[1508] However U.S. intelligence officials said "publicly blaming Russian President Vladimir Putin's intelligence services would bring instant pressure on Washington to divulge its evidence, which relies on highly classified sources and methods."[1509] Regardless, the United States issued on 7 October a statement of blame,[1510] continuing their "name and shame" strategy.

[1507] Eric Lichtblau and Eric Schmitt, "Hack of Democrats' Accounts Was Wider Than Believed, Officials Say," *The New York Times*, August 10, 2016.

[1508] Susan Cornwell, "U.S. House Democratic leader blames Russians for 'electronic Watergate'," *Reuters*, Politics Section, August 11, 2016.

[1509] Warren Strobel and John Walcott, "U.S. weighs dangers, benefits of naming Russia in cyber hack," *Reuters*, United States Edition, August 1, 2016.

[1510] Director of National Intelligence, "Joint DHS and ODNI Election Security Statement," Press Release, October 7, 2016: 1.

Russian Foreign Minister Sergei Lavrov said it was flattering but a baseless accusation, in not seeing "a single fact, a single proof."[1511]

The absence of presented evidence in October 2016 of Russian culpability is counter to the 2015 UN Group of Governmental Experts report that accusations of "wrongful acts brought against states should be substantiated."[1512] As a matter of policy, formulating the right kind of response for deterrence in this case is not straightforward. American agencies assembled a menu of options for President Obama ranging from exposing President Putin's financial ties to oligarchs to manipulating the computer code used by Russia in designing its cyberweapons.[1513] Some of the options were rejected as ineffective and others as too risky. For the first, James Lewis doubted "using intelligence findings to embarrass Mr. Putin... would be the solution."[1514] For the latter, to manipulate or even expose Russian hacking tools, which they hold dear, risks exposure of American software implants. For specific sanctions in retaliation, the impact is questionable given the limited effect of sanctions levied on Russia for the Crimea incursion.[1515] And the use of offensive cyber means to attack Russian networks would likely induce rapid escalation while the U.S. cannot ensure escalation dominance.[1516] For deterrence by denial, the

---

[1511] Nicole Gaouette and Elise Labott, "Russia, US move past Cold War to unpredictable confrontation," *CNN News*, October 12, 2016.

[1512] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, 22 July 2015: 13.

[1513] David E. Sanger, "Obama Confronts Complexity of Using a Mighty Cyberarsenal Against Russia," *The New York Times*, December 17, 2016.

[1514] David E. Sanger and Nicole Perlroth, "What Options Does the U.S. Have After Accusing Russia of Hacks?" *The New York Times*, October 8, 2016.

[1515] Karoun Demirjian, "Lawmakers say Obama should start thinking about sanctioning Russia for hacking, *The Washington Post*, September 15, 2016.

[1516] Adam Segal, "After Attributing a Cyberattack to Russia, the Most Likely Response is Non Cyber," *Net Politics*, Council of Foreign Relations, October 10, 2016.

DNC announced the creation of a Cybersecurity Advisory Board "composed of distinguished experts in the field"[1517] to prevent future attacks and other Democratic organizations have been "shoring up their cybersecurity defenses,"[1518] which might all prove to be hopeless given the APT groups ability to easily bypass security defenses if determined to do so. Whereas they did not try very hard in a less aggressive, risk adverse phishing attempt to penetrate the Republican National Committee computers at the time of the DNC hack.[1519]

For the strategy of deterrence by entanglement, the question begs was the DNC intrusion really outside international norms of acceptable behavior? [1520] Michael Schmitt said "hacking the DNC's emails is an act of political espionage, which is not a breach of international law."[1521] Nonetheless, Schmitt said Russia's apparent attempt to influence the outcome of the election "probably violates the international law barring intervention in a state's internal affairs."[1522] Yet what proof besides circumstantial[1523] exist that Russia directly gave the material to WikiLeaks or that the release was directed by Russia?[1524] Even though the U.S. believed President Putin most

---

[1517] Rich Edson, "DNC creates 'Cybersecurity Advisory Board,' will notify staff affected by hack," *Fox News*, August 11, 2016.

[1518] Eric Lichtblau and Eric Schmitt, "Hack of Democrats' Accounts Was Wider Than Believed, Officials Say," *The New York Times*, August 10, 2016.

[1519] Shane Harris, Devlin Barrett and Julian E. Barnes, "Republican National Committee Security Foiled Russian Hackers," *The Wall Street Journal*, December 16, 2016.

[1520] Warren Strobel and John Walcott, "U.S. weighs dangers, benefits of naming Russia in cyber hack," *Reuters*, United States Edition, August 1, 2016.

[1521] Ellen Nakashima, "Russia's apparent meddling in U.S. election is not an act of war, cyber expert says," *The Washington Post*, February 7, 2017.

[1522] Ibid.

[1523] Threat Connect Research Team, "Guccifer 2.0: All Roads Lead to Russia," Featured Article, July 26, 2016.

[1524] Mark Pomerleau, "Cyber issues from the Aspen Security Forum," *C4ISRNET*, August 4, 2016.

likely gave broad direction to hack U.S. political institutions, a senior administration official said at that time "We don't have Putin's fingerprints on anything or a piece of paper that shows he signed the order."[1525] The U.S. assessment based on analysis of intelligence, not any evidence, depicts how hard it is to achieve attribution to satisfy international law criteria for State responsibility.[1526] This synopsis of deterrence strategy shortfalls is further exacerbated by FireEye saying the two APT groups "wanted experts and policy makers to know that Russia is behind it [the DNC hack]."[1527] Finally, on 29 December, President Obama imposed sanctions on Russian entities,[1528] expelled 35 Russian intelligence operatives, and closed two Russian recreational compounds in the United States.[1529] In addition, a Joint Analysis Report released data on malware used by Russian intelligence services.[1530] President Putin said Russia wouldn't retaliate and expel U.S. diplomats and even invited their children to a New Year's celebration at the Kremlin, in a public display of restraint aimed to embarrass the Obama administration.[1531]

1525 Shimon Prokupecz and Jeff Zeleny, "Intel analysis shows Putin approved election hacking," *CNN News*, December 15, 2016.

1526 International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries,* fifty-third session, 2001: Article 8.

1527 Patrick Tucker, "Russia Wanted to be Caught, Says Company Waging War on the DNC Hackers," *Defense One*, July 28, 2016.

1528 President Barak Obama, "Taking Additional Steps to Address to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," Executive Order and Annex, The White House, December 29, 2016.

1529 President Barak Obama, "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment," The White House, December 29, 2016.

1530 Office of the Press Secretary, "Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment," The White House, December 29, 2016.

1531 James Marson and Anne Ferris-Rotman, "Putin Says He Won't Retaliate," *The Wall Street Journal*, December 31, 2016.

The reality today is advanced actors continue their operations at a high pace, adapting in the open, with little risk of real punishment. The failure of cyber deterrence strategies highlighted by the U.S. election hacking episode, despite the past eight years of efforts by the Obama administration,[1532] leaves open the question of what about the strategy of active cyber defense to deny benefits or impose costs? To get into the DNC network, Crowdstrike suspected the APT groups may have targeted employees with "spearphishing" emails,[1533] a preferred vector used by both Cozy Bear and Fancy Bear to target their victims.[1534] The use of this common attack vector which has such a high success rate meant penetration was probably inevitable.[1535] After which Cozy Bear installed the SeaDaddy implant and Fancy Bear installed X-Agent malware for automatic or remote execution,[1536] placing themselves already at phase five of the cyber kill chain. Although the DNC information technology team did notice some unusual network activity and reported it in late April, the files were already stolen and the damage done. Inside the network, the groups did have to move across two phases of the kill chain after installation, which opens the possibility that active cyber defense capabilities could have stopped the attack before action on objectives. FireEye has seen Cozy Bear on some systems "moving laterally within a network. They know that their tool is going to be detected by a system that they're about to move to and they'll do it anyway because they're such skilled hackers that they can compromise the system and then jump to another system and get what they need before they can be

---

[1532] David Fidler, "President Obama's Pursuit of Cyber Deterrence Ends in Failure," *Net Politics*, January 4, 2017.

[1533] Ellen Nakashima, "Russian government hackers penetrated DNC, stole opposition research on Trump," *The Washington Post*, June 14, 2016.

[1534] FireEye, "APT28: At the Center of the Storm," Special Report, January 2017: 11.

[1535] Kaspersky, "The Dangers of Phishing: Help Employees Avoid the Lure of Cybercrime," White Paper, 2015: 1-8.

[1536] Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," CrowdStrike Blog, June 15, 2016.

quarantined."[1537] Active cyber defense operates at cyber relevant speed,[1538] leveling the playing field to isolate the threat.

The President of Crowdstrike said the DNC "was not engaged in a fair fight" since "you've got ordinary citizens who are doing hand-to-hand combat with trained military officers."[1539] Yet CrowdStrike, a leading private firm, are not ordinary citizens, but undoubtedly experts in the field. They not only identified the two Russian intelligence-affiliated hacker groups in the network, but watched advanced methods to avoid detection, such as changing implants, modifying persistence methods, and moving to new command and control channels.[1540] CrowdStrike considers the APT groups to be the best of all the numerous nation state, criminal, hacktivist and terrorist groups they encounter. In the DNC incident, CrowdStrike was in the network with them and in the best position to launch countermeasures outside the network. If the attackers were already at exfiltration, maybe CrowdStrike could have seen the files sitting on an overseas server. General Michael Hayden said he is "aware of a company that did see its data stolen, was able to track where it had gone" and "it is not yet the waking hours during the work week of the country in which they believe the source of the attack emanated... and so it's just sitting there on this server in a third country place waiting for the thieves to come grab it and bring it home."[1541] Maybe a licensed private company, deputized under existing law, and under proper government oversight and supervision, could have traced and deleted the DNC files.

1537 Patrick Tucker, "Russia Wanted to be Caught, Says Company Waging War on the DNC Hackers," *Defense One*, July 28, 2016.

1538 U.S. Department of Defense, *Strategy for Operating in Cyberspace*, July, 2011: 7.

1539 Ellen Nakashima, "Russian government hackers penetrated DNC, stole opposition research on Trump," *The Washington Post*, June 14, 2016.

1540 Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," CrowdStrike Blog, June 15, 2016.

1541 General Michael V. Hayden, "HBO What to Do About Cyberattack," Council on Foreign Relations Event, October 6, 2015.

Concluding Considerations

In the summer of 2015 eight top congressional leaders were briefed that Russian hackers were attacking the Democratic Party, but not the target because the information was so secret.[1542] A year and a half later, CrowdStrike provided proof through malware analysis that the APT group Fancy Bear that struck the Democratic National Committee was a unit of the GRU, Russia's Main Intelligence Directorate.[1543] The apparent motivation to affect U.S. public opinion appears to have been greater than any perceived risk induced by current deterrence strategies. For deterrence is a matter of perception, that "resides ultimately in the eye of the beholder."[1544] Lieutenant General James McLaughlin has stated that the Defense Department, in a whole-of-government approach, seeks to "deny the adversary the ability to achieve the objectives of a cyber attack, so our adversary will believe any attack will be futile." Furthermore, the adversary must believe "that our ability to respond to an attack will result in unacceptable costs imposed on them" through the use of "a variety of mechanisms, including economic sanctions, diplomacy, law enforcement, and military action."[1545] Cumulatively these statements describe the desired outcomes of the contemporary deterrence strategies of retaliation, denial and entanglement. The problem today is malicious actors in cyberspace do not believe that "a threat of retaliation exists, the intended action cannot succeed, or the costs outweigh the benefits of acting."[1546] It would be

---

[1542] Mark Hosenball and John Walcott, "Exclusive: Congressional leaders were briefed a year ago on hacking of Democrats – sources," *Reuters*, Politics Section, August 12, 2016.
[1543] Thomas Fox-Brewster, "This Android Malware Ties Russian Intelligence to the DNC Hacks," *Forbes*, December 22, 2016.
[1544] Michael Mandelbaum, "It's the Deterrence, Stupid," *The American Interest*, July 30, 2015.
[1545] Thomas Atkin, James K. McLaughlin and Charles L. Moore, "Statement before the House Armed Services Committee," June 22, 2016.
[1546] Department of Defense. *Joint Operations.* Joint Publication 3-0. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 17 January 2017: VI-4.

naïve and negligent to think they will not try "again and again."[1547] Another strategy is necessary to induce the perception of risk and repercussion into the wide range of malicious actors engaging in cyber attacks.

