Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law

Emily B. Bordelon

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Fall 2016

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial fulfillment of the requirements for graduation from the Honors Program of Liberty University.

_____

Steven Samson, Ph.D.
Thesis Chair

_____

Stephen Parke, J.D.
Committee Member

_____

Durrell Nelson, M.F.A.
Committee Member

_____

James H. Nutter, D.A.
Honors Director

_____

Date

Abstract

The increased use of cyber warfare, accomplished by both state and non-state actors, raises questions about traditional approaches to security and what can be done to stop threats in a technology-driven society. This thesis analyzes how cyber actions interact with geopolitics and how that relationship can provide a foundation for states to approach creating a cyber security strategy. Specifically, there should be a strategy of deterrence and then an international system of norms and laws. The first part of this thesis will address the connections between cyberspace and geography. It will then lay out the strategy of deterrence and how the international sphere should approach the new type of war.

Acknowledgements

I would like to thank the members of my committee, Dr. Steven Samson, Dr. Stephen Parke, and Professor Durrell Nelson, for their assistance in writing my thesis. I would also like to thank Professor William Waddell for lending his time and expertise. I deeply appreciate the knowledge, mentoring, and encouragement that my committee has provided. My understanding of the topic, and the quality of my thesis, has benefited greatly as a result.

Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law

States are confronted with security questions along a broad spectrum, covering the land, air, and sea. The modern age has added a new realm to warfare: cyberspace. Cyber warfare operates through technology and provides information and power to states as well as individuals. Because of this, states need to adapt to new threats. Policymakers need to understand the emerging climate of warfare and approach it with vigilance. The solution will not be an easy one and will require multiple steps to cover the different types of attacks that can occur. Though cyberspace has a virtual component, it is founded in physical spaces. This means that a strategy should be developed within that framework.

Cyberspace Encounters Geography

The political sphere has been influenced by how power and space interact. States are determined by the territory that they are able to control, as defined by their borders. Their power is not grounded in a theoretical position but connected to geographical space. A state's power only goes as far as a fictional line that is constructed across a solid physical object. Political actors, individual men and states alike, have respected a geographical system and expanded it to the air and sea as well. Physical spaces have been connected with the essence of power since the foundation of the modern state. However, there is a debate about whether this framework can continue in the new era of technology.[1] States have access to new means of attack and espionage through cyber systems that were not available in the previous decades. Non-state actors, such as private

[1] John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," *American Foreign Policy Interests* 36, no. 5 (2014): 286.

individuals, also have access to cyberspace. This raises the question of whether or not a framework of geopolitical sovereignty is still the best to follow.

The first point to address is that cyber actions do not take place separate from a physical place. Cyberspace relies on a physical infrastructure to function.[2] It is a connected system of computers, servers, grids, the Internet, and other network channels.[3] To start an action in cyberspace, there needs to be a computer that is connected to a network. It can then proceed into the very detailed depth of a virtual realm. But the internal world of cyberspace depends on the initial access through a physical piece of technology.

Along with the technology, the second physical aspect of cyberspace is the people. People determine the nature of cyberspace and shape what it looks like.[4] Every idea and piece of technology that can be found on the Internet is the product of a person's idea. There is no part of cyberspace that was not initially created by an individual. It is also connected to people because if cyberspace is used in an attack, whether that is against a state or private business, people are both the perpetrators and the victims. For example, when a business is hacked and information is stolen, that information belongs to someone. Whether he or she is actively involved in the business or not, that person is now involved. People determine what occurs in the cyber realm.

However, there are outside sources that can persuade an individual to act in certain ways. These sources can be traced to geopolitics. This is the case because

---

[2] John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," *American Foreign Policy Interests* 36, no. 5 (2014): 286-7.

[3] David Clark, "Characterizing Cyberspace: Past, Present, and Future," *Office of Naval Research*, March 12, 2010, 2.

[4] Clark, "Characterizing Cyberspace," 4.

geography plays a role in determining where people act and whom they act against.[5] A key factor in this dynamic is politics. Geography and politics interact and determine the target of the attack.[6] Here geopolitics is centered in cyberspace.

This is not a new dynamic in cyberspace. It has been operating and directing nations for years. In 2008, Georgia and Russia were involved in a conflict and started to use cyber capabilities. Russia combined its military operations with cyber capabilities to increase its strategic advantage against a vulnerable Georgia.[7] It was coordinated at the state level against another state and had far reaching consequences. Georgia's network was compromised and its cyber capabilities were limited so that a response could not be launched.[8] Russia used its technology to further its military's advancement.

