HARVARD NATIONAL SECURITY JOURNAL

ONLINE FEATURES

So You're Telling Me There's A Chance: How the *Articles on State Responsibility* Could Empower Corporate Responses to State-Sponsored Cyber Attacks

By Daniel Garrie and Shane R. Reeves[1]

> *"[U.S] information systems face thousands of attacks a day from criminals, terrorist organizations, and more recently from more than 100 foreign intelligence organizations."*[2]

> *Looking forward, if the pace and intensity of attacks increase and are not met with improved defenses, a backlash against digitization could occur, with large negative economic implications. Using MGI data on the technologies that will truly matter to business strategy during the coming decade, we estimate that over the next five to seven years, $9 trillion to $21 trillion of economic-value creation, worldwide, depends on the robustness of the cybersecurity environment.*[3]

I. Introduction

Corporate America is facing a relentless wave of state sponsored hostilities in cyber space.[4] Prominent recent examples include: Russia "attack[ing] the U.S. financial system" and

---

[1] Daniel B. Garrie is the executive managing partner for Law & Forensics, a legal consulting firm that works with clients across industries on software, cybersecurity, e-discovery, and digital forensic issues. He is also an accomplished electronic discovery Special Master hearing disputes throughout the United States. In addition, he is a Partner at Zeichner Ellman and Krause, responsible for the firm's cyber security and privacy practice and is an Adjunct Professor of Law at Cardozo Law School specializing in Information Governance.
Shane R. Reeves is a Lieutenant Colonel in the United States Army. He is an Associate Professor and the Deputy Head, Department of Law at the United States Military Academy, West Point, New York (shane.reeves@usma.edu). The views expressed here are his personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy, or any other department or agency of the United States Government. The analysis presented here stems from his academic research of publicly available sources, not from protected operational information.

[2] *U.S. Cyber Command: Organizing for Cyber Space Operations: Hearings Before the H. Comm. on Armed Services,* 111th Cong. 1 (2010) [hereinafter Hearings] (statement of Rep. Skelton, Chairman, H. Comm. on Armed Services).

[3] *See* McKinsey & Company, INSIGHTS & PUBLICATIONS, May 2014 *available at:* http://www.mckinsey.com /insights/business_technology/the_rising_strategic_risks_of_cyberattacks.

[4] Cyberspace is defined as "a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunications networks." U.S. DEP'T OF DEF. QUADRENNIAL DEFENSE REVIEW REPORT 37, February 2010 [hereinafter QDR]. The Tallinn Manual defines cyber space as "[t]he environment formed by physical and non-physical components, characterized by the use of computers and the electromagnetic spectrum, to store, modify, and exchange data using

stealing data from J.P. Morgan Chase & Company in August 2014;[5] the December 2014 North Korea hack of Sony over the release of a comedy titled "The Interview,"[6] and the continuing efforts of Chinese military unit 61398 to gain access to strategically important corporate intellectual property.[7] Whether motivated by economics, ideology, or nationalism, the cyber targeting of corporations is increasingly the modus operandi of hostile state actors.[8] Leaving this tactic unchecked poses a significant risk to both corporate interests and U.S. national security.[9]

computer networks." TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 193 (Michael Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

[5] *See, e.g.,* Michael A Riley & Jordan Robertson, *FBI Said to Examine Whether Russia Tied to JPMorgan Hacking*, BLOOMBERG (Aug. 27, 2014), http://www.bloomberg.com/news/articles/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking ("Russian hackers attacked the U.S. financial system in mid-August, infiltrating and stealing data from JPMorgan Chase & Co..").

[6] *See, e.g.*, David E. Sanger & Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES (Dec. 17, 2014), http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=1. "The Interview," a comedy about an assassination attempt on dictator Kim Jong-un, offended North Korea and was the reason for the cyber assault on Sony. *See id.*

[7] *See* Zoe Li, *What we know about the Chinese army's alleged cyber spying unit*, CNN (May 20, 2014), www.cnn.com/2014/05/20/world/asia/china-unit-61398/ (stating that "141 companies targeted by unit 61398, out of which 115 were in the United States" and are "blue-chip companies in important industries such as aerospace, satellite and telecommunications, and information technology—strategic industries that were identified in China's five year plan for 2011 to 2015."). *See also* Frank Langfitt, *U.S. Security Company Tracks Hacking To Chinese Army Unit*, NPR (Feb. 19, 2013), http://www.npr.org/2013/02/19/172373133/report-links-cyber-attacks-on-u-s-to-chinas-military (discussing the link between Unit 61398 and cyberattacks on dozens of American companies). Hackers affiliated with the Chinese government are considered the most energetic and aggressive international actors. *See, e.g.,* Craig Timberg, *Vast majority of global cyber-espionage emanates from China, report finds*, WASH. POST, Apr. 22, 2013, *available at* http://www.washingtonpost.com/business/technology/vast-majority-of-global-cyber-espionage-emanates-from-china-report-finds/2013/04/22/61f52486-ab5f-11e2-b6fd-ba6f5f26d70e_story.html (reporting that of 120 incidents of government cyber espionage, 96 percent came from China).