An alternative strategy of active cyber defense would embrace a combination of internal systemic resilience to deny benefits and tailored disruption capacities to impose costs. Internal systemic resilience starts with closing the gap in time from compromise to discovery inside the network. Mandiant claims that its Red Team is able to "obtain access to domain administrator credentials within three days of gaining initial access" to a system.[1548] The firm argues that once credentials are found, it is "only a matter of time before an attacker is able to locate and gain access to the desired information." They conclude that if the average time to discovery is now at 146 days, that is at least 143 days too long.[1549] In response, active cyber defense can detect, verify and remediate activity along the cyber kill chain to withstand the attack. It does not matter if attribution exists to identify exactly who is the actor, only that the attack is stopped before harm or damage from the breach occurs, to deny benefit of the attack. Outside the network, to impose costs, maybe the time has come to use tailored disruption capacities that target hackers "with some of their own weapons: government-sanctioned malware or ransomware, software that locks down a computer without a user's consent."[1550]

For deterrence to be effective, the strategy must be based on capability (possess means to influence behavior), credibility (instilling believability), and communication (of right message).[1551] The level of skill seen in the DNC hacks is not limited to APT groups, as Kevin

---

[1547] Patrick Tucker, "Russian Hackers Will Try 'Again and Again,' Warns Samantha Power, *Defense One*, January 17, 2017.

[1548] M-Trends 2016, 4.

[1549] Ibid, 4.

[1550] Adrienne Lafrance, "Hacking and the Future of Warfare," *The Atlantic*, June 12, 2015.

[1551] Department of Defense. *Joint Operations.* Joint Publication 3-0. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 17 January 2017): xxii.

Haley, director Symantec Security Response states "Advanced criminal attack groups now echo the skill sets of nation-state attackers."[1552] Active cyber defense has the capability to withstand an attack by any of these actors through use of numerous heuristics or attack detectors combined with automated remediation actions. Also, the DNC hack represents another use of proxy groups for plausible deniability, codified in the "inevitable Kremlin response: Prove It."[1553] Inside the network, active cyber defense has the credibility to block the attack before objectives, denying the need to "prove it," or even better, outside the network, to find the files and take discrete action. Finally, the DNC hack that induced unprecedented interference in the electoral process of a nation signifies a test by Moscow of the limits of acceptable state behavior in cyberspace.[1554] Signaling, a corollary to communication, is a foreign policy instrument "to change the cost-benefit calculations of states engaging in or sponsoring" malicious cyber activity.[1555] Any decision to legally allow companies to engage malicious actors would communicate national resolve. Senator Whitehouse has said that "policymakers should consider allowing companies to engage in "active defense" of their networks," ranging from "tracking the flow of a company's information across networks," or to hack back where it seems "to make sense in certain, very narrow circumstances."[1556] Although the parameters and limitations have yet to be fully explored, the empirically grounded midrange theory of active cyber defense, comprised of the

---

[1552] "Rene Millman, "Cyber-criminals becoming increasingly professional," *SC Magazine,* April 13, 2016.

[1553] Andrew Roth, "How the Kremlin is sure to keep its fingerprints off any cyberattack," *The Washington Post*, August 2, 2016.

[1554] Matthijs Veenendaal, Kadri Kaska, Henry Rõigas and Can Kasapoglu, "DNC Hack: An Escalation That Cannot Be Ignored," Tallinn, Estonia, NATO Cooperative Cyber Defense Center of Excellence, August 5, 2016.

[1555] Sico van der Meer, "Signalling as a foreign policy instrument to deter cyber aggression by state actors," Policy Brief, Clingendael, Netherlands Institute of International Relations, December 2015: 1-6.

[1556] Sean Lyngaas, "Sen. Whitehouse proposes a cyber IG for civilian agencies," *Federal Computer Weekly*, June 6, 2016.

concepts of systemic resilience and disruption capacities, potentially meets the conditions of capability, credibility and communication to be considered or selected as an alternative strategy to achieve deterrence within the cyber arena.

APPENDIX

National Strategy Agenda

The general theory of strategy enables a nation to cope with serious challenges to national security. For the United States, the President declares that "significant malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States continue to pose an unusual and extraordinary threat to the national security, foreign policy and economy of the United States."[1557] Yet this threat is not unique to the United States. In a 2016 industry survey of medium size organizations representing 10 countries across North America, Europe, Asia Pacific, and Latin America, the percentage compromised by at least one successful cyber attack in the past twelve months ranged from 63 to 89 percent, with more than half between one to five times.[1558] For these countries and any other, the principles and priorities of a national security strategy can guide the use of power and influence in countering the cyber threat. The strategy can signal resolve and readiness to deter, and if necessary to defeat malicious actors that threaten the advancement or survival of national interests. A smart national security strategy relies not only on military power to protect interests but draws upon all elements of national strength as means in a comprehensive national security agenda.

For the deterrence of malicious actors in cyberspace, evidence has shown that the strategy of active cyber defense is technically capable and legally viable, at least to some extent, to enable the achievement of the central premise of deterrence; the altering of the behavior of an actor. Active cyber defense reinforces both deterrence by denial and deterrence by retaliation. A national strategy agenda for active cyber defense has promise to instill in an actor the belief that the intended action cannot succeed and that a threat of retaliation exists. According to Admiral

[1557] Aaron Boyd, "Obama: Cyberattacks continue to be national emergency," *Federal Times*, March 10, 2016.

[1558] CyberEdge Group, "2016 Cyberthreat Defense Report," Current Security Posture, 2016: 7.

Mike Rogers, Director of the National Security Agency, "We are in a world now where, despite your best efforts, you must prepare and assume that you will be penetrated."[1559] His warning to the audience at a London Stock Exchange event came shortly after similar comments by Jonathan Kidd, the Chief Information Security Officer for the United Kingdom Met Office that "You can't assume you're not already compromised."[1560] In response, Kidd contends the best course of action is to develop a strategy on how to deal with that reality. That strategy is one of active cyber defense that embraces a combination of internal systemic resilience to halt malicious cyber activity after an intrusion with tailored disruption capacities to thwart malicious actor objectives. Therefore to implement a strategy of active cyber defense, a national strategy agenda would be based on the two pillars of resilience to withstand a cyber attack and disruption to obstruct the malicious actor.

The first pillar of resilience prepares society for surprise in cyberspace through implementation of automated and integrated capabilities that act only inside organizational boundaries. The second pillar of disruption averts malicious actor asymmetries in cyberspace through countermeasures performed either by or under the supervision and approval of proper authorities. Since resources for a national strategy agenda will never be limitless, policy tradeoffs and hard choices among many competing priorities will have to be made. In order to set the debate for implementation by any country, this appendix begins by delineating how the national strategy pillars of resilience and disruption, enabled through a comprehensive approach, reside currently in principle in the cyber security strategies of international organizations and multiple nations. The appendix then explores architectures and arrangements in work in the United States to strengthen the two pillars for adaptation or use as deemed fit by other nations. The appendix finishes with policy recommendations and priority suggestions to guide tradeoffs

---

[1559] Privacy Section, "'It is not about if you will be penetrated, but when,' warns NSA chief," *Computing*, 16 July 2015.

[1560] Hacking Section, "'You can't assume you're not already compromised,' warns Met Office CISO," *Computing*, 5 June 2015.

and choices in action plans that implement a national strategy agenda for active cyber defense based on the two pillars of resilience and disruption.

Cyber Security Strategies

A national security strategy addresses the top strategic risks to national interests. Enduring national interests typically fall into four categories, namely the security of the nation and its citizens; a strong economy that promotes prosperity; respect for universal values; and a rules-based international order. To advance these interests most effectively, leaders pursue a national security agenda that allocates resources and prioritizes efforts according to strategic risk. For the United States, standing at the top of the list of strategic risks is a catastrophic attack on the U.S. homeland or critical infrastructure. Consequently the present U.S. National Security Strategy stresses the importance of "fortifying our critical infrastructure against all hazards, especially cyber espionage and attack." That objective necessitates working with the owners and operators of critical cyber infrastructure across every sector to decrease vulnerabilities and increase resilience.[1561] In essence, this mandate means using a comprehensive approach which brings together all elements of society to make the nation resilient in the face of diverse threats. For that reason, Presidential Policy Directive, PPD-21 "advances a national unity of effort to strengthen and maintain" not just secure and functioning, but also resilient critical infrastructure.[1562] The emphasis on unity of effort for the purpose of resilience is also found in other cyber security strategies of international organizations and multiple nations.

[1561] Executive Office of the President, *National Security Strategy*, (Washington, DC: The White House, February 2015): 1-13.

[1562] Executive Office of the President, *Presidential Policy Directive on Critical Infrastructure Security and Resilience*, PPD-21, (Washington, DC: The White House, February 12, 2013).

Internal Systemic Resilience

Resilience at the international level is particularly important because digitally interconnected infrastructures that span the globe create both dependencies and vulnerabilities. The potential impact on society of disruptions to this fragile equilibrium makes interaction between the private sector which owns and operates most critical infrastructure and the public sector crucial to managing risk.[1563] The Cybersecurity Strategy of the European Union highlights the value of this interaction in a guiding principle that all relevant actors, whether the private sector or public authorities, need to recognize shared responsibility to ensure security of information and communications technologies. Accordingly, the European Union made "achieving cyber resilience" the first strategic priority for action in their Strategy.[1564] To promote cyber resilience among members, the European Union Strategy recognizes a substantial effort is necessary to enhance private and public capacities and processes to prevent, detect and handle cyber security incidents. Since gaps exist in national capacities, the European Union suggests members adopt a national strategy and cooperation plan, with incentives for private actors to invest in security solutions and provide reliable data on cyber incidents.[1565]

A central principle of the National Cyber Security Strategy of the Czech Republic is a "comprehensive approach to cyber security based on principles of subsidiarity and cooperation."[1566] The nation aims for coordination of activities and enhancement of trust among all stakeholders. Main goals for protection of national critical information infrastructure include: to enhance network resistance and integrity, share information in an efficient manner, and

---

[1563] Dave Clemente, "Cyber Security and Global Interdependence: What is Critical?" Chatham House, February 2013: viiix.

[1564] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7 February 2013: 3-4.

[1565] Ibid, 5-6.

[1566] National Security Authority, *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020*, 2015, 9.

increase capacities for active cyber defense and cyber attack countermeasures. Likewise, the Italian National Strategic Framework for Cyberspace Security recognizes that network interdependence, asymmetric threats and the pervasive nature of cyberspace calls for a holistic approach and synergistic effort of all involved stakeholders. A strategic guideline of the Italian Strategy that echoes the tenets of active defense is to "leverage the national capability to analyze, prevent, mitigate and effectively react to the multi-dimensional cyber threat."[1567] The National Cyber Security Strategy of the United Kingdom specifically calls for Active Cyber Defense as a Defend Element in order to implement "security measures to strengthen a network or system to make it more robust against attack."[1568]

The Estonian Cyber Security Strategy recognizes that civilian and military resources must be integrated into a functioning whole to ensure the ability to provide national defense in cyberspace. One of the aims of this Strategy is to "describe methods for ensuring the uninterrupted operation and resilience of vital services."[1569] Therefore the information systems that are necessary for the operation of vital services are to be managed in a way that provides the means to manage risks. Furthermore, the Estonian Strategy dictates that civil and military cooperation must "function adequately in cyberspace with regards to warning, deterrence and active defense."[1570] The Cyber Security Strategy of Georgia also aims to set up a system that will "facilitate resilience of cyber infrastructure against cyber threats."[1571] It calls for cooperation modalities between state agencies that extend to public-private partnerships. Like for Estonia, the Georgian Strategy appeals for a new legislative framework in order to develop and implement effective security measures.

