Crossing the Line: The Law of War and Cyber Engagement - Applying the Existing Body of Law to This New National Security Threat

Sandra Hodgkinson

Follow this and additional works at: https://scholar.smu.edu/til

Recommended Citation
https://scholar.smu.edu/til/vol51/iss3/10

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in International Lawyer by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
I. Introduction

Over the past decade, there has been a growing awareness of the threat caused by the increasing reliance on cyberspace and the risk to national security it brings. Cyber “attacks” against the U.S. government can be launched by a variety of actors with different motivations for intelligence collection, data or intellectual property theft, espionage, or ultimately to threaten our national security by offensively crippling a military asset or critical U.S. infrastructure. Notwithstanding, a large majority of cyber incidents are often aimed at data theft for personal gain, rather than launched by would-be enemy nations as an instrument of warfare. Whatever the motivation, the damage from a cyber-attack can be serious, and can put our national interests at risk.

When we talk about “crossing the line,”—we are discussing at what point the law of armed conflict is triggered in a cyber “attack” which would justify a lawful military response. This is a very narrow subset of current cyber events, and it requires its own set of laws and policies. The last ten years has seen a significant shaping of the law in this area and even a growing consensus between the U.S. and the international community as to when a cyber-event has crossed the threshold into becoming an “armed attack.”

This short article will, at a very high level, discuss the threshold jus ad bellum question that other panelists are also addressing. In addition, this article will focus on what the practical effect of a cyber “armed attack” means and how some of the law of armed conflict principles may apply. Volumes can be written about these topics, but the goal here, in this panel, is to lay them out for discussion.

1. This presentation was part of a panel discussion during the ABA Spring of the International Section on April 26, 2017 in Washington, DC. Ms. Hodgkinson is a member of the ABA Cyber Task Force, retired Captain from the U.S. Navy JAGC Corps reserves, and former member of the U.S. Government’s Senior Executive Service with positions at DoD, State Department and the National Security Council. She currently works as a Senior Vice President in the defense industry at Leonardo DRS.


What does it mean to be in an “armed conflict” in a cyber-context? Clearly, cyber bombs are not dropping from the sky, but there is a significant threat to national security that arises from a cyber-war. And for those individuals who engage in a cyber-attack, what is their status? Are they lawful “combatants” entitled to prisoner of war status upon capture, and possessing the greatest right of all in wartime—the right to kill? Or, alternatively, are they more akin to the unprivileged belligerents we have seen through the more recent asymmetrical conflicts with Al Qaeda and other terrorist organizations? Are individual “hacktivists” capable of launching a cyber-attack? How do the unique challenges of attribution in cyber space affect the ability of nations to adequately deter, and respond to, cyber threats? And how do the time-tested principles of necessity and proportionality apply to cyber-attacks which have crossed the line? As in wars of the past, does state sovereignty afford nations the right to be “neutral” in these cyber conflicts, even if a cyber-event passes through their networks? And once the line has been crossed, how does that impact the applicability of other cyber-crime laws, espionage laws, and sabotage laws? These are all questions that this panel discussion and supporting paper are designed to address.

This presentation will first provide a quick summary of key developments in the law governing cyber-attacks. Then, it will address the practical implications of being in a cyber-war and discuss the status of individuals involved in this war. Third, it will address the principles of necessity and neutrality. Fourth, the article will discuss the role of state sovereignty and neutrality. Finally, the article will address the applicability of other laws. In its conclusion, the article will raise concerns about areas where the law of armed conflict remains unclear and imperfect in addressing this new threat emanating from the cyber world.

II. Growing Consensus That Cyber Attacks May be Acts of War

In July 2011, the U.S. Department of Defense (“DoD”) launched its first official cyber strategy, and listed cyber space as an “operational domain,” like sea, air, space and land. President Obama, consistent with his National Security Strategy, signed a classified presidential directive related to cyber operations, PPD-20 the following year, which recognized the growth in cyber incidents and threats against the U.S. government. PPD-20 promoted a whole-of-government approach, establishing principles and processes for cyber operations to enable more effective planning, development, and use of our capabilities. PPD-20 aimed to take the least action necessary to mitigate threats and emphasized network defense and law

6. Id.
enforcement as the preferred courses of action. The 2011 DoD cyber strategy, coupled with White House international strategy, together have provided a framework for how the DoD addresses cybersecurity problems with business, civilian government, and by working with international allies to establish international norms. In April 2015, the DoD updated its strategy, providing more detail and clarity, which included a description of the newly developed DoD Cyber Mission Force, created to defend DoD networks, protect U.S. homeland and vital interests, and enable full-spectrum cyber capabilities for military operations.

