Nina Musso
INT 498-01
Professor Cho

# Draft: Cyber Deterrence

## Abstract

The topic of cyber warfare has become increasingly important in today' s world. Few recognize how big of a deal it is with regards to a nation's interests and security. So much of the US economy, government, communications infrastructure, and military rely on the cyber realm that a prolonged absence of them caused by cyber attacks could send the nation into a state of confusion. The reality of cyber attacks and the increase in physical effects varies from the idea of hackers meddling in a system for trivial ends to a threat to a nation's interests. Scholars have long debated on the applicability of cyber deterrence. My intent in this paper is to provide some perspectives and generate discussion on the topic cyber deterrence and kinetic retaliation as being something that is limited and fails to deter future cyber attacks. Cyber deterrence is limited because technology is relatively inexpensive and widely available, it is difficult to attribute blame accurately, and there is difficulty in punishing attackers. When there is no detection or ability to punish, cyber deterrence is essentially pointless.

## Introduction

The rise of the digital age has greatly altered almost every aspect of life.[1] It has become the core that drives most modern enterprises. Many institutions used by civilians, infrastructures, and businesses, and government services have become increasingly reliant on the technologies.[2] There are many positive benefits of technology such as providing efficient ways to communicate,

[1] Goodwin, Tom. "The Three Ages of Digital." *Tech Crunch,* Verizon Media, 23 June 2016, https://techcrunch.com/2016/06/23/the-three-ages-of-digital/.
[2] Ibid.

share ideas, and transfer data. Along with the pros, there are cons that we too rarely discuss that are often overshadowed by the benefits. It was not until 2013 when Edward Snowden revealed to the public about US government surveillance programs that were collecting personal information and tracking people's actions.[3] On an individual level, we see how fragile technology can make us and recognize the infringements on individual rights. On an international level, depending on who collects the information, we recognize the potential threats to national security. Many of us do not realize how dangerous technology can be, especially when the intention is to use the information in a negative manner. For example, data is a crucial resource for organizations and there is an increasing threat to those data.[4] There are different types of cyber threats like authentication violations, which is getting your passwords stolen, or the Trojan horses and viruses, which is the spread of viruses that could erase files and leak information, and fraud.[5] This may sound harmless but an attack on one vulnerable sector can have serious damages on other sectors and start a chain reaction. These types of threats collectively have become known as cyber terrorism. Cyber terrorism is forcused on corrupting all components of technology so that an opponents systems collapses.[6] Depending on what information the attacker has on a nation, it could lead to the downfall of that nation and place the nation at a disadvantage. Governments like the US and Western Europe are well aware of the dangers posed by cyber attacks and are developing strategies of deterrence.[7] The battleground is

[3] "Edward Snowden: Leaks that Exposed US Spy Programme." *BBC News,* BBC, 17 Jan 2014, https://www.bbc.com/news/world-us-canada-23123964.

[4] Kumar, Vipin, Jaideep Srivastava, and Aleksandar Lazarevic, eds. *Managing cyber threats: issues, approaches, and challenges*. Vol. 5. Springer Science & Business Media, 2006. Page 4.

[5] Ibid., page 5.

[6] Ibid., page 7.

[7] Kugler, Richard L. "Deterrence of cyber attacks." *Cyberpower and national security* 320 (2009). https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-13.pdf?ver=2017-06-16-115053-773.

no longer limited by the geographical boundaries, it has expanded to the virtual world of the World Wide Web.

In the past few years, there have been an alarming increase in incidents of cyber attacks and it has become a major concern for all nations.[8] Currently, the socio-political environment is rather volatile and the increase in attacks disrupt the normal way of life.[9] Many scholars like Christopher Haley and Amir Lupovici believe that cyber deterrence can be an effective strategy if factors of capability, credibility, and communication (3 Cs) are strengthened.[10] In their papers, they offered lofty, theoretical ideas but did not provide real examples to support their claims, perhaps it is because some were written at least 10 years ago. I am hoping to add on to existing debates and possibly fill the gap of what scholars like Haley and Lupovici meant by improving deterrence for cyber and offer real examples. From what I gather, the way to improve cyber deterrence all points towards the presence of a kinetic retaliation. Does this mean that kinetic retaliation is needed for cyber deterrence to be successful? For one thing, cyber policies and laws can only do so much in an international setting and are often limited and short lived. Part of the answer for successful deterrence is connected to kinetic responses but I argue that in the end it does little to deter future cyber attacks. There are instances when deterrence can be successful without the use of kinetic force and in the cyber realm, it is not the only viable solution to deter cyber attacks. In this paper, I will shed light on even if these factors 3Cs are strengthened, cyber deterrence will continue to remain troublesome and ineffective. As a result, there is limited

[8] Albahar, Marwan. "Cyber attacks and terrorism: A twenty-first century conundrum." *Science and engineering ethics* 25, no. 4 (2019): 993-1006. https://link.springer.com/article/10.1007/s11948-016-9864-0.

[9] Ibid,.

[10] Haley, Christopher. “A Theory of Cyber Deterrence.” *Georgetown Journal of International Affairs,* 6 Feb 2013, https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley#:~:text=In%20deterrence%20theory%2C%20the%20objective,might%20choose%20to%20stand%20down, AND Lupovici, Amir. "Cyber warfare and deterrence: Trends and challenges in research." *Military and Strategic Affairs* 3.3 (2011): 49-62. https://i-hls.com/wp-content/uploads/2013/02/Cyber-Warfare-and-Deterrence.pdf.

value in pursuing classical deterrence in the cyber realm through denial and punishment because technology is relatively inexpensive and widely available, it is difficult to attribute blame accurately, and there is difficulty when it comes to punishing attackers. When there is no detection or ability to punish, cyber deterrence is pointless.