[1567] Presidency of the Council of Ministers, *National Strategic Framework for Cyberspace Security*, December 2013: 6-20.

[1568] HM Government, *National Cyber Security Strategy 2016-2021*, 2016: 33.

[1569] Ministry of Economic Affairs and Communication, *Cyber Security Strategy 2014-2017*, 2014: 6-8.

[1570] Ibid, 10.

[1571] The Government of Georgia, *Cyber Security Strategy of Georgia 2012-2015*, 2012: 3-5.

In the Pacific, Australia's Cyber Security Strategy emphasizes the need for government and business to collaborate "to strengthen our economy and national security by building greater resilience to cyber security threats."[1572] To achieve the goal of strong cyber defenses, the government will "co-design national voluntary Cyber Security Guidelines with the private sector to specify good practice." Furthermore, it will "establish a layered approach for sharing real time public-private threat information."[1573] Similarly, the Japanese Cybersecurity Strategy recognizes that in order to "counter diversified cyber threats appropriately; the public and private sectors must closely collaborate in sharing information on system failures possibility caused by cyber attacks."[1574] Therefore the Japanese Government intends to work to build platforms for an interactive and advanced information sharing environment. The Japanese Strategy emphasizes the need to limit the information to be shared and conceal informer identities, so they will not suffer unreasonable loss or disadvantage.

Tailored Disruption Capacities

The military has a role in protecting national interests in their assigned missions in defense of the nation. For instance in the United States, U.S. Cyber Command teams with federal, foreign, and industry partners to help "mitigate, halt, and attribute acts of disruption and destruction and campaigns of cyber espionage; dissuade adversaries from malicious behavior; and strengthen the resilience of Department of Defense systems to withstand attacks."[1575] These functions articulated in the Commander's Vision and Guidance require building information

[1572] Australian Government, *Australia's Cyber Security Strategy*, 2016: 23.

[1573] Ibid, 27.

[1574] The Government of Japan, *Cybersecurity Strategy*, Provisional Translation, Cabinet Decision, September 4, 2015: 27.

[1575] Vice Admiral Michael S. Rogers, U.S. Navy, "Beyond the Build: Delivering Outcomes through Cyberspace," The Commander's Vision and Guidance for US Cyber Command, June 3, 2015: 5.

sharing mechanisms to ensure regular contact with those whom Cyber Command operates and fights alongside, both inside and outside the Department of Defense. For instance, Cyber Command teams with the National Security Agency to leverage its proven expertise in intelligence analysis and information assurance. When necessary, the Command will "help other agencies defend the nation against cyber attacks from abroad, especially if they would cause loss of life, property destruction, or significant foreign policy and economic consequences."[1576] And when called upon, Cyber Command will "utilize appropriate authorities and policies, especially in our role as part of the federal government's response to attacks on critical infrastructure."[1577] Besides the United States, a few other nations have developed strategies that embrace broad tenets for use of tailored disruption capacities in a comprehensive approach to cyber security.

The Dutch Defense Cyber Command, established in 2014, is a smaller equivalent of the U.S. Cyber Command. It is the central entity in the Netherlands for the development and use of offensive capability.[1578] The country's Defense Cyber Strategy delineates that offensive cyber capabilities are "aimed at influencing or disabling the actions of an opponent."[1579] Since the digital systems of potential opponents are vulnerable, cyberspace can be used for operations against that opponent. The strategy recognizes that a large scale attack against society could have enormous impact and therefore the armed forces must be capable of taking action against digital threats to society. The armed forces have a core task to make capabilities available to civil authorities on request, and with the proper legal or regulatory basis, measures can be taken to improve the security and availability of Dutch cyberspace. Although in organizing a

---

[1576] Ash Carter, U.S. Secretary of Defense, "Securing the Oceans, the Internet, and Space," Speech to Commonwealth Club, Silicon Valley, March 1 2016: 1-15.

[1577] Vice Admiral Michael S. Rogers, U.S. Navy, "Beyond the Build: Delivering Outcomes through Cyberspace," The Commander's Vision and Guidance for US Cyber Command, June 3, 2015: 6.

[1578] Colonel Hans Folmer, "The Defense Cyber Command, a new operational capability," Magazine Nationale, nr. 5, October 22, 2014.

[1579] Hans Hillen, Minister of Defense, *The Defense Cyber Strategy*, Netherlands, 27 June 2012.

comprehensive approach in response to large-scale digital disruptions, the strategy recognizes that roles, tasks and responsibilities have to be clear.[1580] Any use by the military of capabilities in cyber operations would fall under the categories of Defensive Cyber Operations for proactive detection and termination of intruders and Offensive Counter Operations for preventive attacks.[1581]

In 2015, the Israeli Defense Force decided to establish in two years a Cyber Command to lead the military's operational activities. Although in Israel, protection of computerized systems in the civilian sector has never been put under the protection of the Israeli Defense Force. The reason to limit the military role appears to stem from ethical, ideological and political values. Any further analysis on reasons and roles is difficult as Israel has never published an open, formal cyber security strategy, exercising political preference to avoid formal binding declarations and even using classification to shroud the topic, while they are known to leverage support from the private sector.[1582] Yet the nation has taken public steps to review national cyber policy through commission of their National Cyber Initiative in 2010. A task force was charged with putting Israel among "the top five countries leading the cyber field."[1583] Many of their recommendations centered on aspects of Research and Development infrastructure, collaboration and products. The result of subsequent efforts is impressive as "Israel is responsible for more exports of cyber-related products and services than all other nations combined apart from the United States."[1584] In fact over the past five years, the number of Israeli

[1580] Ibid, 4-16.

[1581] Brigadier General Hans Folmer, "Cyber Commander Panel Remarks," NATO Cooperative Cyber Defence Centre of Excellence, CyCon 2016 Press Release, June 1, 2016.

[1582] Lior Tabansky, "Israel's Cyber Security Policy: Local Response to the Global Cybersecurity Risk," Chapter 21, *Civil Society and National Security in the Era of Cyber Warfare*, IGI Global, 2016: 481-482 and 488-489.

[1583] James Andrew Lewis, "Advanced Experiences in Cybersecurity Policies and Practices," Discussion Paper No. IDB-DP-457, Inter-American Development Bank, July 2016: 24.

[1584] Ibid, 26.

cyber security companies has doubled to 300. Given the propensity of former Israeli Defense Force members, trained to use cutting edge technologies under tight discipline, to join these companies,[1585] there is no shortage of talent for external disruption capacities.

Architectures and Arrangements

Active cyber defense focuses on "the integration and automation of many services and mechanisms to execute response actions in cyber-relevant time."[1586] The term cyber-relevant time ranges from nanoseconds to minutes depending on the location of the malicious actor and activity. The elements of active cyber defense synchronize "the real-time detection, analysis, and mitigation of threats to critical networks and systems."[1587] These active activities strive to stop or limit damage through the integration and automation of cyber-security solutions. Sets of solutions are deployed "across the interior and at the boundary of a network enterprise."[1588] They can be unique tools integrated in a single platform or individual solutions, like for endpoint detection and response. In the United States, a collaborative effort between the National Security Agency, the Department of Homeland Security and the Johns Hopkins University Applied Physics Laboratory has produced the reference architecture for the fundamental concept of Integrated Adaptive Cyber Defense (IACD), supported by a cooperative arrangement for Automated Indicator Sharing (AIS). A key principle in the design of active cyber defense is for response actions to be automatable and not inherently automatic. While the intent is for these

---

[1585] Lior Tabansky, "Israel's Cyber Security Policy: Local Response to the Global Cybersecurity Risk," Chapter 21, *Civil Society and National Security in the Era of Cyber Warfare*, IGI Global, 2016: 482-483.

[1586] MJ Herring and KD Willett, "Active Cyber Defense: A Vision for Real-Time Cyber Defense," *Journal of Information Warfare*, 13.2, 2014: 46.

[1587] National Security Agency Information Assurance Directorate, "Active Cyber Defense (ACD)," Fact Sheet, October 22, 2015: 1-2.

[1588] National Security Agency Information Assurance Directorate, "Active Cyber Defense (ACD)," Frequently Asked Questions, October 22, 2015: 1-2.

actions to stay inside the network, there are other innovative programs in the United States that could lead to military and civilian capacity for disruptive actions outside the network.

Internal Systemic Resilience

Integrated Adaptive Cyber Defense (IACD). The goal of Integrated Adaptive Cyber Defense is to "dramatically change the timeline and effectiveness of cyber defense secure integration and automation" to enable faster response times and defensive capabilities."[1589] The IACD reference architecture is intended to inform and guide "cyber service providers, network owners and product vendors on the capabilities and interfaces that can enable an agile, dynamically responsive and resilient cyber infrastructure."[1590] The concept starts with the premise that two key issues hamper effective cyber defense. The first is malicious actor's ability to reuse cyber-attack tools and techniques against multiple targets because similar organizations do not share information. The second is cyber attack response times are too slow to address alerts, primarily because existing solutions rely on humans in the loop. The latter has become even more severe because of attacker use of automated tools. IACD seeks to reverse these trends by improving cyber security automation and information sharing and encouraging interoperability between commercial tools. Accordingly the concept relies on three foundational capabilities:

- Automation that enables "automated sensing, sense-making, decision-making, and courses of action responses" within cyber-relevant time.

[1589] IACD Community, "Integrated Adaptive Cyber Defense (IACD) Community Day: October 3th, 2016," Email Announcement, September 19, 2016.

[1590] K. Done, et al., "Towards a Capability-Based Architecture for Cyberspace Defense," Concept Paper Approved for Public Release, U.S. Department of Homeland Security, U.S. National Security Agency Information Assurance Directorate, and the Johns Hopkins University Applied Physics Laboratory, AOS-16-0099; September 2016: 1.

- Information sharing that enables “rapid sharing of indicators, analytics and effective courses of action” among organizations.
- Interoperability that enables “a variety of commercial vendors’ tools to function with each other without the need for pairwise, custom interfaces.”[1591]

The capability-based reference architecture supports a vendor-agnostic plug-and-play operating environment to enable organizations to select commercial vendor products that best suit their needs. Ultimately the fundamental objective of IACD is to reduce response time “from months to milliseconds.”[1592] Therefore the reference architecture centers on the integration of solutions that provide the capabilities to accomplish goals that achieve this objective. To promote automation, IACD provides for machine implementation of capabilities to migrate people from ‘in’ to ‘on’ the loop in cyberspace operations. To promote sharing, IACD provides a robust, standards-based sharing capability. To promote interoperability, IACD enables open-standards-based capability interfaces for machine-to-machine information exchange.[1593] IACD conforms to other efforts and environments, such as the NIST Cybersecurity Framework for automation of the Detect function, and to the Cyber Kill Chain for preventing any step to disable the attack. The architecture describes top-level IACD capabilities and functions, to include:

- Secure orchestration, control and management: of “interactions among the IACD capabilities.”
- Control messaging: through “a standard set of messages for compliant components”

[1591] Ibid, 2.

[1592] Peter Fonash and Phyllis Schneck, “Cybersecurity: From Months to Milliseconds,” *Computer,* January 2015: 42-49.

