Beyond state-centrism: international law and non-state actors in cyberspace

Article

Accepted Version

Beyond State-Centrism: International Law and Non-State Actors in Cyberspace

Michael N. Schmitt[1]
Sean Watts[2]

Cyber operations challenge not only the physical and spatial assumptions that guided the formation of much of the public international law inherited from previous generations, they test fundamental premises respecting the identity and status of actors governed by that body of law. Classically, individuals and non-State actors proved relevant to international law only as the agents, proxies, or chattel of States. Significant gaps in resources and capacity between States on the one hand and non-State actors on the other prevented their interactions from demanding significant attention from international law. And in those rare historical instances in which non-State actors could mount serious challenges to State hegemony, like cases of civil war, international law responded with significantly curtailed normative frameworks, such as that found applicable to armed conflicts not of an international character.[3]

Cyber operations, however, appear to present greatly increased opportunities for non-State actors to match, and in some cases even to surpass, State supremacy. Non-State actors capable of mounting cyber operations that profoundly affect States' security, and circumstances in which non-State actors demand as much or more attention than other States, are no longer futuristic or far-fetched—they are the prevailing reality of cyberspace. In addition to constituting a new domain of warfare between States, cyberspace also appears to represent a significantly contested domain between States and non-State actors. As an example, a recent report reveals the United States has resorted to offensive cyber operation in its efforts against Islamic State forces operating in Syria and Iraq.[4]

Still, at present, public international law primarily governs the relationship between States. This is no less true when considering its application to cyber activities involving non-State actors, such as individuals, private companies, hacker groups, criminal groups, or terrorists. Nevertheless, it would be inaccurate to suggest that the international law of cyber operations has no bearing on these activities. This article briefly surveys the intersection of public international law with cyber activities conducted by or against non-State actors. Drawing on the work of the International Group of Experts that prepared *The Tallinn Manual on the International Law Applicable to Cyber Warfare*,[5] it

---

[1] Charles H. Stockton Professor and Director, Stockton Center for the Study of International Law, United States Naval War College; Professor of Law, Exeter University; Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence; Fellow Harvard Law School's Program on International Law and Armed Conflict; Director of Legal Affairs, Cyber Law International. The views expressed are those of the author in his personal capacity.

[2] Professor, Creighton University School of Law; Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence; Reserve Attorney Advisor, United States Strategic Command, U.S. Army. The views expressed are those of the author in his personal capacity.

[3] *See e.g.* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609. By way of illustration, Additional Protocol II includes only 28 articles limiting the conduct of hostilities in non-international armed conflict whereas its counterpart applicable to international armed conflict includes 102 articles in addition to those of the four separate 1949 Geneva Conventions. *Id.*

[4] Ian Duncan, *Pentagon Unleashes Fort Meade Cyberwarriors on Islamic State*, BALTIMORE SUN, 1 MAR. 2016, *available at* http://www.baltimoresun.com/news/maryland/bs-md-isis-cyber-war-20160229-story.html

[5] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., Cambridge University Press, 2013)[hereinafter TALLINN MANUAL].

addresses three topics of particular relevance in this regard that lie outside the normative framework of armed conflict: sovereignty, State responsibility, and the *jus ad bellum*. The first two are presently being examined in much greater depth as part of the NATO Cooperative Cyber Defence Centre of Excellence's Tallinn Manual 2.0 Project's consideration of the peacetime law of cyber operations.[6] These important international norms and their emerging cyber-minded applications constitute critical legal considerations for States engaged in contentious cyber operations with non-State actors.

Sovereignty

The 1928 Island of Palmas arbitral award set forth the classic articulation of the principle of sovereignty: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[7] Pursuant to the principle, a State enjoys sovereign authority with respect all property, persons and activities, whether public or private, on its territory.

The *Tallinn Manual* expresses the principle of sovereignty in the cyber context: "A State may exercise control over cyber infrastructure and activities within its sovereign territory."[8] Today, this premise is relatively well accepted by the international community. For instance, in its 2013 Report, the United Nations Group of Governmental Experts (GGE) concluded "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory."[9] Members of the GGE include Russia and China, both of whom were initially sceptical as to application of international law to cyberspace.[10]

Non-State actors are fully subject to States' exercises of sovereignty. For instance, a State may regulate Internet activities by setting the technical criteria according to which Internet service providers must operate; limit content posted on the Internet from its territory, as in the cases of child pornography or terrorist recruiting; and regulate access to the Internet by individuals, groups or private entities on its territory. A State's sovereignty seldom extends beyond its territory, but the exercise of sovereignty thereon can affect non-State actors located abroad. In the exercise of its sovereign authority, a State may, for example, block or limit access to cyber infrastructure by individuals, groups or private entities located beyond its borders. A State would also be within its rights to regulate e-commerce on its territory, even if an affected private entity operates from another country.

The fact that cyber infrastructure is linked to a global communications network does not constitute a waiver of States' sovereign rights over their cyber infrastructure. This is not to say that sovereignty may be exercised against non-State actors free from international legal limitations. The

---

6 NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 to Be Completed in 2016 at* https://ccdcoe.org/tallinn-manual-20-be-completed-2016.html, last visited 8 Mar. 2016.

