Old Dominion University
ODU Digital Commons

Cybersecurity Undergraduate Research | 2021 Fall Cybersecurity Undergraduate Research Projects

Developing an International Framework for Addressing Non-State Actors in Cyberspace

Joanna C. Di Scipio
William & Mary

Follow this and additional works at: https://digitalcommons.odu.edu/covacci-undergraduateresearch

 Part of the Information Security Commons

Di Scipio, Joanna C., "Developing an International Framework for Addressing Non-State Actors in Cyberspace" (2021). *Cybersecurity Undergraduate Research*. 4.
https://digitalcommons.odu.edu/covacci-undergraduateresearch/2021fall/projects/4

This Paper is brought to you for free and open access by the Undergraduate Student Events at ODU Digital Commons. It has been accepted for inclusion in Cybersecurity Undergraduate Research by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.

Developing an International Framework for Addressing Non-State Actors in Cyberspace

Joanna C. Di Scipio

Coastal Virginia Commonwealth Cyber Initiative

William & Mary

22 November 2021

I. Introduction

On May 7, 2021, Colonial Pipeline shut down its operations following a ransomware attack by the criminal group DarkSide (Bordoff, 2021). It took five days to resume normal operations, but this short period led to panic buying, rising prices, and significant gas shortages. The attack underscores an emerging threat in the landscape of cybersecurity: critical infrastructure attacks carried out by non-state actors.

Non-state actors launch the majority of cyberattacks today (van der Meer, 2020). These attacks are becoming more sophisticated and more frequent--from January to May of 2021, more than $350 million in losses were attributable to ransomware attacks, a 300% increase from 2020 (Cohen & Sands, 2021). A lack of clear rules, consequences, and red lines in the cyber domain signals a tolerance of cyber operations that fall below an apparent threshold of war. Additionally, decisions and policy-making among Western governments have proven to be reactive rather than proactive, hindering their ability to prevent attacks like that of the Colonial Pipeline through the employment of international laws or norms.

While non-state actors are responsible for most cyberattacks, these attacks are often made at the behest of states, signaling the emergence of a new "blended threat"--one that comes from cybercriminals but with state actors that benefit, directly or indirectly from the attack, as the ones ordering the attack (Sanger & Perlroth, 2021). The employment of non-state actors in cyber makes it more difficult for attacks to be attributed back to the governments that ordered them, reducing the threat of retaliation or political blowback to these governments and rendering their

use more appealing. As the threat of attacks from non-state actors grows, traditional defensive strategies prove to be ineffective due to the asymmetrical nature of cyberspace. These kinds of attacks and the inability to defend against them are a grave threat to national security. To avoid national crises driven by non-state actor attacks against critical infrastructure, governments must work together to create an international legal framework that expands the concept of due diligence to include cyberspace, making the threat of retribution or penalties enough to prevent states from employing non-state actors in their offensive cyber operations.

This paper examines state motivations for conducting cyberattacks and employing non-state actors in cyberspace, outlines how critical infrastructure attacks threaten national security and establishes why defending in cyberspace is so tricky. It then outlines the application of the concept of due diligence to kinetic warfare. The Colonial Pipeline attack is used as a case study to demonstrate the risks posed by non-state actors in cyberspace and the culpability of the Russian government in the attack based on current and potential international legal standards. The paper concludes by analyzing how to reform international law to discourage the employment of non-state actors by states to conduct cyber operations.

II. Definitions

The concept of cyberwarfare is relatively new, and the research surrounding it evolves daily. As a result, agreed-upon definitions for cyber-related terms do not exist. For this paper, I will be referring to the definitions outlined by Johan Sigholm in *Non-State Actors in Cyberspace Operations* (2013):

- Cyberspace: "The global, virtual, ICT-based environment, including the internet, which directly or indirectly interconnects systems, networks and other infrastructures to the needs of society" (Sigholm, 2013, p. 6).
- Cyberactions: "A collection of predominantly illegal activities in cyberspace, carried out by non-state actors, causing damage or disruption, in pursuit of various political, economic or personal goals" (Sigholm, 2013, p. 6).
- Cyberattacks: "A subset of cyberspace operations employing the hostile use of cyberspace capabilities, by nation-states or non-state actors acting on their behalf, to cause damage, destruction, or casualties in order to achieve military or political goals" (Sigholm, 2013, p. 6).
- Cyberwar: "Occurs when cyberattacks reach the threshold of hostilities commonly recognized as war by the international community and as defined by international law" (Sigholm, 2013, p. 7).