This operation had its base in geopolitics because the locations of the events were chosen according to virtual locality and then were followed into the physical realm by the military.[9] The cyber events were specific to where the troops were going to be sent. These were coordinated with where specific physical items and individuals could be traced. The optimal goal of the use of cyber warfare was to disorient the Georgian public and limit a counterattack so that the Russian military would have a greater chance of

[5] John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," *American Foreign Policy Interests* 36, no. 5 (2014): 286-7.

[6] Sheldon, "Geopolitics and Cyber Power," 288.

[7] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, 2.

[8] Hollis, "Cyberwar Case Study," 3.

[9] Ibid., 5.

success.[10] The reason that cyber technology was involved in the conflict was to further advance Russia's interest in the physical realm.

Another example of how cyber actions can be motivated by state politics occurred in 2010, when it was revealed that China had been infiltrating U.S. servers while searching for information.[11] China used a flaw in Internet Explorer to execute state espionage against another state.[12] It was a poignant reminder that geographical peculiarities retain their power in cyberspace and that states will take advantage of technology. Internet browsers can be used by anyone in the world. China used them to send malware to a foreign state. This is an example of how cyberspace is an aspect of geographical reality.

Acting according to geographic strategy is not confined to states. Individual actors may choose to attack foreign powers. They can choose their target for political or financial benefits. Either motivation is connected to geopolitics because it derives from a desire to harm a foreign nation. Popular culture conveys ideas about different places that people may absorb or reject.[13] Cultural influences can be as simple as a Saturday Night Live joke about politics or Toby Keith promoting a certain image of America. These convey ideas of what being an American should look like and are associated with the geographical place.[14] Social commentary also presents images about other parts of the world. All of these can influence people to subscribe to their state's national identity.

---

[10] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, 8.

[11] "Aurora Hack Spawns Widespread Concern," *Network Security* 2010, no. 1 (January 2010): 1.

[12] "Aurora Hacks Spawns Widespread Concern," 2.

[13] Jason Dittmer, *Popular Culture, Geopolitics, and Identity* (Lanham, MD: Rowman & Littlefield Publishers, 2010), xvii.

[14] Dittmer, *Popular Culture*, 2.

Geopolitical ideas can circulate through popular culture and influence an individual against another state or his own.

Acts of cyber aggression are connected to geopolitics whether they originate from the state or an individual. Geography plays a large role in determining how a person thinks and against whom he acts. Computers and servers are required for an individual to execute an attack. At its foundation, cyberspace is connected to geography and physical places.

This is an important factor to remember. Political discourse can become very abstract in its approach to cyber security, and it can focus on uncertainty, potential militarization, and perceptions.[15] Policymakers are tempted to focus on aspects of cyberspace that cannot be seen. Cyberspace should not be approached as an abstract field that cannot be influenced by strong material actions. Approaching cyberspace through a geopolitical discourse provides a better framework for policymakers to develop a strategy to promote cyber security.

The Strategy

Deterrence

The connections between cyber actions and geopolitics provide a base from which a strategy of deterrence can be used to prevent cyber attacks.[16] The strategy needs to be developed on two levels to address different cyber threats and provide the most protection. States need to create a strategy of deterrence that accounts for the different type of threats that they face.

---

[15] David Barnard-Wills and Debi Ashenden, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk," *Space and Culture* 15, no. 2 (2012): 110, Sage.

[16] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?," *Strategic Studies Quarterly*, September 2010, 102.

It is important to define what type of deterrence should be used in cyberspace. Two types of deterrence should be applied: deterrence by punishment and deterrence by denial. Deterrence by punishment relies on the threat of effective retaliation in response to an attack.[17] Deterrence by denial is a strategy that works to convince would-be attackers that they will be unsuccessful, convincing them that there is no value in making an attempt.[18] A state should use this dual approach when creating its strategy of deterrence.

The first concept of deterrence is deterrence by punishment. This is a common type of deterrence that has been used in military affairs for decades. It is one state telling another state that there will be a counterattack if it is harmed. This form of classical deterrence relies on the assumption that an actor does not have a desire to be harmed. Hence, if the actor believes that there will be a harsh enough consequence to his actions, he will not commit them. This logic should be applied to cyberspace to discourage states from cyber war.