7 *Island of Palmas* (Neth. v. U.S.) 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

8 TALLINN MANUAL, *supra* note 5, at 15. The *Tallinn Manual* defines cyber infrastructure as "The communications, storage, and computing resources upon which information systems operate." *Id.* at 258. It encompasses, but is not limited to, all hardware associated with cyber activities.

9 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, 24 June 2013, p. 8 [hereinafter UN GGE 2015 Report].

10 Some scepticism appears to linger. *See* UN General Assembly, Letter dated 9 January from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/69/723, 13 Jan. 2015. The letter emphasizes aspect of sovereignty noting, "policy authority for Internet-related public issues is the sovereign right of States . . . ." *Id.* at 3.

exercise of sovereignty is subject to other aspects of public international law. In particular, international human rights law regulates States' cyber activities with respect to individuals.[11]

Sovereignty is also the source of States' authority to protect private and public activities and infrastructure on their territory from harm, whether cyber or non-cyber in nature. This is so irrespective of whether the source of a harmful cyber operation is a State or a non-State actor, and regardless of whether the entity conducting the operation is located in the State's territory or abroad. To illustrate, if a private company is the target of harmful cyber operations by either another State or private malicious hackers abroad, the State that hosts the affected company may take cyber or non-cyber measures to protect it. As will be discussed, in certain cases the measures may involve cyber responses that would otherwise be unlawful, even, in extreme cases, a violation of the prohibition on the use of force.

Because States enjoy sovereignty over their territory to the exclusion of other States,[12] a State's cyber operations against private cyber infrastructure can amount to a violation of another State's sovereignty. The Permanent Court of International Justice observed in the *Lotus* case, "the first and foremost restriction imposed by international law upon a State is that . . . it may not exercise its power in any form in the territory of another State."[13] Thus, in some cases the mere conduct of a cyber operation against non-State actors might violate the sovereignty of a State. These situations clearly include those involving cyber operations that usurp the governmental authority of the territorial State, as in law enforcement cyber operations by another State that target private companies without that State's consent,[14] and those directed at private cyber infrastructure that is located aboard a sovereign platform, such as a warship.[15] However, beyond these exceptional cases, the law as to when an operation against a non-State actor violates the sovereignty of the State where that actor is located is unclear. Wherever the threshold of violation lies, it is the same for both private and public infrastructure.

Uncertainty attendant to the issue was well illustrated in the deliberations of the International Group of Experts that prepared the *Tallinn Manual*. The Group could only agree that a violation of sovereignty occurs when another State's cyber operation "causes damage." It achieved no consensus on the international legal significance of "placement of malware that causes no physical damage (as with malware used to monitor activities)."[16]

The key issue is the characterization of remote operations directed against non-State actors that do not reach the physical damage threshold. In the view of the authors, the *Tallinn Manual*'s functionality test, developed to determine when a cyber operation qualifies as an "attack" during

---

[11] UN GGE 2015 Report, *supra* note 9, at 8 (observing "States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet. . . .").

[12] The Corfu Channel Case (U.K. v. Alb.) 1949 I.C.J. 1 (9 Apr.) at 43 (separate opinion of Judge Alvarez). Judge Alvarez observed, "By sovereignty, we understand the whole body of rights and attributes which as State possesses in its territory, to the exclusion of all other States . . . ." *Id.*

[13] SS Lotus, (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, p. 18 (7 Sep.).

[14] Island of Palmas (Neth. v. U.S.) 2 R.I.A.A. 829, 838 (4 Apr. 1928). The Arbitrator, in its application of the principle of sovereignty to the arbitration, referred not only to independence but also "to the exclusion of any other State, the functions of a State." *Id.*

[15] TALLINN MANUAL, *supra* note 5, at 23. Rule 4 of the *Tallinn Manual* notes, "Any interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty." *Id.*

[16] TALLINN MANUAL, *supra* note 5, at 16. Paragraph 6 of commentary to Rule 1 observes, "A cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty. It certainly does so if it causes damage." *Id.*

armed conflict, can be applied by analogy.[17] By this test, damage to cyber infrastructure includes losses of functionality of cyber infrastructure, or of items that rely on it, such that repair is required to restore functionality. In discussing this approach, the International Group of Experts disagreed over precisely what it means to require repair. However, in the authors' view, the concept means that the cyber infrastructure, such as a SCADA system, requires physical repair, as in replacement of components, or the reinstallation of either the operating system or of data upon which a purpose-built system relies to perform its intended function.

Beyond loss of functionality, the authors concur that if a State gains unauthorized access to a system and manipulates, alters, or destroys data, sovereignty is violated. This is an especially supportable position with respect to significantly deleterious cyber operations that are adverse to the interests of the State, compromise the State's right to independence and exclusivity of control, and are unconsented to and carried out on the State's territory, as in the case of cyber operations that appreciably disrupt commercial activities.[18] Admittedly, this is a broad view of sovereignty, but surely the grant of sovereign authority over activities on a State's territory includes those that manifest there. Some cases, however, remain subject to uncertainty, as with the mere placement of malware that has not been activated by a State into the cyber infrastructure of a private company overseas, extraction of the company's data, or a temporary distributed denial of service attacks against the company.

