International humanitarian law and the conduct of cyber hostilities: quo vadis

Article

Accepted Version

International Humanitarian Law and the Conduct of Cyber Hostilities: Quo Vadis?

Michael N. Schmitt*

I. Introduction

War and international humanitarian law (IHL) exist and evolve in a synergistic relationship. On the one hand, treaty and customary law norms can proactively shape warfare. Although rare, examples include the Blinding Laser Protocol to the Conventional Weapons Convention,[1] adopted before the weapons appeared on the battlefield, and the current campaign to ban autonomous weapons in advance of their full development and deployment.[2]

But on the other, changes in the nature of warfare often determine IHL's path forward, for if IHL is to remain effective, it must remain responsive to the context in which it is to be applied. The most visible way this occurs is through treaties that address developments on the battlefield. Thus, for example, the horrendous suffering of civilian populations during World War II motivated States to adopt the Fourth Geneva Convention,[3] while the risk to civilians posed by landmines led to the Conventional Weapons Convention's Protocol on Anti-Personnel Land Mines[4] and the Ottawa Convention.[5] The same dynamic can also occur through the crystallization of customary international law, as with the emergence of a customary rule of proportionality in response to incidental injury to civilians and collateral damage to civilian objects prior to the adoption of its treaty law counterpart in Additional Protocol I to the 1949 Geneva Conventions in 1977.[6]

Given the practical obstacles to negotiating multilateral treaties and the difficulties associated with identifying sufficient State practice and *opinio juris* to declare that a new customary norm has emerged,[7] IHL typically evolves through subtle shifts in the understanding of States and other key actors as to how extant norms should be interpreted and applied in the face of new developments in

---

* Professor of International Law, University of Reading G. Norman Lieber Distinguished Scholar, U.S. Military Academy at West Point; Charles Stockton Distinguished Scholar-in-Residence, U.S. Naval War College; Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence.

1 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Protocol on Blinding Laser Weapons, Oct. 13, 1995, 1380 U.N.T.S. 370.

2 *Stop Killer Robots*, https://www.stopkillerrobots.org.

3 Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 75 U.N.T.S. 287

4 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as Amended on 3 May 1996, May 3, 1996, 2048 U.N.T.S. 93.

5 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction, Sept. 17, 1997, 2056 U.N.T.S. 211

6 I CUSTOMARY INTERNATIONAL HUMANITARIAN LAW rule 14 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005). Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts arts. 51(5)(b), 57(a)(iii), 57(b), June 8, 1977, 1125 U.N.T.S. 3. This article will use the term "collateral damage" to refer to both incidental injury to civilians and collateral damage to civilian objects.

7 Rome Statute of the International Criminal Court art. 38(1)(c), July 17, 1998, 2187 U.N.T.S. 90. On the emergence of a customary norms, see International Law Commission, *Draft Conclusions on Identification of Customary International Law, with Commentaries* (2018), https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf.

warfare. An example is the notion of direct participation by civilians in hostilities, the topic of a five-year ICRC expert-driven project launched in response to the growing involvement of civilians in military operations.[8] All participants agreed that articulation of the notion in the 1977 Additional Protocols I and II reflected customary international law, such that civilians who directly participate in hostilities lose their protection from attack "for such time" as they so participate. However, the experts came to very different conclusions over, for instance, the treatment of members of organized armed groups and the precise parameters of the phrase "for such time." The resulting ICRC *Interpretive Guidance on the Notion of Direct Participation*,[9] as well as the criticism of various aspects thereof,[10] appreciably influenced legal guidance to armed forces.[11] A transformed battlefield had motivated a shift in the understanding of "direct participation," even if that understanding differed among States and other key IHL actors.

The same dynamic is apparent in the cyber context. New treaty or customary law to govern cyber operations during armed conflict is unlikely to appear in the foreseeable future. Therefore, current and future cyber capabilities and vulnerabilities are driving the positions States and the wider international community take during discussions regarding the interpretation and adequacy of IHL. Military manuals, rules of engagement, and State positions on international law in fora such as the United Nations Group of Governmental Experts and Open-Ended Working Group[12] are undergoing interpretive adjustment in response to the prospect of cyber and cyber-enabled military operations. War is shaping the law.

This article offers tentative reflections on how future conflict may affect the evolution of IHL's conduct of hostilities rules with respect to information and communications technology (ICT), commonly referred to as "cyber capabilities." I shall use the latter term, as it is part of the IHL community's *patois*, but I intend it to refer to ICT capabilities and vulnerabilities more broadly. The reflections are tentative because history has demonstrated that the nature of future wars is seldom reliably predictable. Nevertheless, the difficulty of rendering accurate projections of the future battlespace and its normative impact does not relieve the IHL community of the responsibility for considering how this body of law can operate most effectively in it. It is, after all, better to be poorly prepared for the unexpected than unprepared altogether.

II. Cyber Warfare

The issue is ripe for examination. Today, States field impressive cyber units with missions extending into armed conflict. Prominent ones include Cyber Command (United States), Government Communications Headquarters - GCHQ (United Kingdom), C4i and Cyber Defense Directorate (Israel), Defence Cyber Command (the Netherlands), Main Directorate of the General Staff – GRU

[8] *See* Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARVARD NATIONAL SECURITY JOURNAL 5 (2010). The author was a participant.

[9] INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW (2009)

[10] See the symposium in volume 42 of the *New York Journal of International Law and Policy* (2010).

[11] *See, e.g.,* OFFICE OF THE GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL § 5.8 (rev. ed. Dec. 2016); DANISH MINISTRY OF DEFENCE, MILITARY MANUAL ON THE INTERNATIONAL LAW RELEVANT TO DANISH ARMED FORCES IN INTERNATIONAL OPERATIONS § 2.2 (updated 2020).

[12] *See* United Nations, Office for Disarmament Affairs, *Developments in the Field of Information and Telecommunications in the Context of International Security*, https://www.un.org/disarmament/ict-security/.

(Russia), and the People's Liberation Army Strategic Support Force (China). The number, size, and capabilities of such units are growing globally. Even NATO has promulgated cyber operations doctrine.[13]

And cyber operations have become an integral part of kinetic warfare. Russia has employed its cyber power repeatedly, notably against Georgia in 2008[14] and throughout its ongoing international armed conflict with Ukraine.[15] Australia, the United Kingdom, and the United States have used cyber capabilities during counter-ISIS operations.[16] Israel and Hamas have exchanged cyber blows, sometimes using kinetic means to target cyber capabilities.[17] In modern warfare, cyber influences almost every fight.

Cyber capabilities and reliance are sure to be omnipresent in future battlespaces. For example, communications will be highly cyber-reliant and cyber-vulnerable. For instance, the prospect of swarming drones in future wars depends on their ability to communicate with each other. And today, modern armed forces rely upon chat rooms for fielded units, as was the case of U.S. forces in the remote mountains of Afghanistan.[18]

Numerous factors explain the allure of cyber capabilities. First, they enable means and methods of warfare that would otherwise not be possible. Consider a drone operation launched from an airfield in an area of operations that loiters for many hours over potential targets while transmitting imagery to a distant command center a continent away that then approves the execution of a drone strike by an "aircrew" based in yet another location. The operation is only possible because of the cyber connectivity and computing capability of the various entities involved. Weapons and weapon systems that do not directly or indirectly depend on cyber systems to identify targets, guide weapons, or assess the results of an attack will be increasingly rare, primarily limited to small arms and other personal weaponry.

Similarly, cyber enhances a force's ability to maneuver. Thus, whether a foot patrol using hand-held GPS, aircraft relying on airborne and ground navigational systems, or automated robots transporting equipment and supplies, the movement of personnel and equipment in and around the battlespace will depend on cyber systems. So will intelligence gathering, analysis, and dissemination; command and control; and logistics activities. And many such activities will rely on space-based assets, which are particularly reliant upon, and vulnerable to, cyber activities. The last point is critical. Every cyber or cyber-enabled capability is a vulnerability that is potentially exploitable by the enemy. Such

---

[13] NATO, ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS (AJP 3.20) (January 2020).
[14] ENEKEN TIKK, KADRI KASKA, AND LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 66-90 (2010).
[15] *See, e.g.*, Tom Burt, *Disrupting Cyberattacks Targeting Ukraine*, Microsoft (April 7, 2022), https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/.
[16] *See, e.g.*, Mike Burgess, Director-General, Australian Signals Directorate at Lowry Institute (March 27, 2018), https://www.asd.gov.au/publications/director-general-asd-speech-lowy-institute; Danny Palmer, *British Spies Waged Cyber Campaign Against ISIS, Says GCHQ chief*, ZDNET (Apr. 12, 2018), https://www.zdnet.com/article/british-spies-waged-cyber-campaign-against-isis-says-gchq-chief/; Dina Temple-Raston, *How the U.S. Hacked ISIS*, NPR (Sept. 26, 2019), https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.
[17] NATO Cooperative Cyber Defence Centre of Excellence, *Israeli Attack Against Hamas Cyber Headquarters in Gaza*, https://cyberlaw.ccdcoe.org/wiki/Israeli_attack_against_Hamas_cyber_headquarters_in_Gaza_(2019).
[18] Drew, Christopher, *Military Taps Social Networking Skills,* NEW YORK TIMES (June 7, 2010), https://www.nytimes.com/2010/06/08/technology/08homefront.html.

vulnerabilities will only increase as autonomous and machine learning systems grow in prominence in future warfare.

