The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 14 July 12, 2017

CYBER THREAT TYPES

International Law Playing Cybersecurity Catch-Up (Part One of Two)

By Seth D. Rothman and Andreas S. Baum
Hughes Hubbard & Reed LLP

In today's interconnected world, cybersecurity has become critically important to nation states. Nation states rely on computerized information systems for national defense, infrastructure, banking systems, and e-commerce both within their own borders and in their relationships with other nation states. Yet there are few international laws that specifically address the intersection of international relations and cybersecurity. As is usually the case with emerging technology, the law is lagging behind the times.

In the meantime, policymakers have been trying to extend traditional laws and customs to cybersecurity with varying degrees of success. Cybersecurity does not fit neatly into the pre-existing frameworks due to its amorphous and constantly evolving nature. In the realm of cyberwarfare, for example, policymakers have turned to general principles covering the use of force. But these principles were designed with conventional warfare in mind and are not fully compatible with cyberwarfare.

See also "*Prosecuting Borderless Cyber Crime Through Proactive Law Enforcement and Private Sector Cooperation*" (Mar. 2, 2016).

Cyberwarfare

Cyberwarfare broadly describes warfare that takes place in or through cyberspace (i.e., a proprietary communications network or computer system), but there is no consensus as to the precise meaning or scope of the term.[1] One commentator has defined cyberwarfare as "any military operation designed to attack, deceive, degrade, disrupt, deny, exploit, and/or defend through the information infrastructure with a desired kinetic effect." The kinetic effect may include both a "physical change to the environment" and a "change in the enemies' decision-making."[2]

However cyberwarfare is defined, it has become a very real way to engage in war. Cybersecurity is the newest frontier in defense, and in June 2016, NATO formally recognized cyberspace as the fifth domain of warfare, adding it to the traditional domains of land, sea, air, and space.[3] As NATO Secretary-General Jens Stoltenberg stated, it is impossible to imagine a military conflict today without a cyber dimension.[4] In one celebrated example, Israel used its cybersecurity expertise to disable Syria's air-defense system, allowing Israeli fighter jets to fly undetected into Syrian airspace and destroy a nuclear materials facility.[5]

Despite the ubiquity of cyberwarfare, there is no specific treaty or international convention that governs it. In the absence of any such cyber-specific law, commentators have instead looked to the existing laws of traditional armed conflict.[6] These traditional rules are found primarily in the Charter of the United Nations (U.N. Charter), and U.N. groups of experts have urged their applicability to nation-state behavior in cyberspace.[7]

See also "*In a Candid Conversation, FBI Director James Comey Talks About the 'Evil Layer Cake' of Cybersecurity Threats*" (Jun. 3, 2015); and "*Comey Discusses Cooperation Among Domestic and International Cybersecurity Law Enforcement Communities*" (Jun. 17, 2015).

The Use of Force

International law condemns the use of force. Article 2(4) of the U.N. Charter requires United Nations member states to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[8] This principle is subject to two exceptions: (1) Article 42 provides that the Security

Council "may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security"; and (2) Article 51 recognizes the "inherent right of individual or collective self-defence if an armed attack occurs." Commentators have also suggested a third exception: the right to use force "to avert an overwhelming humanitarian catastrophe."[9]

In traditional warfare, the use of force refers to actions that cause injury or death to humans or physical damage to tangible property, but not to actions constituting economic coercion.[10] While this framework is easy to apply to traditional war, it is far more difficult to apply to cyberwarfare.[11] Cyberwarfare includes a wide variety of measures, ranging from serious attacks on critical infrastructure (e.g., disabling electric, emergency services, telecommunications, or traffic infrastructure) to minor annoyances (e.g., defacing a government website, disabling non-critical websites through short-lived distributed denial of service attacks).

In 2013, the NATO Cooperative Cyber Defence Centre of Excellence ("CCDCOE"), a diverse group of international experts,[12] published the Tallinn Manual on the International Law Applicable to Cyber Warfare. In the Tallinn Manual, the CCDDOE provides eight non-exhaustive factors that may be used to determine if a cyber attack constitutes a "use of force":

- *severity:* the nature and extent of the harm. Consequences involving physical harm to individuals or property will in and of themselves qualify the act as a use of force;
- *immediacy:* the time it takes for consequences to manifest;
- *directness:* the degree of attenuation between the initial act and its consequences;
- *invasiveness:* the degree to which cyber operations intrude into the target State or its cyber systems contrary to the interests of that State;
- *measurability of effects:* the extent to which the consequences are apparent.
- *military character:* the degree to which cyber operations are tied to military operations;
- *state involvement:* the extent to which the State is involved in the cyber operations; and
- *presumptive legality:* "International law does not prohibit propaganda, psychological operations, espionage, or mere economic pressure per se. Therefore, acts falling into these and other such categories are presumptively legal."[13]