III. State Motivations

Why Cyber?

There are a multitude of components in the cyber domain that make its use especially attractive to states. Cyberspace is asymmetric, meaning offensive cyber operations are more effective than defensive cyber operations (Sigholm, 2013). This effectiveness results from the difficulty of predicting cyber attacks, which succeed by exploiting vulnerabilities the victim is unaware of. While cybersecurity experts continuously check for holes in their systems, an

attacker needs to find only one to succeed. Thus, offensive actors have the element of surprise in conducting cyber attacks.

Another upside of cyber operations to states is the difficulty of attribution. Due to the internet's architecture, it is relatively easy for attackers to conceal their identities after carrying out operations, made even easier by the use of non-state actors. Cyberspace is also a reasonably inexpensive realm to operate in. Barriers to entry are low as computers are easily accessible and inexpensive.

The most significant advantage for states conducting cyber attacks is the lack of international agreement and legal standards on cyber. To date, no international laws covering cyber warfare exist, meaning that even if a state is found responsible for a cyberattack, there are no laws or norms for dealing with retribution. Thus, actual consequences could be minor, once again underlining the asymmetric nature of cyberspace, where aggressors stand a chance to emerge from an attack unknown and unscathed.

Types of Non-State Actors

Many different entities are identifiable as non-state actors, ranging from self-taught "script kiddies" to cyber militias. It is helpful to identify the most important groups before analyzing the reasons states employ them.

Individual hackers are individuals with sophisticated enough knowledge of cyberspace to carry out their offensive operations or be hired by states for specific operations. They may also find

'bugs' in adversary networks on their own, information which they, in turn, sell to states (Bussolati, 2015).

Criminal organizations have a degree of structural formality. They benefit from the low threshold to entry in cyberspace and the lack of international cyber law enforcement. Their interests are generally financial. DarkSide is a perfect example of a cybercriminal organization, as they carried out a ransomware attack on the Colonial Pipeline to obtain financial benefit (Bussolati, 2015).

Cyber mercenaries are highly skilled hackers who carry out sophisticated cyber attacks on behalf of clients in the public or private sectors. Hacktivists are informally structured independent organizations that carry out attacks for political or ideological reasons. Patriot hackers, driven by patriot interests to defend their country, are similar to hacktivists (Bussolati, 2015). In 2019, the Russian government employed hacktivists and patriot hackers to conduct a large-scale cyberattack in Georgia that knocked out thousands of websites (Rogusi, 2020).

Why States Employ Non-State Actors

States that commit cyberattacks against adversaries likely want to avoid conflict escalation as a consequence of their attacks. The lack of clear-cut escalation patterns in cyberspace makes it difficult to predict adversary responses if an attack is successfully attributed back to the attacking state, thereby increasing motivations to prevent successful attribution and encouraging the employment of non-state actors. Attribution is a messy and time-consuming process in cyberspace, no matter the source of the attack. However, when a state directs an

"unaffiliated group" to commit an attack on their behalf, it makes attribution nearly impossible (LaFrance, 2017). This makes it difficult for victim states to legitimately launch a counter-attack, which saves the offensive state from the possibly damaging effects of an attack and avoids conflict escalation. States are also saved from the political or economic penalties that may come due to being credibly proven as the aggressor in a large-scale cyber attack.

In addition to the attribution advantage in outsourcing attacks to non-state actors, states looking to infiltrate enemy networks exploit a knowledge advantage. Many individuals and groups are skillful at carrying out sophisticated cyber-attacks. Governments may find that those with the most excellent skills are not directly employed by the state, meaning this level of knowledge is accessible only through non-state actors. The mobilization of non-state actors is relatively quick and cheap, making this knowledge advantage easy to exploit. In conjunction with the benefits of avoiding attribution, this makes the employment of non-state actors appealing to governments.