Several of these new policies have helped shape the overall approach to cyberspace, but what happens when a foreign government uses cyber space to directly attack another country? The 2007 computer network attack on Estonia, generally attributed to the Russian government, was the first reported cyber-attack by one country on another. Heavily reliant on the Internet in cyber space, Estonia’s newspapers were attacked; the banks, police, and government were attacked by botnets, immediately overwhelming the government systems and emergency response systems. Similar computer network attacks from Russia into Georgia in 2008 were also alleged and were more complex, including defacement of government websites and altering news coverage. While Russian government involvement has not been officially proven in either the Estonian or Georgian attacks, several factors have at least demonstrated Russian government complicity in the attacks. As NATO and EU debated whether and how to respond to “attacks” such as these—whether as an armed attack that would trigger collective self-defense under article 5 of the NATO Charter, or something else—Tallinn, the capital of Estonia, became the epicenter for the study of cyber-attacks. From 2009 to 2012, a group of twenty international experts at the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) drafted the Tallinn Manual, which focused on the applications of international law to cyber operations and

---

7. Id.
cyber warfare. Specifically, the Tallinn Manual analyzed when states could respond to cyber-attacks as “armed attacks,” triggering the right of self-defense under international law. Although it has not become a binding legal document, the Tallinn Manual has become an important source of law on this subject.

The U.S. State Department Legal Advisor, Harold Koh, was the first to lay out an official government position declaring that a cyber-attack could be an armed attack. In his speech at a U.S. Government Cyber Conference in September of 2012, he articulated several factors in that determination, which are laid out separately below. In September 2014, NATO followed the U.S.’ lead and also determined that a cyber-attack could justify invocation of Article 5 of the NATO treaty. Under Article 5, the NATO collective self-defense provision, a significant enough cyber-attack on one member of NATO would be considered an attack on them all, justifying a military response. Soon after NATO, a U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, the only U.N. group studying the issue, also affirmed the right of self-defense under Article 51 of the U.N. Charter. Most recently, in October 2017, EU nations drafted a document stating that cyber-attacks can be acts of war, signaling growing solidarity against countries like Russia and North Korea, which has also been alleged to engage in cyber-attacks. As a result, there is sufficiently broad-based international consensus that cyber-attacks can be considered acts of war in appropriate circumstances.

In March 2016, the U.S. Justice Department claimed that members of Iran’s Islamic Revolutionary Guards Corps had launched an online attack against critical U.S. infrastructure in 2013 by entering the computerized command and controls of a dam in New York City. The Iranians also

16. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, 42 (Michael N. Schmitt ed., Cambridge Univ. Press 2013) [hereinafter Tallinn Manual].
17. Id.
24. Dustin Volz & Jim Finkle,
allegedly attacked the New York Stock Exchange, AT&T, and several financial institutions, demonstrating the widespread capabilities of their reach and the vulnerability of all of our institutions to cyber-attacks from foreign governments. Attorney General Lynch worried that an attack on critical infrastructure, particularly like this attack on the computerized systems on a dam, could have a large impact on the safety and welfare of U.S. citizens. The need to ensure that all our government’s assets are protected from cyber-attacks is more critical than ever. What about future attacks on the water supply, transportation infrastructure, hospitals, or larger dams? The February 2017 Tallinn Manual 2.0 analyzes the law applicable to attacks that may not rise to the level of “armed attack,” helping to draw additional distinctions. Most recently, there have been a series of alleged sonic cyber-attacks, accompanied by a high-pitched whine, directed at U.S. Embassy personnel in Cuba. These attacks have reportedly resulted in physical damage to at least twenty-two personnel, including hearing, visual, cognitive, and other sleep and balance related problems. Would such attacks, if we could determine who was carrying them out, be considered “acts of war?”