While cyber operations by a State may violate the sovereignty of the State where the non-State actors are located, cyber operations by non-State actors that are not attributable to a State as described below do not constitute a violation of sovereignty, no matter how destructive or injurious. Of course, cyber operations by non-State actors may well be in violation of the domestic law of numerous States, such as the State of nationality of the non-State actors and the States from which the operations were launched and where they culminated or otherwise had negative effects. But only States violate sovereignty as a matter of international law.[19]

The prohibition of intervention by a State into the internal or external affairs of other States derives directly from the principle of sovereignty. The prohibition consists of two elements. First, the activities in question must be coercive in the sense of compelling the target State to engage in an activity (including taking a decision) it would not otherwise engage in or refrain from activities that it would, but for the coercion, undertake. The International Court of Justice has characterized the element of coercion as "the very essence of prohibited intervention".[20] Thus, for instance, cyber espionage does not constitute intervention unless it clearly involves coercion. Second, acts in violation of the prohibition of intervention must be directed at the *domaine réservé* of the target State. The *domaine réservé* comprises matters that a State is permitted, as a matter of sovereignty, to decide upon freely, particularly its political, economic, social and cultural system.[21] Examples include elections, legislative activities, and providing for the social welfare of the population.

Generally, cyber operations directed at non-State actors such as companies, as in the case of the recent Sony hack,[22] do not qualify as intervention because they are neither intended to coerce the

---

[17] TALLINN MANUAL, *supra* note 5, at 108-09. Paragraphs 10 and 11 of commentary to Rule 30 identify a range of effects on functionality as relevant to determinations with respect to the *ius in bello* threshold of attack. *Id.*

[18] There have been suggestions of an exception in the case of espionage. *See e.g.*, Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VIRGINIA JOURNAL OF INTERNATIONAL LAW 291, 302 (2015).

[19] 1 OPPENHEIM'S INTERNATIONAL LAW: PEACE 385-90 (Robert Jennings & Arthur Watts eds., 9th ed. 1992) (cataloging various violations of sovereignty exclusively in terms of State actions).

[20] Military and Paramilitary Activities in and Against Nicaragua, (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 205 (June 27).

[21] Nicaragua Merits Judgment, ¶ 205.

[22] Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know so Far*, WIRED (12 Apr. 2014) *at* http://www.wired.com/2014/12/sony-hack-what-we-know/

State nor do they reach into the *domaine réservé*. If, however, another State conducts cyber operations against, for example, a State's residents or companies in order to force their host State to take a particular decision on a matter falling within its *domaine reserve,* the cyber operations will qualify as prohibited intervention. Similarly, intervention could involve cyber operations against private infrastructure that relates to the *domaine reserve,* as in the case of cyber operations used to block or alter the advertisements of a particular candidate during an election in another State.

In its *Nicaragua* judgment, the International Court of Justice concluded that indirect support for insurgents or terrorists in another State plainly qualifies as prohibited intervention.[23] The Court specifically characterized as acts of intervention the arming and training of guerrilla forces, which, as discussed below, also constitute uses of force. The Court further cited the financing of guerrilla operations as prohibited interventions, although such activities do not rise to the level of the use of force.[24] In the cyber context, therefore, a State that provides an insurgent group with malware and the training necessary to employ it against another State violates the prohibition on intervention. Financing the group's cyber activities would likewise violate the prohibition. Any cyber operations the State itself conducts in support of the group, such as interfering with the other State's command-and-control or collecting militarily useful information by cyber means and providing it to the group, are clearly encompassed in the prohibition.

Sovereignty is likewise the basis of the right of States to exercise jurisdiction with respect to certain cyber activities and cyber infrastructure. In this regard, the *Tallinn Manual* observes, "…a State may exercise its jurisdiction: (a) over persons engaged in cyber activities on its territory; (b) over cyber infrastructure located on its territory; and (c) extraterritorially, in accordance with international law."[25] Jurisdiction is the authority to prescribe laws and regulations, enforce them, and adjudicate alleged breaches thereof.[26] It is uncontested, as noted in *lit. (a)* and *(b)* of the *Tallinn Manual*'s rule, that States enjoy all three forms of jurisdiction over cyber activities by non-State actors located on their territory and over cyber infrastructure located there that is used or owned by non-State actors.

Lit. (c) of the Rule addresses jurisdiction over persons, cyber infrastructure and activities located or occurring beyond a State's territorial jurisdictional reach. Numerous grounds of varying degrees of acceptance exist upon which a State may exercise its various jurisdictional prerogatives extraterritorially. States enjoy, for example, prescriptive authority over their nationals, including "legal persons" such as companies, wherever they may be with respect to the cyber activities in which they engage.[27] Additionally, a State may exercise jurisdiction pursuant to the passive personality principle when cyber activities harm its nationals, again including legal persons, whether those nationals are on its territory or abroad.[28] By the principle, the State may, for example, adopt legislation proscribing cyber operations against its overseas companies and exercise enforcement and adjudicative jurisdiction when those responsible for operations are either present on the State's territory or the State has secured the consent of the State where the individuals are located to exercise its enforcement jurisdiction on the latter's territory.

