2024

No Body, No Crime: The Advent of Cyberwar and International Humanitarian Law

Emma Reeves Mansour

NO BODY, NO CRIME: THE ADVENT OF CYBERWAR AND INTERNATIONAL HUMANITARIAN LAW

By

EMMA REEVES MANSOUR

SUBMITTED TO SCRIPPS COLLEGE IN PARTIAL FULFILLMENT OF THE DEGREE OF BACHELOR OF ARTS

PROFESSOR OWEN BROWN

PROFESSOR JENNIFER TAW

DECEMBER 15, 2023

Abstract

Cyberwar is a relatively new type of combat that is increasing in popularity and prevalence in modern warfare. Actors are using advanced technology, often in the form of a virus, to target a state's infrastructure, data, and all else that exists online. What is even more alarming than the attacks themselves is the lack of International Humanitarian Law (IHL) to regulate cyberattacks, leaving states and civilians incredibly vulnerable. As the world continues to shift digitally, all actors will become more and more vulnerable to these types of attacks, and it is critical that new law is adopted to ensure that just war is maintained. This thesis argues that IHL must be revisited and updated, surveying three instances of cyberattacks, NotPetya, BlackEnergy, and Stuxnet, to demonstrate the flaws in current international law and the urgency of this problem.

Table of Contents

Acknowledgements

I would like to thank my thesis readers, Dr. Owen Brown and Dr. Jennifer Taw, as well as the rest of my professors across the 5Cs, for making this experience so rewarding and enriching. I am so grateful to go to schools that have incredible professors who seem to know everything about everything – my academic experience has been nothing short of spectacular. The classes I have been able to take over the past four years have made me a more interesting, inquisitive, and smarter person, something I did not think possible as a senior in high school.

I would like to thank my family, who has provided me with unending love and support, and has allowed me every opportunity to get to where I am now. My friends also deserve thanks for making my experience in Claremont more wonderful than I could imagine; as lucky as they may be to have me, I am even luckier to have them. I feel very grateful to be surrounded by these people.

INTRODUCTION

The evolution of war is mirrored closely by the evolution of technology. It has always been a priority to increase efficiency, decrease costs, and gain an edge on competing powers with newer and more powerful weapons. But as technology has seemingly hit a new level of innovation in the past several decades, the weapons and means of modern warfare have strayed further and further from their traditional roots. The best example of this is cyberwar, weapons that are completely digital and invisible but can cause more destruction and disruption than conventional weapons. It is modern warfare at its most modern.

The increasing reliance on the internet, and technology more generally, has had plenty of benefits globally and has fundamentally changed how the world works. One drawback is the increased vulnerability it opens states, private entities, and even civilians to. The infrastructure of the world is becoming more and more digital, giving actors more ground to infiltrate and attack. This paper argues that cyberattacks pose a unique threat to infrastructure and society internationally, and in order to approach this threat, the states must reconceptualize international law to address cyberattacks. Amendments to international law not only aid in the realm of cyberattacks but are also necessary as technology becomes more and more incompatible with current notions of what a fair and just war is. This paper begins by discussing the insufficient role of International Humanitarian Law when it comes understanding cyberwar. I then use three different case studies of notable attacks to illustrate the scope of cyberattacks, how they are unique to conventional weapons, and how IHL fails to incorporate them. I conclude by looking forward at how AI might alter cyberwarfare, and why ultimately this is a pressing issue that needs more attention from international actors.

THE STATUS QUO OF CYBERATTACKS

Cyberattacks are a relatively new weapon. As a product of the interconnectedness of computers and technology, they have only increased in frequency as those things have become more prevalent over the past several decades.[1] As the internet has evolved to be the basis of most infrastructure, for both states and private companies, there are more vulnerabilities that can be attacked. Defining what a cyberattack is has been difficult, not only because it is unclear how decide what constitutes a cyberattack, but also because different nations conceive of them differently. The internet and cyberattacks generally lack tangibility, being based on information and privacy; if there is no physical manifestation of the weapon itself and many attacks , it is not surprising that there is a difference in understandings of what exactly it is. The National Institute of Standards and Technology defines a cyberattack as:

> An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.[2]

This definition captures the technical basis of the idea and will suffice for the purposes of this paper.

Defining a cyberattack is further complicated because of the hundreds of thousands of possible iterations of an attack. Part of that includes the many different possible actors, all of whom have slightly different motivations and tactics. In "Industrial and Critical Infrastructure

---

[1] Libicki, Martin C, and Project Air Force (U.S.). Cyberdeterrence and Cyberwar. RAND, 2009 Accessed 13 Dec. 2023.

[2] Editor, CSRC Content. "Cyber Attack - Glossary: CSRC." *CSRC Content Editor*, csrc.nist.gov/glossary/term/Cyber_Attack#:~:text=Actions%20taken%20through%20the%20use,the%20computers%20and%20networks%20themselves. Accessed 13 Dec. 2023.

Security: Technical Analysis of Real-Life Security Incidents" by Goergios Michail Markrakis et. al, six adversaries are identified based on motivation:

> Outsiders: Most common adversaries, exist outside of physical location of industrial control systems
>
> Insiders: Work within ICS, like a disgruntled employee, leveraging knowledge they have
>
> Criminals/Hacktivists: Working for financial gain or hacktivism, work off of commonly used systems.
>
> Industrial Espionage Actors: Seeking information about the workings of ICS and CI, higher level of skill required
>
> Cyber-terrorists: Target ICS and CI with the purpose of creating mayhem, spreading their own beliefs, and more
>
> Nation-state actors: high level of resources often for political means

For the purposes of this paper, given its focus on international law, it is most likely that the actors discussed belong in the cyber-terrorist or nation-state group. The focus here is cyberattacks as a weapon of war, usually between two states – international humanitarian law governs the actions of a state and how civilians are protected within a war. That said, it is valuable to see the different possible actors and motivations to understand how wide reaching the crime can be, hence the difficulty defining it. Where traditional weapons have one purpose, to destroy, cyberattacks have an incredibly wide scope of uses and do not always require a large number of resources to carry out.