III. Attacks That “Cross The Line”

What does it mean to say that a “cyber-attack” has crossed the line into the threshold of armed conflict? There have been several different definitions over time, all of which have morphed into an understanding that the effects must be permanent and serious. The term “cyber-attack” has been used very broadly to describe “any action taken to undermine the functions of a computer network for a political or national security purpose.” But Rule 30 of the Tallinn Manual defines a “Cyber Attack” more narrowly as “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.” Consistent with the Tallin Manual, in 2012, the U.S. was the first government to publicly state that a cyber-operation resulting in “death, injury, or significant destruction” would likely be

24. Id.
28. Id.
considered an illegal use of force, potentially triggering the right of self-defense under article 51 of the U.N. Charter. The legal test on whether a cyber-incident has crossed the line into an armed conflict is “effects-based,” focusing on the nature and extent of the injury and damage caused on a case-by-case basis and whether it has caused death or destruction. An attack would generally not be considered to have crossed the line when it is reversible or temporary. These definitions have led at least one author to conclude that the attacks in Russia and Georgia, as described above, did not meet the threshold of armed attack, as they did not cause permanent physical damage.

Harold Koh, in declaring the U.S. position on this definition, stated that in assessing whether an event constituted a use of force in cyberspace, a country must evaluate several factors, including: (1) the context of the event; (2) the individual committing the act; (3) the target and location of the attack; (4) and the effects and intent of the act, among other possible issues. He cited specific acts that would constitute a use of force to include cyber operations that would trigger a nuclear plant meltdown, open a dam above a heavily populated area that causes destruction, or operations that disable air traffic control resulting in airplane crashes. Clearly, an attack that brings the same physical damage that dropping a bomb or firing a missile would should also easily meet this threshold and be considered a use of force.

In contrast, the collection of intelligence or exploitation of an enemy, known as Computer Network Exploitation (CNE), using cyber capabilities is not generally considered to be an armed attack, as it does not cause physical or lasting damage. Cyber espionage, psychological operations, and propaganda are likewise generally not considered to be armed attacks. Cyber espionage, under the Tallinn Manual, is a clandestine, or under false
pretenses, act that uses cyber capabilities to gather information and communicate it to an opposing party. The Tallinn Manual does, however, indicate that actions taken by a state’s intelligence agency, or an individual who acts with a nexus to the state, can be attributed to the state and can be considered a use of force.

IV. What Does War Mean and Who Are the Combatants?

Why is there so much discussion about whether a cyber-attack is considered an “act of war”? As a practical matter, what does that mean? Once the threshold for an “armed attack” has been met, we have “crossed the line” into the jus ad bellum world, a different legal regime now applies, and a uniformed military response is lawful in self-defense. Article 51 of the U.N. Charter permits nations to respond to armed attacks in their self-defense, and as discussed above, there is growing consensus of this right.

The individuals responsible for the attack can be considered “combatants,” which means they can be considered as legitimate military targets. In the cyber world, there are several different actors that can carry out cyber-attacks. Among these are militaries, other government agencies, private companies, terrorist organizations, and individual actors sometimes referred to as “hacktivists.” The facts and circumstances surrounding the individual engaging in a possible cyber-attack are central to determining whether that individual can be considered a combatant, and whether the combatant’s status is lawful or unlawful.

In an armed conflict generally, to be considered a lawful combatant, a combatant must be either a member of a regular armed group, or a member of an irregular armed force. Members of a regular armed enemy force, carrying out cyber-attacks as one of their means and methods of warfare, would generally be considered lawful combatants. Moreover, cyber warfare, as long as it is conducted lawfully, can be a legitimate, effective, and precise tool for members of an armed force. In fact, many cyber scholars have recommended that nations choosing to engage in computer network attacks should use only members of their regular armed forces in furtherance

40. Id. at 193.
41. Id. at 51.
42. U.N. Charter art. 51.
43. See Watts, supra note 13, at 241.
45. Id.
47. Id.
of these activities, to ensure the activity is viewed as lawful. If members of a regular armed group carry out cyber-attacks in a manner that is unlawful, however, then they can be tried by a military commission or other national court for any crimes they commit during the conflict, just like any other crime.

For members of an irregular armed group engaged in cyber-attacks, they must meet four criteria to be considered as lawful combatant, as in any conflict. The must be commanded by a person responsible for his subordinates, wear a fixed insignia or emblem recognizable at a distance, carry weapons openly, and follow the laws of war. Failure to meet these four standards results in a classification of “unlawful combatant” or “unprivileged belligerent,” and does not afford the individual the full panoply of protections under the Geneva Conventions—including most specifically, the rights to Prisoner of War (POW) Status, or the right to be considered a belligerent and be eligible to lawfully “kill” enemy belligerents.