[1593] K. Done, et al., “Towards a Capability-Based Architecture for Cyberspace Defense,” Concept Paper Approved for Public Release, U.S. Department of Homeland Security, U.S. National Security Agency Information Assurance Directorate, and the Johns Hopkins University Applied Physics Laboratory, AOS-16-00;9, September 2016: 3.

- Sensor or actuator control and data normalization: for “secure communications of data, commands, and status with heterogeneous collections of sensors and actuators.”
- Sense-Making: that “evaluates cyber events and intelligence data” to determine whether an alert is necessary.
- Decision-Making: which “recommends an appropriate response based on enterprise policies and risks and impact to the enterprise.”
- Response Controlling: that “sequences workflows” and “coordinates responses.”
- Information Sharing: that enables secure communications for “standardized exchanges of indicators of compromise” and “recommended courses of action.”[1594]

The IACD activity above intends to increase the cost of an attack by reducing cyber incident response time and limiting actor ability to reuse tools and techniques. The concept has been proven feasible through spirals that demonstrate how the integration of commercial products can detect malware, generate indicators, initiate and share responses between organizations.[1595]

Automated Indicator Sharing (AIS). IACD conforms to the Cybersecurity Act of 2015 by enabling and promoting trusted information sharing mechanisms.[1596] The Act imposed a 90 day deadline for the Department of Homeland Security, in coordination with other Federal entities, to “develop and implement a capability and process to commence real time, automated sharing of

---

[1594] Ibid, 6-7.

[1595] Gregg Tally, “Proposed Capability-Based Reference Architecture for Real-Time Network Defense,” Concept Briefing Approved for Public Release, the Johns Hopkins University Applied Physics Laboratory, November 16, 2015.

[1596] Bradley Barth, “DHS launches two-way threat sharing system for public-private collaboration,” *SC Magazine*, March 18, 2016.

cyber threat indicators and defensive measures."[1597] In response DHS deployed the Automated Indicator Sharing system, which provides "the capability for the timely exchange of relevant and actionable cyber threat indicators among federal departments and agencies and the private sector."[1598] An example of an indicator is a malicious IP address. The goal of the AIS initiative is to "commoditize cyber threat indicators" so they are "shared broadly among the public and private sector."[1599] The National Cybersecurity and Communications Integration Center manages the system to allow bidirectional sharing with participants, who will not be identified as the source of an indicator unless they grant consent. AIS takes measures to ensure appropriate privacy and civil liberties by performing "automated analyses and technical mitigations to delete Personally Identifiable Information (PII) that is not directly related to a cyber threat;" incorporating "elements of human review on select fields of certain indicators to ensure automated processes are functioning properly;" minimizing "the amount of data" in an indicator to "what is directly related to a cyber threat;" retaining only "information needed to address the cyber threat;" and ensuring any information collected is "used only for network defense or limited law enforcement purposes."[1600]

Also, as mandated by the Cybersecurity Act of 2015, the Department of Homeland Security released guidance to assist private sector and federal entities share cyber threat indicators and defensive measures. DHS published policies and procedures relating to the receipt, processing, and dissemination by all federal entities of cyber threat indicators and

---

[1597] Scott E. Jasper, "U.S. Cyber Threat Intelligence Sharing Frameworks," *International Journal of Intelligence and CounterIntelligence*, Volume 30, Number 1, 2017: 61.

[1598] Ibid.

[1599] Department of Homeland Security, "Automated Indicator Sharing (AIS)," Fact Sheet, September 25, 2016.

[1600] Department of Homeland Security, "Automated Indicator Sharing (AIS)," Fact Sheet, September 25, 2016.

defensive measures submitted through real-time means and through non-automated means,[1601] along with privacy and civil liberties guidelines for such actions.[1602] The Act did specify that besides the creation of a real time, automated process between information systems, other acceptable means for the sharing of cyber intelligence are through electronic mail or media and through an interactive forum on an Internet website. Therefore, DHS offers electronic opportunities to share cyber threat indicators and defensive measures via web form and email. If emailed, DHS requests the following fields: type (either indicator or defensive measure); valid time of incident or knowledge of topic; tactics, techniques, and procedures; and a confidence assertion for the value of the indicator (high, medium or low).[1603] Former Deputy Homeland Security Secretary, Alejandro Mayorkas, remarked at the Billington International Cybersecurity Summit, that the information sharing legislation and platform is a collaborative effort that "protects not just various parts of the economy, but the entire online environment."[1604]

The Automated Indicator Sharing capability leverages STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information) specifications for machine-to-machine communication. STIX is a structured language and TAXII is the preferred mechanism to exchange it. STIX describes "cyber threat information so it can be shared, stored, and [analyzed] in a consistent manner that facilitates automation."[1605] The STIX framework conveys the full range of cyber threat data elements to include observables,

---

[1601] Department of Homeland Security and Justice, "Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government," June 15, 2016: 3-10.

[1602] Department of Homeland Security and Justice, "Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015," June 15, 2016: 3-14.

[1603] United States Computer Emergency Readiness Team, "Automated Indicator Sharing (AIS)," Official Website of the Department of Homeland Security, accessed on September 25, 2016.

[1604] Greg Otto, "U.S. officials: World needs to follow our lead on cyber norms," *Fedscoop,* April 5, 2016.

[1605] The MITRE Corporation, "About STIX," Project Documentation, github, 2016.

indicators, incidents, adversary tactics, techniques and procedures, exploit targets, courses of action (contains defensive measures), campaigns, and threat actors. TAXII standardizes the automated exchange of cyber threat information. TAXII defines "a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries."[1606] TAXII uses an XML data format and HTTP/HTTPS message protocols. International in scope and free for public use, STIX and TAXII are "community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, real-time network defense and sophisticated threat analysis."[1607]

Tailored Disruption Capacities

Cyber Mission Force (CMF). In the United States the build of the Cyber Mission Force at U.S. Cyber Command underpins the Department of Defense's primary missions in cyberspace.[1608] The Department is working to create a total of 133 CMF teams comprised of 6200 personnel and to achieve their full operational capability by September 2018. The teams are:

– Cyber National Mission Force teams to defend the nation by seeing adversary activity, blocking attacks, and maneuvering to defeat them;
– Cyber Combat Mission Force teams to conduct military cyber operations in support of combatant commands;
– Cyber Protection Force teams to defend the DoD information networks, protect priority missions and prepare cyber forces for combat; and

[1606] The MITRE Corporation, "About TAXII," Project Documentation, github, 2016.

[1607] United States Computer Emergency Readiness Team, "Information Sharing Specifications for Cybersecurity," Official Website of the Department of Homeland Security, November 3, 2016.

[1608] Thomas Atkin, James K. McLaughlin and Charles L. Moore, "Statement before the House Armed Services Committee," June 22, 2016.

– Cyber Support teams to provide analytic and planning support to National Mission and Combat Mission teams.[1609]

Portions of the Cyber Mission Force are honing their offensive skills in cyber operations against the self-proclaimed Islamic State. Former Defense Secretary Ashton Carter said "the methods we're using are new...and some of them applicable to the other challenges that I described other than ISIL," namely Iran, North Korea, Russia and China.[1610] The Cyber National Mission Force "plans, directs, and synchronizes full-spectrum cyberspace operations to deter, disrupt, and, if necessary, defeat adversary cyber actors to defend the nation."[1611] Defending the nation missions include defending the U.S. and its interests against cyberattacks of "significant consequence," defense of the nation's critical infrastructure when directed by the president or secretary of defense; and alignment to the most sophisticated cyber adversaries. National Mission Force teams are tasked with the Defensive Cyber Operations – Response Action mission to stop attacks outside the network. They are "trained to the highest technical standards" and "operate in accordance will all legal and policy guidance impacting operations outside friendly cyberspace."[1612]

The obtainment of a dedicated and talented professional cyber force to conduct both offensive and defensive operations is a daunting task for the military given national shortages in

---

[1609] Rich Abott, "U.S. Cyber Command Mission Force Teams Achieve Initial Operating Capability," *Defense Daily*, October 27, 2016.

[1610] Sydney J. Freedberg Jr., "Cyber War Against ISIL Hones Weapons Vs. Russia, China," *Breaking Defense*, February 29, 2016.

[1611] U.S. Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability," U.S. Cyber Command News Release, October 24, 2016: https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/

[1612] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Number 73, 2nd Quarter 2014: 16.

manpower with critical technical skills and competitive pay gaps with the private sector. One way to leverage the civilian workforce is through employment of cyber militias. In the United States, militias are found in the form of National Guard units. General Joseph Lengyel, Chief of the National Guard Bureau told the audience at the North American International Cyber Summit 2016 that "the civilian-acquired skills of its members enable the National Guard to make unique contributions in the cyber realm."[1613] Thus the National Guard works closely with the combatant commands, especially Cyber Command, to fight off cyber incidents. Lengyel went on to say "we practice our capabilities routinely at all levels."[1614] That could include in the fight against the Islamic State, per comments on the 262nd Squadron by Defense Secretary Ashton Carter that "units like this can also participate in offensive cyber operations...to secure the prompt defeat of ISIL."[1615] Carter says use of the National Guard "brings in the high-tech sector in a very direct way to the mission of protecting the country." The Pentagon is building new facilities while the Guard launches 13 new cyber units across the country to have a total of 30 by 2019.[1616] However as the National Guard accelerates the fielding of cyber forces it faces a backlog in training which includes basic skills and certifications.[1617]

U.S. Department of Defense Manual 8570.01 provides guidance for the certification of all military and civilian personnel conducting information assurance functions.[1618] The

---

[1613] Jim Greenhill, "National Guard uniquely positioned to contribute in cyber realm," U.S. Air Force News, October 19, 2016: 15.

[1614] Ibid, 17.

[1615] Andrea Shalal, "U.S. National Guard may join cyber offense against Islamic State: Carter," *Reuters*, March 6, 2016.

[1616] Patrick Howell O'Neil, "Pentagon requests $12 million for new National Guard cyberwar facilities in Maryland," *The Daily Dot*, March 26, 2016.

[1617] Scott Maucione, "As cyber units expand, National Guard has training backlog," *Federal News Radio*, March 15, 2016.

[1618] U.S. Department of Defense, "Information Assurance Workforce Improvement Program," DoD 8570.01-M, Change 4, November 10, 2015.

certification program establishes a baseline understanding of principles and practices for each position, specialty and skill level. Approved baseline certifications and providers are published on the DISA Information Assurance Support Environment website.[1619] For example a common baseline certification is "Comp TIA Security+" for Information Assurance Technician Level I which is obtained by an examination.[1620] More advanced certifications include Global Information Assurance Certification Security Essentials, Intrusion Analyst and Enterprise Defender.[1621] One certification for specialist that appears more applicable for outside the network is Certified Ethical Hacker offered by the EC-Council. A Certified Ethical Hacker is "a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s)."[1622] Courses for the range of certifications are available from a number of training providers, but the lead vendor is SANS whose website links their courses to the certifications.[1623] Of note a new two day course offered by SANS is entitled "Active Defense, Offensive Countermeasures and Cyber Deception" which includes tools "to annoy attackers, determine who is attacking you, and finally, attack the

---

[1619] Information Assurance Support Environment, "DoD Approved 8570 Baseline Certifications," Defense Information Systems Agency Information Assurance Support Environment Website, Accessed on October 23, 2016: http://iase.disa.mil/iawip/Pages/iabaseline.aspx

[1620] CompTIA Security, "CompTIA Security+ Certification," Exam Code SYO-401: Accessed on October 23, 2016: https://certification.comptia.org/certifications/security

[1621] Global Information Assurance Certification, "GIAC Security Essentials," Certifications: Accessed on October 23, 2016: http://www.giac.org/certification/security-essentials-gsec

[1622] EC-Council, "Master the Core Technologies of Ethical Hacking," Programs, Accessed on October 23, 2016: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

[1623] SANS, "Information Security Training Courses," Courses, Accessed on October 23, 2016: https://www.sans.org/course attackers."[1624] Since contractors supporting information assurance functions also have to comply with the certification requirements, private sector personnel could also possess necessary skills for tailored disruption.