LITERATURE REVIEW

Much of the literature provides a robust background introduction into what exactly cyberattacks are and how they are used. Given the newness of the field, which is reflected in newness of literature, there is very little common knowledge that can be relied on for context. "Cybersecurity and Cyberwar: What Everyone Needs to Know?" by P.W. Singer and Allan Friedman, "Cyberdeterrence and cyberwar" by Martin Libicki, and "The Hacker and the State:

Cyberattacks and the New Normal of Geopolitics" by Ben Buchanan were most useful in providing this background information on cyberattacks. Generally, these scholars explain the basis of all cyberattacks: cyberspace and the internet. In doing so, they note that there is a general lack of understanding on how exactly the technology and the internet works, which contributes to vulnerability. After giving a general explanation of the internet, these authors go on to describe the evolution of cyberspace, notably how it has entangled itself into all other sectors, ultimately moving into critical infrastructure. After laying a foundation, they move on to cyberattacks, specifically. They highlight different types of attacks and who is perpetrating the attacks, using some case-studies to supplement. They additionally look at the concept of a cyberwar and how that would work in lieu of a traditional war, both in practice and the theoretical political implications. What these papers lack is an in-depth analysis of specific attacks, including considerations of technical causes, legal problems, and theoretical implications. This paper includes a much more abbreviated version of this, as it situates itself slightly later in the discussion and in a much more specific way. I draw on these works to create a comprehensive background on cyberattacks, laying the groundwork for my arguments. Having a solid understanding of cyberattacks in their simplest forms is critical to understanding how International Humanitarian Law applies to the concept, as well as how the case studies I draw from worked technically. In addition to using this scholarship to provide an overview, I employ them in this paper in conjunction with my case studies to show their real-world application.

This paper draws on three different case studies: NotPetya, Stuxnet, and Blackenergy. These are the most discussed instances of cyberattacks and while literature on the subjects is limited, these three cases have the most scholarship; NotPetya, despite being the most notable of the three, currently receives the least attention in the literature. The cases are discussed in "The

Untold Story of Notpetya, the Most Devastating Cyberattack in History" by Andy Greenberg, "Cyber-Attack against Ukrainian Critical Infrastructure: CISA", "Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyber Warfare", and more, all of which gives and overview of the technicalities of the attacks, some of the context to situate them, and some analysis. This paper will use that to explain what the attacks were, their implications, and most notably how they illustrate some of the drawbacks of current IHL. The wider implications of these case studies are lost in much of the scholarship and this paper will work to fill some of those holes.

Critical infrastructure is a highly discussed target for cyberattacks, given its vulnerabilities and historical attacks. There is a wide berth of scholarship that deals with the subject manner in a number of ways, all working together to form a complete depiction of what critical infrastructure is, how attacks on them may be carried out, and what can be done to prevent these types of attacks. While there is no perfect solution, the folowing variety of authors give suggestions that may help secure infrastructure further. In "Countering terrorism on tomorrow's battlefield", the authors discuss cyberattacks, more specifically attacks on critical infrastructure. This is done largely in the context of NATO and the NATO countries, using NATO's official definition of critical infrastructure and resilience baseline to measure the readiness of states in the event of an attack "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents" by Goergios Michail Markrakis et. al. looks at the vulnerabilities, both technically and systemically, that allow for more cyberattacks to happen. They argue that the two largest problems within Critical Infrastructure (CI) and Industrial Control Systems (ICS) are practitioners having superficial or limited knowledge about the systems they are working with, and the tendency to innovate the systems which introduces more threats. In *Cyber Security: Critical Infrastructure Protection*, the authors detail the threat

of cyberattacks on infrastructure, going into the current security systems in place and previous attacks that inform their work. Notably, chapter 3, Cyber Law and Regulation by Virginia A. Greiman, discusses the need to modernize law globally to keep up with quickly modernizing technology.

All of these texts touch on different angles of infrastructure. This paper uses all of this information to supplement the case studies provided and explain why a threat against infrastructure is so concerning. I additionally use this analysis of critical infrastructure when discussing the role of International Humanitarian Law in order to understand the impact it has on military as well as civilians. While none of them deal specifically with humanitarian law, the analysis of NATO's definitions and applications as well as Greiman's discussion of international law help to inform my arguments on the importance of IHL.

The most limited scholarship is that on IHL and cyberwar, as this niche of scholarship is even newer than cyberwar and thus lacks specificity. The majority of current discussion on the topic discusses how IHL can or cannot be theoretically applied to cyberattacks. Current legal flaws are mentioned along with the interpretation of IHL within the context of cyberattacks, which was done in the Talinn Manual. What literature does exist on the topic was very helpful in informing my arguments. Peter Pascucci gives definitional insight into important legal terms used in war in "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution", and Hensey A. Fenton III builds on this in "Proportionality and its Applicability in the Realm of Cyber-Attacks". This paper adds to the limited discourse on the subject by using these previous analyses on IHL and employing my own to show the limitations of current IHL. I further extrapolate this to apply it to technology more broadly and discuss those concerns. The current scholarship is lacking a specific application of these concerns to case studies, which is

the biggest contribution that this paper makes to scholarship. Seeing the consequences of a lack of updated law is only possible if it's done in a real-world context, which is the use of the case studies in conjunction with the discussion of IHL. Without this, arguments against current IHL seem less pressing and lack the tangibility necessary to propel action.

In a similar vein, there is limited scholarship on how AI will interact with cyberwarfare and the complications this will pose. Rod Thornton and Marina Miron discuss the topic in "Towards the 'Third Revolution in Military Affairs,"' where they discuss Russia's current use of cyberattacks and how that will be innovated once they incorporate AI into their strategy, something they are quickly developing. This paper uses this information to highlight the concerns surrounding AI, which most scholarship does not touch on. I additionally include an analysis of how this interacts with the concerns of IHL, which the current literature notably is lacking. This new contribution to the literature is incredibly important considering the speed at which AI is developing as well as the current political state of Russia specifically. This adds another layer of urgency to my arguments and encourages states to be forward thinking and comprehensive when they address technology use in war; limiting arguments to just one aspect of technology is useful when it comes to specificity but ultimately fails to recognize the threat of pairing multiple technologies.