For a cyber-belligerent who is not connected to a traditional armed enemy force of another nation, they will generally fail to meet these four criteria in a number of ways. The lack of responsible command and failure to wear a distinctive insignia recognizable from a distance will both be very difficult to overcome. A cyber-attacker or “hacker” generally does not distinguish himself, but rather, blends in with the civilian population to launch attacks that are not attributable. Because a computer is generally not going to be considered a “weapon,” or one that could be carried openly, a determination would need to be made that a cyber-attack could be treated as a “weapon” when used to cause harm or as a threat to a nation’s security. It would still nonetheless be difficult to determine what carrying this cyberspace weapon “openly” would entail. Similarly, a cyber-attacker or “hacker” rarely


50. Geneva Convention (III) Relative to the Treatment of Prisoners of War, supra note 46.

51. Id.; see also Regulations concerning the Law and Customs of War on Land, Hague Convention, Oct. 18, 1907; Project of an International Declaration Concerning the Laws and Customs of War, Brussels Regulation, Aug. 27, 1874 (for discussion of the development of these customs under the law of armed conflict).


53. See ANICEE VAN ENGELAND, CIVILIAN OR COMBATANT? A CHALLENGE FOR THE 21ST CENTURY, 45 (2011); Knut Ipsen, Combatants and Non-Combatants, in THE HANDBOOK OF HUMANITARIAN LAW IN ARMED CONFLICTS 65 (Dieter Fleck ed., 1995); Watts, supra note 9, at 241–42.

54. See d’Urso, supra note 52.
acknowledges who they are, making it difficult to claim that they are carrying their computer weapon “openly.” Is it enough to claim the attack once it is launched, or put a label on it (e.g. “From ISIL with Love”), or does it need to be claimed before the attack begins to make it “open”? That would be unlikely, given the surprise nature of most cyber-attacks and the rapid speed at which they occur. One of the key challenges of cyberspace is the lack of attribution, because there is no label on the weapon, like on a traditional bomb or other type of return address. While these characteristics of “distinction,” like being able to see and distinguish an attacking enemy, have been blurred during 20th century conflict where shots and missiles are often fired from a significant distance away, the criteria have nonetheless remained constant under the law.

The last part of the test is that the belligerent follow the law of armed conflict, and therefore the cyber-attack can only be launched against a lawful military objective versus a civilian target or population. Many cyber-attacks that have been seen openly have specifically targeted the civilian population or computer networks, and accordingly, most belligerents would fail to meet this part of the test as well. In nearly all the current attacks we are seeing, these characteristics—lack of attribution or distinctive insignia, failure to carry weapons openly, and attacks launched at civilian objects, versus military ones—ensure that the cyber combatant is at best an unlawful combatant or unprivileged belligerent.

According to the Tallinn Manual, when unlawful combatants take part in hostilities, they forfeit their own protection from such attacks while they participate in the conflict and may be lawfully attacked. This means that cyber attackers may be targeted lawfully by a legitimate armed force exercising self-defense, even though they are not privileged belligerents. Furthermore, contrary to popular belief, a cyber-attack does not need to be countered by a cyber-response, enabling the military force acting in self-defense to use any lawful method of warfare. According to the International Committee of the Red Cross (ICRC), three criteria must be met for a civilian to be considered a combatant because the individual is directly participating in hostilities:

1. The act must cause harm to the military operations or military capacity of a party to an armed conflict or, alternatively, inflict death, injury, or destruction on persons or objects protected against direct attack (threshold of harm);

55. Id.
57. Id.
58. Watts, supra note 13, at 241.
59. Tallinn Manual, supra note 16, at 104 (deriving this rule from Additional Protocol I, Geneva Conventions, art. 51, at para. 3, which is lawfully binding on States party and is considered customary international law by others).
60. Koh, supra note 18.
2. There must be a direct causal link between the act and the harm (direct causation); and
3. The act must cause harm in support of a party to the conflict and to the detriment of another (belligerent nexus).

These criteria are the same in the cyber context and need to be applied to the facts and circumstances of the attack. Further, the ICRC has argued that time and continuity are other elements that must be considered when categorizing a civilian as a lawful military target.