While there are many benefits to using non-state actors to carry out attacks, the choice is not without risk. Governments cannot always exercise direct control over non-state actors, who act as a proxy to attack on the government's behalf (Sigholm, 2013). A failure to correctly scope the scale of an attack or hitting the wrong targets might lead to unwanted escalation. By not conducting the attack themselves, governments cannot ensure avoidance of this error. Hiring an outside group to conduct an attack also leaves governments susceptible to blackmailing, as actors possess potentially damning information regarding the government's culpability. States found to

be the source of an attack risk being labeled as sponsors of terrorism, which could be politically devastating for some nations.

Most of the drawbacks to employing non-state actors are related to the general ambiguity that accompanies operating in cyberspace, which underlines the need for greater international policy and norms outlining state behavior and appropriate retaliatory measures. The benefits of employing non-state actors likely outweigh the risks. However, unintended consequences are avoidable if more energy and resources are devoted to making attribution and consequences more likely to states who use non-state actors to carry out attacks.

IV. Outlining the Issue

It is clear that conducting attacks in cyberspace and employing non-state actors is effective and appealing to states. It is important to understand how serious this development is and the graveness of the threat to victim states.

Critical Infrastructure Attacks as a Threat to National Security

The Colonial Pipeline attack is just one example of potential damages wrought by malicious actors in cyberspace. Day-to-day life and operation in the United States largely depend on highly interdependent information and communication technology (ICT). This means that a significant degree of infrastructure is vulnerable to single points of failure and adversary attacks (Sigholm, 2013). Most of America's critical infrastructure is owned and operated by the private sector, which does not have as many cybersecurity protections as the government, which itself is vulnerable to attacks (Sanger & Perlroth, 2021). Private sector organizations are more vulnerable

to attacks than the government, and the fact that they control most of the nation's critical infrastructure means that an attack successfully carried out on one of these organizations poses a grave threat to national security.

The Colonial Pipeline attack was not just an example of how potentially cataclysmic a large-scale cyber attack could be; it demonstrates to America's adversaries how easy it is to incite chaos across a large part of the country (Sanger & Perlroth, 2021). Just the threat of a gasoline shortage sparked mass panic in the eastern portion of the country, and the group responsible for the attack earned nearly 5 million dollars in ransom payouts (Shear et al., 2021).

Another attack that demonstrates the immediacy of the issue of non-state actors in cyberspace is the Dragonfly 2.0 attack. In this instance, intruders gained access to American power-grid operations with enough control to induce blackouts on American soil (Greenberg, 2017). While they did not act on this power, it demonstrates just how easy it would be for an attacker to quickly wreak havoc on an entire nation. While the attack was eventually attributed to Russia, it was carried out by a non-state cyber espionage group, demonstrating how much skill and sophistication many of these groups possess (Greenberg, 2017).

Cyber Asymmetry: Defense is Hard

One possible remedy to the threat of cyber attacks launched by non-state actors is to ramp up defenses. Unfortunately, cyberspace's asymmetric nature makes it so that offense is much easier than defense. Due to the incredible speed and relative anonymity of attacks, catching an

adversary by surprise is not hard. Because attacks involve exploiting unknown vulnerabilities in target software, they are difficult to predict, giving the attacker the constant upper hand.

The rapidity of attacks in cyberspace heightens the risk of simple misunderstandings leading to crisis escalation (Eilstrup-Sangiovanni, 2018). For example, a victim under attack may try to retaliate to put an end to the attack. However, since attribution is time-consuming, quick retaliation is done without confirming that the predicted aggressor is the true aggressor. An opponent may also have launched an attack inadvertently, meaning that the victim ends up creating a crisis that could and perhaps should have been avoided.

Given the asymmetrical nature of cyberspace, states are encouraged to focus their efforts on offense rather than defense. Not only does this mean that the threat of escalation is great, but protection against cyber warfare is not possible through traditional means. Instead, it must happen through the use of international laws and norms.