METHODOLOGY

This paper applies analysis of International Humanitarian Law to the context of cyberattacks, drawing on academic scholarship in the field to supplement my own analysis. The newness of cyberattacks and cyberwar limits the amount of literature on the topic, especially considering skepticism within the discipline that was alive well into the 2010s. The

aforementioned literature provides plenty of insight and information into the field and function usefully in a number of ways. First, the literature has helped shaped my own argument and analysis of the provided case studies. The case studies were chosen based on their impact on international politics as well as the impact on the discussion surrounding cyberattacks. There are not a great number of 'famous' attacks, or attacks that have enough available information to discuss. These cases are more widely researched and discussed, have had major implications, and are diverse in their nature which helps to show different aspects of cyberattacks. What is also useful is the ability to see the vast change in scholarship over time. The majority of the articles and writing referenced was published the past 10-15 years. This gives insight into the speed at which this technology is changing as well as the speed at which political and academic opinions have changed on it. As I mentioned, the change in skepticism surrounding the topic is incredibly interesting and changed at a shocking speed. Using academic papers in this comparative manner helps to inform the timeline of cyberwar and provides context to arguments that is otherwise not as heavily considered.

I additionally use academic scholarship on International Humanitarian Law to analyze how technology is incompatible with some of the principles, notably proportionality, distinction, and the 'object.' This scholarship is also new within the context of technology, but arguments date back hundreds of years. There is comparatively little literature that includes a discussion of IHL within the lens of cyberattacks – this paper makes a significant effort to show that cyberattacks are not only dangerous in their specific actions, but also in the theoretical discussion of how war should be fought.

APPLYING INTERNATIONAL HUMANITARIAN LAW TO CYBERWAR

The regulation of war has been critical over the course of history in maintaining some sense of fairness and ethics within war, something that is often inherently unfair and unethical. Upkeeping strong and relevant International Humanitarian Law, or IHL, is a crucial part of this process. When it comes to cyberwar, the lack of appropriate law and regulations is concerning; little has been done in the international community to appropriately address new technology. The following looks at some of the problems IHL currently has and the possible implications.

The only comprehensive discussion of international legality of cyberwar is found in the Tallinn Manual, the most recent version being published in 2017, which attempts to apply current IHL to cyberwar.[3] The Manual is made up of contributions by prominent international lawyers with the goal of extending current law to regulate cyberattacks. While it has garnered praise internationally, it has garnered an equal amount of criticism and when put in practice, very few states have integrated their rules.[4] One of the main problems in application comes from the fact that it was created by a group of international experts, rather than states themselves, and states therefore have no obligation to restrict any of their cyber actions. The Manual is a best effort but ultimately shows the main problem at present, which is that IHL is not compatible with modern technology in its current form. Plenty of questions remain unanswered and the lack of law has the potential for dangerous consequences. As such, we will look at areas of incompatibility and some of their possible implications.

The complex role of the civilian is described by Peter Pascucci in "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution." He discusses the principle

[3] Efrony D, Shany Y. A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *American Journal of International Law*. 2018;112(4):583-657. doi:10.1017/ajil.2018.86
[4] Ibid.

of distinction, as outlined in the Geneva Convention: the principle "Requires a party to the conflict to target only other parties to the conflict – a party may not target a civilian or civilian object."[5] This is easier to apply in conventional war – one cannot bomb a building of schoolchildren or attack a parade, for example. However, cyberwar is where this gets blurry. Shared systems by civilians and militaries, unclear thresholds, the confusion over where data stands among all of this, and the definition of 'attack' are all places where the article falls short; this becomes especially relevant in cases of attacks on infrastructure.

Pascucci additionally expands on the idea of what constitutes a civilian object. Under current IHL, "a proposed attack must target an object that has an 'inherent characteristic or attribute which contributes to military action."[6] What it means to contribute to military action is unclear in traditional war and even more so when it comes to internet-based infrastructure or technology, which is often shared by civilians. The nature of an objective is another part of IHL that shares similar issues, meaning "Its 'inherent characteristic of attribute which contributes to military action.'"[7] A trend is clearly emerging: there is no clear line between civilian and military objects/uses when it comes to technology. This provides justification for parties to target digital infrastructure that impacts civilians far more than it may the military under the guise of legally targeting military objects. IHL does not address this vulnerability as there has not been weaponry that blurs the line in the way cyberattacks can. At present, civilians lack any specific protection from cyberwar.

---

[5] Pascucci, Peter. "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution." Minnesota Journal of International Law, vol. 26, no. 2, Summer 2017, pp. 419-460. HeinOnline. Pg 420

[6] Ibid., Pg. 433

[7] Ibid., Pg. 435

Data is arguably the area with the least amount of protection under IHL. The experts involved in creating Tallinn Manual determined that data should not be considered an object – this means that an attack on data is not an attack on an object.[8] Given the importance of data in an information-driven society, this is a shocking conclusion to reach. Data, in its current form, comprises almost the entirety of someone's identity – if taken by the wrong people, data can very easily be used to ruin lives. The loss of data is only difficult to imagine in a world that is transitioning further and further from hard copies of information. This also works itself into a larger discussion of privacy as a right: if personal data is stolen in an attack, that can be a far more damaging loss than a tangible object. Understanding what a loss of data can be goes far beyond just a civilian losing their photos or getting their bank information stolen; the NotPetya case study exemplifies how data erasure can critically harm the world and has the potential to be economically devastating. Ensuring that data has enough value to be given protection under international law should be a priority for states as there is no indication that information is become less digital any time soon. To put it plainly, data is important and must be protected; defining it outside the realm of IHL is a huge vulnerability.