Beyond the standard for a civilian “directly participating” in the conflict above, members of an organized armed group who are engaged in a “continuous combat function” can also be targeted at any time. In the context of cyber-attacks, one author has described “members of an organized group” to include chat rooms or other internet groups. Individuals who provide a “continuous combat function” are administrators and organizers of a cyber community who give its members permission to use its services, other support staff that provides services and technical support, advisors, and the supporting staff that provide services and technical support, and “senior members or moderators” (distinguished from the others by the quality of their contribution to the community). Accordingly, cyber combatants are not in a law-free zone when the law of armed conflict can be applied. Notwithstanding, there may also be criminal laws that criminalize cyber-attacks as well that are applicable.

V. Jus In Bello Rules Of Necessity And Proportionality

A legitimate exercise of self-defense must comply with the principles of necessity and proportionality to be lawful. A state meets the requirement of necessity when it cannot settle the dispute by any other peaceful means and must resort to the use of force. In the cyber context, this is no different. A state will have to articulate the case that it must resort to self-defense, because there is no peaceful way of preventing the attack. Given the time period during which a cyber-attack occurs and the potential severity of the attack, complying with the principle of necessity will not be difficult for the types of cyber-attacks that cross the line into jus ad bellum. Furthermore, the concept of anticipatory self-defense may come into play in
these cyber events as well, when a cyber-attack is imminent.\textsuperscript{68} Anticipatory self-defense, as articulated by Secretary of State Webster in the Caroline affair of 1836, exists when the necessity of self-defense is “instant, overwhelming, and leaving no choice of means, and no moment for deliberation.”\textsuperscript{69} Again, due to the time sensitive nature of cyber-attacks and lack of attribution, there may be times when a nation needs to act in anticipatory self-defense of an impending cyber-attack.

On the concept of proportionality, a state will meet the legal test of proportionality when it limits the use of self-defense to defeat the ongoing attack or deter a future attack.\textsuperscript{70} Proportionality also prohibits attacks that are expected to cause incidental life, injury to civilians, or damage to civilian objects that are excessive in comparison with the concrete military advantage to be gained.\textsuperscript{71} In the cyber world, proportionality will require an assessment of the effects of cyber weapons on military and civilian personnel and infrastructure, the physical damage that cyber-attack may cause, and the potential effects of such an attack on civilian objects, including civilian computers that may be linked to computers that are considered to be lawful military objectives.\textsuperscript{72} In assessing proportionality, beyond the damage from the cyber-attack, commanders need to also consider the indirect effects that the cyber-attack may cause, which are second and third order effects that may occur through intermediate events.\textsuperscript{73} These indirect effects, however, must be expected in order for a commander to be held accountable.\textsuperscript{74} Lastly, to be a proportional response, a cyber-attack does not need to be countered with only cyber capabilities, which is to say that a cyber-attack can be countered with any other lawful and proportional military action.\textsuperscript{75}

In the armed conflict context, any military response to a cyber-attack must also be subject to a determination as to whether the weapon itself is lawful.\textsuperscript{76} Generally, a weapons review would determine whether a particular weapon is inherently indiscriminate, which means it could never be used as it does not comply with the principles of necessity and proportionality as discussed above.\textsuperscript{77} Further, each specific use of a particular weapon must also be

\textsuperscript{68} Tallinn Manual, supra note 16, at 63.
\textsuperscript{70} Graham, supra note 66, at 88.
\textsuperscript{71} Int’l Comm. of the Red Cross, Additional Protocol I to the Geneva Conventions, art. 51(b); Eric Talbot Jenson, Cyber Attacks: Proportionality and Precautions in Attack, 89 Nat’l L. Stud. 198, 204 (2013).
\textsuperscript{72} Jenson, supra note 71, at 205; Koh, supra note 18, at 5.
\textsuperscript{73} Joint Chiefs of Staff, Joint Pub. 3-60, Joint Targeting, at I-10 (2007).
\textsuperscript{74} Jenson, supra note 71, at 206.
\textsuperscript{75} Koh, supra note 18, at 5.
\textsuperscript{77} Koh, supra note 18, at 65; see also Tallinn Manual, supra note 16, at 153.
analyzed to ensure that its use complies with the law of armed conflict.78 The U.S. military permits the use of offensive operations in cyberspace which damage or cause destruction as long as they are conducted in accordance with the law of armed conflict.79 Accordingly, there are cyber weapons that are not inherently indiscriminate.80 Cyber weapons have been compared to Precision-Guided Munitions because they have the ability to cause damage to carefully selected and tailored objects.81 This allows cyber weapons to minimize both damage to the individuals delivering the weapon, as well as to innocent civilians not taking part in the conflict, which could be a potential benefit of their use.82 A tailored use of cyber weapons by a military force, for example, is preferable to an attack that causes excessive damage to an unintended target and could cause an escalation of a conflict.83 In the case of the Estonia and Georgia attacks, as examples, the cyberattacks did not result in loss of life or cause significant damage beyond their intended target.84 But there is a general perception that these types of attacks do cause damage to non-military computers and civilians.85