To better understand the impact of cyber on warfare, and cyber-enabled warfare on IHL, it is helpful to tease loose the key characteristics of cyber capabilities and activities. These characteristics not only affect how war will be fought in the future but also influence IHL's interpretation and application. Among the determinative characteristics are the following.

Speed: The speed of warfare will increase dramatically as armed forces exploit cyber capabilities to operate inside their enemy's observe, orient, decide, act (OODA) loop[19] in an effort to control the vector and flow of hostilities and force the enemy into reactive stances. In particular, attacks will be mounted using cyber assets that instantly generate effects. The speed involved will render some defensive measures that rely upon human input ineffective, for advances in cyber capabilities will enable offensive operations that will exceed the human capacity to respond in a timely fashion. This reality will compel armed forces to embrace cyber-enabled automated and autonomous defensive and counter-attack systems to keep pace with their opponent's operations; such systems inevitably will rely on artificial intelligence. In cyberspace, then, the fastest gun may win.

This will challenge current perceptions of the role of humans in implementing IHL in combat, especially when attacks are involved. Today, many observers believe that humans are somehow indispensable to IHL's implementation. But if armed forces cannot exploit battlespace cyber opportunities in a timely fashion or effectively defend themselves against cyber attacks with humans "in" or "on" the loop, reliance upon humans inevitably will diminish. Their use will be viewed as "infeasible" when identifying and engaging cyber targets or defending against enemy cyber operations. Like it or not, future systems will become less and less reliant on human control during individual operations.

Distance: Cyber operations not only occur at unprecedented speeds but can also be launched from unprecedented distances, sometimes without the target knowing the location from which it is being struck. Illustrating this point, in 2019, the Director-General of the Australian Signals Directorate described how Australian cyber operators engaged in operations against Daesh.

> At the height of the fight against Daesh, ASD – working to the direction of the ADF – helped shaped a critical battle. Just as the Coalition forces were preparing to attack the terrorists' position, our offensive cyber operators were at their keyboards in Australia – firing highly targeted bits and bytes into cyberspace. Daesh communications were degraded within seconds. Terrorist commanders couldn't connect to the internet and were unable to communicate with each other. The terrorists were in disarray and driven from their position – in part because of the young men and women at their keyboards some 11,000 kilometres or so from the battle.[20]

Distance in traditional warfare usually translates into a degree of sanctuary due to the range limitations of weapons and weapons systems. Therefore, engaging enemy cyber operators and infrastructure sometimes will be limited to the use of cyber capabilities, for few militaries can effectively strike

---

[19] Clay Chun, *John Boyd and the "OODA" Loop*, U.S. ARMY WAR COLLEGE WAR ROOM (Jan. 87, 2019), https://warroom.armywarcollege.edu/special-series/great-strategists/boyd-ooda-loop-great-strategists/.

[20] Mike Burgess, Director-General, Australian Signals Directorate, *Address at Lowry Institute: Offensive Cuber and the People Who Do It* (March 27, 2019), https://www.asd.gov.au/publications/director-general-asd-speech-lowy-institute.

kinetically far from the area of active kinetic engagement. Equally, it will drive the enemy to operate from neutral territory, which presents further practical and legal obstacles to responding effectively.

Precision: Advances in weapons precision have dramatically improved the "probability of kill" (PK) during attacks while mercifully decreasing the likelihood of incidental injury to civilians or collateral damage to civilian objects (jointly referred to as "collateral damage" in this article). Cyber operations or operations reliant on cyber capabilities will enhance the trend towards ever-greater precision. The oft-used illustration is the use of Predator and Reaper remotely piloted aircraft (RPA). Despite assertions to the contrary, these systems can avoid, if employed with the care IHL demands, collateral damage that otherwise might be caused in a piloted attack. For instance, RPA can loiter in the target area for extended periods to more reliably identify the target and execute the strike when collateral damage is least likely. And individuals who are far removed from the enervating stress and personal danger that always attends combat operate them.

Cyber capabilities, in large part, undergird this and other advances in precision. As in the case of the RPA, such capabilities may reside in the weapons systems themselves. But in others, as with cyber intelligence, surveillance, and reconnaissance (ISR) operations that feed into the targeting process, the cyber capability itself is what enhances an attack's precision, and, therefore, the opportunity to avoid collateral damage.

Options: Moreover, cyber capabilities can offer alternative ways better to achieve an attacker's objectives in the battlespace and/or limit collateral damage. In this regard, it is essential to understand that modern warfare is not about destroying the enemy's forces or equipment (attrition warfare). Instead, the metric for success in the battlespace is the degree to which a desired effect on the enemy is achieved.[21]

Cyber capabilities open new opportunities for destroying, damaging, or neutralizing a target to achieve the desired effects. Taking a simple example, bombing operations centres can disrupt enemy command and control. But if cyber operations against the centre's internal communications systems are possible, the same effect can be achieved without placing civilians or civilian property in the vicinity of the target at risk.

Additionally, cyber capabilities can enable an attack on a different target to achieve the desired effect. Consider a kinetic kill operation against an enemy satellite using an anti-satellite missile (ASAT), which poses the risk of space debris that would endanger civilian systems. But a cyber operation against the ground station controlling the satellite equally could render the satellite useless by, for example, altering its orbit or simply turning it off. Similarly, a cyber denial of service operation against logistics systems that manage the movement and distribution of material may be more effective in disrupting enemy logistics and less likely to cause collateral damage than kinetically attacking the material, transports, or logistics hubs themselves.

And cyber capabilities can enable the neutralization of targets that is hard to achieve by kinetic means. For instance, it would be difficult, and dangerous for both the attacker and the civilian population, to attempt to disrupt military air traffic control (ATC) over a large area through a bombing campaign

[21] US Air Force, *The Effects-Based Approach to Operations (EBAO)* (Nov. 4, 2016), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-0/3-0-D06-OPS-EBAO.pdf.

against distributed ATC assets. But cyber operations against the system's network could generate that effect, for instance, by altering information in the system to an extent that causes a loss of confidence in it while placing civilians at less risk.

In some cases, cyber capabilities can also be used to deny the enemy use of assets that the attacker may need in future operations. Consider a draw bridge over a river that enemy troops must cross but upon which the civilian population also relies. If the movable section of the bridge can instead be locked in the up position by cyber means, it will remain usable by the attacking force should it later need to cross the river itself. It can also be unlocked to facilitate civilian movement when doing so would not benefit enemy operations. And having a fully functioning bridge would be useful once the occupation force assumes its responsibility for control over and governance of the occupied territories.

Shared systems: Cyber capabilities are not a panacea for collateral damage avoidance. Many military cyber capabilities rely on cyber infrastructure that is shared with civilian users, so-called "dual-use" objects. While dual-use targets are common in the non-cyber battlespace (e.g., dual-use airfields and other lines of communication), they are pervasive in cyberspace. Even when a cyber operation is directed against a discrete cyber military objective, there is a risk of bleeding over into civilian systems, as vividly illustrated in the case of Stuxnet.[22] Moreover, it is difficult to "map" the consequences of a cyber attack, either because the technological wherewithal is lacking or because the enemy has masked its system to limit an attacker's ability to identify vulnerabilities. These realities tend to exacerbate the likelihood of collateral damage during cyber operations.

Short notice development: Because cyber operations against the enemy will necessitate identifying unique vulnerabilities in its cyber infrastructure, cyber "weapons" in the form of malware and other exploitive code, whether offensive or defensive, sometimes will need to be created "on the fly, that is, developed, fielded, and employed on the "cyber battlefield," beyond the traditional development and acquisition systems. This raises questions about the ability of the attacker to thoroughly review and assess their use and the potential impact on the civilian population and infrastructure.

Transparency: A further legally relevant characteristic of cyber operations is that they are less transparent than their kinetic counterparts. This, in part, results from their non-physical character (although they may generate physical effects). For example, an aircraft, warship, or soldier can be seen by the naked eye or using relatively accessible hardware such as radar, whereas "seeing" a cyber attack requires highly technical equipment operated by specially trained personnel. An explosion is similarly apparent to anyone within seeing or hearing distance, and its results can readily be observed after the fact. By contrast, because the effects may be non-physical, a cyber attack may be mounted without its target knowing it has been targeted for some time (if ever). For instance, malware may be used to alter data used for navigation or targeting in a way that disrupts operations without announcing its presence. This phenomenon is, of course, only exacerbated by the speed at which cyber warfare occurs.