When applying deterrence to cyberspace, what type of aggression will justify retaliation must be made clear. Similarly, the level of retaliation that is justified must be determined. Cyber aggression varies from espionage to combined operations with the military like Russia used in 2008. A strategy of deterrence must account for the varying types of attacks. Because of this, retaliation should be proportional to the type of attack.[19]

---

[17] Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?," *Journal of Strategic Security* 7, no. 1 (2013): 55.

[18] Iasiello, "Is Cyber Deterrence Illusory," 55.

[19] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 28.

The punishment need not be the same type of attack, but it must be deemed equally detrimental.

This is an important distinction because a state does not want an attack to escalate. Keeping the threat of retaliation to the same degree of damage is the best way to keep the attacker from issuing a counterattack.[20] While a state does not want its information stolen, it is comparatively better than being attacked militarily. Any retaliatory strike should take into account the amount of damage it will inflict and the probable response of the other state. Deterrence as punishment is only successful if it does not lead to another attack.

Critics of deterrence in cyberspace cite attribution as a reason against implementing the strategy.[21] Attribution is the lack of ability to find the perpetrator of the attack. Often, an attacker can hide where he is working and make it difficult to find him. This means that a threat of retaliation fails because the attacker believes that he will not be found and can, therefore, not be attacked.

However, the problem of attribution is often overstated. While it is true that there are times where an attacker is difficult to find, it should not define the approach to cyberspace.[22] One way that people can be traced is through the connection between cyberspace and geopolitics. Cyber attacks function through a constant connection to materiality. This connection can be through the physical means of the attack or through

---

[20] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 28.

[21] Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?," *Journal of Strategic Security* 7, no. 1 (2013): 58.

[22] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security* (Washington, D.C.: National Defense University Press, 2009), 309.

the motivation. Because of that, there are different ways that the source of the attack can be found.

The first way that a state can trace an attacker is through the physical means of the attack. Each hack leaves behind a certain amount of information through an IP address. That information can then be traced with the goal of re-creating a trail to the original source. This is specific to geography because an IP, Internet protocol, address can provide a latitude and longitude. A state can use it to take a cyber attack out of a virtual reality and place it into the physical world.

Geopolitics can also help resolve the attribution problem by providing a lens through which investigators can determine a motive. Attackers are motivated by specific politics or driven by their home states.[23] If the state trying to retaliate can figure out the reason behind the attack, it can place the origin within a specific geography. Doing so would increase the chances of success if a state were to adopt a deterrence by punishment strategy.

The second type of deterrence, deterrence by denial, can also be applied to resolve the problem of attribution. The reason behind this is that deterrence by denial does not rely on knowing the attacker. A state uses its own measures to send the signal to any potential attacker that it will fail. It is presented to the general population instead of a specific individual. The goal of this style of deterrence is to show impenetrability. Deterrence by punishment relies on a threat. Both are useful in cyberspace but are presented in different scenarios.

---

[23] John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," *American Foreign Policy Interests* 36, no. 5 (2014): 286-7.

Because deterrence by denial is a signal that an attack will be unsuccessful, it is a system of defense. A state invests in its infrastructure so that it cannot be violated. This should be a priority. One way this can implemented is through devoting resources to developing technology. Cyber attacks rely on one form of technology penetrating, or beating, another. A state can decrease the likelihood of this occurring by promoting cyber growth within its domestic sphere. Specifically, the state should work on creating nuanced systems and training people who know how to use them. Having a system of technology that surpasses other states is beneficial in preventing cyber attacks.

When pursuing better technology, states should remember that a large part of their defense will rely on the lack of human error. No policy can be made with the assumption that people will respond perfectly. This means that states must create defensive strategies that take into account human error and other possible failures.[24] There should be fallbacks built into the system's design so that, if an attack were to occur, an error would not derail the defense system.

This leads to another important tactic that can be employed in cyber defense: education. Educating people as to what a potential threat would look like and constantly being on the lookout are beneficial to a state's strategy.[25] Educating the public makes a broad audience aware of the threat and what potential enemies can do in cyberspace. This will lead them to increase their personal cyber security as well as be more alert to what is going on around them, bolstering the state's security. And it supports deterrence by denial because it sends a signal to a would-be attacker that people are aware of the threat

[24] Tim Ridout, "Building a Comprehensive Strategy of Cyber Defense, Deterrence, and Resilience," *The Fletcher Forum of World Affairs* 40, no. 2 (2016): 81, ProQuest.