VI. State Sovereignty And Neutrality

While the concepts of state sovereignty and neutrality apply in cyberspace, the challenge of attribution makes them even more complex. In the cyberattacks in Estonia, Georgia, and Stuxnet, none of the sovereign governments alleged to have committed the attacks have admitted responsibility for them.86 The attribution issue, therefore provides both a sword and a shield for governments. They are often unable to determine in a timely manner whether and when an attack was launched from within their territory (to accept responsibility), and this very uncertainty affords states with the ability to initiate their own attacks knowing full well that timely attribution will be challenging.87

States have the right develop their cyberspace in any manner free from interference by other nations.88 The Tallinn Manual sets forth the principle that sovereign states have control over their cyberspace.89 This affords

78. Id.
82. Id.
83. Bellovin et al., supra note 80.
84. Id.
85. See Acton, supra note 81.
87. Id.
88. Id. at 288.
States the right to exercise territorial jurisdiction over cyberspace activities within their country and to protect their internal cyber space from threats emanating from outside of the State. Not every cyber intrusion into a foreign nation will constitute a violation of sovereignty, however, it is generally considered that there must be some degree of damage. For example, cyber espionage is an act that is not considered to be a violation of sovereignty as espionage itself is not considered to be unlawful under international law. As espionage does not generally cause damage, this makes sense. The U.S. articulated in its 2011 International Strategy on Cyberspace that activities such as network attack, exploitation of networks, and other hostile acts that might threaten peace and security or harm civil liberties and privacy could be considered violations of sovereignty. Consistent with the growing body of law in this area, there must be some damage to violate sovereignty.

As part of this right to exercise territorial sovereignty over their cyberspace, states are also considered to have a duty to prevent their territory from being used for cyberattacks against other states. These duties may include the need to increase law enforcement through passing more criminal laws, investigating possible violations, and prosecuting perpetrators.

In a traditional state-on-state conflict, state sovereignty prevents states from using force without a self-defense justification under article 51 of the U.N. Charter, a U.N. Security Council resolution, or the consent of the nation in question. When you have crossed the line in an armed conflict in the cyber context, a state must still take the sovereignty of other nations into account. The jurisdiction of the state being attacked will govern the activities in that state. In addition, however, an offensive cyber-attack conducted against one state may also have effects on a third state, due to the interconnected nature of cyberspace. In fact, one of the challenges to state sovereignty with cyberattacks is an email or cyber malware that may be broken up into data packets and transmitted through a number of third states without the sender knowing about it or being able to control it. The transit states are not, and would not want to be, held accountable for data sent through their territory, and likewise, the sending state would not want to be held accountable for violating the sovereignty of the transit states. Accordingly, while states have an affirmative obligation to prevent their

91. Id. at 11.
93. Heintschel von Heinegg, supra note 90, at 12.
94. Jensen, supra note 86, at 298.
95. U.N. Charter art. 51.
96. Koh, supra note 18, at 6.
97. Id.
98. Jensen, supra note 86, at 280.
99. Id.
territories from being used for attacks against other states and must take action against those who do, knowledge or presumptive knowledge of the attack is necessary.100

Sovereign states are also legally responsible for cyber activities carried out by private individuals considered to be “proxy actors,” who are acting under the direction, control, or instruction of a State.101 As long as the State exercises sufficient control over an individual engaged in illegal cyber activity, the State will assume responsibility for the act.102 States also have an obligation not to allow their state to be used for an act that violates the territorial integrity of another state, even in the cyber context.103 Notwithstanding, the majority of the Group of Experts drafting the Tallinn Manual did not believe that the mere failure of a State to police its own territory, without providing some substantial support or cyber defenses, would constitute a use of force.104 While again, the attribution challenges of cyber space make determining when the State is actually involved in a cyberattack through their own actors or proxy actors, the customary law of armed conflict has more recently added additional authority to take action against a state that is “unwilling or unable” to prevent a cyberattack from occurring.105 While the “unwilling or unable” test may not have been applied openly in the cyber context yet, its acceptability by the U.S. and other key allies in the use of force arena indicates that it could ultimately be applicable for a cyberattack that crossed the line into armed conflict. If the current sonar attacks in Cuba, for example, cross the line into the threshold of armed conflict, then the Cuban government, which is “unwilling or unable” to prevent these attacks from continuing to occur, may end up being held accountable for these attacks. Certainly, if evidence demonstrates that the government is providing substantial support or cyber defenses to protect individuals, then it should already be held accountable.