Another question that cyberattacks pose is how to determine what is proportional in an attack that can be difficult to quantify in terms that traditional attacks usually are, like combatant death, civilian death, and more. Cyberattacks generally do not involve specifically killing individuals, as will be illustrated by the case studies below; this is not to say that they cannot, as explained in the context of critical infrastructure. What is most difficult to gauge is the effect on civilians, and principle that has been vital in the discussion of proportionality. Hensey A. Fenton

[8] Ibid., Pg. 432

III discusses these complications in "Proportionality and its Applicability in the Realm of Cyber-Attacks," writing,

> Though it is assumed that the law of armed conflict applies to cyber-attacks, applying a proportionality analysis to cyber warfare is a difficult task. Such an application requires one to determine what systems are "dual use" (i.e. systems employed by the military and civilians) and to distinguish within such systems, what is civilian from what is military. Additionally, the existence of dual-use systems heightens the likelihood of collateral damage. Furthermore, the presence of knock-on effects (i.e. indirect effects that result from a given action but are not immediately discernable) and the requirement that they be included in a proportionality analysis present added complications.[9]

Without a clear metric to determine the impact of an attack, a proportionate response is incredibly difficult to gauge. Technology is so inherent in civilian life that most attacks on a system ultimately are an attack on civilians, meaning that a proportionality calculus should be done in any instance of a cyberattack. The standard is applied based on the attack at launch,[10] not effects of that attack – in another context, that would mean if someone shot a gun intending to only hit one person but ultimately killed five, IHL principles of proportionality would say a proportional response would be held in comparison to the one-person intention.

In the case of cyberattacks, determining proportionality is almost impossible given the previous definitions; data would not be factored in, for example, because it isn't an 'object.' The current reading of IHL would not account for any collateral damage that comes as a result of an attack, which allows attackers to get away with almost everything in the attack. One concern is how this might incentivize cyberattacks over other attacks – perhaps there is an argument that this is better than conventional war because of the lack of legal and physical consequences, but if IHL accommodated modern technology, ideally no type of attack would be incentivized.

---

[9] Hensey Fenton III, Proportionality and its Applicability in the Realm of Cyber Attacks, 29 *Duke Journal of Comparative & International Law* 335-359 (2019)
[10] Ibid., Pg. 448

One more notable way that current international law falls short, beyond in protecting citizens, is the current definition of attack. It is currently defined as "acts of violence against the adversary." It is not surprising that this is difficult to apply to cyberattacks, many of which do not appear violent in nature. The Tallinn Manual reaffirmed this definition, as well as the United States Department of Defense Law of War manual. Tallinn specifically defines a cyberattack as "a cyber operation, whether offensive of defensive, that is reasonably expected to cause injury or death to persons or destruction to objects."[11] Given the previous discussion of what constitutes an object, many cyberattacks would fall short of the definition. Once again, this leaves civilian and governmental data without international protections.

These are just some of the obvious ways that IHL is incompatible with cyberwar. Despite the best efforts of international scholars, trying to apply current law to cyberwar does not sufficiently protect civilians. The law was simply not written with this type of technology in mind and trying to fit it within current parameters is reductive of the threat itself. With this in mind, I would argue that states must urgently add to IHL to specifically address some of the ways technology has fundamentally changed war. Reframing proportionality, what constitutes an attack, and the scope of an attack are all ways that civilians would be better protected by the law. It is incredibly difficult for states to come to an agreement on any international law and the fact that this is such new territory with little precedent is not going to help. That should not stop them from making it an international priority.

This importance of this analysis cannot be overstated – without any regulations, actors may use cyberattacks much more excessively and likely at the expensive of civilians. The next

[11] Ibid., Pg. 444

section of this paper will use case studies of three significant attacks to show the application of the problems in IHL presented above.

CASE STUDY 1: NOTPETYA

In June of 2017, beginning in Ukraine and spreading globally, the most destructive cyberattack of all time was carried out by Russia.[12] The main victim was A.P. Møller-Maersk, also known as Maersk, a Danish shipping and logistics company. Maersk's reach is wide, with eight business units with a wide range of functions globally. They are critical to global shipping, accounting for about a fifth of the worlds shipping capacity, and general logistical functions, to put it simply.

Without warning, the computers at Maersk began shutting down inexplicably and globally. It quickly became clear that this was not a malfunction, but an attack. IT staffers could do nothing to restart the systems and had to instead work to disconnect the entire global network, hoping to stop the spread of the virus.[13] Within hours, the global supply chain was partially halted, and it was estimated by the White House that the cost of the attack was approximately $10 billion. It was devastating.

This attack presented as a ransom attack, with screens showing a message that read "oops, your files are encrypted" and prompting payment of $300 worth of bitcoin.[14] While this mirrors other cyberattacks that aim for ransom, it was obviously not the aim of the attackers. With the

[12] Greenberg, Andy. "The Untold Story of Notpetya, the Most Devastating Cyberattack in History." *Wired*, Conde Nast, 22 Aug. 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[13] Ibid.

[14] Ibid.

context of the hackers being Russian and the target being a Ukrainian company, the political motivations become far more obvious. Russia and Ukraine had been in what was effectively a war for years at that point. By using a Ukrainian software as the starting point for the attack, the message was clear: do not ally yourself with them. Russia would not go as far as to physically attack all the countries using the software, but they could 'attack' Ukraine with the intention of hurting everyone else in the process and use the attack to shape global politics.[15] By using a cyberattack, something with very little applicability to current international law, they were able to carry out a massive attack without repercussions.

The attack was successful because of several factors, the first being the technical success of the virus itself, NotPetya. The point of access was planted far before the attack – Russian military hackers had hijacked a company called the Linkos group, which works on a software called M.E. Doc. M.E. Doc is a popularly used accounting software that is commonly used by business professionals in Ukraine and is installed on a large number of PCs. The hackers were able to use M.E. Doc as an entry point into a Ukrainian Maersk employee's PC. From there, they used a flaw in Microsoft Windows called EternalBlue, which had been discovered by the US National Security Administration (NSA) and subsequently leaked; this of course informed hackers globally on a point of entry that could be exploited.[16] This was then paired with Mimikatz, which was originally made to show another flaw in Microsoft systems where passwords remained stored on systems. The two, when paired, were very powerful: by accessing computers that are still infected with EternalBlue, one could find the password information

[15] Buchanan, Ben. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press, 2022.