The paper is organized in the following structure with first defining cyber deterrence. Then it moves on more in depth discussion on existing debates regarding deterrence and whether or not it is applicable to the virtual space. Next, case studies will be broken down into two groups: one being non-kinetic retaliation focusing on the US, Russia, and China relations, and second being kinetic retaliation focusing on US and Israel actions. These cases will help to show whether or not kinetic retaliation is the sole answer for a successful cyber deterrence. Subsequently, I will analyze the consequences of a kinetic response and show that the unintended consequences does nothing to deter future actions, and contributes to the failure of cyber deterrence. Then I will conclude with a recommendations section that points out the most effective ways to address cyber attacks.

## What is Cyber Deterrence?

To understand what cyber deterrence is, we have to first understand the concept of deterrence. Deterrence is not a new phenomenon, it has been around since the 1950s.[11] Shortly after World War II deterrence rose in prominence, where bargaining power was employed to avoid wars, specifically nuclear war, through means of intimidation.[12] During the Cold War with the Soviet Union, the deterrent strategy was largely shaped by the US effort to build a nuclear offensive that can inflict massive retaliation in response to Soviet nuclear efforts.[13] Accordingly,

[11] Taddeo, Mariarosaria. “The Limits of Deterrence Theory in Cyberspace.” Page 341.
[12] Ibid.
[13] Kugler, Richard. “Deterrence of Cyber Attacks.” page 10.

the states assumed that the Soviet Union would act rationally.[14] In terms of defining deterrence, it is difficult to pinpoint one definition since there is no consensus on one definition. Some scholars believe that the concept of deterrence cannot be separated from the threat of punishment. In different papers, the concept has been used with slight variations. For example, Thomas Schelling, a classic theorist, stressed the importance of threat when talking about deterrence in *The Strategy of Conflict* and in *Arms and Influence,* he provided a broad definition of deterrence as to prevent an action through the fear of consequences.[15] Glenn Snyder, another classic theorist, defined deterrence as dissuading others by sanctions or rewards.[16] Generally speaking, deterrence is a strategy to prevent or influence an adversary from attacking by making the adversary see that the costs of the action will not be worth it. As noted by Bendiek and Metzger in "Deterrence Theory in the Cyber-Century: Lessons From a State-of-the-Art Literature Review", deterrence requires two components. The first is the intention to defend and second is the ability to achieve defence.[17] In other words, it is a coercive strategy with the goal of convincing the opponent to behave in a desirable way. When applied to the cyber realm, it is known as cyber deterrence, which focuses on the prevention of cyber attacks.

### *Classical vs Modern Interpretations*

Cyberspace is multidimensional and involves the public and private sectors.[18] This means that governments do not have the same level of control as they would have in a physical

[14] Ibid.

[15] Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, Mass.: Harvard University Press, 1960), p. 6 AND Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press, 1966), p. 71.

[16] Glenn H. Snyder. *Deterrence and Defense: Toward a Theory of National Security*. (Princeton, N.J.: Princeton University Press, 1961), pp. 9–10.

[17] Bendiek, Annegret and Metzger, Tobias. "Deterrence Theory in the Cyber-Century: Lessons From a State-of-the-Art Literature Review." *Lecture Notes in Informatics,* Gesellschaft for Informatics (2015). https://subs.emis.de/LNI/Proceedings/Proceedings246/553.pdf. Page 555.

[18] Harding, Brian. "Cyber Deterrence." *Air University,* Air Force Institute, 11 Feb 2016, 812931.pdf. Page 2.

space.[19] The classical interpretation of deterrence is through denial and punishment.[20] Deterrence by denial is a strategy where opponents are physically prevented from obtaining technology that will be used to threaten another state.[21] For this to be successful, denial must meet three criterias: capability, which refers to the ability to procure material, capacity, and the means of conducting a successful attack, credibility, which refers to the belief that the opponent must have that the defending state is capable of inflicting harm and will use that capability, and communication, which means the defending states ability to communicate the threat and costs clearly.[22] Deterrence by punishment is a way to discourage undesirable behaviour and the strategy of punishment is seen as a last resort.[23] Modern interpretations of cyber deterrence have extended to include deterrence by futility, which is meant to deter future attackers by minimising the effects of a cyber attack. The method to deter is to prevent the adversary from hacking successfully in the first place.

## Cyber Deterrence Debate and Failures

There has been ongoing debate on whether or not cyber deterrence is achievable. According to pro-deterrence theorist Sir Michael Quinlan, there is “no such thing as an undeterrable state”, deterrence to be successful, regardless of which realm.[24] However, thus far, there has not been any one-hundred percent success deterrence case in the cyber realm. Other pro scholars believe that cyber deterrence can be a great strategy only if changes are made to strengthen the 3Cs.

[19] Ibid., page 3.

[20] Lowther, Adam. "Understanding Deterrence." Chapter 3 in Deterrence in the Twenty-first Century., London, UK: Proceedings. September 2010.

[21] Ibid.

[22] Kenneth Geers, “The Challenge of Cyber Attack Deterrence.” Law & Security Review, Vol 26, 2010.

[23] Lowther, Adam. "Understanding Deterrence."