For cyber activities that have crossed the line into armed conflict, the concept of neutrality also applies. For the purposes of cyber-attacks, neutrality applies to a neutral state that is not party to the conflict, as well as its territorial sea and the outer space above the country.106 These neutral states are protected from direct attacks and from having cyber weapons moved across their territory, however they may be subjected to spill-over

100. Heintschel von Heinegg, supra note 90, at 16.
101. Id. at 12.
102. Id. at 17; see Tallinn Manual, supra note 16, at 36.
105. Elena Chachko & Ashley Deeks, Who is on Board with “Unwilling or Unable?”, LAWFARE (Oct 10, 2016, 1:55 PM), http://www.lawfareblog.com/who-board-unwilling-or-unable (discussing the developing customary international law of the “unwilling or unable” doctrine); Ashley Deeks, “Unwilling or Unable”: Toward a Normative Framework for Extraterritorial Self-Defense, 52 VA. J. INT’L L. 483, 499 (2012) (general discussion of development of “unwilling or unable” doctrine as a norm).
effects that may be *de minimis* to an otherwise legitimate military attack. These neutral states may not knowingly allow any party to the conflict to establish cyber infrastructure on their territory, or they may lose their status as neutrals. Further, a failure of a neutral country to stop a belligerent from launching offensive cyber activities from their territory will justify offensive cyber activities against them from the aggrieved State.

VII. Other Laws

As indicated in the Introduction, volumes can be written analyzing each of the above principles of armed conflict and how they may apply in the cyber context, using both recent examples and hypotheticals. But it is important to remember that only the narrowest subset of cyber activities end up crossing the *jus ad bellum* line into being categorized as an “armed attack.” For the remainder of cyber intrusions, denial of services, intelligence collection and theft, a full range of State diplomatic and criminal options are still available. States can use diplomatic engagement, sanctions, or other economic or political pressure to stop foreign governments from engaging in potentially unlawful cyber activities. NATO and the UN have spent considerable resources in discussing approaches to unlawful cyber activities and how to both deter and criminalize them. Most countries, like the U.S., continue to criminalize unlawful cyber activities so that they can fine or imprison individuals who commit cyber-crimes, as long as they can figure out who they are and apprehend them. The Snowden case, for example, has shown the challenges associated with prosecuting an individual who has sought safe-haven from a foreign country, Russia. Moving forward, the development of additional cyber tools to deter unlawful cyber activities will be critical, as the use of force should only be considered for that small grouping of cyber activities that cross the line.

VIII. Conclusion

International law, and specifically the law of armed conflict, does apply in cyberspace to those cyber activities that have been determined to “cross the line” from cyber incidents to cyber “attacks” within the meaning of article 51 “self-defense” under the U.N. Charter. While nations have been slow to recognize this authority, there has been growing consensus on the applicability of this legal framework and the broader *jus in bello* rules on

107. *Id.* at 250-52.
108. *Id.*
109. *Id.* at 254.
112. U.N. Charter art. 51.
which it provides some clarity. Notwithstanding, even though there is consensus that a cyber-attack can be an armed attack, the permanency, physical damage, and severity of the attack needed to cross this threshold has ensured that very few attacks seen to date would cross the line into the realm of conflict. The lack of attribution and the unique challenges of sovereignty in cyber space make the need for clarity and state practice even more significant.

Once the line has been crossed, however, conflict-based rules on the status of individuals, legality of weapons, principles of necessity and proportionality, state sovereignty, and even targeting rules all have some applicability. Given the very limited subset of attacks that have ever met the high threshold of “armed attack,” there is very little established state precedent to inform and guide future practice on how exactly all these conflict-based rules do apply, even though there has been significant attention and analysis put into thinking through these issues. As with all armed conflict, unfortunately, to develop the much needed state practice on the use of force in the cyber context, we will need to witness more cyber-attacks that do cross the line.