Defense Innovation Unit Experimental (DIUx). In May 2015 the Pentagon set up a new office in Silicon Valley to harness the creativity of the West Coast technology community.[1625] The Engineer and Navy SEAL that initially manned the Defense Innovation Unit Experimental or DIUx for short were picked for their tech sector experience and entrepreneurial mindsets. Their goal was to search out commercial dual-use technologies, to include in cyber.[1626] Less than a year later the U.S. Defense Secretary overhauled the leadership, structure, reporting and resources of the office. It had suffered from an overly broad purpose and unrealistic demands.[1627] DIUx 2.0 was launched by the Secretary with new processing power in funds and a new operating system of partner style leadership.[1628] A third feature was the creation of offices in other innovation hubs, starting with Boston and Austin.[1629] The result of the reboot was award of a total of $36 million in contracts for 12 projects via an acquisition technique named Commercial Solutions Opening. The largest of the awards for $12.7 went to Tanium to build a cyber

---

[1624] SANS, "Active Defense, Offensive Countermeasures and Cyber Deception (Two-day Version)," Course, Accessed on October 23, 2016: https://www.sans.org/course/active-defense-offensive-countermeasures-and-cyber-deception-two-day-version

[1625] Patrick Tucker, "Pentagon Sets Up a Silicon Valley Outpost," *Defense One*, April 23, 2015.

[1626] Marcus Weisgerber, "Pentagon Sends an Engineer and a Navy SEAL to Woo Silicon Valley," *Defense One*, August 5, 2015.

[1627] Ben FitzGerald and Loren DeJonge Schulman, "The DIUx is Dead, Long Live the DIUx," *Defense One*, May 12, 2016.

[1628] U.S. Department of Defense, "Secretary of Defense Speech, Remarks Announcing DIUx 2.0," As Delivered by Secretary of Defense Ash Carter, Mountain View, California, May 11, 2016: http://www.defense.gov/News/Speeches/Speech-View/Article/757539/remarks-announcing-diux-20

[1629] Billy Mitchell, "DIUx expands to Austin, Texas," *FedScoop*, September 14, 2016.

situational awareness platform to monitor millions of DoD computer endpoints in real-time,[1630] in effect enabling timely detection that could lead to rapid response to harm.

Then Defense Secretary Carter highlighted in his remarks announcing DIUx 2.0 that "another way we're investing in innovation is through people," by providing "on-ramps and off-ramps for technical talent to flow between DOD and the tech sector."[1631] An example of this ramp is the Defense Digital Service office that brings civilian techies into the Pentagon for a project or period of time to do something meaningful, including improving cybersecurity.[1632] One of the very first initiatives of the office in May 2016 was the "Hack the Pentagon" program, the first federal "bug bounty."[1633] Hackers were given legal consent to perform specific techniques against Defense Department websites and received financial awards for submitting vulnerability reports. HackerOne, a Silicon Valley firm that offers vulnerability disclosure as a service assisted in recruiting 1,410 participants that generated 1,189 vulnerability reports over three weeks.[1634] The program was so successful that a second round was contracted in October 2016 with HackerOne and also Synack, but this time for more sensitive systems. A former NSA employee said these ethical hackers will "look outside the box to come up with creative attacks in the same way an attacker would."[1635] A new Pentagon vulnerability disclosure policy will allow hackers to submit information with a high level of anonymity with no restrictions on

---

[1630] Jared Serbu, "DIU-X Touts $36 Million in Rapid Contracts, But Most Dollars Went to Established Firms," WFED AM Radio, Washington DC, October 17, 2016.

[1631] U.S. Department of Defense, "Secretary of Defense Speech, Remarks Announcing DIUx 2.0."

[1632] Sydney J. Freedberg Jr. "SecDef Carter Wants YOU for the Defense Digital Service," *Breaking Defense*, September 14, 2016.

[1633] Jim Garamone, "Defense Digital Service Chief Brings Private-Sector Expertise to Job," *DoD News*, June 10, 2016.

[1634] U.S. Department of Defense, "Hack the Pentagon," Fact Sheet, June 17, 2016.

[1635] Jared Serbu, "Pentagon launches next round of 'bug bounties,' including cyber tests of sensitive systems," WFED AM Radio, Washington DC, October 24, 2016.

citizenship.[1636] The obtainment of this type of skilled talent through private sector arrangements proves that building capacity for external disruption is feasible and legitimate.

Policies and Priorities

Tony Scott, U.S. Federal Chief Information Officer candidly stated in late 2015 "as cyber threats become increasingly sophisticated and persistent, so must our actions to tackle them."[1637] His remarks heralded the release of the Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Government. The Plan's second objective is the most pertinent to the strategy of active cyber defense, namely: "Timely Detection of and Rapid Response to cyber incidents."[1638] Accordingly CSIP directs a series of actions to "improve capabilities for identifying and detecting vulnerabilities and threats, enhance protections of assets and information, and further develop robust response and recovery capabilities to ensure readiness and resilience when incidents inevitably occur."[1639] Specific improvements for objective two include examine private sector technologies for behavioral-based analytics, implement automated indicator sharing, and create incident response best practices to ensure appropriate mitigation in a timely manner. Consistent with these broad themes, a national strategy agenda to implement the strategy of active cyber defense based on the pillars of resilience and disruption can be based on the following policy recommendations and priority suggestions.

[1636] Zachary Fryer-Biggs, "Pentagon rolls out new policy, rewards for hackers," *Jane's Defence Weekly*, 30 November 2016: 11.

[1637] Greg Otto, "White House cyber plan sets tough deadlines," *FedScoop*, October 30, 2015.

[1638] Shaun Donovan and Tony Scott, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government, Office of Management and Budget, October 30, 2015: 2.

[1639] Ibid, 5.

Internal Systemic Resilience

Policy: Encourage the adoption of integrated and automated capabilities, informed by cyber threat intelligence, that can detect, verify and remediate malicious activity in cyber-relevant time.

Priorities:

1. Design common open standards for active cyber defense inside the network that are applicable across the government as well as for critical infrastructure.
    a. Promulgate a reference architecture that centers on the automation and integration of services and mechanisms to reduce response time from months to milliseconds.
    b. Adopt, adapt, or develop common communications mediums, standard interfaces, and standard message sets to enable security tool interoperability.
    c. Demonstrate the art-of-the-possible to defenders and influence the marketplace of cyber security solutions including endpoint detection and response.

2. Create incentives to adopt common open standards for active cyber defense that can enable responsive and resilient critical infrastructure to manage the risk of cyber attack.
    a. Provide relief from regulatory requirements, certifications for government usage, or preferences for government contracts or grants.
    b. Reduce cyber insurance premiums based on positive security posture assessments of capabilities that prevent financial or data loss, service interruption, legal action, system or reputation damage.
    c. Offset world-wide shortage of cybersecurity professionals with automated intrusion responses as the number of devices, systems and networks grow at an exponential rate.[1640]

[1640] Peter Fanosh and Thomas Longstaff, "Narrowing Cyber Workforce Gaps with Intrusion Detection and Response Automation," *Crosstalk*, March/April 2016: 4-9.

3. Develop and implement a capability and process to commence real time, automated sharing of cyber threat indicators and defensive measures between private and public entities.

   a. Grant legal protections in the form of antitrust exemptions and liability immunity to private entities that send the government indicators or measures.
   b. Create a voluntary system that will encourage private and public entities to share indicators or measures while protecting classified information, intelligence sources and methods, and privacy and civil liberties.
   c. Issue guidelines for the receipt, processing, and dissemination by the government of indicators and measures submitted through real-time and non-automated means, to include guidelines concerning privacy and civil liberties.
   d. Leverage proven specifications and mechanisms for machine-to-machine transmission of indicators and measures between private and public entities.

<u>Tailored Disruption Capacities</u>

Policy: Allow either state agencies or licensed private companies, whichever is best positioned to respond to breaches, to deploy their comparative advantage in securing victim networks.

Priorities:

1. Create a legal framework that accommodates the use of disruptive countermeasures outside the network by properly authorized entities under certain conditions.

   a. Recognize authorized circumstances for the State to employ countermeasures that are acceptable under international law, primarily for an injured state, in a plea of necessity, or in respond to a lack of due diligence.
   b. Codify if a law enforcement or intelligence agency could deputize private firms to act under their authority in pursuing attackers under current provisions (such as 1030(f) in the CFAA in the United States) in limited circumstances and whether those provisions provide immunity for the firm:

i. If not, determine if a lack of explicit self-defense provisions in domestic law does not preclude the application of common law defense of property by licensed private companies.
ii. Or at a minimum, add a qualified active defense right to domestic law that provides licensed private companies with immunity from liability for third-party harm if caused during state authorized responses.

2. Create habitual relations with cyber security industry firms and personnel to employ cutting edge technologies in detection, verification, and remediation of malicious cyber behavior.
   a. Establish government outreach programs to find, adopt, and harness commercial dual-use high tech solutions that enable responses in cyber relevant time.
   b. Employ commercial and public skill sets in crowd sourced solutions to security challenges beyond the scope and capability of government agencies such as in bug bounty programs.
   c. Engage leading cyber security vendors in the investigation of high profile breaches to leverage and position their talent in the cyber kill chain of the most sophisticated actors.

3. Identify thresholds and circumstances for either state government or licensed private companies acting under their authority to respond outside the network to a cyber attack.[1641]
   a. Determine if the establishment of clear "red lines" for cyber attacks that warrant a response is necessary or if best left undefined to allow for some level of strategic ambiguity for political decisions.[1642]
   b. Delineate what thresholds warrant a military response, such as in defense of the nation and its interests against "attacks of significant consequence" defined in the

[1641] Paul Rosenzweig, et al. "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense," *The Heritage Foundation*, May 5, 2017: 1-11.
[1642] Mark Pomerleau, "Cyber red lines: ambiguous by necessity?" *C4ISRNET*, September 8, 2016.

United States as loss of life, significant property damage, serious adverse foreign policy consequences, or serious economic impact.[1643]

c. Determine if responses to cyber attacks that below the threshold of "significant consequences" are more suited for other agencies or licensed private companies as the military is "not involved in the majority of major cyber incidents that occur."[1644]

The above policy recommendations and priority suggestions are by no means exhaustive but offer a start point for action plans. Another source to ponder is the Active Cyber Defense Task Force Project Report released in October 2016 that specifies an explicit set of relevant actions for government agencies and private sector companies to facilitate the implementation of their proposed framework for active defense.[1645] Pertinent to consideration of any actions are remarks made by the Deputy Commander, U.S. Cyber Command Lieutenant General James McLaughlin, regarding their success will be dependent on the ability to acquire "the latest, best offensive and defensive tools available" combined with the "quality" and "proficiency" of people to use them.[1646] A national strategy agenda for active cyber defense based on the two pillars of resilience and disruption will bring in the best people and capabilities to achieve deterrence within the cyber arena.

1643 U.S. Department of Defense, "The DoD Cyber Strategy," April 2015: 4-5.

1644 Mark Pomerleau, "CYBERCOM not involved in most incidents," *C4ISRNET*, September 21, 2016.

1645 Center for Cyber & Homeland Security, "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," Project Report, The George Washington University, October 2016: 31-33.