In the Tallinn Manual 2.0, a follow-on work to its original analysis, the CCDCOE confirmed that its "analysis rests on the understanding that the pre-cyber era international law applies to cyber operations, both conducted by and directed against states." The original Tallinn Manual focused on the most severe cyber operations – those that "violate the prohibition on the use of force in international relations, entitle states to exercise the right of self-defense, and/or occur during armed conflict." The Tallinn Manual 2.0 extends the analysis to the more common cyber incidents that fall below the thresholds on the use of force or armed conflict, but which states encounter on a day-to-day basis.[14]

Commentators have also debated whether a cyber attack is an "armed attack" that justifies the use of self-defense under Article 51.[15] This debate is complicated by the fact that, even in the context of traditional warfare, the definition of an "armed attack" is unclear. The International Court of Justice (ICJ) has issued several decisions suggesting that only the gravest uses of force rise to the level of armed attacks, but it has not provided any additional guidance as to what that means.[16]

Moreover, even if the threat of an armed attack exists, it may not justify acting in self-defense. Numerous scholars have argued that the right to self-defense requires three conditions: necessity, proportionality, and immediacy. In the words of then-Secretary of State Daniel Webster, who first set forth these principles in 1842, a state may act in self-defense only when the "necessity of that self-defence [is] instant, overwhelming, [and] leaving no choice of means, and no moment for deliberation."[17]

As a practical matter, it is difficult to apply Webster's principles to cyber attacks. A state typically acts out of necessity when it is threatened by a known assailant, but cyber attacks hit without any prior notice or threat, and they are often carried out by unknown hackers.[18] Even determining the country of origin can be difficult, as hackers can mask that information or operate out of remote locales. Immediacy is another problem, since cyber attacks may not have immediate effects – e.g., the implantation ofmalicious software that takes time to work or lies dormant until activated.

At bottom, the question of what constitutes the "use of force" – or an "armed attack" giving rise to the right to self-defense – remains difficult to answer in the context of cyberwarfare. While it is widely recognized that traditional laws of armed conflict apply to cyberwarfare, drawing analogies between traditional warfare and cyberwarfare continues to be problematic in practice.

Other International Treaties

Cyberwarfare may also implicate other principles and sources of international law. For example, cyber attacks may fail to discriminate between civilian and military targets, a core principle of traditional warfare.[19] This principle is enshrined in the Geneva Conventions, Additional Protocol I (Protocol I), Article 48:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[20]

Although Protocol I has not been universally ratified – notable exceptions include the United States, Israel, Iran, Pakistan, India, and Turkey – it is generally accepted that Article 48 of Protocol I "reaffirms a general rule of international law that has never been questioned despite being frequently disregarded in State practice."[21] Numerous commentators have urged that this general rule of international law be extended to cyberwarfare, with the idea that cyber attacks can be limited to government or military targets without causing collateral damage to civilian targets.[22]

Cyberwarfare could potentially be subject to other laws of armed conflict, including, for example, the Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict (1954) (the Cultural Property Convention). The Cultural Property Convention defines cultural property as:

> (a) movable or immovable property of great importance to the cultural heritage of every people, such as monuments of architecture, art or history, whether religious or secular; archaeological sites; groups of buildings which, as a whole, are of historical or artistic interest; works of art; manuscripts, books and other objects of artistic, historical or archaeological interest; as well as scientific collections and important collections of books or archives or of reproductions of the property defined above;
> (b) buildings whose main and effective purpose is to preserve or exhibit the movable cultural property defined in sub-paragraph (a) such as museums, large libraries and depositories of archives, and refuges intended to shelter, in the event of armed conflict, the movable cultural property defined in sub-paragraph (a);
> (c) centers containing a large amount of cultural property as defined in sub-paragraphs (a) and (b), to be known as "centers containing monuments."[23]

These provisions could apply to cyberwarfare in two ways. First, digital reproductions of pre-existing cultural property and born-digital works that exist only in digital form could qualify as cultural property under Article 1(a).[24] Second, data centers containing servers hosting such cultural property could qualify as cultural property under Article 1(b).

See also "*How GE's Global CPO Approaches Shifting Regulations With Dynamic Implications*" (Aug. 24, 2016).

Seth Rothman is a litigation partner at Hughes Hubbard & Reed LLP who focuses his practice on complex commercial litigation, arbitration, products liability and mass torts. He has more than 25 years of experience representing clients in courts throughout the country, in arbitrations, and before other tribunals. He has been involved in high-stakes matters on behalf of leading pharmaceutical companies, financial institutions, and multinational corporations. Rothman is co-chair of the firm's Asia Pacific practice group and has significant experience representing Japanese clients in international arbitrations and U.S. litigation. Seth is also co-chair of the firm's data privacy and cybersecurity practice group and co-chair of the eDiscovery Practice Group. In these capacities, he has advised clients on compliance, cybersecurity, data privacy, document management, eDiscovery, and litigation preparedness. He writes and speaks regularly on cybersecurity, data privacy, and eDiscovery.