[25] Ridout, "Building a Strategy," 81.

and are doing all they can to prevent it from occurring. It involves the state as well as private entities.

Adopting this form of deterrence is also beneficial because it provides another level of protection against lone actors. Retaliation can be difficult to accomplish if a decision must be made over a state acting against a lone individual. If a state were to act against an individual without the approval of the sovereign state within whose territory he resides, the likelihood of escalation is high. This can make the threat of retaliation against lone actors difficult. Deterrence by denial is meant to be the best option. It provides incentives against an actor trying to commit his attack because a state's defensive measures are so strong that the likelihood of succeeding is very low.

However, if deterrence by denial is unsuccessful against a lone actor, states are still able to use deterrence by punishment. A lone or non-state actor commits his attack in a geographical area and relies on material supplies to succeed. As mentioned, deterrence by punishment does not need to be the same type of attack as the initial harm. In the case of a lone actor, it would be a response that harms what they need or care about. A state could respond by cutting off their means of supplies and travel. Lone and non-state actors are not protected because they do not have a territorial state. They rely on material objects to accomplish their cyber attacks and can, hence, be found and punished.[26]

A dual system of deterrence by punishment and deterrence by denial also helps states offset the cost of having a deterrence strategy. This is important because the key reason to employ a strategy against cyber attacks is to prevent them at the lowest cost.

[26] John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," *American Foreign Policy Interests* 36, no. 5 (2014): 286-7.

Deterrence by retaliation can lower the cost of cyber defenses.[27] Resources and effort are put into inhibiting an attacker's attempt by threatening retaliation.[28] If the threat is successful, then there is no attack. No added resources need be expended for defense.[29] It would be very expensive to focus solely on defense. For example, in 2009 the federal government sought $7.3 billion to protect government computers.[30] The billions of dollars in expenditures do not guarantee that the U.S. is impenetrable. It would also be unwise to focus exclusively on offense. The threat of retaliation is insufficient if there is no system to support it. A dual system of deterrence by punishment and deterrence by denial is necessary to support a strong system of cyber security for an individual state.

Because of this, states should adopt both deterrence by punishment and deterrence by denial. Doing so means that the state approaches the problem of cyber attacks from both an offensive and a defensive perspective. This is important because these two options support one another and create a dual strategy whereby a state can choose one or both to deploy according to the situation. If a state were to rely solely on one aspect, an unexpected attack could be catastrophic.[31] A two-prong system is the best way to approach threats.

International Law

The second part of the strategy is developing an international system of norms and laws. States should not isolate themselves in cyberspace but should work with one

---

[27] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 33.

[28] Libicki, *Cyberdeterrence*, 34.

[29] Ibid.

[30] Ibid., 32.

[31] Aaron Wildavsky, *Rights and Regulations: Ethical, Political, and Economic Issues* (San Francisco, CA: Pacific Institute for Public Policy, 1983), xvi.

another. They should seek international consensus on actions because, while deterrence is helpful, it is not able to resolve every type of cyber threat.[32] A system of international norms, supported by laws, can support an individual state's fight for cyber security. If that is implemented, the likelihood of cyber attack occurring is greatly diminished.

There is also the question of international legitimacy. The world is not a system of states that act without others noticing and responding with approval or condemnation. For example, the United States condemned Russia's annexation of Crimea as an illegal use of force under international law.[33] There is a general understanding as to what is acceptable for states to do and what is not. A strategy of cyber security is a new policy area for states and needs to be addressed in conjunction with other nations.

The first thing that needs to be addressed in the international arena is the international definition of cyber war. A definition of what constitutes an attack for a state would help develop a legitimate system of deterrence in the international sphere. A historical way of approaching conflict is through the laws of war. A way to establish a legitimate system in cyber war is to look at the international legal documents that address just war and what actions constitute attacks and when force is allowed.

Such a document is the United Nations Charter. It addresses the matter of "force" in Article 2(4). Specifically, it says that a member of the UN shall not use the threat of force against another state unless it is otherwise lawfully qualified.[34] Cyber operations

---

[32] Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *International Law and Politics* 47, no. 327 (May 21, 2015): 354.

[33] Kristina Daugirdas and Julian Davis Mortenson, "United States Condemns Russia's Use of Force in Ukraine and Attempted Annexation of Crimea," *The American Journal of International Law* 108, no. 4 (October 2014): 784, ProQuest.