Cyber operations are also less transparent because of the difficulty of reliably attributing a cyber attack, either due to a lack of technological capability or because the enemy is engaged in deception, such as spoofing or false flagging. Cyber operations demand secrecy since the conduct of cyber warfare often depends on an attacker's identification of exploitable vulnerabilities. As a result, defenders must

---

[22] Peter W. Singer, *Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons,* 47 CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW 79, 84-85 (2015).

endeavor to frustrate an enemy's understanding of its systems, and attackers must avoid transparency lest the enemy be alerted and remedy the exploited vulnerability. And cyber capabilities are sometimes "use and lose" assets. As noted in U.S. Cyberspace doctrine, "Using a cyberspace capability that relies on the exploitation of technical vulnerabilities in the target may reveal its functionality and compromise the capability's effectiveness for future missions."[23]

Availability: Cyber capabilities are often more accessible to States and non-State actors than traditional weaponry. They are cheaper to acquire, and there are many more sources, such as independent malware developers marketing their products on the dark web, from which to obtain them. This is because of the ease of development compared with traditional weapons production and the lack of a strict regime for controlling their transfer.[24] Moreover, the parties to a conflict sometimes can develop cyber capabilities themselves, as their development does not necessitate physical infrastructure, such as factories.

It also is easier to outsource operations to non-State groups such as "patriotic hackers" or private companies than is the case with conventional military operations, for more individuals or groups wield effective cyber capabilities than can conduct kinetic operations. Again, this is due to the ease and low cost of development and employment of cyber capabilities. It also results from the possibility of mounting cyber operations far from the zone of active hostilities, where the non-State individuals or groups conducting them generally face little risk.

This has a leveling effect strategically and operationally. Shifting the balance of traditional military wherewithal is difficult. It is expensive, depends on the market availability of military hardware for States that do not produce their own systems, requires significant production capacity for States that manufacture systems, and takes time. By contrast, for the reasons noted above, militarily weaker States can offset some of that disadvantage by acquiring cyber capabilities that can generate significant effects in the battlespace and thereby affect the strategic calculus of an adversary's leadership. The fact that one State has more tanks than another, for example, may not be a significant advantage if the latter can disrupt the command and control of those tanks. Similarly, a militarily much more powerful State may hesitate to act if it knows its adversary can cause significant disruption to, for instance, its economy. Cyber capabilities are a valuable asymmetrical tool for a State that does not want to go toe-to-toe with its enemy.

III. Drivers of Normative Change

The international community is slowly beginning to opine on how IHL must be applied in this new cyber environment. For instance, the U.S. Department of Defense's *Law of War Manual* devotes an entire chapter to the subject.[25] Other new or updated manuals are likewise addressing the matter, an

---

[23] JOINT CHIEFS OF STAFF, CYBERSPACE OPERATIONS, Joint Publication (JP) 3-12, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[24] In the Wassenaar Arrangement, participating States agree to require an export license for certain items, such as intrusion software. It is not a ban on export and there is no means to legally bind members. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (July 12, 1996, as amended), https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-Public-Docs-Vol-I-Founding-Documents.pdf. See explanation at Secretariat, The Wassenaar Arrangement, https://www.wassenaar.org/about-us/.

[25] DoD Law of War Manual, *supra* note 11, ch. XVI.

important example being that of Denmark.[26] States are also promulgating cyber rules of engagement.[27] And the UN Group of Governmental Experts on cyber matters finally acknowledged, after some hesitation,[28] the applicability of IHL in cyberspace in its 2021 report,[29] while the Compendium of State views annexed to the report contains multiple affirmations and expansions of that acknowledgment.[30] Finally, individual States are also issuing broad statements on international law and cyber operations, the most in-depth analysis of IHL being that of the French Ministry of the Armies in 2019.[31]

Such normative examination is not limited to States. To an ever greater extent, non-State actors are exploring how IHL governs cyber operations during an armed conflict, with the ICRC leading the way.[32] The most granular assessment of IHL's impact on cyber operations is the *Tallinn Manual* project by two so-called "International Groups of Experts."[33] In January 2022, a third phase of the project was launched that will reconsider IHL in cyberspace based on State and non-State actor analysis since the last edition in 2017.

During these and other assessments, the mere availability of cyber capabilities sometimes determines how existing IHL rules are applied to cyber operations. For instance, as will be discussed, the requirement to take precautions in attack to verify a target's status as a military objective will dictate using cyber means to do so, if available and use is feasible in the circumstances. Similarly, taking precautions in attack requires selecting the means or method of warfare that will minimize harm to civilians and civilian objects, so long as the attacker sacrifices no military advantage. If an attacking force has access to cyber capabilities that could achieve the desired effect without the risk to civilians and civilian property posed by a kinetic attack, use of those capabilities is legally required. [34] In such cases, cyber capabilities simply represent another asset to which the commander must apply IHL rules.

However, the unique characteristics of cyber capabilities outlined in the previous section also will force a change in how the IHL rules are understood when applied in the cyber context. Shifts in the law, whether in the form of new law, the falling into desuetude of old law, or contextual reinterpretation of extant law, necessarily reflect the balance between military necessity and humanitarian concerns that has pervaded IHL since at least the 1868 St. Petersburg Declaration's acknowledgment of the

---

[26] Danish Military Manual, *supra* note 11.
[27] Most are classified. But see unclassified examples of cyber ROE in the NEWPORT RULES OF ENGAGEMENT HANDBOOK, § 2.5 and series 131-132 (2020), published as 98 INTERNATIONAL LAW STUDIES.
[28] See discussion in Michael N. Schmitt, *The Sixth United Nations GGE and International Law in Cyberspace*, JUST SECURITY (June 10, 2021).
[29] Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, ¶ 71(f), U.N. Doc. A/76/135 (July 14, 2021).
[30] Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution 73/266, U.N. Doc. A/76/136 (July 13, 2021).
[31] Ministry of the Armies, Republic of France, *International Law Applied to Operations in Cyberspace*, § 2.2 (2019).
[32] *See, e.g.*, ICRC, *Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts* (May 2021), https://www.icrc.org/en/document/avoiding-civilian-harm-from-military-cyber-operations.
[33] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt, gen. ed., Cambridge U.P. 2017)
[34] Additional Protocol Additional I, *supra* note 6, art. 57; 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, rule 15 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005).

need to fix the "limits at which the necessities of war ought to yield to the requirements of humanity."[35] A State's willingness to acquiesce to the emergence of new, or evolution of existing, IHL largely depends on its auto-balancing of combat effectiveness in securing national interests and its commitment to humanitarian ends.

That is not an easy task when it comes to cyber. Uncertainty regarding current and future cyber capabilities hobbles assessments of military necessity and humanitarian considerations. How effective will such systems be? To what extent are cyber capabilities and the options they make possible likely to shape future conflict? What future opportunities do cyber capabilities offer the military on the one hand and the civilian community on the other? To what extent do those capabilities also represent vulnerabilities? Assessing the balance in the cyber context involves an uncertain cost-benefit analysis.

To complicate matters, humanitarian values have evolved. What States deem an essential humanitarian interest in the future may not be reflected in rules crafted over a half-century ago. Nowhere is this truer than with respect to cyber activities. Societies are in their infancy in terms of reliance on cyberspace. Consider the response to the COVID-19 pandemic. From the development and dissemination of tests and vaccines to public health messaging, it has depended on cyber systems. As this societal dependency on cyberspace continues to grow, it will be seen by States engaged in warfare as both an opportunity and threat. They will want IHL to protect their societies' activities in cyberspace, but they are likely to equally want to exploit the enemy's reliance thereon.

Analysis of the effects cyber-enabled warfare may have on IHL, and vice versa, must proceed from the assumption that although non-State entities, such as the ICRC, civil society, and various individuals, influence the future course of IHL, States will continue to exercise decisive sway over its development because of their continued monopoly over formal law-making. Thus, how this military – humanitarian considerations balance plays out in their assessments of possible IHL interpretations will determine whether they read the rules permissively or restrictively, that is in favor of leeway in conducting cyber operations or turning to the law to constrain them.

At the same time, States' interpretations will be informed by the extent to which they believe IHL "works" and does so equally. Even if a State wants to use the law to safeguard its reliance on cyberspace for non-military activities, if it believes the other side will ignore the law, it may well conclude it does not make sense to pursue a restrictive course of action. This reality will be exacerbated by the limited transparency of cyber operations, for that lack of transparency will frustrate attribution, thereby allowing the enemy to hide violations behind denials. This possibility will cause States to hesitate further before embracing restrictive rules that they fear only they will follow.

Technology will also influence the pace, degree, and nature of change. Some States may seek rapid interpretive forward motion to prevent cyber development from getting out of hand, as was the intent of the failed attempts to regulate air warfare before World War II[36] and to limit nuclear proliferation

---

[35] 1868 St. Petersburg Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Dec. 11, 1868, reprinted in 1 American Journal of International Law 95 (1907). On my views regarding the balance, see Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law*, 50 VIRGINIA JOURNAL OF INTERNATIONAL LAW 795 (2010).