[8] Cyber attacks motivated by ideology or nationalism can also be defined as cyberterrorism. *See generally* CATHERINE THEOHARY & JOHN ROLLINS, CYBERWARFARE AND CYBERTERRORISM: IN BRIEF (May 27, 2015), *available at* http://fas.org/sgp/crs/natsec/R43955.pdf.

> Cyberterrorism can be considered 'the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.'...Cyberterrorists are state-sponsored and non-state actors who engage in cyberattacks to pursue their objectives….There are no clear criteria yet for determining whether a cyberattack is criminal, an act of hactivism, terrorism, or a nation-state's use of force equivalent to an armed attack. Likewise, no international, legally binding instruments have yet been drafted explicitly to regulate inter-state relations in cyberspace.

Id.

[9] *See, e.g.,* DANIEL GARRIE & MITCHELL SILBER, CYBER WARFARE: UNDERSTANDING THE LAW, POLICY, AND TECHNOLOGY 5-6 (2014) (discussing various cyber hostilities against corporations by state actors).

While non-state cyber threats to corporations are no less pernicious,[10] a broad array of federal statutes that regulate computer-related misconduct address such threats.[11] This domestic legal regime provides a victimized corporation both a criminal and civil roadmap for addressing a cyber incident.[12] By contrast, it is international law that regulates the response when a state conducts hostile cyber activity against a corporation. International law currently prohibits non-state actors—including corporations—from responding to state hostility themselves.[13] Only state actors have the legal authority to respond to other state actors.[14] As a result, a targeted corporation must hope that its host state will act on behalf of its interests. Unfortunately, despite some recent efforts to build a more robust public-private partnership to address state sponsored cyber hostilities, government responses are unpredictable and have proven inadequate at defending corporate interests.[15] As the frequency and intensity of state sponsored hostile activity increases, this arrangement is becoming untenable.

Is it possible to give corporations greater discretion in how they defend their interests from hostile state cyber activity without undercutting the well-established international norm that only states can act against other states? The answer to this question is a limited "yes." International law recognizes the authority of a state to empower private corporations to assume certain governmental functions.[16] These governmental functions may include responding with cyber countermeasures that are traditionally off-limits to corporations.[17] However, the delegation of this governmental authority does come with risk for the state. Since the corporation is viewed as an appendage of the government, the authorizing state retains legal responsibility for the countermeasures.[18] It is therefore imperative for the authorizing state to clearly articulate the parameters on these actions in order to avoid violating international law or, more importantly, inadvertently causing an armed conflict.

This article will begin with a brief summary of the international legal framework that regulates state interactions. The legal authority for government sanctioned corporate

---

[10] The damage to corporations by cyber criminals and non-state cyber groups can be immense as illustrated by the February 2015 hack of Anthem Incorporated Insurance Company. *See, e.g.,* Susanna Kim, *Anthem Cyber Attack: 5 Things That Could Happen to Your Personal Information*, ABC NEWS (Feb. 5, 2015), http://abcnews.go.com/Business/anthem-cyber-attack-things-happen-personal-information/story?id=28747729 (noting that over 80 million personal records were exposed to include those of children and non-customers).

[11] *See generally* Daniel Garrie & Shane R. Reeves, *An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors*, CARD. L. REV. 48-60 (forthcoming Spring 2016).

[12] *See, e.g.*, *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009); *Bittman v. Fox*, 2015 U.S. Dist. LEXIS 70249 (N.D. Ill. June 1, 2015); *Mahoney v. Denuzzio*, 2014 U.S. Dist. LEXIS 10931 (D. Mass. Jan. 29, 2014).

[13] *See generally* Shane Reeves, *To Russia with Love: How Moral Arguments for a Humanitarian Intervention in Syria Opened the Door for an Invasion of the Ukraine*, 23 MICH. S. INT'. L. REV. 199-229 (Fall 2014) (discussing the reason why states maintain the exclusive right to use force).

[14] *See* Garrie & Reeves, *supra* note 11, at 62-70 (reinforcing why corporations cannot be viewed as state actors or unilaterally respond to state sponsored hostile cyber activity).

[15] *See id*. at 75-76.

[16] *See* Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83, Annex, Art. 5, U.N. Doc. A/RES/56/83 Dec. 12, 2001) [hereinafter Articles on State Responsibility] (stating an "entity which is not an organ of the State" may be empowered to exercise elements of governmental authority).

[17] TALLINN MANUAL, *supra* note 4, at 30-31 (discussing private corporations being granted authority by a government to conduct offensive computer network operations against another state).

[18] *Id.* (noting that "a State is responsible for the acts of non-State actors where it has 'effective control' over such actors").

countermeasures, as well as the limitation on these actions, becomes apparent through this framework. The reasons that targeted states need to invoke this authority and how they should limit the countermeasures will follow. The article will conclude with a recommendation that host states, despite the associated risks with such a decision, empower victimized corporations with the authority to use countermeasures in response to hostile state cyber activity.