Deterrence

When traditional forms of defense do not prove viable, deterrence seems like an excellent option. In its purest form, deterrence prevents actions based on the threat of counteraction. During the Cold War, nuclear arms buildups served as a form of deterrence, as states knew that response to a launch of a nuclear attack would be cataclysmic for them, serving to effectively prevent any offensive action (Mauroni, 2019).

At first glance, deterrence seems like a practical option for preventing large-scale attacks by aggressors in cyberspace. If states can signal that the threat of retaliation outweighs the

benefits of attack, they can effectively prevent an attack from happening. In reality, the difficulty of signaling in cyberspace makes deterrence largely unfeasible.

The difficulty of signaling in cyberspace comes from its asymmetric nature and attribution difficulties. States cannot credibly signal retaliation when they do not have mechanisms for quickly and accurately determining who is behind an attack. Signaling's complexity also occurs because it is impossible to demonstrate to an adversary the ability to attack a critical system without giving away the flaw the aggressor plans to exploit, which can then be patched. Thus, the only way for a state to credibly signal its ability to carry out a cyberattack is to conduct it, defeating the purpose of deterrence (Smeets, n.d.). It is also difficult to specify the magnitude of an intended counter-strike, as the unpredictable nature of cyberspace makes it challenging to anticipate the scale of attacks. The plethora of non-state actors in the cyber domain further complicates deterrence. It cannot be assumed that non-state actors are rational actors in the same way that it can be assumed state actors are rational actors (Smeets, n.d.).

Deterrence has been successful when new and pressing challenges like the Nuclear crisis emerge, but it is not appropriately suited for cyberspace. Given this, dealing with non-state actors in cyberspace requires the creation of new international norms that go beyond traditional means.

V. Due Diligence & Non-State Actors in Kinetic Warfare

Before assessing what culpability a state should face for attacks committed by non-state actors at their behest or within their borders, it is helpful to look at the concepts of due diligence

and imputed responsibility and their interpretations in kinetic warfare. Due diligence is "an obligation for states to take measures to ensure that their territories are not used by any actor to harm other states" (van der Meer, 2020). Closely linked is the concept of imputed responsibility, which means holding states responsible for the actions of non-state actors, usually when they have failed to practice due diligence to prevent attacks (Graham, n.d.).

Historically, state responsibility for an attack carried out or planned within their borders had to pass the "effective control test," which was established by the International Court of Justice (ICJ) in *Nicaragua v. The United States* (Graham, n.d.). The ICJ determined that although the US had financed, organized, trained, and armed the Contra rebels, who attacked the Nicaraguan government, they did not have "effective control of the military or paramilitary operations in the course of which the alleged violations were committed," so they were not found responsible for the actions of the Contras (Graham, n.d.).

In contrast, in 1999, the International Criminal Tribunal for the former Yugoslavia (ICTY) broadened the concept of state responsibility following crimes committed during the Yugoslav Wars. States could now be held responsible for "for the actions of a militarized group when that state had coordinated or assisted in the general planning of the group's military activity" (Graham, n.d.). Moving past "effective control," states were now responsible for actions committed by non-state actors as long as they were involved in those actions in some capacity. Under this interpretation of state responsibility, states who direct non-state actors to commit

cyber crimes are responsible for those crimes, even if they do not exercise total control over the actor during the attack. Nevertheless, it remains difficult to prove that a state directed an attack.

The concept of state responsibility broadened further following the September 11 attacks to include a failure to prevent a state's territory from being used as a base from which to launch attacks against other states (Graham, n.d.). UNSC Resolutions 1368 and 1373 determined the US invasion of Afghanistan was an appropriate exercise in self-defense, as the Taliban harboring of Al-Qaeda made them partially responsible for the attack (Bussolati, 2015). The Taliban had imputed responsibility for the 9/11 attacks because they failed to practice due diligence in preventing the attacks and holding accountable those responsible. In the context of cyber warfare, this interpretation of state responsibility would ascribe responsibility to states who have not taken appropriate measures to prevent their countries from being used as a base from which to launch attacks.