[16] Ibid., Pg. 286

stored in the system there to get access to all other operating systems on the network. NotPetya used these vulnerabilities to access the system from just one computer, lock them down, and encrypt the master boot records.[17] The computers could not be saved and thus began the global shut down. It should be noted that the only backup of the system that could be recovered after the attack was in Ghana, which had survived because it was disconnected during a previous power outage. Without this single disconnection, the entire system would have had to be rebuilt from the ground up.

The second factor that played into the success of the attack was easily preventable but a common problem when it comes to cyberattacks: human error. Some of the Maersk servers were running on Windows 2000 and despite a push from the IT team in 2016 to update and preemptively secure the servers, it was pushed to the backburner in lieu of more profitable updates. Ultimately, this laziness ironically cost the company between $250 and $300 million dollars. It is notable that Maersk did not suffer financially more than anyone else. In fact, the greatest losses were felt by Merck, a pharmaceutical company, FedEx, a shipping company, and Saint-Gobain, a French construction company.[18]

As the most successful attack in history, NotPetya gives insight into some of the theoretical questions and complications within cyberattacks. The first insight this gives us is the potential scope of an attack. What started at a small company in Ukraine led to a $10 billion global breakdown in a variety of different sectors that took months to fix. It also highlights the power of cyberattacks that cannot be replicated with conventional weapons. Russia carried out a global

---

[17] Lika, Reyner Aranta, et al. "Notpetya: Cyber attack prevention through awareness via Gamification." *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2018, https://doi.org/10.1109/icscee.2018.8538431.

[18] Buchanan, Pg. 289

attack without any consequences and while it was ultimately traced to them, it took some time. While the actual impact of the attack was devastating, the strategic implications can be even more powerful. The strategic potential of a cyberattack ought to be factored in more highly in considering the likelihood of cyberattacks and the form they take: it can be untraceable, it can be more wide reaching than weapons, and it can be more disruptive than weapons. A final takeaway goes beyond the specifics of this attack or cyberattacks in general. NotPetya was so devastating it begs the question of what can be considered critical infrastructure. While this attack was not deadly and did not target electricity or water, it was debilitating. We are faced with a reality where digital systems are critical to the functioning of society, which heightens the stakes of a cyberattack. Information from the past decade exists almost exclusively digitally and wiping it out would have enormous effects on the function of daily life, as well as historical records of the past decade or two. In theory, this can be done with conventional weapons, by bombing a data facility for example. However, it is difficult to achieve the full erasure that was almost achieved in this instance; the only backup that remained was in Africa and was untouched because its connection broke and was not fixed.

In regards to IHL, NotPetya serves as an excellent way to illustrate some of the problems outlined above. The first is the problem of collateral damage, which is not attributed to the attacker under IHL. While the initial attack was damaging, the collateral damage is what characterizes the scope of the attack. Shipping was halted worldwide, data was lost, and companies lost billions of dollars as a result; ironically one of the companies affected could not

receive help from their insurance because the action was deemed 'warlike.'[19] The after affects and collateral damage from the attack was took up the bulk of damages, though because it was Data based IHL would not agree that it was a civilian object that was attacked. This concepted is important, especially in the application to cyberwar, because very few cyberattacks target one thing and have no further outside damage. An attack on a corporation as structurally important as Maersk is ultimately just a global attack; though it sounds extreme, there was no possibility that the damages would be contained to the company.

This attack also illustrates the concern of what data means in an attack. As I stated earlier, all of the structural data within the company was completely wiped, save for one saved copy in Africa which just happened to be disconnected. Had that copy not been there, the company would have had to internally rebuild its entire system essentially from the ground up.[20] This would have taken only taken longer than it already took to get the company back online, costing the global market even more. This highlights the importance of data and why it needs to be protected in the same way we protect other valuable objects: it was the foundation of global shipping and without it, things just stopped. Even though the importance of Data is clearly demonstrated by the fallout of this attack, the severity would not be captured by any application of IHL, which would not consider Data an object that can be attacked.

Despite NotPetya being arguably the biggest cyberattack in history, there were very few repercussions. This can be attributed to how IHL cannot interact with cyberattacks; the lack of specific laws concerning cyberattacks makes it so attacks are not assigned the blame that they

---

[19] "Notpetya: The Cyberattack That Shook the World." *The Economic Times*, economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the

[20] Greenberg

ought to be. Beyond IHL, NotPetya informs the international community on the scope of possible attacks, the need for contingency when it comes to data, and the importance of taking small steps like updating system to prevent large scale problems to occur.

CASE STUDY 2: BLACKENERGY

In many ways, power grids are the foundation of everything we do. In a technology-reliant world, power is a prerequisite for existence in most states. As such, any problems within power grids can have wide-reaching consequences, making them an ideal target for attack. Power grids are the systems of generation, transmission, and distribution of energy that provide power for something, in this case a state or states.[21] The power begins in a plant and is distributed through power lines; while the technical makeup of a plant or system may vary, they share general characteristics and are nearly identical in their function. Without power, lights do not work, water does not run, and many other basic functions of life halt. While many places have access to generators, which can be used in the event that something goes wrong at a power plant, this is dependent on the ability to purchase expensive equipment and the foresight to understand how much one would need in the event of a blackout**;** given the lack of predictability in cyberattacks, a blackout could last for an hour or for weeks. In short, most states are reliant on the power grids in their fully functional capacity. This all gives context to a 2015 attack in Ukraine.

[21] "How Does the U.S. Power Grid Work?" *Council on Foreign Relations,* Council on Foreign Relations, www.cfr.org/backgrounder/how-does-us-power-grid-work. Accessed 11 Dec. 2023.