---

[23] Nicaragua Merits Judgment, ¶ 205.

[24] Nicaragua Merits Judgment, ¶ 228.

[25] TALLINN MANUAL, *supra* note 5, at 18. This observation regarding jurisdiction achieved unanimous agreement from the International Group of Expert as Rule 2.

[26] AMERICAN LAW INSTITUTE, 1 RESTATEMENT OF THE LAW THIRD: THE FOREIGN RELATIONS LAW OF THE UNITED STATES 235, 304, 320 (1986) [hereinafter U.S. RESTATEMENT THIRD].

[27] *Id.* at § 402(2) (observing, "a state has jurisdiction to prescribe with respect to . . . the activities, interests, status, or relations of its nationals outside as well as within its territory.")

[28] *Id.* at § 402(2), comment g. The comment does not extend passive personality jurisdiction for ordinary torts, reserving exercises to serious crimes such as terrorism. *Id.*

Pursuant to the protective principle, a State may also exercise jurisdiction with respect to cyber activities that threaten State security, solvency, or other key State interests.[29] As an example, a State may criminalize the forgery of its currency or official documents by cyber means. Finally, the universality principal extends the jurisdiction of all States to certain international crimes, such as genocide and certain war crimes.[30] Pursuant to universal jurisdiction, all States enjoy authority over cyber attacks that violate key international humanitarian law prohibitions, like those outlawing attacks against the civilian population and civilian objects during armed conflicts, or with respect to the use of cyber means to launch or otherwise facilitate a genocide.[31] This is so whether the enumerated crimes are engaged in by the organs of a State or non-State actors and irrespective of the nationality or location of the offences' victims.

In international law the rights of States as sovereigns are often accompanied by corresponding obligations. Many of these State obligations operate with respect to controlling the activities of non-State actors. The most significant obligation in the cyber context emanating from the principle of sovereignty is that of due diligence. Pursuant to the principle, restated in cyber terms by the *Tallinn Manual*, "a State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."[32] This *Tallinn Manual* rule has since been affirmed by States participating in the UN Group of Governmental Experts process.[33] The obligation applies to the use of both public and private cyber infrastructure on the territory.

Due diligence obligations arise in a number of circumstances. For instance, if non-State actors are conducting hostile cyber operations from a State's territory into another State, the former is obliged to terminate the operations.[34] Similarly, if non-State actors in one State take control of cyber infrastructure in a second State and use it to mount cyber operations against a third State, the second State shoulders the same obligation. Due diligence obligations also attach in situations in which a State takes control, or otherwise uses, cyber infrastructure in another State to conduct cyber operations against non-State actors in a third State or in which a State's agents operate from another State's territory to mount the attacks. Finally, due diligence obligations can apply even to cyber operations by non-State actors against other non-State actors abroad.

Disagreement exists as to whether the obligation of due diligence imposes a requirement to prevent cyber infrastructure on a State's territory from being used for purposes that violate obligations owed other States. The better position is that States are only obliged to terminate on-going or imminent cyber operations. In doing so, they need only take those measures that are reasonable in the circumstances. For instance, take the case of an activist group operating from State A that conducts destructive cyber operations against a company in State B using cyber infrastructure in State C. Suppose that in order to effectively stop the on-going operations, State C would have to shut down significant segments of its national cyber network. That State is entitled to take the severity of those effects into consideration when determining whether to put an end to the non-State-actor's use the cyber infrastructure.

---

[29] *Id.* at § 402(3).
[30] *Id.* at § 404.
[31] *Id.*
[32] TALLINN MANUAL, *supra* note 5, at 26. The *Manual*'s Rule 5 addresses due diligence. Cyber infrastructure that is under exclusive government control is illustrated by that located on a State's military bases abroad.
[33] UN GGE 2015 Report, *supra* note 9, at 8 (observing "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs").
[34] Corfu Channel Case (U.K. v. Alb.) 1949 I.C.J. 1, 22 (9 Apr.).

State Responsibility

Addressing State responsibility in a cyber context, the *Tallinn Manual* observes, "A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation."[35] The international obligation underlying responsibility may be based in either treaty or customary international law, while attribution refers to legal, as distinct from factual, attribution. When these two criteria are met, the State concerned is responsible for an "internationally wrongful act".[36] Internationally wrongful acts may consist of affirmative actions, such as damaging cyber operations against private infrastructure located on another State's territory, or failure to comply with a duty like exercising reasonable due diligence to terminate harmful non-State cyber operations being conducted from the State's territory against another State.