[34] Michael N. Schmitt, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), 153.

need to be approached in the context of this article. This Article does not prohibit states from acting against other states in every instance. There are times when it is considered justified. The question is situated around what constitutes a "use of force."[35]

The easiest way to approach the discussion is to look at the type of cyber events that can result in physical harm. This type of attack is equal to an armed attack and is considered force.[36] For example, it could be an attack on an electrical system that controls waterworks, thereby causing a flood.[37] Or it could be an attack on the electrical grid that might have varying physical repercussions: one being that life-support machines would shut down.[38] An attack that damages a country or its population in a material way is considered an armed attack.

The general interpretation of force is that a use of force is anything that harms a country's critical infrastructure. Such an attack involves one state using armed force against another because it damages another state's ability to operate. It is not simply a state improving its position by stealing information from another. This distinction becomes problematic where critical infrastructure is defined differently by each nation. In the context of cyber warfare, that leaves open an opportunity for escalation via harm to vital infrastructure. A general consensus should be reached for what type of infrastructure is of enough importance to justify a retaliatory response.

---

[35] Michael N. Schmitt, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), 154.

[36] Marco Roscini, "World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force," *Max Planck Yearbook of United Nations Law* 14 (2010): 88.

[37] Roscini, "World Wide Warfare," 115.

[38] Ibid.

For example, the 2003 U.S. National Strategy to Secure Cyberspace describes vital systems as the "physical and cyber assets of public and private institutes in…agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy transportation, banking and finance, chemicals and hazardous materials, and postal shipping."[39] This definition presents a list of national services that should operate unhindered after an attack for the attack not to be considered an armed attack. States that do not have the same scope of infrastructure as the U.S. can still create a legal clause outlining what services are necessary to keep their country secure. They might not reach the same scale but states that have access to cyber space would include agriculture, food, water, public heath, and other services that other states can agree are vital. A consensus should be reached that all these elements constitute critical infrastructure.

Cyber attacks can also be considered a use of armed force because states have included such attacks in their military doctrine.[40] China, Israel, and Germany have cyber units as part of their military strategy.[41] Many states include it in their military activity. This could be seen in the war between Russia and Georgia in 2008. Cyber technology can bolster military activities and will continue to be used in conjunction with armed forces. A definition of what constitutes an armed attack should include cyber actions.

If an attack does not fall within the criteria outlined above, is it an armed attack? Because cyber attacks can be varied, they should not be defined by narrow criteria. The

---

[39] Marco Roscini, "World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force," *Max Planck Yearbook of United Nations Law* 14 (2010): 117.

[40] Roscini, "World Wide Warfare," 107.

[41] Ibid., 97-8.

definitions should be in place along with criteria for how to evaluate scenarios that do not meet the set definitions. Cyber attacks should be evaluated along the following criteria: severity, invasiveness, and immediacy.[42]

Severity should be the first factor that a state looks at when a non-conventional attack occurs. Severity is determined by the scale, scope, and duration of the consequences of the attack.[43] A state can look at the how many people will be affected by the attack and whether it will impact their lives for a short or long period of time. If there is not a long-term consequence, the state may find that the attack was not very severe. Likewise, a state can look at how far the attack reached. If the attack did not touch a large area, then the cost of directly responding to the attack probably outweighs the damage of the attack.

The second factor is invasiveness. This factor considers whether or not a system is penetrated.[44] A significant portion of cyber attacks involves hacking information systems. If there are no repercussions to someone's physical well-being or infrastructure, hacking does not constitute a use of force. This is a key factor because cyber technology is a large component of modern state's intelligence gathering.[45] China has used its cyber capabilities to try to gain information. It is regarded as invasive but does not constitute an act of force.

The final factor that should be evaluated is immediacy. States should keep in mind how much time they have to respond to the attack. If the consequences of the attack

---

[42] Michael N. Schmitt, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), 155-6.

[43] Schmitt, *Proceedings*, 156.

[44] Ibid.

[45] Ibid.

occur quickly, there is less of a chance of reaching a peaceful solution.[46] This framework helps justify a state using a threat of force or force against another state after an attack. Creating an international consensus on the legal definition of cyber attack as force and then creating a framework to evaluate attacks will help states formulate their responses to a cyber attack.

After creating an international consensus that cyber attacks constitute an armed attack, states need to agree as to how the laws of war should address cyber threats. The first law of just war is *jus ad bellum*. *Jus ad bellum* includes the rules that regulate the use of armed force by states in international relations.[47] Agreement by the international community to a definition of force handles a large part of this theory. *Jus ad bellum* allows for action against other states in the case of self-defense and in cases where the state's sovereignty has been violated.