1646 Aaron Boyd, "Cyber teams' first live campaign: fighting ISIS," *C4ISRNET*, September 21, 2016.

BIBLIOGRAPHY

I. Unpublished Sources

Ars Technica

Business Wire

BuzzFeed

Crosstalk

Dark Reading

Digital Dao

Federal News Radio

Global Knowledge

Information Age

Inside Cybersecurity

IRC Radio

ISACA Now

Krebs on Security

Live Events

Malware Statistics

MITRE Corporation

Morningstar

Motherboard

National Defense

Net Politics

Network World

Nextgov

NPR

Politico

Press TV

PR News Wire

Security Studies
Seculert
Softpedia
Voice of America
WhatIs
Wired
Zdnet

II. Government Official Publications – By Country

Australia. Australian Government. *Australia's Cyber Security Strategy*, 2016.

Czech Republic. National Security Authority. *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020*, 2015.

Estonia. Ministry of Economic Affairs and Communication. *Cyber Security Strategy 2014-2017*, 2014.

European Commission. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7 February 2013

Georgia. The Government of Georgia. *Cyber Security Strategy of Georgia 2012-2015*, 2012.

Italy. Presidency of the Council of Ministers. *National Strategic Framework for Cyberspace Security*, December 2013.

Japan. The Government of Japan. *Cybersecurity Strategy*, Provisional Translation, Cabinet Decision, September 4, 2015.

North Atlantic Treaty Organization. "The North Atlantic Treaty," April 4, 1949.

————— . *Assured Access to the Global Commons*. Norfolk, VA: Allied Command Transformation April 2011.

————— . "Wales Summit Declaration." Wales: North Atlantic Council, September 2014.

The Netherlands. Minister of Defense. *The Defense Cyber Strategy*, June 2012.

United Kingdom. HM Government. *National Cyber Security Strategy 2016-2021*, 2016.

————— . Ministry of Defence. "The Comprehensive Approach." Joint Discussion Note 4/05. Joint Doctrine and Concepts Centre, 2006.

————— . Ministry of Defence “Future Operating Environment 2035,” First Edition, Joint Doctrine and Concepts Centre, December 2015.

United Nations. “Charter of the United Nations,” October 24, 1945.

————— . “Responsibility of States for Internationally Wrongful Acts,” General Assembly Resolution 56/83, December 12, 2001.

————— “Creation of a global culture of cybersecurity and taking stock of national efforts to protect information infrastructures,” General Assembly Resolution 64/211, December 21, 2009.

————— . “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” A/68/98. 24 June 2013.

—————. “International code of conduct for information security,” Document 69/723, January 13, 2015.

————— . “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,” A/70/174, 22 July 2015.

United States. Executive Office of the President. *The Comprehensive National Cybersecurity Initiative*. Washington, DC: The White House, March 5, 2010.

————— . Executive Office of the President. *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communication Infrastructure*. Washington, DC: The White House, May 2009.

————— . Executive Office of the President. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: The White House, May 2011.

————— . Executive Office of the President. *Executive Order -- Improving Critical Infrastructure Cybersecurity.* Washington, DC: The White House, February 12, 2013.

————— . Executive Office of the President. *National Security Strategy*. Washington, DC: The White House, February 2015.

————— . Executive Office of the President. *Presidential Policy Directive – on Critical Infrastructure Protection.* PPD-63.Washington, DC: The White House, February 12, 2016.

———. Executive Office of the President. *Presidential Policy Directive – United States Cyber Incident Coordination.* PPD-41.Washington, DC: The White House, July 26, 2016.

———. Department of Defense. *Joint Terminology for Cyberspace Operations*. Washington, DC: Office of the Vice Chairman, Joint Chiefs of Staff, November 2010.

———. Department of Defense. *Joint Operations*. Joint Publication 3-0. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, August 11, 2011.

———. Department of Defense. *Joint Operation Planning.* Joint Publication 5-0. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, August 11, 2011.

———. Department of Defense. *Countering Air and Missile Threats*. Joint Publication 3-1. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, March 23, 2012.

———. Department of Defense. *Cyberspace Operations*. Joint Publication 3-12 (R). Washington, DC: Office of the Chairman, Joint Chiefs of Staff, February 5, 2013.

———. Department of Defense. *The National Military Strategy*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, June 2015.

———. Department of Defense. *DOD Dictionary of Military and Associated Terms.* Washington, DC: Office of the Chairman, Joint Chiefs of Staff, October 15, 2016.

———. Department of Defense. *Law of War Manual*. Washington, DC: Office of General Counsel, June 2015 (Updated December 2016).

———. Department of Defense. *Strategy for Operating in Cyberspace*. Washington, DC: Office of the Secretary of Defense, July 2011.

———. Department of Defense. *Cyberspace Policy Report*. Washington, DC: Office of the Secretary of Defense, November 2011.

———. Department of Defense. *Quadrennial Defense Review Report*. Washington, DC: Office of the Secretary of Defense, May 2014.

———. Department of Defense. *Military and Security Developments Involving the People's Republic of China*. Washington, DC: Office of the Secretary of Defense, April 2015.

———. Department of Defense. *The DoD Cyber Strategy*. Washington, DC: Office of the Secretary of Defense, April 2015.

———. Department of Defense. *Unity of Effort Framework Solution Guide.* Suffolk, Virginia: Joint Staff J-7, August 2014.

———— . Department of Homeland Security. *National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security, 2013.

———— . Strategic Command, *Deterrence Operations Joint Operating Concept*, Version 2.0, Washington, DC: December 2006.

———— . National Institute of Standards and Technology, *Managing Information Security Risk*, NIST Special Publication 800-39, March 2011.

———— . National Institute of Standards and Technology, *Glossary of Key Information Security Terms*, NISTIR 7298 Revision 2, May 2013.

———— . National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4, April 2013.

———— . National Institute of Standards and Technology, *Guide to Cyber Threat Information Sharing*, NIST Special Publication 800-150, October 2016.

———— . National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014.

III. Cyber Industry Publications

Akamai, "Cloud Security Solutions," White Paper, 2015.

———— . "Kona Site Defender," Product Brief, 2015.

Armor. "Threat Intelligence," ebook, 2016.

Carbon Black. "Disrupting the Threat: Identify, Respond, Contain & Recover in Seconds," White Paper, 2014.

———— . "Breach Detection: What you need to know," eBook, 2016.

CrowdStrike. "Global Threat Intel Report," 2015.

———— . "Indicators of Attack versus Indicators of Compromise," White Paper, 2015.

CyberEdge Group. "2015 Cyberthreat Defense Report: North America & Europe," March, 2015.

———— . "2016 Cyberthreat Defense Report," 2016.

Cyveillance. "Intelligence for Security," January 2015.

Dell Secure Works. "Inside a Targeted Point-of-Sale Data Breach," January 2014.

———. “Eliminating the Blind Spot: Rapidly detect and respond to the advanced and evasive threat,” White Paper, 2015.

———. “Underground Hacker Markets,” Annual Report, April 2016.

FireEye. “APT28: A Window into Russia’s Cyber Espionage Operations,” Special Report, 2014.

———. “Cybersecurity’s Maginot Line: A Real World Assessment of the Defense-in-Depth Model,” 2014.

———. “FireEye Threat Intelligence: Get the Intelligence and Context You Need to Help Identify, Block and Respond to Advanced Attacks,” Data Sheet, 2016

Fortinet, “Threat Landscape Report,” October 2016.

Hexis Cyber Solutions. “How to Automate Cyber Threat Removal,” A HawkEye G Technical White Paper, Release 3.1, October 2015.

———. “Active Cyber Defense: Integrated, Automated, Effective,” December 11, 2015.

Hewlett Packard Security Research. “Syrian Electronic Army,” Briefing Episode 3, April 2013.

———. “Islamic Republic of Iran,” Briefing Episode 11, February 2014.

———. “Profiling an enigma: The mystery of North Korea’s cyber threat landscape.” Briefing Episode 16, August 2014.

Hewlett Packard Enterprise. “Companies Cautiously Optimistic About Cybersecurity,” In-depth Analysis, January 2016.

IBM Corporation, “Combat the latest security attacks with global threat intelligence,” 2016.

Imperva. “An Anatomy of a SQL Injection Attack,” Hacker Intelligence Summary Report, Monthly Trend Report #4, September 2011.

———. “The Anatomy of an Anonymous Attack,” Hacker Intelligence Summary Report, 2012.

———. “DDoS Threat Landscape Report 2015-2016,” August 2016.

Intel Corporation. “The Cybersecurity Framework in Action: An Intel Use Case,” 2015.

Kaspersky Global Research and Analysis Team. “The NetTraveler (aka Travnet),” 2013.

———. “Future Risks: Be Prepared,” Special Report, 2014.

———. “The Dangers of Phishing: Help Employees Avoid the Lure of Cybercrime,” 2015.

LightCyber. “Closing the Breach Detection Gap,” Data Sheet, 2015.

———. “The New Defense against Targeted Attacks,” White Paper, March 2015.

————— . “Magna Detection Technology,” White Paper, November 2015.

Looking Glass. “Addressing the Cyber Kill Chain.” Research Note, 2016.

Lumension. “Redefining Defense-in-Depth,” White Paper, March 2014.

Mandiant. “APT1: Exposing One of China’s Cyber Espionage Units,” February 27, 2013.

————— . “M Trends 2015: A View from the Front Lines,” Threat Report, 2015.

————— . “M Trends 2016: Special Report,” February 2016.

McAfee. “Net Losses: Estimating the Global Cost of Cybercrime,” June 2014.

Neustar. “DDoS Attacks & Protection Report,” Annual Report, April 2016.

Noveta. “Operation Blockbuster: Unraveling the Long Threat of the Sony Attack,” February 2016.

Palo Alto Networks, “Breaking the Cyber Attack Lifecycle,” March 2015.

Ponemon Institute, “The SQL Injection Threat Study,” April 2014.

————— . “2014 Global Report on the Cost of Cyber Crime,” October 2014.

————— . “2016 State of Endpoint Report,” April 2016.

Securosis. “Defending Against Denial of Service Attacks,” October 2012.

————— . “Defending Against Application Denial of Service Attacks,” December 2013.

Solutionary. “Global Threat Intelligence Report,” NTT Group 2016.

Sophos. “Next-Generation Endpoint Protection Explained,” White Paper, April 2016.

SurfWatch Labs. “Dark Web Situational Awareness Report,” 2015.

Symantec Corporation. “Internet Security Threat Report,” Volume 19, April 2014.

————— . Dragonfly: Cyberespionage Attacks Against Energy Suppliers,” July 7, 2014.

Threat Connect, “A Financial Giant’s Threat Intel Success Story,” Case Study, August 2016.

Tripwire, “Layered Security: Protecting Your Data in Today’s Threat Landscape,” 2014.

————— . “Conquer the Top 20 Critical Security Controls,” 2104.

————— . “Solutions for Endpoint Detection and Response,” Solution Brief, 2015.

Verizon. “2016 Data Breach Investigations Report,” May 2016.

Websense Security Labs. “The Seven Stages of Advanced Threats,” 2013.

————— .“Point-of-Sale Malware and the Seven Stages Attack Model,” 2014.

————— .“2015 Threat Report,” 2015.

IV. Newspapers and Internet-based sources

ABC News

Agence France-Presse

Associated Press

Baltimore Sun

BBC News

Bloomberg News

Breaking Defense

CNBC News

CNN Politics

Christian Science Monitor

Computer

Computer Weekly

Computing

Computing News

C4ISR & Networks

Daily Herald

Defense Daily

Defense One

Defense News

Federal Times

Fedscoop

Forbes

Fox News

Government Computer News

Information Security Magazine

Information Week

International Herald Tribune

Janes's Defense Weekly

Network World

PC World

Reuters

RT News

SC Magazine

Spiegel Online

Tech Target

The Daily Beast

The Daily Dot

The Diplomat

The Economist

The Guardian

The Hill

The Irish Times

The Los Angeles Times

The National Interest

The New York Times

The Register

The Wall Street Journal

The Washington Post

USA Today

U.S. Naval Institute

US News and World Report

Washington Times

Yahoo News

V. Academic Literature

i. Books

Allison, Graham, and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis.* Second Edition, New York: Addison Wesley Longman, 1999.