II. International Law and State Relationships

Public international law governs the interaction between states.[19] Within this broad category of international law there are more specialized sub-categories including the law of state responsibility, the *jus ad bellum*, and the *jus in bellum*. The law of state responsibility outlines the obligations states owe to each other as well as their concomitant responsibilities if they commit an internationally wrongful act.[20] When these internationally wrongful acts are interpreted as a use of force state relations may devolve into armed conflict as a result.[21] The international law which regulates armed conflict is comprised of two distinct strands known as *jus ad bellum and jus in bello. Jus ad bellum,* which lays the framework for when a state actor may resort to war, is "governed by an important, but distinct, part of the international law set out in the United Nations Charter,"[22] and only allows for the use of force in cases of self-defense or if condoned by the collective judgment of the international community.[23] *Jus in bello*, on the other hand, governs the actions of those participating in a conflict by establishing a delicate balance between military necessity—"the wartime necessity of killing and destroying military objectives" — and humanity—"the wartime requirement of preventing unnecessary suffering and protecting the civilian population."[24] The International Committee of the Red Cross (ICRC), in describing the differences between the two stated that "*[j]us ad bellum* refers to the conditions under which one may resort to war or to force in general; *jus in bello* governs the conduct of belligerents during a war, and in a broader sense comprises the rights and obligations of neutral parties as well."[25]

---

[19] *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 101 (1987) (defining international law as "rules and principles of general application dealing with the conduct of States and of international organizations and with their relations inter se, as well as some of their relations with persons, whether natural or juridical.")

[20] *See generally* TALLINN MANUAL, *supra* note 4, at 25-35.

[21] *See* Brian J. Bill, *The Rendulic "Rule": Military Necessity, Commander's Knowledge, and Methods of Warfare*, *in* 12 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 119, 119 (2009) (discussing the reality that at times states will result to warfare to resolve differences).

[22] GEOFFREY BEST, WAR & LAW SINCE 1945 5 (2002). .

[23] When can a state justifiably exercise its right of self-defense is debatable and outside the scope of this article. For a more detailed discussion *see generally* INT'L & OPERATIONAL LAW DEP'T, THE JUDGE ADVOCATE GENERAL'S LEGAL CTR. & SCH., U.S. ARMY, LAW OF ARMED CONFLICT DESKBOOK 29-35 (2010) [hereinafter DESKBOOK] (discussing the various views on the inherent right of self-defense in *jus ad bellum*).

[24] Major Shane R. Reeves & Lieutenant Colonel Jeremy Marsh, *Bin Laden and Awlaki: Lawful Targets*, HARV. INT'L REV., web perspectives (Oct. 26, 2011), *available at*: http://hir.harvard.edu/bin-laden-and-awlaki-lawful-targets (last visited 4 June 2013).

[25] Robert Kolb, *Origin of the Twin Terms Jus Ad Bellum/Jus In Bello*, 320 INT'L REV. RED CROSS 553, 553 n.1, (Oct. 31, 1997), *available at* http://www.icrc.org/eng/resources/documents/misc/57jnuu.htm (last visited 22 June 2013).

As this section addresses the legal justification for a response to hostile cyber activity only the law of state responsibility and the *jus ad bellum* will be discussed.[26] The law of state responsibility provides a path for more aggressive corporate responses to hostile cyber activity. However, if this corporate response is too aggressive, it may be construed as an illegal use of force or even an armed attack. Consequently, the corporation may be responsible for triggering the *jus ad bellum* and dangerously elevating the cyber incident into a justification for a military response. State actors would be foolish to authorize a private corporation to start an armed conflict. It is therefore important to briefly examine how the law of state responsibility provides for the empowerment of a corporation victimized by a hostile state cyber act and the consequences if those actions are misinterpreted.

A. The Law of State Responsibility and Corporate Countermeasures

State responsibility for committing an international wrongful act is found in customary international law and reflected for the most part in the International Law Commission's Articles of State Responsibility.[27] Underlying these articles is a belief in the inviolability of state sovereignty[28] and the need to hold accountable those states that violate international law. The articles "do not attempt to define the content of the international obligations, the breach of which gives rise to responsibility" but rather to outline the "general conditions under international law for the State to be considered responsible for wrongful acts or omissions."[29] The Articles of State Responsibility therefore do not simply codify the legal rights and obligations of state actors but also outline in broad terms the consequences of a violation of international law.[30]

One possible consequence for a state that chooses to commit an international wrongful act is entitling a targeted state to resort to countermeasures.[31] "Countermeasures are actions by an injured State that breach obligations owed to the "responsible" State (the one initially violating its legal obligations) in order to persuade the latter to return to a state of lawfulness."[32] In other words, a state victimized by another is authorized to use acts traditionally prohibited under international law to force the offending state to comply with its legal obligations. As countermeasures are intended to induce a state to comply with international law rather than as a punitive response, these acts are limited in severity and disallowed immediately upon cessation

---

[26] An analysis of the *jus in bello* in cyber space is irrelevant to this section. For a detailed discussion on *jus in bello* in cyber space see Michael Schmitt, *The Law of Cyber Warfare: Quo Vadis*, 25 STAN. L. & POL'Y, 269, 289-299 (2014).

[27] "It must be noted, however, that the law of armed conflict contains a number of specific rules on State responsibility for violation thereof." TALLINN MANUAL, *supra* note 4, at 29.

[28] "Sovereignty in the matters 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." *Island of Palmas* (Neth. v. U.S.) 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

[29] Articles of State Responsibility and Commentaries, General Commentary (1), *available at* http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [hereinafter Commentaries].

[30] *Id.* at art. 3.