Another law of just war is *jus in bello*. *Jus in bello* raises the questions of necessity, proportionality, distinction, and neutrality.[48] The first question relates to the type of advantage that a cyber attack will give the attacker. It makes one state look at the military advantage gained from the hostile act made by another.[49] This subset of *jus in bello* needs to be contextualized in cyber warfare with the new understanding that a military attack does not need to involve physical movements or troops on the ground. A cyber attack can be an armed attack even without using material forces.

---

[46] Michael N. Schmitt, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), 156.

[47] Marco Roscini, "World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force," *Max Planck Yearbook of United Nations Law* 14 (2010): 88.

[48] Oona A. Hathaway et al., "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (August 2012): 850, JSTOR.

[49] Hathaway, "The Law of Cyber-Attack," 850.

This leads to the second principle of *jus in bello*, which is proportionality. Proportionality prohibits an attack that might result in civilian death, injury, or property damage that would be excessive compared to a military attack.[50] The deterrence strategy outlined previously created a framework that aligns with this principle by advocating for a response in kind. A consensus needs to be developed on the international scale that states may act in the same manner in their approach to cyber threats. This means that the type of damage a cyber attack can cause and the long-term consequences need to be anticipated.[51] A state should draft its response even before knowing the full extent of the damage. States should work together to prevent excessive retaliatory action. Such an action would include a retaliatory attack against a civilian network after being attacked by the military. This would violate the principle of distinction in *jus in bello*. States are required to distinguish between civilian and military targets when crafting their attacks.[52] In the context of cyber warfare, this principle prohibits cyber-attacks that are uncontrollable and could harm either civilian or military assets.[53] However, there is a caveat. Civilians lose their right to immunity when they play a direct part in an attack or act as combatants.[54] If a civilian attacked a state or worked for the state, he or she is culpable. A state needs to evaluate the type of target it is pursuing as it works towards cyber security.

---

[50] Oona A. Hathaway et al., "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (August 2012): 850, JSTOR.

[51] Hathaway, "The Law of Cyber-Attack," 851.

[52] Ibid., 851.

[53] Ibid., 852.

[54] Ibid., 853.

The final point posed by *jus in bello* is neutrality. A matter of debate is whether a state is responsible for an actor within its territory.[55] This question also needs to be situated under the rules of *jus ad bellum*. If there is not agreement between states on who is responsible and an attack occurs, the possibility for either escalation or an attacker to go unpunished increases. An international agreement needs to be reached on how states should approach individual actors.

One trait that states can look for is "uniform hackers."[56] As previously mentioned, some states have military cyber units. They could deploy a few individuals to commit an attack while attempting to conceal their direct connections to the state. Individuals could also be hired by the state to complete an attack.[57] A prime example of this occurred in 2008 when Russia hired an outside firm to conduct the attacks against Georgia.[58] They are believed to have hired the Russian Business Network, a cybercrime syndicate that commits attacks against various states for hire.[59] The state should be held responsible if it hires an outside actor to commit an attack. The state provides the intent and the cyber crime firm provides the means.

A legal foundation for accountability can be found in the Articles on the Responsibility of States for Internationally Wrongful Acts, which were adopted by the International Law Commission in 2001. Article 8 states that the actions of a person or a group "shall be considered an act of a State under international law if the person or group

---

[55] Marco Roscini, "World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force," *Max Planck Yearbook of United Nations Law* 14 (2010): 97.

[56] Roscini, "World Wide Warfare," 97.

[57] Ibid., 99.

[58] Ibid.

[59] Ibid.

of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[60] This means that if a state employs or commands an individual or group to attack another state, it is responsible for that action. Russia was responsible for hiring the Russian Business Network to attack Georgia. There should be a broad international consensus that what is written in the International Law Commission applies to the international community and cyber warfare. If an actor is connected to a state, the attacked state is justified in holding the aforementioned state accountable.

A remaining issue is how to approach actors that do not work with a state. On a domestic level, such actors are approached through deterrence by denial. They can also be approached in the international sphere. One way of doing so is to create international alliances that address cyber activities.[61] This is vital because an attack could come from anywhere in the world. The problem is a global one that should be approached through global cooperation.[62] It is not a simple problem that can be solved by a state's military might. Cyberspace presents a unique opportunity for an attacker to conceal his identity. The ambiguity and the distance between origin and attack it affords mean that the stratagem is difficult to combat. Alliances can create a network that defines the area a nation has to protect if attacked.