In 2015, Ukraine's power grid was attacked with BlackEnergy malware by Sandworm, an Advanced Persistent Threat (ATP) operated by the Russian military.[22] People in the energy sector received emails with Microsoft attachments, which, when opened, installed the virus on their computer systems. This gave hackers access to the information stored on the system and eventually informed them enough to carry out the shutdown several months later. The attack focused on three distribution companies and as far the impact of the shutdown, over 200,000 Ukrainians were left without power for several hours until it was manually restored. [23] As of 2021, the US government has concluded that the attack was carried out by Russian Nation-State Actors which makes sense considering their relationship with Ukraine and the historical context of 2015 Russo-Ukrainian relations. [24] While not fatal or particularly dangerous, the attack gives insight into the scope of a possible cyberattack on power infrastructure as well the ease at which it can be deployed. This should strike concern for other states.

This attack gives us several important insights into the threat of cyberattacks on infrastructure and beyond. The first takeaway is that this type of attack, which initially relied on a lack of distrust by employees and a low level of vigilance, is not uncommon. Similar tactics have been employed in other situations, notably in the Stuxnet attack, which used a thumb drive to infect the Iranian systems. Phishing scams have become increasingly popular and effective in

[22] Mueller, Grace B., et al. "Cyber Operations during the Russo-Ukrainian War." *CSIS*, www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war. Accessed 11 Dec. 2023.

[23] "Cyber-Attack against Ukrainian Critical Infrastructure: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, 4 Mar. 2021, www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

[24] Ibid.

recent years.[25] These tactics may seem reliant on luck but are very effective because of how difficult it is to solve for human error. Defense can be improved, and technology can be coded more securely, but it is almost impossible to warn people against the thousands of small ways that they leave their systems open to attack. This same problem manifested in NotPetya, where the vulnerability came from a Microsoft system that was long overdue for an update. The second takeaway is that the actual technology of the infrastructure must be considered, in this Ukraine's dated powerplant. In contrast, many states, notably the US, have begun to completely innovate their infrastructure system to streamline them via industrial control systems, relying heavily on the internet to communicate between systems. While convenient, it comes at the cost of a closed system, or one inaccessible from the outside. If a similar attack occurred on a US power plant, where the problem might not be physically fixable because of the updated system, there is no way to tell how long infrastructure would be down and civilians would be without power. While the problem is, of course, the attackers themselves, a priority on innovation in systems without the same priority given to securitizing the systems are what leave them most vulnerable.

Though the impact on Ukraine was minimal in the grand scheme of things, that does not illustrate the extent of a possible attack. It is not difficult to imagine the existential impact of a large population not having access to power or other basic infrastructures. In the case of a theoretical attack on the US, developed by insurance undewriter Lloyd's of London, Robert Knake *says in* "*A Cyberattack on the U.S. Power Grid*"*:*

[25] Violino, Bob. "Phishing Attacks Are Increasing and Getting More Sophisticated. Here's How to Avoid Them." *CNBC*, CNBC, 10 Jan. 2023, www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html.

> The Lloyd's scenario estimates economic costs of $243 billion and a small rise in death rates as health and safety systems fail. While darker scenarios envision scarcity of water and food, deterioration of sanitation, and a breakdown in security, leading to a societal collapse, it would be possible to mitigate the worst effects of the outage and have power restored to most areas within days. At this level of damage, the American public would likely demand a forceful response, which could reshape U.S. geopolitical interests for decades. Traditional military action, as opposed to a response in kind, would be likely.[26]

Knake's claims sound extreme but they do highlight the severe security threat posed by a cyberattack on infrastructure. Access to power, heat, water, transportation, and more are critical to the functioning of society as well as basic needs of a population. If the proper contingency plans are in place, this could be avoided, but it is unlikely that any government or state is prepared for long-term or repetitive attacks. Given how this attack played out as well as the predicted worst-case scenario, it is clear that the threat posed by cyberattacks on infrastructure cannot be understated.

Beyond the tangible consequences, the applications of international law to BlackEnergy helps to illustrate the gaping holes that were outlined above. The most applicable idea here is the role of a 'dual use' system, which includes infrastructure – while the power grid is not a military system, it contributes to military use which makes it a viable target. This then leads to the next problem of how IHL fails to protect civilians in cases of cyberattacks. While the military was involved, it is obvious that this attack is directed at civilians who took the brunt of the fallout in the form of a power outage. It is easy to brush this aside given the lack of long-term damage, but an effective contingency plan is not guaranteed. The damage could have been much worse on the military and civilians, as mentioned above, but IHL would do little to factor that into

[26] Knake, Robert K. *A cyberattack on the US power grid*. Council on Foreign Relations., 2017., Pg. 3

considerations of whether this was just or not. Having clear laws on the matter would help to prevent future attacks that take advantage of technology to attack civilians.

CASE STUDY 3: STUXNET

Cyberattacks extend beyond infrastructure system to defense systems. The most notable of these attacks, and one of the first cyberattacks that had publicly available details, was Stuxnet. In the early 2000s, Iran began developing their nuclear programs, a concern for several global powers who did not want Iran to have nuclear capabilities. First among that group was Israel, who saw Iran as their number one enemy and threat. As such, the US and Israel set out to stop them. Israel, as a potential target, had been hoping to preemptively strike Israel,[27] at which point President Bush met with Israeli Prime Minister Benjamin Netanyahu and discussed an anonymous cyberattack, which they called Olympic Games. In a similar fashion to NotPetya, this attack was ideal because it allowed the two powers to attack Iran without using physical weapons, which would be an act of war.

The goal of the attack was to target the nuclear facilities, specifically the centrifuges which were being used to enrich uranium; by manipulating the speed of the centrifuges, they could cause them to explode. They used the Stuxnet code, which was the most highly sophisticated code made at the time and had no possible defense because it was a completely new code. They were able to use Microsoft digital certificates to access the otherwise inaccessibly air gapped computers, meaning the computers were on their own closed system, not connected to a system that could be externally accessed. Because it looked like any other Microsoft certificate, users

[27] Jenkinson, Andrew. Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyber Warfare. CRC Press, 2022., Pg. 20

downloaded them without second thought. The code was dormant in the systems for 13 days when it was finally triggered and the attack began. The systems began malfunctioning and exploding and ultimately did stop production, though just temporarily. The attack was far more impactful in its political implications than it was in the physical goal, and set a completely new precedent in the world of cyberattacks.