[31] *See* Articles on State Responsibility, *supra* note 16, art. 22 ("The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State in accordance with chapter II of part three.").

[32] Michael Schmitt, *International Law and Cyber Attacks: Sony vs. North Korea,* JUST SECURITY (Dec. 17, 2014), http://justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/.

of the triggering illegal act.[33] Most importantly, countermeasures must not involve the threat or use of force as these acts are exclusively regulated by the United Nations Charter and customary international law.[34]

The Tallinn Manual[35] notes the applicability of countermeasures to cyber space. It provides that "a state injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures" against a responsible state.[36] Internationally wrongful acts can range from the severe—such as a violation of the United Nations Charter—to the more benign—such as a breach of the non-intervention principle.[37] What is clear is that a state actor conducting hostile cyber operations against a corporation unquestionably commits an internationally wrongful act.[38] It is irrelevant whether these activities are physically destructive or injurious, but only that they are unlawful and detrimental.[39] How the internationally wrongful act is interpreted will, however, drive the response. If the cyber activity targeting the corporation is an armed attack, the host state's right

[33] Articles on State Responsibility, *supra* note 16, art. 49-52.
[34] *Id.* at art. 50(1)(a); TALLINN MANUAL, *supra* note 4, at 38.
[35]The Tallinn Manual on the International Law Applicable to Cyber Warfare was drafted by a group of international law experts at the behest of the NATO Cooperative Cyber Defence "to help government's deal with the international legal implications of cyber operations." *See Manual Examines How International Law Applies to Cyberspace,* IT WORLD, Sept. 3, 2012, http://www.pcworld.com/article/261850/manual_examines_how_international_law_applies_to_cyberwarfare.html (last visited Sept. 12, 2015).
[36] TALLINN MANUAL, *supra* note 4, at 36.
[37] *Id.* at 29-30.
[38] Schmitt, *Quo Vadis*, *supra* note 26, at 275-76 (2014) ("hostile cyber operations directed against cyber infrastructure located on another state's territory, whether government or not, constitute, *inter alia*, a violation of that state's" sovereignty.). *See also* Schmitt, *Sony vs. North Korea, supra* note 32 (noting that North Korea's cyber hostilities directed at Sony violated the sovereignty of the United States).
[39] Schmitt, *Sony vs. North Korea, supra* note 32 ("it would seem reasonable to characterize a cyber operation involving a State's manipulation of cyber infrastructure in another State's territory, or the emplacement of malware within systems located there, as a violation of the latter's sovereignty. This being so . . . it violated U.S. sovereignty.").

of self-defense option to use force applies.[40] For those hostile cyber acts falling below the armed attack threshold, non-forceful countermeasures are an appropriate and authorized response.[41]

In almost all situations countermeasures are reserved for use by a victimized state. The Articles of State Responsibility make clear that violations of a state's sovereignty by non-state actors are not permitted. Article 2 expresses that "[t]here is an internationally wrongful act of a State when conduct consisting of an action or omission" is attributable to the State.[42] Inclusion of "omission" as a form of attribution is important as a non-state actor, in this case a corporation, could respond in such a way that the government becomes responsible. For this reason a corporation is unauthorized to unilaterally engage a state participating in hostile cyber activities.[43]

However, there is an exception to this general rule: An injured state which decides to invoke its right to use countermeasures may empower a non-governmental entity to act on its behalf. Article Five of the Articles of State Responsibility states that an "entity which is not an organ of the State" may be permitted by domestic law to exercise elements of governmental authority.[44] The term "entity" may include "public corporations, semi-public entities, public agencies of various kinds and even, in special cases, private companies, provided that in each case the entity is empowered by the law of the State to exercise functions of a public character normally exercised by State organs."[45] While the definition of "governmental authority" is intentionally left vague to accommodate various interpretations, the use of a countermeasure is clearly within any reasonable interpretation of this term.[46] In fact, countermeasures are a

---

[40] Cyber intrusions can range from a violation of sovereignty, to an unlawful intervention, to a use of force, to an armed attack. What rises to the level of an armed attack is debatable but most agree that there is a difference between a "use of force," and an "armed attack." *See Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, 1986 I.C.J. 14, 191 (June 27) [hereinafter *Nicaragua v. United States*](stating it is necessary to "distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."). *But see* Harold H. Koh, Address at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Maryland: International Law in Cyberspace (Sept. 18, 2012) *in* HARV. INT'L L.J. ONLINE 1, 3 (2012) (stating that the United States position is that the "inherent right of self-defense potentially applies against any illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response."). The U.N. Charter does not define a "use of force" leaving some discretion to individual states. The International Criminal Tribunal for the Former Yugoslavia somewhat addressed this issue by stating "an armed conflict exists whenever there is a resort to armed force between State or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State." *Prosecutor v. Tadic*, Case No. IT-94-1AR72I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Oct. 2, 1995). Though not addressing the definition directly this statement infers "that activities that directly lead to an armed conflict may be a use of force." *See* GEOFFREY S. CORN ET AL., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 15 (2012).