[36] For instance, the 1923 Hague Air Warfare Rules were never adopted. Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare. Drafted by a Commission of Jurists at the Hague, December 1922 - February 1923, https://ihl-databases.icrc.org/ihl/INTRO/275?OpenDocument.

in the immediate aftermath of that conflict.[37] That intent also undergirded the successful effort to ban blinding lasers that culminated in the 1995 Protocol IV to the 1980 Convention on Certain Conventional Weapons.[38] Moreover, if a State is confident about its assessment of what future cyber capabilities and vulnerabilities will look like, it might wish to seize the initiative to push the interpretive endeavor in a favorable direction, as some State have already done.[39] But others may adopt a wait-and-see approach in order to avoid locking in interpretations of the law that will prove disadvantageous should the technology not move in an anticipated direction.

Interpretive activism may also be motivated by a desire to achieve greater legal clarity. Generally speaking, States that are vulnerable to their potential adversary's cyber operations will tend to favor clarity. So too will States that view IHL as an effective shield against cyber operations that threaten entities and activities they wish to safeguard during armed conflict. And it must be remembered that offense moves faster than defense in cyberspace, which is an incentive to applying normative brakes on the enemy's operations. Of course, it is also possible that a State may adopt definitive *permissive* interpretations to play to its cyber superiority.[40]

On the other hand, some States may seek continued ambiguity, for ambiguity maximizes operational flexibility (the fact that it does so for the enemy as well is sometimes lost on those in advising and decision-making roles). These States see clarity as tying their hands, or at least as premature until they better understand the risks and benefits of cyber operations during armed conflict and understand what they give up through the restrictive IHL interpretations. Generally speaking, ambiguity is likely to be supported by States that enjoy cyber superiority, both offensively and defensively, and those skeptical of IHL's effectiveness. To some extent, this might explain the hesitancy to address two key questions discussed below regarding how IHL governs cyber operations, the meaning of the term "attack" and whether data is an "object."[41]

As should be apparent, then, competing dynamics are at play in the predictive endeavor of assessing the direction IHL will take regarding the conduct of cyber hostilities – restrictive versus dynamic, fast versus slow, and clarity versus ambiguity. What States see in terms of these conflicting approaches depends on where they stand. Interestingly, they may be conflicted on all these matters. For instance, a Ministry of Defense may seek permissive rules, a slow pace of interpretive development, and ambiguity, whereas Ministries responsible for the well-being of the civilian population might take the opposite approach. Cyber IHL development is a multifaceted, multi-dimensional puzzle.

---

[37] For instance, the failed Baruch Plan, Department of State, Office of the Historian, *The Acheson-Lilienthal & Baruch Plans*, 1946, https://history.state.gov/milestones/1945-1952/baruch-plans.

[38] Protocol on Blinding Laser Weapons, Oct. 13, 1995, 1380 U.N.T.S. 370.

[39] France has, to date, produced the most granular exposition of how it believes international law governs cyberspace. France, Ministries of the Armies, *supra* note 31.

[40] For instance, Israel has opined that "when a cyber operation is expected to cause physical damage, will it satisfy this element of an attack [the requisite damage] under LOAC. In the same vein, the mere loss or impairment of functionality to infrastructure would be insufficient in this regard, and no other specific rule to the contrary has evolved in the cyber domain." Roy Schöndorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 INTERNATIONAL LAW STUDIES 395, 400 (2021). By this interpretation, the prohibition on attacking civilian objects will usually be inapplicable to cyber operations directed against them

[41] See discussion in Michael N. Schmitt, *Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations*, 101(1) INTERNATIONAL REVIEW OF THE RED CROSS 333 (2019).

IV. The Conduct of Cyber Hostilities

In offering my thoughts on how cyber warfare will likely impact the IHL rules regarding the conduct of hostilities in the face of these competing approaches, I will track the general process by which the armed forces engage in targeting during armed conflicts. They must first assess whether the means or method employed is lawful. If so, it must be determined whether the operation is an "attack," for if it is not, the rules limiting and prohibiting attacks do not apply. Should the operation qualify as an attack, it may only be directed at lawfully targetable persons and military objectives and must not violate IHL rules like those prohibiting indiscriminate attack. Assuming these hurdles are crossed, the attacker will take precautions in attack to minimize civilian harm to the extent feasible. Finally, the attack may not violate the rule of proportionality.

Lawful Means and Methods

Under customary IHL, States must review "means of warfare" (weapons and weapons systems) before fielding them in combat to ensure their intended use complies with IHL and other rules of international law.[42] Additionally, in the study, development, acquisition, or adoption of means *or* "methods of warfare" (tactics, the way the means are employed), States that are Party to Additional Protocol I must, pursuant to Article 36 of that instrument, conduct a review to assess compliance with their treaty and customary international law obligations.[43]

When the *Tallinn Manual* experts first considered the application of these requirements between 2009 and 2013, there was consensus that cyber operations used cyber "means" and involved cyber "methods." Specifically, they defined "cyber weapons" as "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, that is, that result in the consequences required for qualification of a cyber operation as an attack."[44] As cyber means of warfare, they would require legal review before use. This characterization has presented two challenges.

The first is the speed at which cyber operations unfold. Weapon reviews can be time-consuming; indeed, States conducting them often produce formal, in-depth written assessments. Yet, given the speed of cyber operations, which may involve the short-notice development of an exploit in response to a just-discovered vulnerability in the enemy's system, there will be less time for careful analysis than

---

[42] Tallinn Manual 2.0, *supra* note 33, rule 110. The obligation derives from the longstanding requirement that operations be conducted pursuant to IHL. Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, art. 1, Oct. 18, 1907, 36 Stat. 2277; 1949 Geneva Conventions. Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 1, Aug. 12, 1949, 75 U.N.T.S. 3; Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, art. 1, Aug. 12, 1949, 75 U.N.T.S. 85; Geneva Convention (III) Relative to the Treatment of Prisoners of War, art. 1, Aug. 12, 1949, 75 U.N.T.S. 135; Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, art. 1, Aug. 12, 1949, 75 U.N.T.S. 287.

[43] Additional Protocol I, *supra* note 6, art. 36. Many States have acknowledged the requirement for a weapons review of cyber capabilities in their national statements on IHL and cyber operations. *See, e.g.*, Compendium, *supra* note 30, at 7 (Australia); 23 (Brazil); 38-39 (Germany); 93 (Switzerland).

[44] Tallinn Manual 2.0, *supra* note 33, rule 103. On the IHL definition of "cyber attack," see *id.*, rule 92.

is currently available when legal experts in Ministries of Defense or other higher headquarters conduct such reviews beyond the battlespace, perhaps before the conflict even began.[45]

Given this operational reality, many weapons reviews of cyber means of warfare will have to be conducted quickly, perhaps even in operations centers, by legal advisers who do not specialize in cyber matters. Additionally, individual commanders will wield the power of approval, often exercised in the heat of battle. It seems inevitable that normative expectations regarding the sufficiency of the required reviews will likely drop in such an environment, for weapons review procedures will have to be fast and agile.

Even more fundamentally, it is increasingly questioned whether cyber capabilities qualify as means of warfare at all. For instance, the United States increasingly uses the term "cyber capabilities" rather than, for example, "cyber weapons" in its guidance to the armed forces.[46] Working with a colleague at the Naval War College, I have concluded that such capabilities are not means of warfare, although their use qualifies as a method of warfare. At the risk of oversimplification, our view is that cyber capabilities are communications with cyber infrastructure; they do not qualify as weapons because they lack the terminal effect that typically characterizes weapons.[47]

This is by no means a consensus view. But it is appealing to States concerned that a weapons review requirement, especially if not relaxed as suggested above, would impose a condition that sometimes would defeat the objective of operating quickly enough to get inside the enemy's OODA loop. In some cases, it could negate the effectiveness of the cyber operation altogether, as when a cyber capability must be developed and employed quickly to take advantage of a fleeting opportunity.

Should interpretation move in this direction, and I believe it will, non-Parties to Additional Protocol I will not have to conduct a weapons review before employing a cyber capability. But, of course, the operation still would have to comply with all applicable IHL requirements on the conduct of hostilities, such as proportionality and taking precautions in attack. Parties to Additional Protocol I would continue to be required to conduct the review because a cyber capability qualifies as a method of warfare.

Attack

Many rules regarding the conduct of hostilities are conditioned on the cyber operation in question qualifying as an "attack," as that term is used in IHL. For instance, it is prohibited to "attack" civilians and civilian objects, disproportionate "attacks" are forbidden, feasible precautions must be

---

[45] *See, e.g.*, U.S. practice. U.S. Department of Defense, Directive 5000.1, The Defense Acquisition System ¶ E1.1.15, at 7 (2018); Headquarters, Department of the Army, Army Regulation 27-53, Review of Legality of Weapons Under International Law (1979); Secretary of the Navy, SECNAV Instruction 5000.2E, Department of the Navy Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System (2011); Secretary of the Air Force, Air Force Instruction 51-401 (2018).