[24] Michael Quinlan, “Deterrence and Deterrability,” in Deterrence and the New Global Security Environment, ed. Ian R. Kenyon and John Simpson (London: Routledge, 2006), 5.

On the other side, scholars believe that cyber deterrence is not achievable and are focused on the challenges posed by cyber deterrence. They argue that deterrence is not applicable to the cyber realm because deterrence is a psychological process which fails due to misperceptions.[25] Deterrence depends on “the perceptions of both the actors and the targets, and the ability to communicate those views clearly”, which leaves a lot to interpretation.[26] Cyber deterrence is expected to fail due to the factors of capabilities, credibilities, and communication that the pro-deterrence side says needs to be strengthened.[27] And according to Joseph Nye, there are four factors that are in the way of cyber deterrence success and that is retaliatory threat, denial by defense, fear of entanglement, and norms.[28] Cyber warfare enables opponents to move confrontations in a sphere where they can maximize profits without taking a huge risk.[29] This makes deterrence difficult to accomplish because the ability to retaliate is greatly reduced and thus the credibility of the threat is lessened.[30] The challenge with credibility is the defenders willingness to use its capabilities in fear that things would go out of hand.[31] The problem may escalate into something that is more dangerous.[32] In turn this signals to the opponent that the defender is unlikely to respond and may result in the opponent taking more risks to challenge the defender. The third issue is the defender’s ability to communicate the threat.[33] In order to convey a message, the defender must identify the opponent, otherwise it is an empty threat.[34] Cyber attacks are often done anonymously and there is usually no identifiable physical

[25] Kugler, Richard. “Deterrence of Cyber Attacks.” Page 10.
[26] Nye, p. 53
[27] Lupovici, Amir. "Cyber warfare and deterrence: Trends and challenges in research." P. 52.
[28] Nye, “Deterrence and Dissuasion in Cyberspace,” Page 53.
[29] Taddeo, Mariarosaria. “The Limits of Deterrence Theory in Cyberspace.” Page 341.
[30] Ibid.
[31] Ibid., page 342.
[32] Ibid.
[33] Ibid., page 343.
[34] Morgan, Patrick. “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm.” *The National Academies Press*, 2010. https://www.nap.edu/read/12997/chapter/1. Page 56.

location.[35] Defense in the cyber realm is porous in nature since every system is different and has vulnerabilities, which limits the potential to deter new attacks.[36] If cyber deterrence is not done correctly, the consequences range from exposing knowledge to revealing assets and strategies.[37]

The flaw of cyber deterrence is that it does not offer advice on how to avoid crises or how to decide whether the national interests at stake are sufficient enough to warrant the use of physical response.[38] Accordingly, deterrence remains in the cognitive domain, and is essentially an influence operation shaped by the interplay of credibility, capability, and communication.[39] Unlike the Cold War, deterrence was risky but it was successful because first, it was credible since the US made efforts to not only maintain it but improve it, second during the time, nuclear war was not viewed as isolated from larger events, and third, US deterrence strategies prevented the Soviets from any favorable gains.[40] That being said, cyber deterrence is nowhere near that of the Cold War deterrence.

## Deterrence is not Applicable to the Cyber Realm

Typically, deterrence is employed by military strategies to prevent the proliferation of nuclear arms among states. Considering how vast the cyber realm is with essentially no physical boundaries, it is not feasible to apply deterrence to it in the same way as nuclear deterrence. Cyberspace is organized differently, accessed by many users, and there is the presence of

[35] Kostyuk, Nadiya. "Determinants of the Cyber Escalation Ladder." *The Cyber Defense Review,* Army Cyber Institute, 2018, pp. 124, https://ezproxy.tcnj.edu:2117/stable/pdf/26427380.pdf?ab_segments=0%252Fbasic_search_gsv2%252Fcontrol&refreqid=excelsior%3Aa9cb0f2eb08765d2e8828289bd3bdade.

[36] Shad, Dr. Muhammad. "Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions." *Policy Perspectives,* Pluto Journals, pp. 45, https://ezproxy.tcnj.edu:2117/stable/pdf/10.13169/polipers.15.2.0041.pdf?ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3A966b08c092096dff3e9cef6f1ee2f131.

[37] Ibid. page 46.

[38] Kostyuk, Nadiya. "Determinants of the Cyber Escalation Ladder." Page 132.

[39] Ibid.

[40] Kugler, Richard. "Deterrence of Cyber Attacks." page 12.

non-state actors.[41] Instead, deterrence should be seen as a mitigating effort that leads potential attackers to believe it is not in their best interest to attack. These efforts can be enhanced by improving the accuracy of attribution, the description of cyber incidents, and ensuring that timely action is taken against cyber attackers. Cyber deterrence is not limited to relationships between states but has expanded to incorporate the malicious activity of non-state actors. Cyber attacks can be undertaken by almost anyone, with or without state affiliation, who has computing knowledge.

Traditional deterrence theory is difficult to be applied to cyberspace since it is very different from the conventional and nuclear counterparts. The consequences of cyber-attacks vary from negligible to potentially severe. In contrast to the Cold War, cyber deterrence offers a low-cost, low consequences, and non-attributable means for weakening an adversary.

In support of the "no" side of the cyber deterrence debate, a critical issue that scholars do not talk about is understanding what type of actors are likely to pose cyber threats. Many view cyber attackers as mainly lonewolf hackers with malicious intent, or small criminal groups intending to profit off of the information collected. Other actors are terrorist groups, rogue states, and big powers with political or ideological agendas. These actors will use cyber threats to pursue strategic goals and use the information as instruments of persuasion and coercion. Understanding these different types of actors, will enable a more effective deterrent strategy.