[41] *See* Schmitt, *Quo Vadis*, *supra* note 26, at 284. Professor Schmitt notes that "as a practical matter, characterization of a cyber operation as a wrongful use of force merely serves to label the state involved as a violator of international law." *Id.* State responses to uses of force are capped "at the non-forceful countermeasures level, an armed attack gives the targeted state the right to respond with its own use of force." *Id. (internal citation omitted)*. *See also* TALLINN MANUAL, *supra* note 4, at 17 ("Actions not constituting an armed attack but that are nevertheless in violation of international law may entitle the targeted State to resort to countermeasures").

[42] *See* Articles on State Responsibility, *supra* note 16, art. 2.

[43] *See generally id.* art. 49-54.

[44] *See id.* art. 5.

[45] Commentaries, *supra* note 29, at 43.

[46] *See id.* at 128-29 (describing the use of countermeasures).

relatively minor exercise of government authority in comparison to how the Tallinn Manual illustrates the appropriate use of Article Five in cyberspace. Examples offered include a "private corporation that has been granted the authority by the government to conduct offensive computer network operations against a state" and "empowering a private entity to engage in cyber intelligence gathering."[47] International law and specifically the Articles of State Responsibility therefore allow for the delegation of authority to use countermeasures, and in particular cyber countermeasures, to private corporations.[48]

B. What are the Risks?

Authorizing a private corporation to use countermeasures is an intriguing idea but comes with significant risk for the state. A state may "outsource the taking of lawful cyber actions to private entities" but it also "shoulder[s] legal responsibility for the actions."[49] Through domestic law the state delegates to the private entity the power to exercise governmental authority.[50] In doing so, the private entity is the equivalent of a government agency making any approved measures logically attributable to the authorizing state.[51] Similarly, any actions of the private entity not authorized by the domestic legislation are not attributable to the state.[52] Thus, if a corporation is empowered to use cyber countermeasures in response to a state sponsored hostile cyber act, these government sanctioned actions would be "considered an act of the State under international law, provided [they are] acting in that capacity in the particular instance."[53]

The risk to the authorizing state is further amplified by the requirement that countermeasures not violate the State obligation to refrain from the threat or use of force as embodied in the United Nations Charter.[54] Compliance with this limitation is particularly difficult in cyber space as the definition of "cyber use of force" is unclear. Professor Michael Schmitt notes that this topic frustrated the International Group of Experts convened to write the Tallinn Manual.[55] Out of this frustration the group

> developed a nonexclusive list of factors that would likely influence the characterization of cyber operations by states as uses of force: severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legality. Additional factors found meaningful by the Experts included, inter alia, the prevailing political environment, the nexus of an operation to prospective military force, the attacker's identity, the attacker's

---

[47] TALLINN MANUAL, *supra* note 4, at 31.
[48] Schmitt, *Sony vs. North Korea*, *supra* note 32.
[49] *Id.*
[50] Commentaries, *supra* note 29, at 43 (noting that Article 5 is clearly limited to entities which are empowered by internal law to exercise governmental authority).
[51] *See* Articles on State Responsibility, *supra* note 16, art. 5.
[52] TALLINN MANUAL, *supra* note 4, at 31 ("it is important to emphasize that State responsibility is only engaged when the entity in question is exercising elements of governmental authority.").
[53] Schmitt, *Sony vs. North Korea*, *supra* note 32.
[54] *See* Articles on State Responsibility, *supra* note 16, art. 50. The Tallinn Manual notes that a majority of the International Experts agreed that this prohibition also applies to cyber countermeasures. TALLINN MANUAL, *supra* note 4, at 38.
[55] *See* Schmitt, *Quo Vadis*, *supra* note 26, at 280.

> track record with respect to cyber operations, and the nature of the target. These and other factors operate in concert as states make case-by-case determinations.[56]

In applying the above listed factors and methodology it is easy to see how a corporate cyber countermeasure could be characterized as an unlawful use of force. If so characterized, the countermeasure would violate international law and, as the corporation would be acting under governmental authority, the violation would be attributable to the host state.[57]

Perhaps more significantly, a corporate cyber countermeasure authorized by the host state may be interpreted as an armed attack and potentially escalate into a military engagement.[58] It is important to note that the U.N. Charter prohibits the threat or use of force by any state.[59] This prohibition has only two generally recognized exceptions.[60] The first exception reserves to the Security Council the right to "determine the existence of any threat to the peace, breach of the peace, or act of aggression," and the power to "decide what measures shall be taken . . . to maintain or restore international peace and security."[61] The second exception ensures that states retain the "inherent" right of individual or collective self-defense if they are the victim of an armed attack.[62] This right is a well-established international norm existing prior to the drafting of the U.N. Charter and is generally recognized as customary international law.[63] International law thus imparts on the state independent authority to determine when it is necessary to exercise their inherent right to self-defense.

So when would a cyber countermeasure be significant enough to allow a state to invoke its inherent right of self-defense?[64] Again, similar to "use of force," it is difficult to define "armed attack" in cyber operations. While any cyber "use of force that injures or kills persons or

---

[56] *Id.* at 280-81 (*citing* TALLINN MANUAL, *supra* note 4, at 47-52).

[57] This problem is particularly acute as it is likely that "[t]he use of force threshold, wherever it may presently lie, will almost certainly drop in lock step with the increasing dependency of states on cyberspace." *Id.* At 281.