[46] For instance, the DoD Law of War Manual notes, "[n]ot all cyber capabilities . . . constitute a weapon or a weapon system." DOD Law of War Manual, *supra* note 11, § 16.6. And the U.S. Air Force's The Law of War regulation, requires that the Air Force "conduct[] legal reviews of all weapons, weapon systems and relevant cyber capabilities, acquired or modified by the Air Force to ensure compliance with the law of war, domestic law, and international law at the earliest stage possible in development (prior to procurement or acquisition)." Air Force Instruction 51-401, *supra* note 45, ¶ 5.

[47] Jeffrey Biller and Michael N. Schmitt, *Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare,* 95 INTERNATIONAL LAW STUDIES 179 (2019).

taken during an "attack" to minimize harm to civilians and civilian objects, and "attacks" against certain specially protected objects and persons are prohibited.

In a widely accepted definition of the term, Additional Protocol I, Article 49, provides that the term refers to "acts of violence against the adversary, whether in offence or in defence."[48] The challenge is determining how this definition applies in the cyber context. There is widespread consensus that operations causing physical damage, destruction, injury, or death qualify as an attack to which the attack rules apply.[49] For instance, a cyber operation that interferes with the cooling system of infrastructure, thereby causing physical damage to that infrastructure, is an attack. If the infrastructure is civilian, the cyber operation will violate the prohibition on attacking civilian objects. Agreement also exists that if a cyber operation's direct and foreseeable consequences generate the requisite effects, it is an attack.[50] Examples include operations against a power grid during a winter storm that could lead to death due to loss of heating and a cyber operation targeting a food supply chain that results in starvation. The unsettled issue is whether cyber operations that do not have these direct or indirect effects can qualify as an attack.

Some states, like Israel, have taken the position that they do not so qualify.[51] By limiting "attacks" to cyber operations causing damage or injury, the military can conduct operations targeting civilian infrastructure that could contribute to defeating the enemy. A psychological operations campaign in which a DDoS operation targets enemy civilian media to undercut support for the enemy's war effort or counter the enemy's disinformation campaign is an example on point. Although media infrastructure, as such, does not qualify as a military objective and is, therefore, a civilian object, the fact that transmissions are only blocked or altered means the operation is not an attack and therefore does not run afoul of the prohibition on targeting civilian objects.

Other States take positions that cut in the opposite direction. For instance, "Germany defines a cyber attack in the context of IHL as an act or action initiated in or through cyberspace to cause harmful effects on communication, information or other electronic systems, on the information that is stored, processed or transmitted on these systems or on physical objects or persons. The occurrence of physical damage, injury or death to persons or damage or destruction to objects comparable to effects of conventional weapons is not required …."[52] Among States in this camp, France has offered the most detailed assessment. Its Ministry of the Armies has announced, "France does not characterise a cyberattack solely on the basis of material criteria. It considers that a cyberoperation is an attack where the targeted equipment or systems no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not. If the effects are temporary and/or reversible, the attack is characterised where action by the adversary is necessary to restore the infrastructure or system (repair of equipment, replacement of a part, reinstallation of a network, etc.)."[53]

---

[48] Additional Protocol I, *supra* note 6, art. 50(1).
[49] See discussion at Tallinn Manual 2.0, *supra* note 33, rule 92 and accompanying commentary.
[50] Tallinn Manual 2.0, *supra* note 33, rule 92, ¶ 15; ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts, Position Paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (English version), 2019, at 7.
[51] Schöndorf, *supra* note 40, at 400.
[52] Germany, On the Application of International Law in Cyberspace - Position Paper 8 (March 2021).
[53] France, Ministry of the Armies, *supra* note 31, at 13.

The *Tallinn Manual* experts could not agree on the issue beyond characterizing permanent loss of functionality of the targeted infrastructure or objects relying upon it as "damage" in the "attack" sense.[54] The ICRC agrees that cyber operations causing a loss of functionality should qualify as an attack, for "an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the IHL rules on the conduct of hostilities."[55] Some countries, such as New Zealand, have taken a similar stance.[56] Because cyber operations open an entire range of new targets, and targeting them can dramatically disrupt daily life for the civilian population without physically endangering civilians, my view is that the notion of attack must at least include cyber operations interfering significantly with functionality, lest the military humanitarian considerations balance lean too far in the direction of the former.

Some observers would go even further. The view of three prominent ICRC lawyers is representative.

> Article 48, alone or in combination with Articles 51(1) and 57(1) of AP I, should be interpreted as prohibiting cyber operations designed solely at disrupting internet services for the civilian population even if such cyber operations do not disable objects or otherwise have consequences that qualify them as attacks. The civilian use of the Internet is today so all-pervading that any other interpretation would leave an important gap in the protection that IHL affords to civilians against the effects of hostilities carried out by cyber means.[57]

States are unlikely to adopt such an approach in the near term, for qualifying mere disruption as an attack takes too much off the table for them, at least as it stands today. Therefore, I have suggested a policy-focused stop-gap approach to the issue. By it, States would, as a matter of policy, refrain from cyber operations against civilian infrastructure or data that would significantly interfere with "essential civilian functions or services." Further, they would abstain from conducting cyber operations to which they believe IHL rules do not apply (because, for instance, the operation does not qualify as an attack) if the "expected concrete negative effects on individual civilians or the civilian population are excessive relative to the concrete benefit related to the conflict that is anticipated to be gained through the operation."[58]

Over time, States must achieve some degree of consensus on this central issue. In my estimation, they will reject the narrow position by which only operations causing physical damage or injury are subject to IHL's attack rules. The growing reliance of their societies on activities in cyberspace, and the attendant vulnerability that reliance represents, will demand a broad interpretation of the term attack. While there are sometimes military advantages to be gained by targeting civilian infrastructure in a non-destructive or injurious manner, the need for militaries to conduct such operations is unlikely to keep pace with civilian reliance on cyberspace.

---

[54] Tallinn Manual 2.0, *supra* note 33, rule 92, ¶ 10.
[55] ICRC, Position Paper, *supra* note 50, at 7-8.
[56] New Zealand Office of Foreign Affairs and Trade, The Application of International Law to State Activity in Cyberspace, December 10, 2020, at 5.
[57] Laurent Gisel, Tilman Rodenhauser, and Knut Dörmann, *Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflict*, 102 INTERNATIONAL REVIEW OF THE RED CROSS 28, 325 (2020).
[58] Schmitt, Warfare 3.0, *supra* note 41.

How attacks are understood in this broad interpretation will be the question. Surely, the loss of functionality approach will broaden beyond the permanent loss of functionality. We already see this in the French interpretation, by which even temporary or reversible effects qualify as an attack when the operation makes it "necessary to restore the infrastructure or system."[59] In this approach, the effect on the infrastructure is the driver. Alternatively, interpretations that depend on the nature of the infrastructure or the severity of the consequences resulting from the operation might emerge. IHL already exhibits both approaches, albeit in other contexts. Special protections (for instance, that protecting installations containing dangerous forces) illustrate the former, whereas we see the latter in, for instance, IHL protection of the environment. The direction of interpretation is clear, but the path it will take to get there is not.

Targetable Objects

The next step in the targeting analysis is determining whether it is lawful to attack the proposed target. This depends on the customary IHL principle of distinction.[60] Reflected in Article 48 of Additional Protocol I, it provides: "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[61] In practice, the principle and the rules that derive from it limit the set of lawful targets to military objectives, combatants, members of organized armed groups, and civilians directly participating in hostilities.

Military objectives are "objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[62] An object that fails to satisfy this definition may not be attacked, although harm to it (collateral damage) is permissible so long as compliant with the rule of proportionality and the requirement to take precautions in attack.[63] The prohibition on attacking civilian objects has generated numerous conundrums, two of which are of particular interest in the cyber context. A third is unique to the cyber environment.

First, there is broad agreement that war-fighting objects like military cyber infrastructure, cyber systems integral to weapons systems, and other "military" equipment and systems qualify as military objectives. Likewise, there is consensus that objects "supporting" military operations, like a factory producing military equipment or a logistics hub, qualify as military objects.