While it is self-evident that States are responsible for the cyber activities of their organs,[37] especially the armed forces or security services, there are four situations in which a State bears responsibility for the cyber operations of non-State actors. First, a non-State actor is equated to a State organ when it has been empowered by the State's domestic law to exercise elements of governmental authority,[38] that is, engaging in an activity for the State that States typically perform. As an example, if a State's military contracts with a private company to conduct offensive cyber operations during an armed conflict, the State will be responsible for any of the company's cyber activities that violate international law, such as breaches of neutrality by impermissible use of neutral cyber infrastructure.[39] In these cases, the State will be responsible even for *ultra vires* acts so long as the private person or entity concerned was operating in its empowered capacity.[40] To illustrate, the State would bear responsibility for the violation of neutrality in the previous example even if it had instructed the company not to conduct operations involving neutral cyber infrastructure.

Secondly, cyber activities of non-State actors are attributable to a State when the non-State actor operates on the instructions of the State.[41] This basis for attribution differs from the previous bases in the sense that the non-State actors serve as an auxiliary to the State rather than take on a governmental function. Moreover, the activities may, but need not be, authorized by the law of the State concerned. For instance, if a State instructs a hacker group or a private company to probe for vulnerabilities in another State's cyber infrastructure in the hope of subsequently exploiting any that are discovered, the company's cyber operations are attributable to the State. In the event they breach an obligation owed the target State by the instructing State, the latter will be responsible for any ensuing internationally wrongful act.

Thirdly, non-State actor cyber operations conducted pursuant to the direction and control of a State are attributable to that State.[42] Although the terms 'direction' and 'control' differ, they have been encompassed by the International Law Commission in its commentary to the Articles of State Responsibility in the expression 'effective control', which was coined by the International Court of

---

[35] TALLINN MANUAL, *supra* note 5, at 29.

[36] International Law Commission, Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83 annex, U.N. Doc. A/RES/56/83, art. 2 (12 Dec. 2001) [hereinafter Articles of State Responsibility].

[37] *Id.* at art. 4(1).

[38] *Id.* at art. 5.

[39] TALLINN MANUAL, *supra* note 5, at 31. Comment 8 to Rule 6 cites the example of a Computer Emergency Response Team authorized by domestic legislation to respond to harmful cyber operations against governmental cyber infrastructure. *Id.*

[40] Articles of State Responsibility, *supra* note 36, art. 7.

[41] *Id.* art. 8.

[42] *Id.*

Justice in its *Nicaragua* judgement.[43] Broadly speaking, effective control means the State determines the specific cyber operations the non-State group will conduct and has the power and authority to approve or disapprove them. As noted by the Court in the non-cyber context, a State's assistance in the form of merely "financing, organizing, training, supplying, and equipping" the non-State group in a manner that enables its operations does not rise to the level of effective control.[44] Thus, for instance, providing malware to a non-State group for general use against another State does not result in attribution of the group's cyber operations. Indeed, even the "planning of the whole of its operation" does not suffice.[45]

Although a State's involvement in a non-State group's cyber operations against another State may not reach the effective control threshold, that involvement may nevertheless constitute an internationally wrongful act on its own accord. As noted above, financing a group's cyber operations against another State or providing the training necessary to conduct them qualify as a prohibited intervention into the internal affairs of that State. The State will shoulder responsibility for the intervention, even though it is not responsible for the acts of the group.

Unlike cyber activities of non-State actors that are undertaken pursuant to a State's law and amount to the exercise of governmental authority, attribution on the basis of instructions or effective control does not extend to *ultra vires* acts.[46] As an example, a non-State hacker group may be operating under the effective control of a State in conducting cyber operations targeting another State. If the group has been instructed by the State to refrain from particular types of operations or from targeting particular cyber infrastructure, and the group disregards those instructions, the State will not bear responsibility for the operations.

Finally, the cyber operations of non-State actors are attributable to a State when it acknowledges and adopts those operations.[47] Attribution on this basis involves more than merely expressing support or encouragement for the non-State actor. Rather, the State must embrace the conduct as its own, especially by engaging in activities that perpetuate the actions.[48] In the cyber context, a likely scenario would involve the State publicly approving of the cyber operations of a hacker group and then facilitating their continuance by, for example, providing further cyber capabilities to the group.

In addition to affixing responsibility, international law offers remedial measures to States that fall victim to internationally wrongful acts. States targeted by cyber operations that qualify as internationally wrongful acts are entitled to take, within strict parameters, "countermeasures" in response.[49] Countermeasures are cyber or non-cyber actions that would amount to an internationally wrongful act by the 'injured' State but for the fact that they are a response directed at the State conducting the initial wrongful act (the 'responsible' State).[50] It is their qualification as a countermeasure that precludes their wrongfulness. Such measures must be designed solely to compel the latter to desist in its unlawful course of conduct,[51] may not be punitive in purpose,[52]

---

[43] International Law Commission, Articles of State Responsibility with commentaries, G.A. Res. 56/10 Supplement No. 10, UN Doc. A/56/10, art. 8, ¶ 7 (10 Aug. 2001) [hereinafter Articles of State Responsibility Commentaries]; Military and Paramilitary Activities in and Against Nicaragua, (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 115 (June 27).

[44] Nicaragua Merits Judgment, ¶ 115.

[45] Nicaragua Merits Judgment, ¶ 115.