The first step to create an alliance system is complete once there is an international consensus of what constitutes a cyber attack, providing a basis from which to act. From there, nations should agree to cooperate on information sharing, evidence

[60] Marco Roscini, "World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force," *Max Planck Yearbook of United Nations Law* 14 (2010): 99.

[61] Frank J. Cillufo and Sharon L. Cardash, "Cyber Domain Conflict in the 21st Century," *The Whitehead Journal of Diplomacy and International Relations* 14, no. 1 (December 2013): 45, ProQuest.

[62] Oona A. Hathaway et al., "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (August 2012): 880, JSTOR.

collection, and prosecution of those who committed the attack.[63] Each step is necessary to creating an alliance and signing a treaty. Each brings different benefits to resolve unique problems when confronted with cyber war.

Information sharing is foundational because cyberspace relies on information. At its core, the reason why cyber attacks are so dangerous is because modern societies rely on technology to retain and relay information. The world is connected through technology. Cyberspace is built into this system and an attack can take full advantage of its vulnerabilities. Information sharing is important because it can help a state that has suffered a cyber attack overcome it and pursue the perpetrator. A state's ally can assist it in vital information as it searches for the attacker.

Information sharing should be used in conjunction with evidence collection. A consistent problem with cyber attacks is attribution. As previously argued, cyber attacks connection to geography can help overcome that problem. There are material factors and geographical motivations that can help a state trace the origins of the attack. However, there are legal obstacles that could prevent a state from pursuing this track. The attacker may have committed the attack within the sovereign territory of another state. This would prevent the state from pursuing further evidence. For the investigation to continue, an agreement should provide that states will work with one another to collect and share evidence after a cyber attack.[64] This will help resolve the problem of attribution and increase the likelihood of catching the perpetrators of cyber attacks.

---

[63] Oona A. Hathaway et al., "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (August 2012): 880, JSTOR.

[64] Hathaway, "The Law of Cyber-Attack," *880.*

The third step is for states to adopt an agreement to work together towards prosecuting those that participate in cyber attacks that cross national borders.[65] Prior to this, states must establish steps to prevent cyber attacks or to work towards catching the people who make them occur. It is also important that states have an established plan in place for when they catch the attackers. Because attacks can happen on an international scale, there needs to be an international framework.

The way this can be done is through creating Mutual Legal Assistance Treaties, or MLATs, that apply to cyber warfare.[66] This is important because MLATS are treaties that apply to law enforcement and entities involved in criminal investigations.[67] They include facets that would be beneficial for prosecutors and are created with a goal of helping them when a case becomes cross-national. Some features of a MLAT can include requesting searches, extradition, freezing assets, and serving judicial documents.[68] A key facet of this process for cyber warfare is the process of extradition. If a state finds that the attacker acted within a separate sovereign state's territory without instruction or coercion from that state, the state is not liable for the lone actor. This means that deterrence by punishment is not a viable strategy and deterrence by denial has already failed because an attack has occurred. The state needs another option.

---

[65] Oona A. Hathaway et al., "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (August 2012): 880, JSTOR.

[66] Scott J. Shackelford, "The Law of Cyber Peace," *Kelly School of Business Research Paper* 16, no. 56 (July 5, 2016): 48, Social Science Research Network.

[67] T. Markus Funk and Virginia M. Kendall, Hon., "The Role of Mutual Legal Assistance Treaties in Obtaining Foreign Evidence," *Global Litigator* 40, no. 2 (2014): 1.

[68] Funk and Kendall, "The Role of Mutual Legal Assistance Treaties," 2.

An MLAT with an extradition clause should provide that option. The state where the attacker operated would be under an obligation to arrest and extradite the individual, reliant on sufficient evidence being presented that he caused the attack. If it were to refuse to do so, the offended state could suspect that it was involved in the attack and pursue other options. An MLAT is a necessary component in helping a state bolster its ability to prosecute criminals in an international climate.

The last facet of what can be done in the international sphere applies to developed countries. Some nations, like the United States, are heavily dependent on technology. Other nations are further behind, although they are growing in their technological pursuits. This creates a vastly uneven field for cyber attacks. A way to resolve the differences is for more developed nations to assist developing nations when they confront a cyber threat.[69] It will prevent the developing state's infrastructure from being harmed as well as help the nations surrounding it. The more states that are equipped to confront cyber threats, the more secure the international community is.[70] The leading countries in the world have an incentive to help the countries around them. Working in the international sphere will bolster their domestic attempts to secure their cyber assets.