Asada, Sadao. *From Mahan to Pearl Harbor: The Imperial Japanese Navy and the United States.* Annapolis, MD: Naval Institute Press, 2006.

Barros, J. *The Corfu Incident of 1923.* Princeton University Press, 1965.

Betz, David J., and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power.* Oxon: Routledge, 2011.

Blaire, Dennis C., et. al. "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," Project Report, The George Washington University, October 2016.

Brodie, Bernard. *The Absolute Weapon* (New York, 1946).

Cable, James. *Gunboat Diplomacy 1919-1991.* London: Palgrave Macmillan, 1994.

Coleman, Kevin G. *The Cyber Commander's eHandbook: The Strategies and Tactics of Digital Conflict*. McMurray, PA: Technolytics, 2013.

Chang, Amy. "Warring State: China's Cybersecurity Strategy." Center for a New American Security, December 2014.

Clausewitz, Carl von. *On War*, trans, Michael Howard and Peter Paret, Princeton University Press, 1976.

Clemente, Dave. "Cyber Security and Global Interdependence: What is Critical?" Chatham House, February 2013.

Demchak, Chris., et al. *Designing Resilience: Preparing for Extreme Events.* University of Pittsburgh, September 2010.

————— . *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*, University of Georgia Press, September 2011.

Flynn, Matthew J., *First Strike: Preemptive War in Modern History.* New York and Oxon: Routledge, 2008.

Freedman, Lawrence. *Deterrence.* Cambridge: Polity Press, 2004.

George, Alexander L. and William E. Simon. *The Limits of Coercive Diplomacy*. Boulder, CO: Westview, 1994.

Goldman, Emily O. *Power in Uncertain Times.* Stanford University Press, 2011.

Graham-Yooll, Andrew. *Imperial Skirmishes: War and Gunboat Diplomacy in Latin America.* Brooklyn, NY: Olive Branch Press, 2002.

Gray, Colin S., *The Implications of Preemptive and Preventive War Doctrines: A Reconsideration*, Carlisle, PA: Strategic Studies Institute: July 2007.

————— . *The Strategy Bridge: Theory for Practice,* Oxford University Press, 2010.

————— . *Perspectives on Strategy,* Oxford University Press, 2013.

Heuser, Beatrice. *The Evolution of Strategy: Thinking War from Antiquity to the Present.* Cambridge University Press, 2010.

Holland, John H. *Complexity: A Very Short Introduction.* Oxford University Press, 2014.

Ishizu, Tomoyuki and Raymond Callahan. "The Rising Sun Strikes: The Japanese Invasions," *The Pacific War.* Oxford: Osprey Publishing Ltd, 2010.

Kamman, W., *A Search for Stability.* University of Notre Dame Press, 1968.

Libicki, Martin C., *Cyberdeterrence and Cyberwar,* Santa Monica, California: RAND Corporation, 2009.

Luttwak, Edward N. *The Political Uses of Sea Power.* Baltimore and London, The John Hopkins University Press, 1974.

————— . *Strategy: The Logic of War and Peace.* Cambridge and London: The Belknap Press of Harvard University Press, 1987.

Morgan, Patrick M., *Deterrence: A Conceptual Analysis*. Beverly Hills, CA: Sage Publications, 1977.

————— . *Deterrence Now*, (Cambridge University Press, 2003).

————— . *International Security: Problems and Solutions*, (Washington, DC: CQ Press, 2006)

Owens, William A. et. al. *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington DC: The National Academies Press, 2009.

Record, Jeffrey. *Japan's Decision for War in 1941: Some Enduring Lessons*, Carlisle, PA: Strategic Studies Institute: February 2009.

Schelling, Thomas. *The Strategy of Conflict.* Cambridge: Harvard University Press, 1960.

———— . *Arms and Influence.* New Haven and London: Yale University Press, 1966.

Schmitt, Michael. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press, May 2013.

———— . *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press, April 2017.

Shulsky, Abram N. *Deterrence Theory and Chinese Behavior.* Santa Monica, CA: RAND Corporation, 2014.

Snyder, Glenn H. *Deterrence and Defense: Toward a Theory of National Security*. Princeton University Press: 1961.

Spector, Ronald H., *Eagle against the Sun: The American War with Japan.* New York: The Free Press, 1985.

———— . *At War, At Sea: Sailors and Naval Combat in the Twentieth Century.* New York: Viking Penguin Publishers, 2001.

Tikk, Eneken, et al. "International Cyber Incidents: Legal Considerations." Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2009.

ii. Articles in Journals and Edited Volumes

Aaronson, Michael et al. "NATO Countering the Hybrid Threat," *PRISM,* Vol. 2, No. 4, (September 2011), pp. 111-124.

Arimatsu, Louise. "A Treaty for Governing Cyber-Weapons," *Proceedings 4th International Conference on Cyber Conflict*, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2012, pp. 91-110.

Berkowitz, Marc J. "Shaping the Outer Space and Cyberspace Environments," Scott Jasper, Ed. *Conflict and Cooperation in the Global Commons.* Washington, DC: Georgetown University Press, 2012, pp. 190-213.

Bonner, E. Lincoln, III. "Cyber Power for 21st- Century Joint Warfare," *Joint Force Quarterly,* Number 74 (3rd Quarter 2014): pp. 102-109.

Brodie, Bernard. "Unlimited Weapons and Limited War," *The Reporter*, November 18, 1954: pp. 16-21, Assessed on May 29, 2017: http://www.unz.org/Pub/Reporter-1954nov18-00016.

Burr, William. “How to Fight a Nuclear War” *Foreign Policy* (September 14, 2012), Assessed on May 29, 2017: http://foreignpolicy.com/2012/09/14/how-to-fight-a-nuclear-war/.

Chilton, Kevin, and Greg Weaver, “Waging Deterrence in the Twenty-First Century,” *Strategic Studies Quarterly*, Vol. 3, Issue 1, (Spring 2009): pp. 31-42.

Demchak, Chris.“Cybered Conflict, Cyber Power, and Security Resilience as Strategy,” *Cyberspace and National Security*, Washington DC: Georgetown University Press, 2012, pp. 121-136.

————— . “Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI),” Vol. 14, No. 3, *Journal of Comparative Policy Analysis: Research and Practice* (July 12, 2012): pp. 254-269.

————— . “Economic and Political Coercion and a Rising Cyber Westphalia,” *Peacetime Regime for State Activities in Cyberspace*, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2013: pp. 595-620.

————— . and Peter Dombrowski, “Cyber War, Cybered Conflict, and the Maritime Domain,” *Naval War College Review* (April 1, 2014): pp. 71-96.

Denning, Dorothy E. “Obstacles and Options for Cyber Arms Controls, Heinrich Boll Foundation Conference, Berlin, Germany, June 29-30, 2001.

————— . and Bradley J. Strawser. “Active Cyber Defense: Applying Air Defense to the Cyber Domain,” *Cyber Analogies.* Naval Postgraduate School, 2014: pp. 64-75.

————— . Dorothy E. Denning, “Rethinking the Cyber Domain and Deterrence,” *Joint Force Quarterly*. Number 77 (2nd Quarter 2015): pp. 8-12.

Dewar, Robert S., “The Triptych of Cyber Security: A Classification of Active Cyber Defense,” *Proceedings 6th International Conference on Cyber Conflict.* Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, June 2014, pp. 7-21.

Drezner, Daniel W. “The Hidden Hand of Economic Coercion,” *International Organization*, Cambridge University Press, vol. 57, Issue 03, 2003, pp. 643-659.

Farwell, James P., and Rafal Rohozinski, “The New Reality of Cyber War,” *Survival: Global Politics and Strategy*, Vol. 54, No. 4, August 1, 2012: pp.107-120.

Finnemore, Martha and Kathryn Sikkink. “International Norm Dynamics and Political Change,” *International Organization*, Vol. 52, Issue 4 (Autumn 1998): pp. 887-917.

Forester, Schuyler. “Strategies of Deterrence,” “Theoretical Foundations: Deterrence in the Nuclear Age.” *American Defense Policy.* Baltimore, MD: Johns Hopkins University Press, September 1990, pp. 42-51.

————— . “Strategies of Deterrence,” Scott Jasper, Ed. *Conflict and Cooperation in the Global Commons*, Washington, DC: Georgetown University Press, September 2012: pp. 55-67.

Freedman, Lawrence. “The First Two Generations of Nuclear Strategists.” *Makers of Modern Strategy.* Princeton University Press, 1986, pp.735-778.

————— . “Deterrence: A Reply,” *The Journal of Strategic Studies*, Vol. 28, No. 5, October 2005: pp. 789-801.

Goodman, Will. “Cyber Deterrence: Tougher in Theory than in Practice?” *Strategic Studies Quarterly,* Vol. 4, Issue 3 (Fall 2010): pp.102-135.

Gray, Colin S., “Strategy in the Nuclear Age: The United States, 1945-1991.” *The Making of Strategy*, Cambridge University Press, 1994, pp. 579-613.

————— . “The Whole House of Strategy.” *Joint Force Quarterly,* Issue 71 (4th Quarter, 2013): pp. 58-62.

Glenn, Russell W. “Thoughts on Hybrid Conflict,” *Small Wars Journal.* (March 2, 2009): pp.1-8.

Glosson, Anthony D. “Active Defense: An Overview of the Debate and a Way Forward,” *Mercatus Center* (August 2015): pp. 3-28.

Harrington, Sean L. “Cyber Security Active Defense: Playing with Fire or Sound Risk Management,” *Richmond Journal of Law & Technology*, Volume XX, Issue 4 (September 17, 2014): pp. 1-41.

Harrison, Roger, et al. “Space Deterrence: The Delicate Balance of Risk,” *Space and Defense,* Vol. 3, No.1 (Summer 2009): pp. 1-29.

Hart, B.H. Liddell. “The Theory of Strategy,” *Military Strategy: Theory and Application.* Carlisle Barracks: US Army War College, 1983: pp. 3-22/23.

Herring M.J. and K.D. Willett. “Active Cyber Defense: A Vision for Real-Time Cyber Defense,” *Journal of Information Warfare,* Vol.13, No.2, 2014: pp. 46-55.

Hinkle, Katharine C. “Countermeasures in the Cyber Context: One More Thing to Worry About,” *The Yale Journal of International Law Online*. Vol. 37, Fall 2011: pp. 11-21.

Hughes, Geraint. "Ukraine: Europe's New Proxy War?" *Fletcher Security Review,* Vol. I, Issue II (Spring 2014): pp. 106-118.

Hutchins, Eric M. et al. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, March 2011.

Iasiello, Emilio. "Hacking Back: Not the Right Solution," *Parameters*, Vol. 44, No. 3, (Autumn 2014): pp. 105-113.

Jackson, Stephen. "NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack," Center for Infrastructure Protection & Homeland Security, George Mason University, August 16, 2016.

Jasper, Scott. "Are US and Chinese Cyber Intrusions So Different?" *The Diplomat* (September 9, 2013)

————— . and Scott Moreland. "A Comprehensive Approach to Multidimensional Operations," *Journal of International Peacekeeping.* Vol. 19 (2015): pp. 191-210.

Jentleson, Bruce. "Coercive Diplomacy: Scope and Limits in the Contemporary World," Policy Analysis Brief, *The Stanley Foundation*, December 2006; pp. 1-12.