## Case Studies - Non-Kinetic Cyber Response

Since the rise of the digital age, there have been thousands of cyber attacks. The normal response to these attacks is always reactive. When an adversary hacks into a system, the

[41] Kenneth Geers, "The Challenge of Cyber Attack Deterrence."

defender's response is placing sanctions or amending cyber policies.  Thus far, these actions are limited and do not deter future attacks.

Internal laws and policies regarding cyberspace have existed since the early 1900s.  In the 1907 Hague Conventions where nations were required to recognize cyber neutrality and layed out acceptable expectations.[42]  For a nation to claim cyber neutrality, “a nation cannot originate a cyber attack, and it also has to take action to prevent a cyber attack from transiting its internet nodes” and all nations are expected to recognize this right.[43]  This law is rather weak and limited because it is difficult to implement and if a nation fails to take accurate measures against an adversary, it risks losing the cyber neutral status.  On top of that, there is no consequence of violating this international law and completely relies on the honor code system.

*U.S.*

Focusing on just American, in ways of combating cyber attacks, deterrence has been discussed in some key strategy documents.  With the growing prospect of cyber threats, the White House in 2003 issued the *National Strategy to Secure Cyberspace* that articulated three cyber policies of preventing the cyber attacks, reducing vulnerability to them, and minimizing the damage and being able to recover.[44]  However, these policies contained little on how to actually prevent the attacks.  In regards to the concept of deterrence, it stated that “a U.S. response might not be limited to criminal prosecution of cyberspace criminals and that the United States reserves the right to respond in an appropriate manner”.[45]  This is not only lacking

[42] Korns, Steohen and Kasteberg, Joshua. “Georgia's Cyber Left Hook.” *U.S. Army,* 7 Apr. 2009, https://www.army.mil/article/19351/georgias_cyber_left_hook.
[43] Ibid.,
[44] Kugler, Richard. “Deterrence of Cyber Attacks.” https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-13.pdf?ver=2017-06-16-115053-773.  Page 2.
[45] Ibid.,

but it is extremely vague. In another strategy document issued in 2006 called the *National Security Strategy of the United States of America*, nine goals and policies were laid out. The policies ranged from terrorism to preventing the spread of mass destruction. Where the document fell down was that it devoted little on cyber threats and how to deter it. Although there has been an exponential increase in these policies, there is still much at risk and it is essentially all talk, with limited actions.[46] For example, the 2016 election was a wake-up call for the US that the digitized election systems are vulnerable to cyber attacks. The attack was traced to the Russians who targeted US campaigns, candidates, and operations intended to undermine American confidence in democracy.[47] According to the Center for Strategic and International Studies, efforts were made to secure infrastructures and basic cyber policies have been implemented and the US is in a better position to deal with cyber threats now.[48] However, there is more to do to ensure complete resilience from cyber attacks.

### *Russia*

The cyber capabilities of Russia is one of the most sophisticated. The Office of U.S. National Counterintelligence noted "Moscow's highly capable intelligence services are using HUMINT [human intelligence], cyber, and other operations to collect economic information and technology to support Russia's economic development and security".[49] Russia conducts extensive cyber attacks on the U.S because it deems America as a long-term threat. The Wall

[46] "CSIS Cyber Policy Task Force." *Center for Strategic & International Studies,* CSIS, https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/other-projects-cybersecurity-7.

[47] "CSIS Election Cybersecurity Scorecard: The Outlook for 2018, 2020 and Beyond." *Center for Strategic & International Studies,* CSIS, https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/csis-election-cybersecurity.

[48] Ibid.,

[49] NCIX Report, supra, at p. 5. http://www.ncix.gov/publications/reports/fecie_
all/Foreign_Economic_Collection_2011.pdf

Street Journal reported in 2009 that Russia had penetrated the U.S. electrical grid that did not cause any damages but it left behind software programs where the purpose was to navigate U.S. systems and controls to map out infractures.[50] The F.B.I is aware of these attacks and having an effective response to deter Russia is challenging. In the Pentagon, plans were drawn on how to counter Russian actions but they were never formally presented to the president, and thus, failed to go into effect. In the 2016 U.S. Presidential election, Russia was suspected of hacking and influencing the outcome of the election process. There was no retaliation of any kind. At the Group of 20 meeting in China, Obama gave Putin a warning of "a strong American response if there was continued effort to influence the election or manipulate the vote" according to White House officials.[51] In the current Biden administration, Russia cyber related attacks are an ongoing issue. The administration hopes to deter intrusions on governmental and corporate systems. To address it, actions used would be a combination of economic sanctions, private actions, and an executive order to strengthen federal government networks.[52] The outcome of this is yet to be determined but it is highly likely that it will be unsuccessful given that sanctions have already been attempted by other countries. Strengthening governmental networks might work but given the nature that cyberspace evolves, it may provide temporary success. Various investigations are underway to understand the tools and tradecraft of Russia in their attempt to

[50] Cilluffo, Frank J. "Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure." *US House of Representatives, Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Homeland Security Policy Institute,* The George Washington University, the National Security Archive Website 20 (2013). https://www.defensetech.org/meetings/HM/HM08/20130320/100523/HHRG-113-HM08-Wstate-CilluffoF-20130320.pdf. P. 10