The political role of this attack is an important part of the Stuxnet story and sheds light on the strategic role that cyberattacks can play. Jon Lindsay, an expert in the field, argues in "Stuxnet and the Limits of Cyber Warfare" that Stuxnet shows that cyberattacks need not be a concern and will not progress to much in the future.[28] At the time, this was a relatively sound argument – Stuxnet, for all that went into it and its goals, was relatively unsuccessful. Iran has continued its nuclear program and likely has achieved the threshold for enriched uranium.[29] He argues that rather being purely a technical success, Stuxnet illustrates the political role that cyberattacks can play, writing,

> An alternative interpretation of these same facts is that cyber attack can be an indication of successful deterrence rather than its failure… The United States sought to halt Iran's nuclear program, but it also desired to avoid sparking a new war while already fighting two costly and unpopular wars on Iran's borders with Iraq and Afghanistan… A covert option, like Olympic Games, that would delay nuclearization and buy time for diplomacy and sanctions to work would be an attractive alternative to American policymakers…[30]

The real use of Stuxnet was not slowing down Iran's nuclear program, though that was certainly a benefit. It was a strategic move by the US execute what Lindsay describes as 'secret

---

[28] Jon R. Lindsay (2013) "Stuxnet and the Limits of Cyber Warfare", Security Studies, 22:3, 365-404, DOI: 10.1080/09636412.2013.816122

[29] Hansler, Jennifer. "Top US Defense Official Says Iran Could Produce 'one Bomb's Worth of Fissile Material' in 'About 12 Days' | CNN Politics." *CNN*, Cable News Network, 28 Feb. 2023, www.cnn.com/2023/02/28/politics/kahl-iran-nuclear-deal/.

[30] Lindsay, "Stuxnet and the Limits of Cyber Warfare"

diplomacy;' cyberattacks are ideal for this kind of work because it does not require any physical aggression or movement by the military and inherently does not need public support or approval. The US was able to maintain control over both Iran and Israel without putting any lives in danger. This advantage is unique to cyberattacks and may be incentive for states to employ the tactic.

Stuxnet is a case that is best suited for the current iteration of IHL, though it is not a perfect match. What makes this more applicable was the specificity of the attack; it had a very narrow target and there was not room for much collateral damage. The facility and machinery targeted were military and not a dual-use system, unlike the other targets from the above case studies. The damage was limited to the nuclear reactors and collateral damage was minimal, as the goal of the attack was just to damage the nuclear reactors, not to cause state-wide disruption. Civilians were untouched and the damage fit nicely within definition of object. Even so, the same questions regarding the application of proportionality remain and the proper action on Iran's part is unclear. What we can glean from this case is that IHL is most applicable when the attack is more politically motivated or specifically focused, rather than widely destructive; the US was not attempting to destroy or disrupt as much as it wanted to position itself and shape politics in the middle east.

Stuxnet, while not the most effective of cyberattacks, exemplifies what a cyberattacks can achieve if they are pointed in their goals; regardless of the state of nuclearization in Iran, Israel did not end up initiating any traditional military action because the US had strategic reason to support a cyberattack instead. While traditional weapons can be used for political signaling, Stuxnet shows that cyberattacks are incredibly effective when used strategically while still having tangible effects, which pure signaling cannot achieve. These benefits may incentivize the

use of cyberattacks, which can only be done safely if IHL is updated to accommodate attacks that are not as narrowly focused. The next section will supplement this with more unique ways that cyberattacks are set apart from conventional weapons.

UNIQUENESS TO CONVENTIONAL WEAPONS

In many ways, a cyberattack, or cybersecurity, may not seem like a threat that should be prioritized. Or, they can be prioritized and dealt with in the same way all other threats are dealt with: states attempt to become stronger, more powerful, or cater their defense systems to defend against a specific attack. However, cyberattacks have several facets that set it apart from other weapons and systems, making them a unique threat that states must address accordingly. Both technically and theoretically, cyberattacks hold different power than traditional weapons and conflating them put states a severe disadvantage. In order to be ready to appropriately address and anticipate any cyberattacks, especially those on infrastructure, states must prepare accordingly.

The first thing that ought to be considered when it comes to cyberattacks is the difficulty in anticipating them. In many ways, they are impossible to truly anticipate in the same way bombs may be anticipated. This is not to say that traditional attacks are easy to anticipate in the moment, but generally states have an idea of what their adversaries have in their stockpiles and can prepare themselves for those. The power in these weapons is not necessarily in their technicalities but rather in the force itself – a bomb is a bomb, and if it hits it hits. While the specifics of an attack may not be predictable, the weaponry generally is, and a state can prepare. In contrast, the power of cyberweaponry is in their surprise. If a state had any idea of the technical aspects of a virus, for example, they would be able to better counter it, leaving the technology virtually useless. As such, it is incredibly difficult to anticipate the technology used

in a cyberattack. Often, the cyberattack uses new technology that foreign states would not be familiar with and would certainly not have the means to defend themselves immediately. The infrastructure itself is equipped with general defense systems and the security personnel familiar with cybersecurity generally. They are ill prepared for a specialized or 'new' attack, which is what cyberattacks generally look like. The inability to truly anticipate what an attack will look like sets victim states at a severe disadvantage and sets cyberattacks apart from traditional weaponry that is better understood.