Jervis, Robert. "Deterrence Theory Revisited," *World Politics*, Vol. 31, No. 2, Princeton University Press, January 1979: pp. 289-324.

__________ . "Deterrence and Perception," *International Security*, Vol.7, No. 3, Winter 1982/1983: pp. 3-30.

Joubert, V. "Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?" *Research Paper,* No. 76, Rome: NATO Defense College, May 2012: pp. 1-8.

Jun, Jenny, et al. "What Do We Know About Past North Korean Cyber Attacks and Their Capabilities?" Center for Strategic & International Studies, Korea Chair Platform, December 12, 2014: pp 1-2.

Kesan, Jay P. and Ruperto Majuca, "Optimal Hackback," *Chicago-Kent Law Review*, Vol. 84, Issue 3, Article 10, (June 2009): pp. 831-838.

———— . and Carol M. Hayes. “Thinking Through Active Defense in Cyberspace,” *Proceedings of a Workshop on Deterring Cyberattacks*, Washington, DC: The National Academies Press, 2010: pp. 327-341.

Koval, Nikolay. “Revolution Hacking,” *Cyber War in Perspective: Russian aggression against Ukraine*, Tallinn, Estonia: Cooperative Cyber Defense Center of Excellence, 2015: pp 55-58.

Kramer, Franklin D., and Melanie J. Teplinsky. “Cybersecurity and Tailored Deterrence,” Atlantic Council, Issue Brief, December 2013: pp 1-10.

Lachow, Irving, et al. “Cyber War: Issues in Attack and Defense,” *Joint Force Quarterly*, Issue 61 (2nd Quarter 2011): pp. 18-23.

———— . “Active Cyber Defense: A Framework for Policy Makers,” Center for a New American Security, February 2013: pp. 1-10.

Laver, Harry S., “Preemption and the Evolution of America’s Strategic Defense,” *Parameters* Vol. 35 No. 2 (Summer 2005): pp.107-120.

Lebow, Richard Ned. “Deterrence: Then and Now,” *Journal of Strategic Studies*, Vol. 28, No. 5, October 2005: pp. 765-773.

Leed, Maren. “Offensive Cyber Capabilities at the Operational Level.” Center for Strategic & International Studies. September 2013: pp. 1-9.

Lewis, James. “Rethinking Cyber Security – A Comprehensive Approach.” Sasakawa Peace Foundation, Tokyo. September 12, 2011: pp. 1-7.

———— . “Private Retaliation in Cyberspace,” Commentary, Center for Strategic and International Studies, May 22, 2013.

———— . “Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage.” Center for Strategic and International Studies, March 13, 2014, pp 1-8.

———— . “Economic warfare and cyberspace.” *China’s cyberpower: International and domestic priorities.* Austrian Strategic Policy Institute, Special Report, November 2014, pp. 2-8.

———— . “The Role of Offensive Cyber Operations in NATO’s Collective Defense,” *Tallinn Paper.* No. 8 (2015): 1-12.

———— . "Advanced Experiences in Cybersecurity Policies and Practices," Discussion Paper No. IDB-DP-457, Inter-American Development Bank, July 2016.

Libicki, Martin C., "Pulling Punches in Cyberspace," *Proceedings of a Workshop on Deterring Cyberattacks.* Washington, DC: The National Academies Press, 2010, pp 123-147.

———— . "Why Cyber War Will Not and Should Not Have Its Grand Strategist," *Strategic Studies Quarterly*, Vol. 8, Issue 1 (Spring 2014): pp. 23-39.

Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly*, Vol. 6, Issue 3 (Fall 2012): pp. 46-70.

———— . with William A. Owens and Kenneth W. Dam. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington DC: National Academies Press, 2009.

Litwak, Robert and Meg King. "Arms Control in Cyberspace?" *Wilson Center*, October 2015: pp. 1-8.

Lotrionte, Catherine. "A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence," *Georgetown Journal of International Affairs,* Special Issue (December 23, 2013): pp. 71-84.

———— . "State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights," *Emory International Law Review*, Vol. 26 (May 28, 2013): pp. 825-919.

Lykke, Jr., Arthur F. "Toward an Understanding of Military Strategy," *Guide to Strategy*, Carlisle Barracks: US Army War College, February 2001: pp 179-186.

Lynn, William J., III. "Defending a New Domain." *Foreign Affairs.* Vol. 89, No. 5 (September/October 2010): 97-108.

Lowther, Adam. "The Evolution of Deterrence," *Thinking About Deterrence.* Maxwell Air Force Base, Alabama: Air University Press, 2014: pp. 3-16.

Maurer, Tim. "Cyber Proxies and the Crisis in Ukraine," *Cyber War in Perspective: Russian aggression against Ukraine.* Tallinn, Estonia: Cooperative Cyber Defense Center of Excellence, 2015: pp.79-85.

Maybaum, Markus. “Technical Methods, Techniques, Tools and Effects of Cyber Operations,” *Peacetime Regime for State Activities in Cyberspace.* Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2013, pp. 103-131.

Mazanec, Brian M. “Why International Order in Cyberspace Is Not Inevitable,” *Strategic Studies Quarterly,* Vol. 9, Issue 2 (Summer 2015): pp. 78-84.

McGee, Shane, et al. “Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense,” *Journal of Business & Technology Law.* Vol.8, Issue 1, Article 3 (2013): pp. 1-48.

Meyer, Paul. “Cyber-Security through Arms Control,” *RUSI Journal.* Vol. 156, No. 2 (April/May 2011): pp. 22-27.

Morgan, Patrick M., “Taking the Long View of Deterrence,” *The Journal of Strategic Studies*,” Vol. 28, No. 5, October 2005: pp. 751-763.

————— . “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” *Proceedings of a Workshop on Deterring Cyberattacks.* Washington, DC: The National Academies Press, 2010, pp. 55-76.

Nye, Joseph S., Jr. “Cyber Power,” Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010: pp 1-23.

————— . “Deterrence and Dissuasion in Cyberspace,” *International Security*, Vol.41, No. 3, Winter 2016/2017: pp. 44-71.

Osula, Anna-Maria and Henry Roigas. “International Norms Limiting State Activities in Cyberspace,” *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2016: pp.11-22.

Owens, William A. “The Once and Future Revolution in Military Affairs,” *Joint Force Quarterly* (Summer 2002): pp. 55-61.

Pawlak, Patryk. “Confidence Building Measures in Cyberspace: Current Debates and Trends,” *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2016: pp. 129-153.

Payne, Keith B. and C. Dale Walton. “Deterrence in the Post-Cold War World,” *Strategy in the Contemporary World.* Oxford University Press, 2002, pp. 161-182.

Pierker, Benedikt. “Territorial Sovereignty and Integrity and the Challenge of Cyberspace,” *Peacetime Regime for State Activities in Cyberspace*, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2013: pp 189-216.

Pihelgas, Mauno. “Back-Tracing and Anonymity in Cyberspace,” *Peacetime Regime for State Activities in Cyberspace.* Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2013: pp. 31-60.

Richardson, John. “Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield,” *Journal of Computer & Information Law.* Vol. 29, Issue 1 (Fall 2011): pp. 1–37.

Rid, Thomas and Peter McBurney. “Cyber-Weapons,” *RUSI Journal*, Vol. 157, No. 1 (February/March 2012): pp. 6-13.

Rintakoski, Kristina and Mikko Autti. *Trends, Challenges and Possibilities for Cooperation in Crisis Prevention and Management.* Helsinki, Finland: Crisis Management Initiative, June 17, 2008, pp. 1-34.

Roberts, Peter and Andrew Hardie. “The Validity of Deterrence in the Twenty-First Century,” Royal United Services Institute, Occasional Paper, August 2015, pp .1-36.

Rosenzweig, Paul. “International Law and Private Actor Active Cyber Defensive Measures,” *Stanford Journal of International Law,* Vol. 47, (May 27, 2013): pp. 1-13.

————— , et al. “Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense,” *The Heritage Foundation*, No. 3188, May 5, 2017: pp 1-11.

Rowe, Neil C., et al. “Challenges in Monitoring Cyberarms Compliance,” *International Journal of Cyber Warfare & Terrorism.* Vol 1. No. 1 (January-March 2011): pp. 1-14.

Schmitt, Michael. “Attack as a Term of Art in International Law: The Cyber Operations Context,” *Proceedings 4th International Conference on Cyber Conflict.* Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, June 2012, pp. 283-294.

————— . and Liis Vihul. “Proxy Wars in Cyberspace: The Evolving International Law of Attribution.” *Fletcher Security Review.* Vol I, Issue II (Spring 2014): pp. 57-67.

————— . ““Below the Threshold” Cyber Operations: The Countermeasures Response Option and International Law,” *Virginia Journal of International Law.* Vol. 54: No. 3 (August 2014): pp. 697-732.

———— . "International Law and Cyber Attacks: Sony v. North Korea," *Just Security.* (December 17, 2014): pp. 1-5.

———— . "The Law of Cyber Targeting," *Tallinn Paper.* No. 7 (2015): pp. 1-20.

———— . "In Defense of Due Diligence in Cyberspace," *Yale Law Journal Forum.* Vol. 125, No. 68, June 22, 2015, pp. 1-14.

———— . and Liis Vihul. "The Nature of International Law Cyber Norms," *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2016: pp. 23-47.

Sheldon, John B. "The Rise of Cyberpower," *Strategy in the Contemporary World.* John Baylis, James J. Wirtz, and Colin S. Gray, editors, 5th Ed. Oxford University Press, 2016, pp. 282-298.

Slocombe, Walter. "The Countervailing Strategy." *International Security*, Vol. 5, No. 4 (Spring 1981): pp. 18-27.

Smith, Bruce P. "Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help," *The Journal of Law, Economics & Policy*, Vol 1, Issue 1.2 (2005): pp. 177-178.

Stinissen, Jan. "A Legal Framework for Cyber Operations in Ukraine," *Cyber War in Perspective: Russian aggression against Ukraine.* Tallinn, Estonia, Cooperative Cyber Defense Center of Excellence, 2015, pp. 123-134.

Stytz, Martin R., and Sheila B. Banks, "Toward Attaining Cyber Dominance," *Strategic Studies Quarterly* Vol. 8, Issue 1 (Spring 2014): pp. 55-87.

Tertrais, Bruno. "Iran: An Experiment in Strategic Risk-Taking," *Survival: Global Politics and Strategy.* Vol. 57, Issue 5 (October-November 2015): pp. 67-73.

Walt, Stephan M., "Which Works Best: Force or Diplomacy?" *Foreign Policy*, (August 21, 2013), Assessed on May 28, 2017: http://foreignpolicy.com/2013/08/21/which-works-best-force-or-diplomacy/.

West, Zach. "Young Fella, If you're looking for Trouble I'll accommodate you: Deputizing Private Companies for the use of Hackback," *Syracuse Law Review*, Vol. 63, No. 119, (November 2012): pp. 119-146.

Whyte, Christopher. “On the Future of Order in Cyberspace,” *Strategic Studies Quarterly* Vol. 9, Issue 2 (Summer 2015): pp. 69-77.

Williams, Brett T., “Ten Propositions regarding Cyberspace Operations,” *Joint Force Quarterly*, Issue 61 (2nd Quarter 2011): pp.11-16.

————— . “The Joint Force Commander’s Guide to Cyberspace Operations,” *Joint Force Quarterly*, Number 73 (2nd Quarter 2014): pp. 12-19.

Ziolkowski, Katharina. “General Principles of International Law as Applicable in Cyberspace,” *Peacetime Regime for State Activities in Cyberspace*, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2013: pp. 135-188.

————— . “Confidence Building Measures for Cyberspace – Legal Implications,” Tallinn, Estonia, Cooperative Cyber Defense Center of Excellence, 2013: pp. 1-13.