Andreas S. Baum is an associate in Hughes Hubbard & Reed's Litigation department and a member of the firm's arbitration & alternative dispute resolution practice. Baum worked as an analyst at a boutique strategy consulting firm in Boston, and can apply both technical and business skills to complex issues in litigations and arbitrations. He focuses his practice on international disputes and has extensive experience with issues involving the application of public international law. Before joining Hughes Hubbard & Reed, Baum served as a legal intern at the International Criminal Tribunal for Rwanda, where he assisted in the prosecution of war crimes and crimes against humanity.

The authors are grateful for the assistance of Casey Duffy in preparing this article.

[1] *See, e.g.*, Mathew Borton et al., "Cyberwar Policy," 27 J. Marshall J. Computer & Info L. 303, 304 (2009-2010); John Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield," 29 J. Marshall J. Computer & Info. L.1, 7 (2011-2012) ("However, it remains unclear what a cyber war is within the definition of international law. This is due in part to the fact that there is considerable disagreement about whether a cyber war has in fact occurred anywhere in the world.").
[2] Mathew Borton et al., supra note 2, at 305, 314.
[3] Julian E. Barnes, "*NATO Recognizes Cyberspace as New Frontier in Defense*," Wall Street Journal., June 14, 2016, (last visited Jan. 29, 2017).
[4] *Id.*
[5] *See, e.g.*, Sharon Weinberger, "*How Israel Spoofed Syria's Air Defense System*," Wired (Oct. 4, 2007), (last visited Feb. 6, 2017).
[6] *See, e.g.*, Matthew Hoisington, "*Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*," 32 B. C. Int'l & Comp. L. Rev.439, 441; Tom Papain, "North Korea and Cyberwarfare: How North Korea's Cyber Attacks Violate the Laws of War," 11 J. Korean L. 29 (2011-2012); International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, "Tallinn Manual on the International Law Applicable to Cyber Warfare", at 29-41 (Michael N. Schmitt ed., Cambridge Univ. Press 2013) (Tallinn Manual).
[7] See United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", U.N. Doc. A/68/98 at 8 (June 24, 2013); see also United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," U.N. Doc. A/70/174 at 12 (July 22, 2015).
[8] U.N. Charter art. 2, para. 4.
[9] Michael Wood, "*International Law and the Use of Force: What Happens in Practice?*," 53 Indian J. of International Law 345, 352 (2013).
[10] See Hoisington, supra note 7, at 447 (citing Vida M. Antolin-Jenkins, "*Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?*", 51 Naval Law Review 132, 134-35 (2005)).
[11] *See, e.g.*, John Dever and James Dever, "*Cyberwarfare: Attribution, Preemption, and National Self Defense*", 2 J.L. & Cyber Warfare 25, 30 (2013).

[12] According to the CCDCOE's website (https://ccdcoe.org/), "Belgium, the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the United States are signed on as Sponsoring Nations of the NATO Cooperative Cyber Defence Centre of Excellence. Austria and Finland have become Contributing Participants and Sweden is well on its way of doing the same. The Centre is staffed and financed by member nations and is not part of NATO's military command or force structure."
[13] *Tallinn Manual, supra* note 7, at 49-51.
[14] NATO Cooperative Cyber Defence Centre of Excellence,Research (last visited Feb. 6, 2017).
[15] *See, e.g.*, Dever and Dever, *supra* note 12, at 28 ("Despite the emphasis on the importance of cybersecurity in policy documents, there has been little discussion about when a cyberattack on the U.S. or conducted by the U.S. on another country becomes more than just interference in another country's affairs, and reaches the level of an armed attack that can be responded to in self-defense."); *see also* Papain, *supra* note 7, at 42.
[16] *See* Dever and Dever, *supra* note 12,at 31-32.
[17] Letter from U.S. Secretary of State, Daniel Webster to Lord Ashburton (Aug. 6, 1842) (last visited Jan. 29, 2017).
[18] See Hoisington, supra note 7, at 451.
[19] Ruth Wedgwood, "Proportionality, Cyberwar, and the Law of War," 76 Int'l L. Stud. Ser. U.S. Naval War C. 219, 221 (2002) ("Over the centuries, the operational harshness of warfare has been challenged by the ideals of proportionality and discrimination. These ideals of the profession of arms, implemented by military commanders and their legal advisors, ask for a critical distinction between civilian and military targets, and teach that military advantage always must be measured against civilian loss. Cybernetic conflict may pose new hazards to civilian safety, taxing our traditional notions of the division between the battlefield and civilian life.")
[20] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3.
[21] Fausto Pocar, "To What Extent Is Protocol I Customary International Law?" 78 Int'l L. Study. 337, 345 (2002).
[22] *See, e.g., Tallinn Manual, supra* note 7, at 113; Papain, supra note 7, at 47-49.
[23] Convention for the Protection of Cultural Property in the Event of Armed Conflict art. 1, May 14, 1954, 249 U.N.T.S. 240.
[24] *See* Heather Harrison Dinniss, "*Cyber Warfare and the Laws of War*" 230-32 (Cambridge University Press 2012).