[51] Lipton, Eric and et.al. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.". *The New York Times,* The New York Times Company, 13 Dec. 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[52] Sanger, David and et. al. "Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China". *The New York Times,* The New York Times Company, 23 March 2021, https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html.

influence the election.[53] In terms of cyber deterrence, “there has been relatively no cost to this kind of asymmetric information and cyber campaign from Russia...other than new sanctions passed by Congress to address cyber activity, very little has been done to counter this type of campaign”.[54] During the Obama administration, different kinds of deterrence was pursued for cybersecurity. The cyberdefenses sought deterrence by denial, which hoped to deny adversaries benefits gained through cyber attacks. They also included deterrence by punishment by warning that the risks greatly outweigh the gains and “suffer unacceptable costs”.[55] Deterrence by punishment gained more attention because other strategies were not working.[56] The administration believed that strengthening international law and norms on cyberspace would work and offered policies for the UN Group of Governmental Experts to consider. One policy was “states should not conduct or support cyberopertations that damage or impair critical infrastructure or harm information systems used by another state’s computer emergency response teams” and another was “states should respond to requests for assistance by other states whose critical infrastructure experiences malicious cyberacts”.[57] These policies sound good on paper but are not effective and cyberespionage continued. Sanctions placed on Russia did little and sparked debates on where that was enough to deter Russia and other countries. Russia brushed off the sanctions as something minor since Trump was going to be the next president. Going back to deterrence by punishment, it intensified debates because politicians and experts disagreed on whether it made sense in the cyber realm.

[53] Zarate, Juan. “The Cyber Attacks on Democracy.” *The Catalyst: A Journal of Ideas From the Bush Institute,* Fall 2017, https://www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy.html.

[54] Ibid.,

[55] Fidler, David P., "The U.S. Election Hacks, Cybersecurity, and International Law" (2017). Articles by Maurer Faculty. 2607. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3607&context=facpub. P. 338.

[56] Ibid., p 338.

[57] Ibid., p 340.

Russia has also conducted cyber operations in other countries such as Estonia. On April 27, 2007, Estonia was hit by major cyber attacks that lasted for weeks. "Online services of Estonia banks, media outlets and government bodies were taken down by unprecedented levels of internet traffic" and resulted in the inability to utilize online services and communicate.[58] Estonia being part of NATO was also part of the Article Five alliance, where members would help and defend each other in any form of attacks. However, this agreement is pointless in cyberspace because "Article Five would only be triggered if a cyber-attack results in major loss of life equivalent to traditional military action".[59] Although the attacks were from a Russian IP address, there was no evidence that the order for the attack was given by the Russia government or loss of lives and thus there was no retaliation.

When confronted with the attacks, the Russian government denied any involvement. Cyberspace has proven to be a goldmine for criminals with opportunities for profits. In 2011, Russia's cyber markt was pegged at $2.3 billion and there are indications that crime organizations are joining hands "by sharing data and tools" to increase their take.[60]

### *China*

Another country with sophisticated cyber capabilities is China. They have demonstrated a striking level of perseverance as evident in the number of attacks and acts of espionage it has committed. Reports from the U.S. National Counterintelligence characterizes these activities as rising to the level of strategic threat to the U.S. national interests.[61] China's aggressive data

[58] McGuinness, Damien. "How a Cyber Attack Transformed Estonia." *BBC News,* 27 Apr. 2017, https://www.bbc.com/news/39655415.

[59] Ibid.,

[60] Group IB, State and Trends of the Russian Digital Crime Market 2011, p. 6, http://groupib.com/images/media/Group-IB_Report_2011_ENG.pdf.

[61] "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace", Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011 (October 2011). http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf .

collection seems to target whatever (military, commercial) will further secure an advantage for the country over competitors and adversaries. According to the Mandiant report, the culprit behind the theft of "hundreds of terabytes of data from at least 141 organizations...beginning as early as 2006" is the Chinese PLA Unit 61398.[62] Like Russia, the Chinese government denies hacking allegations. The U.S. response to these cyber attacks is taking a tougher tone on China. Although it represents a good step forward, it is only the beginning of a long path that we are traveling too slowly and weakly on. Thomas Donilon, the National Security Advisor, stressed the importance of handling this problem with China. He called on China to stop their intrusive activities and tried to engage in a constructive dialogue to establish acceptable cyberspace norms.[63] However, getting China to comply was useless and the problem remains.

## Case Study- Kinetic Cyber Response

Given the failures of cyber deterrence addressed prior, perhaps kinetic retaliation is needed to deter cyber attacks. Here I will address two cases where a nation responded with drone strike to get rid and prevent adversary attacks. The first case is the US response to an ISIS hacker and the second Israel response to Hamas. In both cases we see that the physical response worked but the questions remain as to where or not it is the appropriate response.

### *US Drone Strike on ISIS Hacker*

The rise of the Islamic State of Iraq and Syria (ISIS) has dramatically impacted Iraq, Syria, and most of the Middle East. ISIS continues to grow and with their systematic abuses of human rights and violations of international law, they are a threat to international peace and

[62] Rains, Tim. "The Threat Landscape in China: A Paradox" (March 11, 2013). http://blogs.technet.com/b/security/ .