The question is whether so-called "war-sustaining" objects are military objectives. War-sustaining objects indirectly make possible the war effort, such as an aspect of the economy that provides the

---

[59] France, Ministry of the Armies, *supra* note 31, at 13.
[60] Customary International Humanitarian Law, *supra* note 6, rules 1 and 7. The genesis of the principle is the 1868 St. Petersburg Declaration, which provides that "the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy." Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, 29 Nov./11 Dec. 1868, reprinted in 18 AMERICAN JOURNAL OF INTERNATIONAL LAW SUPPLEMENT: OFFICIAL DOCUMENTS 95 (1907).
[61] Additional Protocol I, *supra* note 6, art. 48.
[62] Additional Protocol I, *supra* note 6, art. 52(2); Customary International Humanitarian Law, *supra* note 6, rule 8.
[63] Additional Protocol I, *supra* note 6, arts. 51, 57; Customary International Humanitarian Law, *supra* note 6, rules 14-21.

funding it requires (e.g., drug production in Afghanistan[64]). They are civilian objects that some States would assert have been transformed into military objectives by virtue of their "sustaining" function. The United States is one of the few States that have gone so far.[65] Most States exclude war-sustaining objects from qualification as military objectives, as did a group of distinguished IHL experts, including me, convened by the International Law Association to examine conduct of hostilities issues.[66]

Cyber capabilities make possible the attack on war-sustaining entities as never before because most of them rely on cyber systems to function. The paradigmatic example is export oil production, storage, and transportation. As with the notion of attacks, the greater the disruption of civilian life, the more heavily humanitarian considerations must weigh in the military-humanitarian considerations balancing. Because war-sustaining activities and their associated infrastructure are both especially vulnerable to cyber operations and increasingly crucial to civilian life, the minority war-sustaining position is likely to fade over time. Indeed, whereas the United States is not highly vulnerable to kinetic attacks on its own war-sustaining entities, such as its financial sector system, it is susceptible to cyber operations against them, a fact that will likely shift the U.S. perspective on the matter. Additionally, because war-sustaining objects contribute only indirectly to the enemy's military operations, an argument that countervailing military considerations should stand in the way of that trend is a hard one to make.

The second conundrum is how to treat "dual-use" objects like an airfield used for both civilian and military purposes or an apartment complex in which a single apartment is used for military purposes such as command and control or weapons storage. Among States and many IHL experts, the prevailing interpretation has been that any use, no matter how slight, renders the object, or at least the parts that are not easily severable, a military objective.[67] As such, it becomes lawfully targetable.[68]

This approach is problematic when applied to cyber activities, for military and civilian cyber activities often depend on the same cyber infrastructure. Dual-use in the cyber context has become an omnipresent reality that will only grow over time. Consider the fact that well over a half million miles of maritime submarine cables carry over 95 percent of international data,[69] some of which enable military communications or are of military value. The cables are quite vulnerable to tapping; numerous

---

[64] Michael N. Schmitt, *Targeting Narcoinsurgents in Afghanistan: The Limits of International Humanitarian Law*, 12 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 301 (2009).
[65] DoD Law of War Manual, *supra* note 11, § 5.6.6.2; Brian Egan, Legal Adviser, Department of State, Remarks to the American Society of International Law: International Law, Legal Diplomacy, and the Counter-ISIL Campaign, April 1, 2016, published in 92 International Law Studies 235 (2016). *See also* Ryan Goodman, *The Obama Administration and Targeting "War-Sustaining" Objects in Noninternational Armed Conflict*, 110 AMERICAN JOURNAL OF INTERNATIONAL LAW 663 (2016).
[66] International Law Association Study Group on the Conduct of Hostilities in the 21st Century, *The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare*, 93 INTERNATIONAL LAW STUDIES 322, 341 (2017).
[67] *See, e.g.*, DoD Law of War Manual, *supra* note 11, § 5.6.1.2; Tallinn Manual 2.0, *supra* note 33, rule 101; HPCR, MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE 119 (Cambridge UP, 2013).
[68] In the cyber context, see NEW ZEALAND DEFENCE FORCE, MANUAL OF ARMED FORCES LAW, § 8.10.22 (2019); U.S. Submission to 2014-2015 GGE (Oct. 2014), reprinted in DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 732, 736 (CarrieLyn D. Guyman ed., 2014).
[69] Colin Wall, *Invisible and Vital: Undersea Cables and Transatlantic Security, Center for Strategic and International Studies* (June 11, 2021), https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security; Douglas R. Burnett, *Submarine Cable Security and International Law*, 97 INTERNATIONAL LAW STUDIES 1659 (2021).

nations already engage in the activity, placing the cables at risk.[70] Moreover, they may be cut with devastating results for the country into and out of which they travel, especially when served by a single submarine cable.

There is no question that these cables are military objectives under the contemporary reading of the law, even though the amount of civilian traffic dwarfs the military communications passing through them. As early as 1923, an international arbitration panel addressing the cutting of a British-owned cable by the United States during the Spanish-American War concluded that the action was permissible because it carried military information between Spain and its colonies.[71]

But cutting a submarine communications cable today would be highly disruptive for the civilian population. The rule of proportionality does not provide a remedy because, as presently understood, it only encompasses "incidental loss of civilian life, injury to civilians, damage to civilian objects" when assessing whether the civilian harm would be "excessive." Such collateral damage would be unlikely when cutting a cable. Of course, the cable scenario is but one example. Today, many military operations rely on civilian infrastructure or systems, such as off-the-shelf computers, dual-use satellites, or civilian communications networks. Thus, humanitarian considerations will loom large in any interpretive endeavor. Yet, so too do military considerations, for dual-use objects cannot be taken off the targeting table altogether.

There are two ways around this dilemma. The first is to adopt the approach briefly outlined above vis-á-vis the term attack. As a matter of policy, States could elect to refrain from conducting cyber attacks (or kinetic attacks generating cyber-related consequences) against dual-use objects that would significantly affect "essential civilian functions or services." Movement in this direction is already discernable in the persistent discussion among States over protecting "critical infrastructure" from hostile cyber operations.[72]

Should such a policy be widely adopted, it might mature over time into special protection under IHL, as with installations containing dangerous forces in Additional Protocol I.[73] The challenge would be determining where to draw the line between that dual-use infrastructure entitled to special protection and that protected only by the rule of proportionality and the requirement to take precautions in attack. In all likelihood, the dynamic of interstate negotiation and compromise would lead to relatively weak protection.

The alternative is to interpret the notion of military objectives more stringently in the dual-use context by adopting a threshold of use below which the current or future military use does not transform the civilian object into a military objective. This approach is appealing, for there must be a point at which the consequences for the civilian population so outweigh the military value of an operation that it would be contrary to the IHL balancing principle to treat the object as a military objective. Of course,

---

[70] Larisa Brown, *New Defence Chief Warns of Russian Threat at Sea; "Phenomenal" Increase in Submarine Activity*, THE TIMES (Jan. 8, 2022), at 1.

[71] Eastern Extension, Australasia and China Telegraph Company, Ltd. (Gr. Brit. V. U.S.), 6 Reports of International Arbitral Awards 112 (Arb. Trib. 1923).

[72] For instance, NATO has opined that the status of a targeted system as critical infrastructure is a factor to consider when assessing whether the operation is a use of force under the *jus ad bellum*. NATO, ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS [AJP-3.20 (ed. A, v.1)], at 20 (2020).

[73] Additional Protocol I, *supra* note 6, art. 56.

much of this work is already done by the proportionality rule, including a possible reinterpretation of the consequences that factor into that rule (see below). But it could also be accomplished by requiring a particular degree of military use before the transformation occurs. However such an approach might take shape, I believe the military-humanitarian considerations balancing will drive our understanding of what qualifies as a military objective in the direction of making it harder to so qualify when the civilian population is affected.

The third conundrum is how to treat data. IHL prohibits attacks on civilian objects. This raises the question of whether data is an object such that a cyber operation altering or deleting civilian data 1) amounts to an attack on a civilian object and 2) collateral damage to it caused during an attack on a military objective must be considered in the proportionality assessment and precautions in attack determination. This matter has been the subject of scholarly comments and State treatment. Israel, for example, takes the position that data is not an object and, therefore, not protected as a civilian object.[74] By this interpretation, all data is targetable unless it directly affects tangible objects, in which case the question is whether those effects qualify the operation as an attack. This was the view taken by most *Tallinn Manual* experts[75]; it gives parties to a conflict the most flexibility when conducting cyber operations.

Others have claimed data is an object. This view has found particular traction in the academic community[76] and enjoys some support among States.[77] It maximizes the protection of civilian activities that are reliant upon cyber systems. And it is a logical argument in many cases. For instance, if a physical documents archive is a civilian object protected by IHL, what is the logic to justify denying that status to an equivalent electronic archive?

As is apparent, these competing views attribute greater weight to one side or the other in the military - humanitarian considerations balancing. Indeed, the experts involved in the International Law Association project mentioned above could achieve no consensus on the matter.[78] The problem is that both have much to recommend them but also have serious shortcomings. In particular, if data is not an object, parties to a conflict can broadly disrupt civilian activities in the enemy's territory. As the ICRC has correctly observed, "[e]xcluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap."[79] But if data is an object, activities that have long been part of warfare, such as psychological operations targeting the enemy civilian population, are largely prohibited in the cyber context.