[46] Articles of State Responsibility Commentaries, *supra* note 43, art. 7, comment ¶ 9.

[47] *Id.* art. 11.

[48] United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran) 1980 I.C.J. 3, ¶ 74 (24 May).

[49] Articles of State Responsibility, *supra* note 36, art. 22.

[50] *Id.*

[51] *Id.* art. 49(1).

[52] Articles of State Responsibility Commentaries, *supra* note 43, art. 49, comment 1.

must be proportionate,[53] and may not breach and obligation a third State.[54] Although it is a matter of some dispute, the most defensible view is that countermeasures may not involved cyber operations at the use of force level.[55]

Non-State actors may not take countermeasures; such measures are a response reserved to States. Recall, however, that internationally wrongful acts by States may involve cyber operations directed at non-State actors, as with a State's cyber operations against a company in another State that breach the latter's sovereignty. In such cases, the company must look to a State authorized to conduct countermeasures under the law of State responsibility. There is, however, no bar to the State in turn authorizing the company concerned, or another non-State actor, to conduct the countermeasure on its behalf.

Analogously, countermeasures may not be taken against a non-State actor unless that actor's cyber operations are attributable to a State. This is because only States commit, as a matter of law, internationally wrongful acts. However, in such situations the principle of due diligence may come into play. A State that fails to exercise due diligence with respect to non-State actor cyber operations from territory that are directed at cyber infrastructure in another State is in breach of its due diligence obligation to the target State. As such, it has committed an internationally wrongful act to which the target State is entitled to respond with countermeasures.

There is no requirement that the injured State react to another State's internationally wrongful act with a countermeasure that involves the same obligation that the responsible State breached. This opens the door to the injured State responding to the breach of the due diligence obligation it was owed with a cyber countermeasure involving, *inter alia*, the principle of sovereignty. The paradigmatic example is a hack back against the non-State actor, for recall that a breach of sovereignty may involve cyber operations directed against private cyber infrastructure located on the State's territory. In that the hack-back qualifies as a countermeasure, its wrongfulness is precluded under the law of State responsibility. It must be cautioned in this regard that any such response must be proportionate to the responsible State's due diligence obligation, rather than to the cyber operation of the non-State actor, since it is the former, not the latter, that gives rise to the right to engage in a countermeasure.[56]

In exceptional situations, States may resort to the plea of necessity to respond to cyber operations conducted by non-State actors. Actions pursuant to the plea are available when cyber operations directed against the State constitute a "grave and imminent peril" to the State's "essential interest."[57] If the severity of the cyber operations faced by the State reach this threshold, the target State may take measures that would otherwise constitute an internationally wrongful act vis-à-vis other States.

Although the threshold for engaging in cyber operations pursuant to the plea of necessity is high, and while the plea is unavailable when the response would present an analogous threat to the essential interest of other States, the plea of necessity affords targeted States a great deal of flexibility. As an example, a State facing such a situation may respond by hacking back against the non-State actors themselves, or the cyber infrastructure being used by them, irrespective of any attribution of their conduct to a State. This is so even if the State into which the targeted State is

---

[53] Articles of State Responsibility, *supra* note 36, art. 51.

[54] Articles of State Responsibility Commentaries, *supra* note 43, art.49, comment 5 (noting, however, that incidental effects on third State parties are lawful).

[55] Military and Paramilitary Activities in and Against Nicaragua, (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 249 (June 27); Articles of State Responsibility Commentaries, *supra* note 43, art. 50(1), comment 3.

[56] Articles of State Responsibility, *supra* note 36, art. 51.

[57] *Id.* art. 25.

responding, or which is affected by the response, has not breached a due diligence (or any other) obligation owed the State invoking the plea.

The *jus ad bellum*

Article 2, paragraph (4) of the United Nations Charter, which is reflective of customary international law, prohibits the use of force by one State against another, except in situations of self-defence or when authorized by the UN Security Council.[58] The *Tallinn Manual* articulates the prohibition in cyber terms: "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."[59]

Although cyber operations of non-State actors do not violate this prohibition unless they are attributable to a State (and in such circumstances responsibility rests with the State rather than the non-State actor in question), those conducted by States against non-State actors may implicate the prohibition. For instance, a State's cyber operations directed at non-State actors in another State constitute a violation of the prohibition when sufficiently severe to cross the use of force threshold. In this regard, a violation of the use of force prohibition operates in a manner that is consistent with a breach of sovereignty on the basis of cyber operations targeting private cyber infrastructure.

Unfortunately, the threshold at which cyber operations qualify as a use of force is highly uncertain. Yet clearly, any State cyber operation resulting in physical damage to private cyber infrastructure on another State's territory would qualify. It is reasonable to extend the notion of damage to those cyber operations that result in a loss of functionality, as discussed above with respect to sovereignty, of cyber infrastructure or equipment or other items that rely on that infrastructure to operate.[60]

It is also well-settled, as the International Court of Justice opined in the *Nicaragua* judgment, that arming and training guerrilla forces engaged in violence against another State qualifies as a use of force.[61] By analogy, it would violate the prohibition of the use of force to provide cyber weapons and the training necessary to use it to insurgents, terrorists, hacker groups or individuals conducting cyber operations against another State at the use of force level, although financing would, as discussed, only qualify as intervention.