[58] *See id.* at 284 ("the consequences of a situation in which a state mounting a cyber operation miscalculates how the targeted state will characterize it (and respond based on that characterization) are graver with respect to the armed attack threshold.").

[59] U.N. Charter, art. 2, para. 4 ("All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state"). The U.N. Charter's general prohibition on the use of force echoes the ban on wars of aggression, or "the renunciation of war as an instrument of national policy," agreed to in the Kellogg-Briand Pact of 1928. *See* Treaty Between the United States and Other Powers Providing for the Renunciation of War as an Instrument of National Policy, 94 LNTS 57 (1928).

[60] "Consent" is considered by some as a third exception to the general prohibition on the use of force. *See, e.g.,* CORN ET AL., *supra* note 40, at 17. However, consent is more properly viewed as a state allowing force to be used within its own territory; therefore an exception to the rule prohibiting the use of force need not apply. *See* DESKBOOK, *supra* note 23, at 31 ("Consent is not a separate exception to Article 2(4). If a state is using force with the consent of host state, then there is no violation of the host state's territorial integrity or political independence; thus, there is no need for an exception to the rule.").

[61] U.N. Charter, art. 39.

[62] *Id.* at art. 51.

[63] *See Nicaragua v. United States*, *supra* note 40, at § 187("The exception of the right of individual or collective self-defense is also, in the view of States, established in customary law, as is apparent for example from the terms of Article 51 of the United Nations Charter, which refers to an "inherent right"); YORAM DINSTEIN, WAR, AGGRESSION, AND SELF DEFENSE 181 (2005). For a discussion on the customary definition of self-defense see Reeves, *To Russia with Love, supra* note 13, at 220-21.

[64] It is again important to note that most international law experts agree that not all "uses of force" equate to an "armed attack." *See, e.g.,* TALLINN MANUAL, *supra* note 4, at 47, 52.

damages or destroys property" is clearly an armed attack[65] the "requisite degree of damage or injury remains . . . the subject of some disagreement."[66] What is left unclear is whether cyber countermeasures not resulting in physical damage or injury, but generating "severe non-destructive or non-injurious consequences," constitute an armed attack.[67] In its characterization of these forms of cyber operations the United States has stated that "under some circumstances, a disruptive activity in cyberspace could constitute an armed attack."[68] Broadly interpreting an "armed attack" in cyber space to include not only destruction or injury but also serious disruptions to the functioning of the state is increasingly the international norm.[69] It is therefore possible that a cyber countermeasure that is too aggressive may fall within this more general definition of armed attack. The result would be a perverse situation where the aggressor state, whose actions initially justified the use of cyber countermeasures, could use military force as an act of self-defense against the victim state.[70]

III. Why Should a State Risk Empowering a Corporation with Cyber Countermeasures?

The risks to state actors, who remain legally accountable for any corporate use of cyber countermeasures, are significant, particularly for those corporate acts that could be misconstrued as an illegal use of force or an armed attack. For this reason, it would seem unlikely that a state would delegate countermeasure authority to a corporation. However, the advent of cyberspace has fundamentally altered the traditional landscape for international relations. As a result, states have been forced to re-think their approach to a myriad of issues including how best to protect corporations targeted by state actors in cyberspace.[71] However, this approach can only work if the domestic law that empowers the corporation also has clearly articulated limitations in order to mitigate many of the associated concerns with this proposal. Discussion of why corporations need this authority, and how to limit the risk presented by cyber countermeasures, follows.

A. Cyberspace: Opportunity and Danger

The importance of cyberspace in the contemporary business environment cannot be overstated which makes any state sponsored hostile cyber activities that target private corporations potentially devastating. Cyberspace has become ubiquitous for corporations and absolutely essential for conducting business operations.[72] In a survey of nearly four hundred

---

[65] TALLINN MANUAL, *supra* note 4, at 55.
[66] Schmitt, *Quo Vadis*, *supra* note 26, at 282.
[67] *Id.*
[68] *See, e.g., Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General,* 18, U.N. Doc. A//66/152 (July 20, 2010)(stating "under some circumstances, a disruptive activity in cyberspace could constitute an armed attack.").
[69] *See generally* Schmitt, *Quo Vadis*, *supra* note 26, at 282-83.
[70] U.N. Charter, art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.").
[71] *See, e.g.,* Schmitt, *Quo Vadis*, *supra* note 26, at 299 (discussing how armed conflict is transformed by cyber operations).
[72] ERIC A. FISHER ET AL., CONG. RESEARCH SERV., R42984, THE 2013 CYBERSECURITY EXECUTIVE ORDER: OVERVIEW AND CONSIDERATIONS FOR CONGRESS 1 (Mar. 1, 2013) (noting how heavily corporations rely upon computer technology to operate their business operations).

businesses conducted by the Journal of Law and Cyber Warfare nearly 11% of corporations surveyed reported generating or using data equaling that stored by the Library of Congress.[73] The survey also found that the reliance on data, and the more general use of cyberspace for corporate operations, is not limited to "just a handful of industries" but rather is pervasive throughout almost all businesses.[74]

Cyberspace, described by one author "as all of the computer networks in the world and everything they connect and control,"[75] offers unique opportunities and exciting possibilities to businesses.[76] However, the very reasons that businesses so heavily rely upon cyberspace are why hostile state actors target these corporations. Access to cyberspace is not limited to the technologically advanced, does not require extensive computer sophistication, and is possible from almost any location.[77] These attributes are advantages for businesses attempting to reach new customers and create organizational efficiencies. Yet, the borderless nature of cyberspace coupled with how easy it is to access the domain creates a staggering number of ways in which a cyber dependent corporation is vulnerable to exploitation.[78] For a hostile state this unparalleled ability to exploit a corporation is enticing and one of the primary reasons cyberspace is increasingly attractive.