[63] Donilon, supra.

security.[64] The US, along with countries in Europe and the Middle East, have taken on crucial roles in combating ISIS. Since 2014, airpower has had a major role in Operation Inherent Resolve (OIR). Through strategic airstrikes, ISIS offensives on Baghdad, Erbil, and Kobani were halted, and ISIS finances were weakened from targets on their cash reserves and oil business.[65] In addition to that, Iraq and Syria were able to retake territory from ISIS. However, this does not mean that the ISIS threat is over. Instead, the threat has expanded to the virtual world. As early as 2015, the terrorist organization has used the internet to fulfill their goals of radicalization.[66] ISIS's use of cyberspace became known as the cyber jihad, which "refers to use of 21st century technological tools and cyberspace (the environment in which communication between computer and networks occurs) in order to promote the notion of violent jihad against those classified by its followers as enemies of Islam".[67] According to American officials and studies, ISIS targets and exploits online networks (Twitter, Facebook, Instagram) at an unprecedented scale with up to 90,000 posts a day disseminating propaganda.[68] Cyber jihad has become an integral part of ISIS's overall strategy.

On August 28, 2015, US admitted to a drone strike targeted at ISIS hacker Junaid Hussain. Hussain was the Islamic State's chief English-language cyber influencer, where he plotted cyber attacks, recruited, and inspired others to follow the same path.[69] as alleged to have hacked websites and Twitter accounts, and posting personal information about US military

[64] "About Us - The Global Coalition to Defeat ISIS." *U.S. Department of State,* U.S. Department of State, *https://www.state.gov/about-us-the-global-coalition-to-defeat-isis/*.

[65] Wasser, Becca, Stacie L. Pettyjohn, Jeffrey Martini, Alexandra T. Evans, Karl P. Mueller, Nathaniel Edenfield, Gabrielle Tarini, Ryan Haberman, and Jalen Zeman, The Role of U.S. Airpower in Defeating ISIS. Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/research_briefs/RBA388-1.html.

[66] Hoffman, Adam and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)." https://www.inss.org.il/wp-content/uploads/systemfiles/adkan18_1ENG%20(5)_Hoffman-Schweitzer.pdf. Page 71.

[67] Ibid., page 71-72.

[68] Ibid., page 73.

[69] Hamid, Nafees. "The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain." *Combating Terrorism Center,* Apr. 2018, https://ctc.usma.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/.

officials and making threats against them.[70] Hussain was a threat to nations and became the first hacker in history to be killed by an airstrike. From this, some ISIS cyber capabilities were crippled and it serves as a template for future cyber actions against terror groups and deter cyber attacks. In actually taking action, it took the US a while to identify Hussain and locate his whereabouts.

The drone strike did nothing to stop cyber operations conducted by ISIS. Instead, since the strike, there has been expansion in ISIS cyber capabilities to inflict damages and "manipulate the resources of cyberspace for recruitment and the spread of propaganda".[71] This has allowed ISIS activists to outpace national cyber security efforts. On top of this, ISIS cyber jihad strategy encourages "lone wolf" attacks, who are not officially connected to the organization but are inspired.

*Israel Drone Strike on the Hamas*

There has been a long history of conflict between Israel and Palestine. Both want the same land and a compromise has been difficult to achieve. Their claims date back thousands of years and the current political conflicts began in the early 20th century.[72] Hamas, the Palestinian faction that controls the Gaza Strip, between Israel and Egypt, have fallen into "a bloody and

[70] Lawson, Sean. "With Drone Strike on ISIS Hacker U.S. Escalates its Response to Cyber Attacks." *Forbes,* 12 Sept. 2015, https://www.forbes.com/sites/seanlawson/2015/09/12/with-drone-strike-on-isis-hacker-u-s-escalates-its-response-to-cyber-attacks/?sh=7c1c4834b6a8.

[71] Smith, Troy E. "The Specter of Cyber in the Service of the Islamic State: The Zeros and Ones of Modern Warfare." *American Intelligence Journal*, vol. 34, no. 1, 2017, pp. 54–58. *JSTOR*, www.jstor.org/stable/26497117. Page 54.

[72] Beauchamp, Zack. "What are Israel and Palestine? Why are they Fighting?" *Vox,* Vox Media, LLC., 14 May 2018, https://www.vox.com/2018/11/20/18080002/israel-palestie-conflict-basics.

fiery dance" in the past few years.[73] Both sides remain in a constant state of on and of conflict, always on the verge of turning into major war.

On May 5, 2019, the Israely Defense Force (IDF) successfully removed the cyber threat posed by Hamas. Hamas were building cyber operations that were aimed at "harming the quality of life of Israeli citizens", which meant anything from attacking civilian infrastructure to interrupting communications and military operations.[74] The IDF targeted a building where the Hamas cyber operatives worked and after the strike, they no longer had cyber capabilities. The strike was the first true example of a physical attack being used as a real-time response to digital aggression.

After the Israely drone strike, violence erupted as Hamas and launched their attacks. "Hamas fired more than 600 rockets into Israel, while the IDF conducted its own strikes against hundreds of what it characterized as military targets".[75] As a result of these physical attacks, hundreds were wounded and at least 27 Palestinians and 4 Israeli citizens were killed; tensions between Israel and Hamas worsened and protests and violence have broken out periodically.[76] The current relations between Israel and Palestine is spilling over into the cyber realm with increases in cyber aggression.[77]

[73] Holmes, Oliver. "Israel-Hamas Relations: A Predictable but Fatal Dance." *The Guardian,* Guardian News & Media Limited, 26 Mar 2019, https://www.theguardian.com/world/2019/mar/26/israel-hamas-relations-a-predictable-but-fatal-dance.