VI. The Colonial Pipeline: A Case Study

The Colonial Pipeline supplies nearly half the fuel consumed along the Eastern Seaboard, moving around 2.5 million barrels of gasoline per day. Shortly after the attack, a run on gas stations caused price rises and extreme shortages. In Georgia and South Carolina, the price of regular gasoline went up 8%, and 50% of stations reported having no gasoline (Brodoff). In the District of Columbia, 90% of stations had "no gas" signs. This attack provides an excellent blueprint for what future attacks carried out by non-state actors could look like, reveals flaws in current mechanisms for dealing with non-state actors in cyberspace, and demonstrates the need

for international norms that would hold the Russian government directly responsible, even if direct attribution is not possible.

The Colonial Pipeline attack was a ransomware attack carried out by the criminal extortion ring DarkSide, who locked the company out of their computers and held data hostage until they paid a fee (Cohen & Sands, 2021). The attack's goal was not to disrupt the US economy but to hold corporate data for ransom, meaning that the motives of DarkSide were primarily financial, as is true for many cybercriminal organizations (Sanger & Perlroth, 2021). The US Cyber Combatant Command was likely authorized to remove DarkSide from the internet, and shortly after Colonial Pipeline paid the ransom, their sites went dark (Sanger & Perlroth, 2021). Following suit, many other ransomware groups announced they were shutting down, demonstrating that retaliatory attacks work when carried out effectively.

Following the attack, President Joe Biden announced that "we do not believe the Russian government was involved" (Jasper, 2021). However, the effects of the attack aligned closely with Russian objectives, and their complacency in allowing cybercriminals to operate from within their borders demonstrates at least passive approval of the attack. The geopolitical motivations for such an attack exist, as Russia has always sought to weaken the West. The country benefits from any chaos that might cause citizens to question the legitimacy of a Western government or leader and sow discord among citizens. Nowhere is this more obvious than in the divisive effects of the 2016 election interference campaign conducted at the behest of the Russian government (Abrams, 2019). While the effects of the Colonial Pipeline attack were relatively short-lived, it

demonstrated both the fragility and vulnerability of the US energy system and the potential for cyberattacks to sow discord and unrest among the US population (Bordoff, 2021).

While there is no direct evidence that the Russian government sponsored the Colonial Pipeline attack, there is evidence of implicit encouragement by the Russian government of criminal hacking within their borders. Russia harbors more ransomware groups than any other country in the world (Sanger & Perlroth, 2021). Not only this, but the Russian government actively protects hackers living within their borders. The Russian government has recruited cybercriminals instead of turning them over to face prosecution for crimes in other countries (Jasper, 2021). The signal sent by Russia is that its borders are a safe haven for cybercriminals.

This raises the question of how much responsibility a government should bear for non-state cyber hackers conducting operations from within their borders. By not actively attempting to prevent ransomware operations, the Russian government appears to be approving of, if not encouraging, cyber crimes intended to weaken the West (Jasper, 2021). Under an expanded concept of due diligence within the cyber realm, the inaction of the Russian government to stop non-state actors from committing cyber crimes could be viewed as a breach of international law. By applying the concept of imputed responsibility, states are justified in launching counter-attacks against the Russian government for self-defense purposes. While there are escalatory risks involved here, being held responsible for the actions of non-state actors on the international stage could encourage the Russian government to at least stop employing

non-state actors to carry out cyberattacks, if not pursue prosecutions for attacks launched within their borders.

VII. Reforming International Law

This paper has established that non-state actors acting at the behest of states pose a grave threat to critical infrastructure and national security. Due to the asymmetric nature of cyberspace, traditional defense is generally not an option, and deterrence in cyberspace is more challenging to achieve than deterrence in the physical domain. Thus, the development of new international laws and norms is necessary to respond to the dangers posed by non-state actors in cyber warfare.