There has been a tendency to treat the issue as a binary one – data either is or is not an object. France has adopted a third approach in which content data is distinguished from process data, the latter

---

[74] Schöndorf, *supra* note 40, at 401.
[75] Tallinn Manual 2.0, *supra* note 33, at 437.
[76] *See, e.g.*, Heather A. Harrison Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 ISRAEL LAW REVIEW 39 (2015); Kubo Mačák, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, 48 ISRAEL LAW REVIEW 55 (2015).
[77] *See, e.g.*, NORWEGIAN MINISTRY OF DEFENCE, MANUAL OF ARMED CONFLICT ¶ 9.59 (2013) ("damage to or destruction of civilian data in connection with an attack against military cyber infrastructure will be equivalent to causing incidental damage, injury or loss by kinetic means"). Curiously, though, the Manual seems to suggest that whether a cyber operation targeting data is a cyber "attack" depends on the physical consequences of the operation, not the mere fact that data is destroyed, damaged or altered. *Id.*, ¶ 9.58.
[78] International Association Study, *supra* note 66, at 339.
[79] ICRC. Position Paper, *supra* note 50, at 8.

referring to the data that enables systems to function. It treats content data, such as records, as an object subject to the prohibition on attacking civilian objects. Yet, in the case of process data, France asserts that it is only the affected cyberinfrastructure that qualifies as an object subject to the rule.[80] In instances of alteration or deletion of civilian process data upon which civilian cyber infrastructure relies, the lawfulness of the cyber operation would therefore be determined primarily by whether it qualifies as an attack under IHL. The French approach is appealing but finding a legal basis for distinguishing between content and process data is problematic.

As noted, I have suggested a policy to deal with the uncertainty over the term attack. The approach applies equally to the problem of how to characterize data. By it, States would accord special protection to certain "essential civilian functions or services" by committing to refrain from conducting cyber operations against data that would interfere with them. Moreover, even if a State mounting the operation views data as failing to qualify as an object, it would not conduct cyber operations against the data if the expected concrete adverse effects on the civilian population are excessive relative to the concrete benefit related to the conflict that is anticipated to be gained through the operation.[81]

Since it balances military and humanitarian considerations, there is a possibility that this policy approach could mature into a rule of international law, either by custom or treaty. Pending that development, which would take some time, the proposed policy approach would respond to humanitarian concerns about protecting the growing reliance on cyberspace without denying the military valuable operations involving civilian data. I remain optimistic that the approach will appeal to States as they grasp the potential disruption of civilian life that targeting data may cause during an armed conflict.

Indiscriminate Attacks

As discussed in the context of weapons reviews, IHL prohibits the fielding of weapons that are incapable of distinction, that is, that cannot be "aimed" reliably at a military objective.[82] Cyber capabilities will seldom violate this prohibition because even capabilities designed to spread randomly within a system can be introduced into closed military networks.

More importantly, it is prohibited to conduct indiscriminate cyber attacks.[83] Indiscriminate attacks are either not directed at a specific lawful target or directed at a lawful military objective without the effects of the attack being controllable in the attendant circumstances.[84] Examples include, respectively, a cyber operation that is not targeted against particular cyberinfrastructure that qualifies as a military objective and placing destructive malware into a military system connected to a civilian network when it is likely to spread uncontrollably throughout that network. IHL also prohibits as indiscriminate the treating of "clearly separated and distinct military objectives located in a

[80] France, Ministry of the Armies, *supra* note 31, at 14.
[81] Schmitt, Wired Warfare 3.0, *supra* note 41, at 345-353.
[82] *See, e.g.*, DoD Law of War Manual, *supra* note 11, § 16.6 ("For example, a destructive computer virus that was programmed to spread and destroy uncontrollably within civilian internet systems would be prohibited as an inherently indiscriminate weapon.").
[83] That the prohibition applies in the cyber context is well-accepted by States. *See, e.g.*, Compendium, *supra* note 30, at 23 (Brazil), 94 (Switzerland); Germany, *supra* note 52 at 9 New Zealand Defence Force, Manual, *supra* note 68, § 8.10.22; U.S. Submission, *supra* note 68, at 68.
[84] Additional Protocol I, *supra* note 6, art. 51(4)(a) and (c); Tallinn Manual 2.0, *supra* note 33, rule 111; Customary International Humanitarian Law, *supra* note 6, rules 12.

concentration of civilian objects" as a single military objective.[85] To illustrate, consider a data center that contains multiple servers, only some of which host military-related data. Targeting the entire facility would be unlawful if it is feasible to identify and target only those servers containing the military data.

The first of these "use" violations is a matter of intent (or lack of it); the attacker either directs the capability against a military objective or not. The increasingly interconnected nature of cyberspace may tempt attackers to simply release a capability into the wild hoping it will affect a military objective. In some cases, the attack might not be indiscriminate because the malware is specific to particular systems that qualify as military objectives. In other cases, the malware may not generate effects that rise to the level of an attack (see above). But beyond those caveats, expect concern about bleeding over into civilian systems to translate into an ever more demanding understanding of what it means to "aim" a cyber capability.

This same dynamic will be at play with respect to the prohibitions on capabilities that have uncontrollable effects and attacks that treat severable objects as a single military objective. Recall that cyber capacities can be designed to be very precise, sometimes affecting only the targeted hardware or software. The ability to design precision into capabilities will inevitably raise the bar for what it means to attack discriminately. Moreover, greater precision makes it harder to treat multiple systems as a single military objective, for precision yields severability.

At the same time, as cyberspace becomes progressively more congested, networked, and complex, and its cyber infrastructure increasingly shared with the military, the risk of uncontrollable effects grows. As a result, we can anticipate a corresponding rise in the threshold for controllability. In particular, the risks posed to the civilian population by malware that is either self-propagating or not designed to attack specific hardware or software will inevitably push the law in this direction.[86] This dynamic will combine with an expected lowering of the threshold at which a cyber operation is characterized as an attack to give the prohibition of indiscriminate attacks a central role in framing cyber operations during armed conflicts.

Precautions in Attack

Even if a cyber operation qualifies as an attack against a military objective and is conducted in a discriminate manner, an attacker must take "precautions in attack" to minimize harm to civilians and civilian objects, at least so long as those precautions do not result in diminished military advantage.[87] This multifaceted obligation appears in Article 57 of Additional Protocol I and, in my estimation,

---

[85] Additional Protocol I, *supra* note 6, art. 51(5)(a); Tallinn Manual 2.0, *supra* note 33, rule 112; Customary International Humanitarian Law, *supra* note 6, rules 13.

[86] In this regard, Laurent Gisel, Tilman Rodenhauser, and Knut Dörmann of the ICRC have noted, "those who develop malware or planned cyber attacks can design their tools without self-propagation functions. In that case, malware cannot spread without additional human intervention. Even if self-propagating, attacks over the years have shown that malware can be designed to only attack specific hardware software. This means that even if malware is programmed to spread widely, it can be designed to only cause damage to a specific target or specific sets of targets." Gisel, Rodenhauser, and Dörmann, *supra* note 57, at 311.

[87] An obligation that is well-accepted by States in the cyber context. *See, e.g.*, Compendium, *supra* note 30, at 22 (Brazil), 38-39 (Germany), 94 (Switzerland); Germany, Position Paper, *supra* note 52, at 9-10; New Zealand Defence Force, Manual, *supra* note 68, § 8.10.19; U.S. Submission, *supra* note 68, at 737; DoD Law of War Manual, *supra* note 11, § 16.5.3.

reflects customary international law.[88] According to the rule, the attacker must do everything feasible to verify that the target is a military objective, select the target and means or method of warfare that will minimize incidental injury to civilians and collateral damage to civilian objects, cancel or suspend the attack if it appears that the target is not a military objective or the rule of proportionality will be violated, and issue warnings unless "circumstances do not permit."

The requirement to take precautions in attack is particularly significant in the cyber context. This is true regarding both cyber attacks and kinetic attacks that are cyber-enabled. Cyber means can be employed to verify the nature of a cyber or kinetic target, add granularity to the proportionality analysis, and serve as a tool in post-strike assessment to determine whether reattack of the target is necessary. Moreover, as noted above, cyber capabilities sometimes can make it possible to achieve desired effects by targeting alternative military objectives, the attack on which poses less risk of collateral damage, as in the case of disrupting a logistics system's functionality, or altering data it relies upon, rather than kinetically attacking lines of communication and storage facilities.

The most significant value of cyber capabilities vis-á-vis precautions in attack may lie in serving as an alternative to kinetic attack. Although not always the case, a cyber attack is usually less destructive, if destructive at all, than a kinetic attack in achieving the desired effect. The disruption of an integrated air defense system by cyber means to allow penetration of enemy-controlled airspace instead of kinetically attacking the system's components, such as radar and surface-to-air missile sites, is illustrative.

That said, many cyber capabilities are "use it and lose it." Even though the employment of a cyber capability against a target may result in less collateral damage, it may be militarily prudent to preserve it for later use when it will yield greater military advantage, avoid more collateral damage, or both. In such cases, the use of cyber would not be "feasible."