[74] Borghard, Erica and Schneider, Jacquelyn. "Israel Responded to a Hamas Cyberattack with an Airstrike. That's not such a Big Deal." *The Washington Post,* 9 May 2019, https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/ AND Cropsey, Seth. "Hamas Cyber Attack and Israel's Armed Response." *Hudson Institute,* Hudson Institute, Inc., https://www.hudson.org/research/15016-hamas-cyber-attack-and-israel-s-armed-response.

[75] Liptak, Andrew. "Israel Launched an Airstrike in Response to a Hamas Cyberattack." *The Verge,* Vox Media, 5 May 2019, https://www.theverge.com/2019/5/5/18530412/israel-defense-force-hamas-cyber-attack-air-strike.

[76] Ibid.,

[77] Hochberg, Leo and Campbell, Eliza. "The Potential Cyber Consequences of Israeli Annexation of Palestinian Territory." *MEI: Peace, Prosperity, Partnership,* Middle East Institute, 20 July 2020, https://www.mei.edu/publications/potential-cyber-consequences-israeli-annexation-palestinian-territory.

## Is Kinetic Retaliation the Right Response?

From what I am seeing, there are basically two approaches to cyber attacks: cyber deterrence and cyber defense. Based on the concerns that the scholars have with cyber deterrence, on the surface a kinetic retaliation seems to solve that problem. A physical response can be communicated clearly, it can be a credible response given a state's military capabilities. Kinetic retaliation may cripple an adversary's cyber capabilities but it does not deter future attacks like the concept of cyber deterrence. In theory it is supposed to work but technology is constantly advancing and hackers are becoming more and more sophisticated. The cyber conflict will continue to evolve and be difficult to eradicate.

Being a more successful response, kinetic retaliation can get out of hand. It can trigger adversaries and escalate into a full on war. The adversaries in term can conduct drone strikes and have the capability to inflict physical harms as well. There is limited value in pursuing classical deterrence in the cyber realm through denial and punishment because technology is relatively inexpensive and widely available, it is difficult to attribute blame accurately, and there is difficulty in punishing attackers. A more effective approach would be focusing on cyber defenses.

## Conclusion

In the age of globalization, where communities are interconnected, a cyber attack can damage a nation's vital infrastructures and threaten national security. Cyberspace being a virtual world is difficult to manage, much less control. There has been much debate on whether or not cyber deterrence can be achievable and the debates will continue. Deterrence, although applicable to nuclear warfare, is limited when applied to the cyber realm for many reasons. The concept of denial and punishment fails to deter cyber attacks because there is nothing to hold responsibility to attackers. Kinetic retaliation as seen with the drone strikes would stop the hackers temporarily but it just agitates adversaries. One would think that a kinetic response would signal to others that a state will have the capability to use brute force but it also fails to deter future attacks.

The most effective way to deter cyber attacks may not be through deterrence or kinetic retaliation, but through the development of a response mechanism to guide deterrence. A resilient system is needed to share collective responsibility in cyber security, increase capabilities through the involvement of penetration detection, create norms with enforcement capabilities, and strengthen international law enforcement, cooperation, and legislation. Without an effective way to combat cyber attacks, the potential damages could extend beyond the technological systems to the loss of lives.

## Bibliography

"About Us - The Global Coalition to Defeat ISIS." *U.S. Department of State,* U.S. Department of State, *https://www.state.gov/about-us-the-global-coalition-to-defeat-isis/*.

Albahar, Marwan. "Cyber attacks and terrorism: A twenty-first century conundrum." *Science and engineering ethics* 25, no. 4 (2019): 993-1006. https://link.springer.com/article/10.1007/s11948-016-9864-0.

Beauchamp, Zack. "What are Israel and Palestine? Why are they Fighting?" *Vox,* Vox Media, LLC., 14 May 2018, https://www.vox.com/2018/11/20/18080002/israel-palestie-conflict-basics.

Bendiek, Annegret and Metzger, Tobias. "Deterrence Theory in the Cyber-Century: Lessons From a State-of-the-Art Literature Review." *Lecture Notes in Informatics,* Gesellschaft for Informatics (2015). https://subs.emis.de/LNI/Proceedings/Proceedings246/553.pdf.

Borghard, Erica and Schneider, Jacquelyn. "Israel Responded to a Hamas Cyberattack with an Airstrike.

That's not such a Big Deal." *The Washington Post,* 9 May 2019, https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/ .

Cilluffo, Frank J. "Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure." *US House of Representatives, Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Homeland Security Policy Institute,* The George Washington University, the National Security Archive Website 20 (2013). https://www.defensetech.org/meetings/HM/HM08/20130320/100523/HHRG-113-HM08-Wstate-CilluffoF-20130320.pdf.

"CSIS Election Cybersecurity Scorecard: The Outlook for 2018, 2020 and Beyond." *Center for Strategic & International Studies,* CSIS, https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/csis-election-cybersecurity.

"CSIS Cyber Policy Task Force." *Center for Strategic & International Studies,* CSIS, https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/other-projects-cybersecurity-7.

Cropsey, Seth. "Hamas Cyber Attack and Israel's Armed Response." *Hudson Institute,* Hudson Institute, Inc., https://www.hudson.org/research/15016-hamas-cyber-attack-and-israel-s-armed-response.

"Edward Snowden: Leaks that Exposed US Spy Programme." *BBC News,* BBC, 17 Jan 2014, https://www.bbc.com/news/world-us-canada-23123964.

Fidler, David P., "The U.S. Election Hacks, Cybersecurity, and International Law" (2017). Articles by Maurer Faculty. 2607. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3607&context=facpub.