States have been reluctant to agree on a legally binding definition of cyberwar or support an international law regarding cyberspace (Sigholm, 2013). Nations benefit offensively from the unclear definitions establishing expected behaviors in cyberspace. As a result they have been given free rein in the kinds of attacks they sponsor and how they sponsor them. As attacks become more sophisticated and countries become bolder, the risk posed to states by this lack of clarity will begin to outweigh the benefits. At that point, it might be too late to establish an international consensus. Thus, time is of the essence to define state responsibility related to non-state actors in cyberspace.

Article 51 of the United Nations Charter establishes that a state may legitimately use force as an instrument of dispute resolution as an act of self-defense (Graham, n.d.). Historically, this has applied to conflicts between states, but following 9/11, the concept broadened to include

states who harbor non-state actors. While the Taliban was not directly responsible for the actions of al-Qaeda, the UN Security Council determined that their inaction in preventing the attack or turning the criminals over to the US government gave them imputed responsibility in the matter.

Expanding the concept of imputed responsibility to include cyberspace is critical in developing an international legal framework. A new international legal framework should focus on clear and necessary actions a state must take to prevent its territory from being used to launch cyberattacks. Actions include enacting strict laws related to cybercrime, conducting investigations into cyberattacks, prosecuting those engaged in cyberattacks, and cooperating with victim states' investigations into those responsible for attacks (Graham, n.d.). A state's failure to meet these objectives would mean that it has, like Afghanistan following 9/11, become a sanctuary state, making it responsible for attacks launched by non-state actors within its borders. This will make victim states justified in self-defense if they retaliate against the state harboring the attackers.

The goal of an international convention of this scope would be to make the use of non-state actors in cyber warfare as unattractive as possible due to the risks of imputed responsibility. One of the biggest attractions of using a non-state actor is the inability of states to attribute an attack to a state without direct proof that the government ordered the attack. An international legal framework on cybercrime committed by non-state actors would make it so that attacks need only be traced back to their point of origin, and state actors that failed to take precautionary measures in preventing the attack would ultimately be responsible, meaning the

lack of easy attribution would no longer be an obstacle to retaliation. Ideally, this would also encourage states to proactively prosecute cybercriminals living within their borders, decreasing the number of non-state actors that could potentially launch devastating attacks.

VIII. Conclusion

In recent years, new developments in cyberspace have outpaced the creation of international laws and norms designed to regulate state actions in the domain. As of this date, there are no international treaties or conventions designed to address cyber-attacks and cyberwarfare. State actors continue to conduct offensive cyber operations partly because of the ambiguity of cyber rules and the asymmetrical nature of the sphere, which allows them to execute damaging attacks quickly. The employment of non-state actors by governments further complicates the issue. It makes it harder to attribute attacks back to the states, thereby reducing any threat of political or economic retribution or traditional forms of retaliation. The Colonial Pipeline attack exemplifies the growing use of non-state actors who act at the best of governments to attack critical infrastructure. For this attack, the criminal cyber organization Dark Side conducted a ransomware attack on a private company integral to the US energy sector. While the Russian government was never directly found responsible for the attack, the actions of DarkSide aligned closely with their motives. Their inaction to prevent the attack or prosecute the attackers signals at least passive approval of the activity, suggesting benefits to examining state roles for non-state actors in the kinetic domain and expanding these frameworks to include cyber.

Following the September 11 attacks on the United States, concepts of state responsibility for non-state actors broadened to include a failure to prevent their borders from being used to attack another state. This broadening allowed the United States to legitimately invoke

self-defense as the motivating factor for their invasion of Afghanistan, as signaled by the UN Security Council's approval of the incursion. Applying a similar concept to cyberspace is the key to discouraging state actors from employing non-state actors to carry out attacks, as the risks of retaliation may become too great if they hold imputed responsibility for the actions of non-state actors within their borders.