Cyber activity is almost immediate, and if desired, relatively anonymous. These traits make cyberspace invaluable to a corporation; but they also incentivize bad behaviour in aggressive state actors.[79] While cyberspace allows a corporation to conduct business incredibly fast it also results in hostile "cyber operations . . . unfold[ing] so quickly that the state cannot" respond.[80] Further, the capability to remain anonymous in cyberspace is interesting to both corporate customers as well as the business itself. Anonymity, however, also makes attributing cyber hostilities to a state actor particularly difficult.[81] A hostile state is not bound by geography, technology, or even the likelihood that a victimized corporation's government will respond due to the speed and attribution difficulties associated with these acts.[82] These dynamics encourage a hostile state actor to target a corporation with relative impunity and little risk. The targeting of corporations in cyberspace is simply too attractive of an option for a motivated state actor not to use. Until there are consequences for the hostile state, there will be an increase in the targeting of corporations in cyberspace. It is therefore imperative to consider alternatives to the status quo including allowing corporations to protect themselves through the use of cyber countermeasures.

---

[73] *See* GARRIE & SILBER, *supra* note 9, at 8-15 (discussing the survey and its results).
[74] *Id.* at 8.
[75] RICHARD A. CLARKE AND ROBERT K. KNAKE, CYBER WAR 69-70 (2014).
[76] Leon E. Panetta, U.S. Sec'y of Defense, Remarks on Cybersecurity to the Business Executives for National Security, New York City (Oct 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 ("Cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and new dangers.").
[77] *See, e.g.* P.W. SINGER, WIRED FOR WAR, 264 (2009).
[78] *See* Garrie & Reeves, *supra* note 11, at 10-26 (discussing different forms of cyber hostilities and how they work).
[79] *See* McKinsey & Company, *supra* note 3 (highlighting the rising strategic risks of cyberattacks on corporations and the difficulty executives are having as "mitigating the effect of attacks often requires making complicated trade-offs between reducing risk and keeping pace with business demands.").
[80] Schmitt, *Quo Vadis*, *supra* note 26, at 276.
[81] *See* GARRIE AND SILBER, *supra* note 9, at 19-40.
[82] *See generally* Hearings, *supra* note 2.

B. What Should Corporations Be Allowed to Do and Not Do

International law, as a general rule, categorically prohibits a corporation from actively engaging a state actor, even if victimized by hostile activity.[83] However, the Articles on State Responsibility liberate corporations to act when their host state delegates through domestic legislation to them countermeasure authority.[84] Currently, despite increased efforts by state actors to protect corporations in cyberspace,[85] government responses to state sponsored cyber hostilities remain slow and often non-existent.[86] Empowering the corporation to act on its own behalf in cyberspace allows for quick and forceful responses to these hostile cyber activities. Further, the host state is at a significant disadvantage to respond as it is often receiving incomplete, second hand information regarding the hostile cyber activity.[87] The victimized corporation, in contrast, is in a much better position to remediate any cyber breaches and to identify the perpetrators. Allowing corporations these self-help measures therefore negates many of the advantages currently enjoyed by hostile state actors in cyberspace.

However, it is essential that there are limits placed on any corporate cyber countermeasures. Domestic legislation delegating countermeasure authority to the corporation must expressly prohibit any actions that may be construed as a use of force.[88] Again, it is important to reiterate that the host state retains responsibility for the consequences of any corporate actions[89] and the intent of allowing cyber countermeasures is to force an aggressor state into compliance with their international legal obligations.[90] Cyber countermeasures are not meant to open the door to armed violence or to "undermine U.S. efforts to establish durable

---

[83] *See generally* Articles on State Responsibility, *supra* note 16.
[84] *See id.* at Art. 22.
[85] The United States has taken significant steps to better coordinate a response to hostile cyber activities targeting corporations by establishing the Cyber Threat Intelligence Integration Center (CTIIC). *See Fact Sheet: Cyber Threat Intelligence Integration Center*, whitehouse.gov (Feb. 25, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center. The CTIIC is intended to be "a national intelligence center focused on 'connecting the dots' regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests," has the mission of assisting "relevant departments and agencies in their efforts to identify, investigate, and mitigate those threats." *Id.* Additionally, on February 13, 2015 the President issued an Executive Order to promote private sector cybersecurity cooperation by authorizing greater intelligence sharing while protecting business confidentiality. Executive Order—Promoting Private Sector Cybersecurity Information Sharing, Feb. 13, 2015, *available at* https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari. It is unclear whether these efforts will have any effect on the ongoing trend of state sponsored cyber activity.
[86] *See, e.g.,* Devlin Barrett & Danny Yadron, *Sony, U.S. Agencies Fumbled After Hacking,* WALL ST. J., Feb. 23, 2015, at B1 (discussing how there are major shortcomings in how the government and companies work together to respond to cyber hostilities and in particular the hack of Sony Entertainment).
[87] *See* Garrie & Reeves, *supra* note 11, at 75-76 ("Unfortunately, in the United States this partnership is in its infancy and is complicated by a host of problems including: distrust between the private and public sector, corporate reputational concerns, potential liability caused by a cyber incident, and sensitivity of operating in a global economy.").
[88] *See supra* text and accompanying notes 49-71 discussing why these acts cannot cross this threshold.
[89] *See* Articles on State Responsibility, *supra* note 16, art. 5.
[90] *See id.* art. 49-52.