Beyond these clear-cut cases, it is unclear where the use of force threshold lies. In particular, the matter of non-destructive cyber operations having severe consequences remains unsettled. In the authors' view, adoption of a severity of consequences approach by States, as distinct from one that focuses on the nature of the consequences (destructive or not), is inevitable. However, only further State practice and expressions of *opinio juris* will refine the threshold. Until that occurs, non-exhaustive factors, as explained in the *Tallinn Manual*, such as severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement, and presumptive legitimacy, offer helpful indicators of when States are likely to characterize a cyber operation against a non-State entity as having crossed the use of force threshold.[62]

Pursuant to Article 51 of the UN Charter and customary international law, States faced with a use of force at the level of an "armed attack" may respond with their own defensive use of force. The *Tallinn Manual* expresses the self-defence rule in cyber terms along with a measure of

[58] UN Charter, arts 39, 42, 51.
[59] TALLINN MANUAL, *supra* note 5, at 42-43.
[60] *See* discussion *supra* accompanying note 17.
[61] Military and Paramilitary Activities in and Against Nicaragua, (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 228 (June 27).
[62] TALLINN MANUAL, *supra* note 5, 48-51; Michael N. Schmitt, *Computer Networks and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 914 (1999).

assessment: "A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects."[63]

As with uses of forces, the precise point at which a cyber operation qualifies as an "armed attack" is unclear. What is agreed is that all armed attacks are uses of force. In the view of the United States, which does not represent the prevailing interpretation, all uses of force are also armed attacks.[64] Thus, in the eyes of the United States, any cyber operation crossing the use of force line authorizes a lawful, forceful response, by either cyber or non-cyber means.

Most other States, as well as a majority of academics, adopt the position of the International Court of Justice in the *Nicaragua* judgement, which regards an armed attack as an especially "grave" type of use of force; hence, the so-called gap between cyber operations that qualify as uses of force and the smaller subset that rise to the level of a use of force.[65] For instance, while the *Tallinn Manual*'s International Group of Experts agreed that the 2010 Stuxnet operation was of sufficient scale and effects to qualify as a use of force, only some of its members regarded Stuxnet as grave enough to qualify as an armed attack.[66] As with use of force, the authors are of the opinion that in the future, the international community will move towards an interpretation of armed attack that is focused on the severity of the consequences of a cyber operation.[67]

A key question in the context of this article is whether a State may respond forcefully to a non-State actor's cyber operation pursuant to the law of self-defence. It is well settled that a State may do so when the non-State actor's operations are, as noted by the International Court of Justice in its *Nicaragua* judgment, conducted "by or on behalf of a State" or the State is substantially involved in them.[68] The unsettled issue surrounds non-State actor operations, including cyber operations, at the armed attack level of gravity that are not conducted on behalf of a State.

The issue took centre stage in the aftermath of the 9/11 attacks by al Qaeda in 2001. Although al-Qaeda did not conduct the assaults on behalf of any State, the Security Council, regional organizations, and many States treated the situation as one in which the United States, *inter alia*, could act in self-defence.[69] When the International Court of Justice subsequently suggested that non-

---

[63] TALLINN MANUAL, *supra* note 5, 53.

[64] U.S. DEP'T OF DEFENSE, LAW OF WAR MANUAL ¶ 1.11.5.2 (2015)[hereinafter DOD MANUAL]. The *U.S. Manual* explains, "The United States has long taken the position that the inherent right of self-defense potentially applies against any illegal use of force." *Id.* (citing Abraham D. Sofaer, *Terrorism, the Law, and the National Defense*, 126 MILITARY LAW REVIEW 89, 92-93 (1989); William H. Taft IV, Legal Advisor, Dep't of State, *Self-Defense and the Oil Platforms Decision*, 29 YALE JOURNAL OF INTERNATIONAL LAW 295, 300-01 (2004).

[65] Nicaragua Merits Judgment, ¶ 191. The Court observed, "As regards certain particular aspects of the principle in question it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms." Nicaragua Merits Judgment, ¶ 191.

[66] TALLINN MANUAL, *supra* note 5, at 58.

[67] For instance, a report that has been approvingly embraced by the Dutch government notes "A serious, organised cyber attack on essential functions of the state could conceivably be qualified as an 'armed attack' within the meaning of article 51 of the UN Charter if it could or did lead to serious disruption of the functioning of
the state or serious and long-lasting consequences for the stability of the state." Dutch Advisory Council on International Affairs and Advisory Council on Issues of Public International Law, Cyber Warfare (Report No. 77, AIV/No. 22, CAVV), December 2011, at 21. The Dutch Government stated that "The findings of the AIV/CAVV with regard to the use of force and the right of self-defence are largely in line with the government's position." Government of the Netherlands, Government response to the AIV/CAVV Report on Cyber Warfare, section 4 (undated).

[68] Nicaragua Merits Judgment, ¶ 195.