International cooperation can come through active assistance and passive agreement of legal definitions. Both are important to the fight against cyber war. For a state to act aggressively against a threat without fear of being condemned, there needs to be a commonly understood definition of what is an attack. An international approach to cyber warfare accomplishes that task. States are also better able to resolve cyber threats if

---

[69] Oona A. Hathaway et al., "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (August 2012): 883, JSTOR.

[70] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, D.C.: Executive Office of the President of the United States, 2011), 15.

they work together. Sharing information and creating MLAT treaties will foster the ability to catch and prosecute the perpetrators of cyber attacks, regardless of where they originate. A state should engage in these international strategies to create strong counter-attack methods.

Conclusion

Cyberspace presents a new arena for policymakers to tackle. For the best solution to be created, cyber actions should be placed within geopolitics. It creates a foundation for people to formulate a better understanding of the threat as well as develop strategies that can approach the physical and virtual aspects of cyber threats. After deploying geopolitical approach, a state should use a strategy of deterrence by punishment and deterrence by denial. It will address state and non-state actors through a dual process of offense and defense. This is a domestic strategy that every state should use. An international approach should also be used to add legitimacy to the domestic systems and bolster their investigations after an attack. Shared understandings of cyber attacks and agreements between states to work together after an attack will help catch attackers. If these steps are followed, states will have a much stronger cyber security strategy.

Bibliography

"Aurora Hack Spawns Widespread Concern." *Network Security* 2010, no. 1 (January 2010): 1-2.

Barnard-Wills, David, and Debi Ashenden. "Securing Virtual Space: Cyber War, Cyber Terror, and Risk." *Space and Culture* 15, no. 2 (2012): 110-23. Sage.

Cillufo, Frank J., and Sharon L. Cardash. "Cyber Domain Conflict in the 21st Century." *The Whitehead Journal of Diplomacy and International Relations* 14, no. 1 (December 2013): 41-47. ProQuest.

Clark, David. "Characterizing Cyberspace: Past, Present, and Future." *Office of Naval Research*, March 12, 2010. 1-18.

Davis, Paul K. "Deterrence, Influence, Cyber Attack, and Cyberwar." *International Law and Politics* 47, no. 327 (May 21, 2015): 327-55.

Daugirdas, Kristina, and Julian Davis Mortenson. "United States Condemns Russia's Use of Force in Ukraine and Attempted Annexation of Crimea." *The American Journal of International Law* 108, no. 4 (October 2014): 784-819. ProQuest.

Dittmer, Jason. *Popular Culture, Geopolitics, and Identity*. Lanham, MD: Rowman & Littlefield Publishers, 2010.

Funk, T. Markus, and Virginia M. Kendall, Hon. "The Role of Mutual Legal Assistance Treaties in Obtaining Foreign Evidence." *Global Litigator* 40, no. 2 (2014).

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly*, September 2010, 102-35.

Hathaway, Oona A. Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." *California Law Review* 100, no. 4 (August 2012): 817-85. JSTOR.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, January 6, 2001, 1-10.

Iasiello, Emilio. "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security* 7, no. 1 (2013): 54-67.

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington, D.C.: Executive Office of the President of the United States, 2011.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington, D.C.: National Defense University Press, 2009.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009.

Ridout, Tim. "Building a Comprehensive Strategy of Cyber Defense, Deterrence, and Resilience." *The Fletcher Forum of World Affairs* 40, no. 2 (2016): 63-83. ProQuest.

Roscini, Marco. "World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force." *Max Planck Yearbook of United Nations Law* 14 (2010): 85-130.

Schmitt, Michael N., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.: National Academies Press, 2010.

Shackelford, Scott J. "The Law of Cyber Peace." *Kelly School of Business Research Paper* 16, no. 56 (July 5, 2016): 16-56. Social Science Research Network.

Sheldon, John B. "Geopolitics and Cyber Power: Why Geography Still Matters." *American Foreign Policy Interests* 36, no. 5 (2014): 286-93.

Wildavsky, Aaron. *Rights and Regulations: Ethical, Political, and Economic Issues*. San Francisco, CA: Pacific Institute for Public Policy, 1983.