"Foreign Spies Stealing U.S. Economic Secrets in Cyberspace", Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011 (October 2011). http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf .

Glenn H. Snyder. *Deterrence and Defense: Toward a Theory of National Security*. (Princeton, N.J.: Princeton University Press, 1961).

Goodwin, Tom. "The Three Ages of Digital." *Tech Crunch,* Verizon Media, 23 June 2016, https://techcrunch.com/2016/06/23/the-three-ages-of-digital/.

"Group IB, State and Trends of the Russian Digital Crime Market". (2011), http://groupib.com/images/media/Group-IB_Report_2011_ENG.pdf.

Haley, Christopher. "A Theory of Cyber Deterrence." *Georgetown Journal of International Affairs,* 6 Feb 2013, https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley#:~:text=In%20deterrence%20theory%2C%20the%20objective,might%20choose%20to%20stand%20down,

Hamid, Nafees. "The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain." *Combating Terrorism Center,* Apr. 2018, https://ctc.usma.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/.

Hochberg, Leo and Campbell, Eliza. "The Potential Cyber Consequences of Israeli Annexation of Palestinian Territory." *MEI: Peace, Prosperity, Partnership,* Middle East Institute, 20 July 2020, https://www.mei.edu/publications/potential-cyber-consequences-israeli-annexation-palestinian-territory.

Hoffman, Adam and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)." https://www.inss.org.il/wp-content/uploads/systemfiles/adkan18_1ENG%20(5)_Hoffman-Schweitzer.pdf.

Holmes, Oliver. "Israel-Hamas Relations: A Predictable but Fatal Dance." *The Guardian,* Guardian News

& Media Limited, 26 Mar 2019, https://www.theguardian.com/world/2019/mar/26/israel-hamas-relations-a-predictable-but-fatal-dance.

Kenneth Geers, “The Challenge of Cyber Attack Deterrence.” Law & Security Review, Vol 26, 2010.

Korns, Steohen and Kasteberg, Joshua. “Georgia's Cyber Left Hook.” *U.S. Army,* 7 Apr. 2009, https://www.army.mil/article/19351/georgias_cyber_left_hook.

Kugler, Richard L. "Deterrence of cyber attacks." *Cyberpower and national security* 320 (2009). https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-13.pdf?ver=2017-06-16-115053-773.

Kumar, Vipin, Jaideep Srivastava, and Aleksandar Lazarevic, eds. *Managing cyber threats: issues, approaches, and challenges*. Vol. 5. Springer Science & Business Media, 2006.

Lawson, Sean. “With Drone Strike on ISIS Hacker U.S. Escalates its Response to Cyber Attacks.” *Forbes,* 12 Sept. 2015, https://www.forbes.com/sites/seanlawson/2015/09/12/with-drone-strike-on-isis-hacker-u-s-escalates-its-response-to-cyber-attacks/?sh=7c1c4834b6a8.

Lebow, Richard N. “Thucydides and Deterrence,” Security Studies 16, no. 2 (2007): 163–188, https://doi.org/10.1080/09636410701399440.

Liptak, Andrew. “Israel Launched an Airstrike in Response to a Hamas Cyberattack.” *The Verge,* Vox Media, 5 May 2019, https://www.theverge.com/2019/5/5/18530412/israel-defense-force-hamas-cyber-attack-air-strike.

Lipton, Eric and et.al. “The Perfect Weapon: How Russian Cyberpower Invaded the U.S.”. *The New York Times,* The New York Times Company, 13 Dec. 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

Lowther, Adam. "Understanding Deterrence." Chapter 3 in Deterrence in the Twenty-first Century., London, UK: Proceedings. September 2010.

Lupovici, Amir. "Cyber warfare and deterrence: Trends and challenges in research." *Military and Strategic Affairs* 3.3 (2011): 49-62. https://i-hls.com/wp-content/uploads/2013/02/Cyber-Warfare-and-Deterrence.pdf.

McGuinness, Damien. “How a Cyber Attack Transformed Estonia.” *BBC News,* 27 Apr. 2017, https://www.bbc.com/news/39655415.

NCIX Report, supra, at p. 5. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Nye, “Deterrence and Dissuasion in Cyberspace,”

Sanger, David and et. al. “Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China”. *The New York Times,* The New York Times Company, 23 March 2021, https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html.

Quinlan, Michael. “Deterrence and Deterrability.” *Deterrence and the New Global Security Environment*, Ian R. Kenyon and John Simpson (London: Routledge, 2006).

Rains, Tim. “The Threat Landscape in China: A Paradox” (March 11, 2013). http://blogs.technet.com/b/security/ .

Smith, Troy E. “The Specter of Cyber in the Service of the Islamic State: The Zeros and Ones of Modern Warfare.” *American Intelligence Journal*, vol. 34, no. 1, 2017, pp. 54–58. *JSTOR*, www.jstor.org/stable/26497117.

Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press, 1966).

Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, Mass.: Harvard University Press, 1960).

Wasser, Becca, Stacie L. Pettyjohn, Jeffrey Martini, Alexandra T. Evans, Karl P. Mueller, Nathaniel Edenfield, Gabrielle Tarini, Ryan Haberman, and Jalen Zeman, The Role of U.S. Airpower in Defeating ISIS. Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/research_briefs/RBA388-1.html.

Zarate, Juan. “The Cyber Attacks on Democracy.” *The Catalyst: A Journal of Ideas From the Bush*

*Institute,* Fall 2017, https://www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy.html.