[69] *See e.g.* S.C. Res. 1368, UN Doc. S/RES/1368 (12 Sep. 2001) (recognizing "the inherent right of individual or collective self-defence"); North Atlantic Treaty Organization, *Statement by the North Atlantic Council*, 40 I.L.M. 1267, 1267 (2001).

State actors are incapable of conducting armed attacks in the legal sense required for self-defence,[70] its position was correctly criticized as ignoring recent history and as a failure to note that the text of Article 51 contains no limitation of armed attacks to actions by or on behalf of a State.[71] Today, States are beginning to openly express the view that non-State actors can launch cyber armed attacks and that qualification of a forceful response as self-defence precludes the wrongfulness of that response.[72] This was also the majority view of the authors of the *Tallinn Manual*.[73]

Assuming, *arguendo*, that non-State actors can mount armed attacks as a matter of law, the question becomes how to respond to cyber attacks launched by non-State actors from abroad when the State from which they are operating either cannot or will not terminate those operations. Responding with a cyber or non-cyber operation at the use of force level would violate the sovereignty of the State where such non-State actors are located, thereby bringing that right into conflict with the victim State's right of self-defence. Some scholars are of the view that respect for the sovereignty of other States is such a foundational principle of international law that it cannot yield even to another State's right of self-defence in such circumstances.[74] Nevertheless, as one of the present authors has explained more fully elsewhere, when international law rights clash, the better approach is to balance those rights in a fashion that most effectively preserves the object and purpose of each.[75] In this case, such a balance would allow for cyber or non-cyber operations at the use of force level against into the State from which the non-State actors are operating if that State is unwilling or unable to terminate the armed attack.[76] It must be emphasized that the balancing requires the State to proceed cautiously and in a limited fashion. For instance, if feasible, it must first warn the State to take action to terminate the activities and its operation must not exceed what is required to put an end to them.

Conclusion

While the State-centric assumptions and foundations of the formative periods of public international law appear to be eroding in many contexts, and perhaps especially in the context of cyberspace, their legal legacy prevails in the extant law. The public international law principles and rules bequeathed by preceding sovereigns remain intently focused on the interactions of States.

---

[70] Case Concerning Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda) 2005 I.C.J. 168, ¶ 146-47 (19 Dec.)(noting that while self-defence would have been available to Uganda had armed attacks been attributable to the Democratic Republic of Congo, no evidence supported such attribution); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶139 (9 Jul.)(noting "the existence of an inherent right of individual or collective self-defence in the case of an armed attack *by one State against another State*.")(emphasis added).

[71] Wall Advisory Opinion (Declaration of Judge Buergenthal), ¶ 6 (asserting, "the United Nations Charter, in affirming the inherent right of self-defence, does not make its exercise dependent upon an armed attack by another State . . . .").

[72] DOD MANUAL, *supra* note 64, at ¶1.11.5.4 (observing, "The inherent right of self-defence, recognized in Article 51 of the Charter of the United Nations, applies in response to any 'armed attack', not just attacks that originate with States)(citing In re Guantanamo Bay Litigation, *Respondents' Memorandum Regarding the Government's Detention Authority Relative to Detainees Held at Guantanamo Bay*, Misc. No. 08-442, 4 (D.D.C., 13 Mar. 2009); Government response to the AIV/CAVV Report, *supra* note 65, section 4 (undated).

[73] TALLINN MANUAL, *supra* note 5, at 59.

[74] *See e.g.* Tom Ruys and Sten Verhoeven *Attacks by Private Actors and the Right of Self-Defence*, 10 JOURNAL OF CONFLICT AND SECURITY LAW 289, 293 (2005)(noting condemnation of Israeli resort to self-defence on Lebanese territory based on the unwilling or unable justification).

[75] Michael N. Schmitt, *Pre-emptive Strategies in International Law*, 24 MICHIGAN JOURNAL OF INTERNATIONAL LAW 513, 540- 543 (2002-2003).

[76] *See also* DOD MANUAL, *supra* note 64, ¶ 1.11.5.3 (describing a U.S. view authorizing resort to self-defence to protect U.S. nationals abroad when the hosting State is "unwilling or unable to protect them.").

International law places States at the centre of its legal regimes, requiring in nearly all cases a State nexus to establish either an internationally wrongful act or an international legal obligation. In many respects, the State-centric legal regime of public international law may seem ill-suited or even inadequate to address the challenges the super-empowered non-State actors of cyberspace present.

Yet, as illustrated by this article, the actions of non-State actors implicate a wide range of long-standing public international law norms. In particular, norms associated with sovereignty, State responsibility, and the *jus ad bellum* offer critical legal limitations and justifications for cyber operations by States against non-State actors. To be certain, the precise contours of their operation in the context of cyberspace remain uncertain. However, their applicability, relevance, and binding nature are subject to little debate. Despite lingering ambiguity and in some cases logical strain, States confronted with cyber operations by non-State actors, as well as States contemplating cyber operations against them, are well advised to carefully analyse and incorporate the existing tenets of public international law into their security planning and cyber operations.