Bibliography

Abrams, A. (2019, April 18). *Here's What We Know So Far About Russia's 2016 Meddling*. Time. https://time.com/5565991/russia-influence-2016-election/

Bordoff, J. (2021, May 17). The Colonial Pipeline Crisis Is a Taste of Things to Come. *Foreign Policy*. https://foreignpolicy.com/2021/05/17/colonial-pipeline-crisis-cyberattack-ransomware-cybersecurity-energy-electicity-power-grid-russia-hackers/

Bussolati, N. (2015). The Rise of Non-State Actors in Cyberwarfare. In *Cyber War*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198717492.003.0007

Cohen, Z., & Sands, G. (2021, May 11). *Four key takeaways on the US government response to the pipeline ransomware attack*. CNN. https://www.cnn.com/2021/05/11/politics/colonial-pipeline-cyber-hearing-senate-homeland-security-committee/index.html

Commondification of cyber capabilites: A grand cyber arms bazaar. (2019). U.S. Department of Homeland Security, Public-Private Analytic Exchange Program.

Eilstrup-Sangiovanni, M. (2018). Why the World Needs an International Cyberwar Convention. *Philosophy & Technology*, *31*(3), 379–407. https://doi.org/10.1007/s13347-017-0271-5

Freedman, L. (2013). Disarmament and Other Nuclear Norms. *The Washington Quarterly*, *36*(2), 93–108. https://doi.org/10.1080/0163660X.2013.791085

Graham, D. E. (n.d.). *Cyber Threats and the Law of War*. *4*, 16.

Graham—Cyber Threats and the Law of War.pdf. (n.d.). Retrieved November 21, 2021, from https://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf

Greenberg, A. (2017, September 6). Hackers Gain Direct Access to US Power Grid Controls. *Wired*. https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/

Izycki, E., & Vianna, E. (2021, February 26). *Critical Infrastructure: A Battlefield for Cyber Warfare?* https://doi.org/10.34190/IWS.21.011

Jasper, S. (2021, June 1). Assessing Russia's role and responsibility in the Colonial Pipeline attack. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/

LaFrance, A. (2017, May 16). *Cyberwar Is Officially Crossing Over Into the Real World*. The Atlantic. https://www.theatlantic.com/technology/archive/2017/05/cyberwar-is-officially-crossing-over-into-the-real-world/526860/

Mauroni, A. (2019, October 8). *Deterrence: I Don't Think It Means What You Think It Means*. Modern War Institute. https://mwi.usma.edu/deterrence-dont-think-means-think-means/

Moone, L., & Quirk, P. (2021, January 15). Want global stability? Modify the U.S. approach to dealing with nonstate armed actors. *Brookings*. https://www.brookings.edu/blog/order-from-chaos/2021/01/15/want-global-stability-modify-the-u-s-approach-to-dealing-with-nonstate-armed-actors/

Nye, J. (2015, May 11). *International Norms in Cyberspace*. Project Syndicate. https://www.project-syndicate.org/commentary/international-norms-cyberspace-by-joseph-s--nye-2015-05

Plakokefalos, I. (2017). The Use of Force by Non-State Actors and the Limits of Attribution of Conduct: A Reply to Vladyslav Lanovoy. *European Journal of International Law*, *28*(2), 587–593. https://doi.org/10.1093/ejil/chx029

Ravinchandran, S. (2011, August 29). Non-State Conflict and the Transformation of War. *E-International Relations*. https://www.e-ir.info/2011/08/29/non-state-conflict-and-the-transformation-of-war/

Rogusi, P. (2020, March 6). *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*. Just Security. https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

Sanger, D. E., & Perlroth, N. (2021, May 14). Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity. *The New York Times*. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

Sankaran, S. (2021, August 30). *Council Post: Is The World Ready For A Cyberwar?* Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/08/30/is-the-world-ready-for-a-cyberwar-/

Shear, M. D., Perlroth, N., & Krauss, C. (2021, May 14). Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers. *The New York Times*.

https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html

Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. *Journal of Military Studies*, *4*(1), 1–37. https://doi.org/10.1515/jms-2016-0184

Smeets, M., & Soesanto, S. (n.d.). *Cyber Deterrence Is Dead. Long Live Cyber Deterrence!* Council on Foreign Relations. Retrieved November 16, 2021, from https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence

van der Meer, S. (2020). *How states could respond to non-state cyber-attackers*. Clingendael Institute. https://www.jstor.org/stable/resrep25677