Moreover, the speed at which cyber exchanges may unfold in future conflict could preclude careful and thorough analysis by mission planners to ensure that cyber targets qualify as lawful, especially when the operation is a defensive response. That need for speed will also narrow the window of opportunity to explore options for minimizing harm to civilians and civilian objects by identifying and striking alternative targets or assessing non-cyber alternatives that generate less impact on the civilian population. Thus, the dilemma is that while there will be a growing military need for speed of response, speed increases the risk of human misattribution and incomplete understanding of knock-on effects.

Accordingly, preprogrammed cyber systems that verify targets and "make" precautions assessments according to algorithms without human involvement are certain to become a feature of the future battlespace. Autonomous systems will also be prevalent, and reliance on artificial intelligence will be widespread. Simply put, the need to ensure the enemy does not operate inside one's OODA loop will loom large in cyber and cyber-enabled warfare. Those who urge that a human must be "in" or "on" the loop to comply with the requirement to take precautions in attack are waging a losing battle, if only due to the inevitable technological realities of future warfare.

---

[88] Additional Protocol I, *supra* note 6, art. 57; Customary International Humanitarian Law, *supra* note 6, rules 15-21; Tallinn Manual 2.0, *supra* note 33, rules 114-120; Prosecutor v. Stanislav Galić, Case No. IT-98-29-T, Trial Chamber judgment, ¶ 58 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 5, 2003).

The precautions in attack requirement to cancel or suspend an attack should it becomes apparent that the target is not a military objective or that executing it will violate the rule of proportionality will likewise be affected by the speed of cyber engagements. That obligation traditionally envisioned, for example, air attacks in which a pilot sees unexpected civilians in the target area and does not attack or "flies away" a weapon that has been released. But although cyber means may help verify the target between the time the decision to attack has been taken and its execution, once the attack is launched, the effect is near-instantaneous; there is no longer an opportunity to react and "knock it off." In the cyber context, therefore, this rule will generally be meaningless.

According to Article 57(2)(c) of Additional Protocol I, the required precautions include "effective advance warning … of attacks which may affect the civilian population, unless circumstances do not permit." Cyber capabilities also will shape future understanding and application of this requirement. For example, cyber means may be used to alert a civilian population of cyber or kinetic attacks. Israel already uses text messaging to warn civilians of imminent airstrikes.[89] It would also be possible, for instance, to warn civilians by cyber means of a cyber operation against dual-use cyberinfrastructure that would allow them to disconnect in anticipation of an attack.

Note that the requirement to warn is not limited to situations in which the attack may cause "incidental loss of civilian life, injury to civilians, [or] damage to civilian objects," the scope aspect of the proportionality rule. Rather, the obligation encompasses any meaningful effect on the civilian population. This could extend to non-destructive and non-injurious bleed-over into civilian cyberinfrastructure that would not qualify as collateral damage under the proportionality rule, rendering the warning requirement especially relevant in the cyber context.

However, the "unless the circumstances do not permit" caveat cuts the other way. A key circumstance is the need for surprise. The speed of cyber operations will make it difficult to warn the civilian population effectively, as might be the case with warning civilians in a building of imminent attack just in time for them to flee. Moreover, preannouncing a cyber attack might enable the enemy to address the vulnerability to be exploited, even if only by taking a targeted system temporarily offline. The same is true from a defensive perspective, for the need to respond immediately to a hostile cyber operation might not allow for a warning.

Thus, cyber capabilities serve both to enable warnings and preclude them. As in contemporary warfare, the prospect of issuing warnings will be assessed case-by-case in future cyber-enabled warfare. Depending on the character of the conflict, the only feasible warning may be a general one that cyber operations will be undertaken or that dual-use cyberinfrastructure is subject to attack.[90] Therefore, defenders should try to segregate military and civilian systems, as it is their IHL obligation to do when feasible.[91]

Proportionality

---

[89] Israel Defense Forces, *How is the IDF Minimizing Harm to Civilians in Gaza?* (July 16, 2014), https://www.idf.il/en/mini-sites/hamas/how-is-the-idf-minimizing-harm-to-civilians-in-gaza/.

[90] In support of general warnings, see ICRC, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 2225 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

[91] Additional Protocol I, *supra* note 6 art. 58; Tallinn Manual 2.0, *supra* note 33, rule 121.

In combat, perhaps the most difficult IHL rule to apply is proportionality. The rule prohibits an attack that "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[92] It is a highly subjective rule that requires comparing dissimilar values – military advantage and civilian harm. All the fault lines that have surfaced in applying the rule during kinetic attacks apply equally in the cyber context, but two loom especially large as war becomes more cyber-enabled.[93]

The first is a practical obstacle. As cyber increasingly becomes a fundamental aspect of future warfare, a lack of transparency regarding cyber connectivity will make it more challenging to assess expected collateral damage. In my estimation, this reality, combined with the greater centrality of cyber activities to civilian life, will inevitably lead to lowering the threshold of certainty at which potential harm to civilians and civilian systems is factored into the proportionality calculations.[94] Only dramatically improved cyber-enabled and cyber-specific sensors that can map networks and assess possible cyber operation knock-on effects would counter this likely trend.

But ebbs and flows in certainty are a constant in warfare as new systems are fielded. Of greater direct cyber relevance is the question of the nature of the civilian harm that is factored into the proportionality assessment. By the rule, only "loss of civilian life, injury to civilians, damage to civilian objects" need be considered. Even if the concept of damage is extended to loss of functionality, most cyber operations affecting the civilian population will not generate collateral effects at that level. Will that mean that proportionality exercises only slight impact on the conduct of cyber hostilities?

From a military perspective, highly inclusive treatment of collateral effects will preclude attacking targets that qualify as lawful military objectives. But on the other hand, limiting the harm caused to the *lex scripta* in the proportionality rule will fail to account for the severe non-destructive and non-injurious collateral harm that the civilian population may suffer during cyber operations against military objectives.

Like the issue of defining an attack in the cyber context, I anticipate a relaxation of the notions of "injury" and "damage." But a countervailing influence will be the desire of the many States to keep from sacrificing the targetability of key military objectives, especially those vulnerable to cyber operations or that cannot be attacked other than by such operations. Thus, although the vector of change likely will be in the same direction as the interpretation of attack, the meaning of data, and other issues discussed in this article, the pace may be slower because of the possibility of rendering otherwise lawful attacks on military objectives unlawful.

---

[92] Additional Protocol, *supra* note 6, arts. 51(5)(b), 57(a)(iii), 57(b); Customary International Humanitarian Law, *supra* note __, rule 14. The application of the rule to cyber operations is widely accepted by States. For instance, it was cited in both the 2015 and 2021. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report, U.N. Doc. A/70/174, ¶ 28(d), (July 22, 2015); GGE 2021 EReport, *supra* note 29, ¶ 71(f).

[93] Tallinn Manual 2.0, *supra* note 33, rule 113 and accompanying commentary.

[94] For my views on the issue of uncertainty during proportionality assessments, see Michael N. Schmitt and Michael Schauss, *Uncertainty in the Law of Targeting: Towards a Cognitive Framework,* 10 HARVARD NATIONAL SECURITY JOURNAL 148 (2019).

V. Concluding Thoughts

Carl von Clausewitz famously observed, "There are very few men-and they are the exceptions-who are able to think and feel beyond the present moment." That may be true, but it does not diminish the need to do so, especially when dealing with war, for the costs of being trapped in the present or past can prove horrific. Failing to try to anticipate the future is irresponsible.

In this article, I have offered my tentative thoughts on how cyber capabilities will likely influence the vector of the law that governs them during armed conflict. Two premises animated the analysis. The first is that international law must reflect the values of the international community that applies it. When those values change, so must the law. This occurs through the adoption of treaties, the crystallization of customary rules, and, most frequently, evolution in the prevailing interpretation of the existing law. As it plays out in IHL, this dynamic is informed by a constant rebalancing of humanitarian and military considerations. Rules of IHL that do not adequately reflect that balance will lose the respect that they require to have an effect in the battlespace.

There is no question that cyber capabilities offer many military benefits during armed conflict. Accordingly, there is a valid military concern that if the IHL rules are interpreted two restrictively, critical military advantage will be sacrificed. Yet, as explained, the reliance of civilian populations on cyberspace will continue to grow. As it does, this reliance can be placed at risk by cyber operations the armed forces might wish to conduct. These civilian considerations exert a strong countervailing influence in the face of cyber capabilities' allure for the armed forces.

The question is how the civilian-military considerations rebalancing will play out. I sense that the law will move in the direction of interpreting the current IHL rules restrictively when applied to cyber operations, that is, in a manner that provides enhanced protection for the civilian population, sometimes at the expense of military advantage.

But I must caution although there are many non-state influences on the process, only States have the authority to make and authoritatively interpret international law. To date, they have been hesitant to venture far into the subject. In doing so, they are forfeiting the opportunity to shape the law that will govern their cyber operations and protect their populations during future conflicts.