international norms" against hacking.[91] Allowing for active defense measures is potentially problematic in cyberspace as these acts can often be misinterpreted as more aggressive than intended. Only through well-established and advertised parameters on the corporate countermeasures can a host state hope to avoid unwanted escalations.[92] It is critical for the host state to ensure that any authorized corporate cyber countermeasures respect the well-established prohibitive use of force model found in international law.[93]

It is also important for the corporate countermeasure authorization to delineate attribution criteria before use. Attribution is a difficulty in cyberspace and can be especially troublesome in the context of state actors.[94] While it is nearly impossible to positively attribute cyber actions with complete certainty, evidence often points to the hostile state.[95] Any domestic legislation empowering a corporation with cyber countermeasure authority must balance the need to respond with the importance of holding accountable the responsible party. Without attribution requirements cyber countermeasures could quickly devolve into simple hack back strategies that are shots in the dark against unknown perpetrators.[96] However, in circumstances where there is strong evidence of state sponsorship of cyber hostilities, corporations must be allowed to respond.[97]

The current paradigm where corporations sit idly by while their interests are assaulted in cyberspace by hostile state actors is impractical. Governments are currently ill-equipped to respond on behalf of the corporation and thus allowing businesses to use self-help protective measures is a logical alternative. Admittedly, the host state assumes risk by authorizing corporate cyber countermeasures. Yet, the peril of this strategy is diminished by clearly establishing in the domestic legislation attribution criteria and the parameters of the corporations cyber countermeasures.

---

[91] Max Fisher, *Should the U.S. allow companies to 'hack back' against foreign cyber spies?*, WASH. POST (May 23, 2013), http://www.washingtonpost.com/blogs/worldviews/wp/2013/05/23/should-the-u-s-allow-companies-to-hack-back-against-foreign-cyber-spies/.

[92] *See* JEFFREY HUNKER ET. AL., INSTITUTE FOR INFO. INFRASTRUCTURE PROTECTION, ROLE AND CHALLENGES FOR SUFFICIENT CYBER-ATTACK ATTRIBUTION 5 (2008) (describing the dangers that come with active defense measures in cyberspace and in particular the possibility of a disproportionate response).

[93] *See* U.N. Charter, art. 2(4).

[94] *See generally* GARRIE AND SILBER, *supra* note 9, at 19-40.

[95] However, there are circumstances when attribution is less of a problem. For example, while North Korea denied being behind the cyber hostilities targeting Sony in December 2014, it poorly veiled its complicity in the hack as it seemed intent on "punishing" the company for its behaviour. *See, e.g.,* John Fingas, *North Korea denies hacking Sony Pictures, but likes that someone did*, Engadget (Dec. 7, 2014), http://www.engadget.com/2014/12/07/north-korea-denies-hacking-sony-pictures/. The United States later publicly attributed the cyber act against Sony to North Korea. *See, e.g.*, David E. Sanger & Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES (Dec. 17, 2014), http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=1.

[96] HUNKER, *supra* note 92, at 5 ("[o]ur legal and policy frameworks for responding to cyberattacks cannot work unless we have adequate attribution; these frameworks remain incomplete because we lack the basis (sufficient attribution) to actually use them.")

[97] Examples include the December 2014 North Korean hack of Sony, *see generally supra* note 95, and the October 2012 Iranian hack of American banks and the oil industry in the Middle East. *See generally* Mike Mount, *U.S. Officials believe Iran behind recent cyber attacks,* CNN (Oct. 16, 2012), http://www.cnn.com/2012/10/15/world/iran-cyber/index.html) (quoting Retired Senator Joseph Lieberman as stating "I don't believe these were just hackers who were skilled enough to cause disruption of the Web sites . . . I think this was done by Iran and the Quds Force, which has its own developing cyber attack capability.").

IV. Conclusion

The hacking of corporations in cyberspace will not stop until hostile states are forced to re-consider the cost of their actions. Delegating cyber countermeasure authority to corporations would be an effective way to start this thought process. However, this article's proposal is not meant to be considered in lieu of a closer relationship between governments and corporations; it is rather intended to be a small part of a broader strategy. Only a robust public-private partnership will provide truly comprehensive solutions to the problems facing corporations in cyberspace.[98] These problems are immense and finding solutions is of critical importance to both corporations and the national security of the United States. Allowing victimized corporations to respond to hostile state cyber activity would be a small, yet positive, step towards a broader solution.

[98] We explain how the public-private relationship could be significantly enhanced in our forthcoming article. *See generally* Garrie & Reeves, *supra* note 11.