Part of what makes cyberattacks so difficult to anticipate is that both attacks and defense must be constantly innovating. As soon as a virus, code, etc. has been deployed, it loses its edge of being a foreign weapon; cyberattacks hold power so long as the state or group it is being deployed against is not familiar with it and therefore cannot respond quickly. In a hypothetical scenario, if State A sends a brand-new virus to State B**,** the second state will have to take critical time figuring out the virus and finding out how to combat it. However, it is only effective if State B was unfamiliar with the technology and not prepared. If State A sends the same or similar virus again, State B will be prepared to spot the virus and deal with it, taking the threat away significantly. This is where traditional weapons have an edge: a bomb is always going to explode in the same way and will always inflict damage. The solution here is to make sure each attack is novel and different enough that no one can be prepared enough to deal with it efficiently. Because of this, both actors and victims must be constantly innovating. The weapon itself needs to be constantly evolving to be on the cutting edge of technology and the defense systems must mirror. It is an endless cycle of anticipating the worst and acting accordingly, setting it apart from traditional weaponry.

These unique aspects of cyberattacks not only show why they are so different from conventional weapons in their use, but also why law pertaining to conventional weapons cannot be cross applied. Trying to have the same conversations about cyberweapons as we are about bombs does a disservice to the unique and advanced technology that states are dealing with. An inability to anticipate an attack may lead to disproportionate responses and novel technology with each attack means constantly changing methods of attack will be employed, each more different and modern than the last. The need to constantly innovate puts an emphasis on speed of modernization that states should keep in mind as IHL remains stagnant. The longer they wait, the more cyberattacks evolve, and the harder it will be to legislate on.

LOOKING FORWARD: AI

The urgency that this problem presents is not because it is going to end the world tomorrow, hopefully. The danger of cyberwar is that it currently has almost nothing governing it and is changing rapidly. One notable consideration is how AI is going to change the technology we are facing in cyberattacks, especially those carried out by Russia. The superpower has been dominant in cyberwarfare over the past decade or so, threatening states globally. Rod Thornton and Marina Miron discuss the topic in "Towards the 'Third Revolution in Military Affairs.'" They discuss Russia's position versus other states when it comes to AI, writing,

> In Russia, in contrast to other countries where AI is being developed, it is the military that is nominally in the vanguard of AI R&D. In the US, China and the UK it is the civilian sector taking the lead in AI development and creating spin-offs in terms of military applications. In Russia, the opposite applies. As First Deputy Minister of Defense Ruslan Tsalikov confirms, in Russia it is the military that 'is currently leading in almost all of the technological breakthrough areas' in relation to AI.[31]

[31] Rod Thornton & Marina Miron (2020) Towards the 'Third Revolution in Military Affairs', The RUSI Journal, 165:3, 12-21, DOI: 10.1080/03071847.2020.1765514

While other states are working to develop AI and use it to their benefit, Russia's concentrated effort may be cause for concern – they have been employing it extensively within their military technology far more than competitors. The way that AI may be used in a cyberattack is twofold, cyber-psychological and cyber-technical. The first employs AI to spread 'black propaganda,' better known as fake news.[32] The impact of misinformation can be devastating to a state, as the authors write, "Without faith in information, governments, societies and military organisations cannot effectively operate. State functions may collapse simply under the weight of an inability to discern truth. A 'cognitive war' would be fought and won."[33] The more refined AI gets, the more difficult it will become to avoid proliferation or prevent it. Just like all cyberattacks, it is predicated on near-constant innovation and keeping up is difficult given the effort of Russia. This certainly would not fall under any definitions in IHL because of the lack of a traditional attack or traditional object, but has the means to create a large amount of disruption culturally.[34] Beyond information, they argue that AI will make finding vulnerabilities in infrastructure and systems much easier and even easier to exploit. If Russia has enough of an edge with AI, and other states aren't prepared, it would be difficult to find a way out of their attacks.

It goes without saying that this is not exclusive to Russia, they just happen to be leading the pack. Any use of AI by a state will change cyberattacks and stray even farther from the current IHL guidelines. Given the current proliferation of AI, it seems that this will happen sooner rather than later, and international readiness is vital.

[32] Ibid., Pg. 16
[33] Ibid., Pg.17
[34] Ibid., Pg. 17

CONCLUSION

While cyberattacks are not at the forefront of war, it is something that is constantly happening, generally without our knowledge. Most organizations, governmental or otherwise, have the infrastructure in place to defend against general attacks and are constantly fixing bugs within their systems, all so that civilians remain generally unaffected and unaware. Even so, not every attack is defendable, which is where cyberattacks can be dangerous. They pose threats to not only the privacy and data of a system but can also pose existential threats if the right infrastructure is targeted. Further, their many unique qualities as a weapon set them apart from traditional weapons, making it more difficult to conceptualize them within international norms and laws. They alter the meaning of the civilian, proportionality is unclear, and repercussions are not clear. In order to maintain fairness in war, as well as safety of populations generally, cyberattacks must be addressed on all levels. We must adjust our understanding of justice in war to account for modern war tactics, international law needs to account for cyberattack in order to guide retributive responses, and all actors must understand the vulnerabilities within their infrastructure to secure themselves.

This paper does not argue for one specific policy, but several glaring problems have become clear that need to be addressed by the international community. When it comes to IHL, new laws must be made that specifically addresses technology. Reliance on new interpretations of current law has failed so far because these new weapons are too different from traditional military technology. Based on the damages in the mentioned case studies as well as looking forward at what cyberattacks may begin to look like, I argue that priority should be given to addressing proportionality and defining the limits of an attack. Proportionality in the case of a cyberattack is difficult to define and without law to regulate it, disproportionate responses and

escalation are likely. These laws should discuss possible outcomes of a cyberattack, like the loss of electricity to a region for three days or financial damages, and how to evaluate the losses in these cases. Creating standards for repercussions or retributive action can help to minimize the risk of escalation while also highlighting the repercussions for those carrying out attacks. Re-evaluating what constitutes an attack will help to include cyberattacks within the definition so that they can be regulated and the targets of the attack, like data or dual-use systems, will be better protected. Properly valuing Data in legal framework is critical for setting a precedent going forward that acknowledges the role it plays in the modern world and can prevent mass losses like the ones seen in NotPetya. More generally, a new definition of attack can ensure all cyberattacks will be acknowledged as such, rather than having room to avoid being labeled as an attack and therefore the consequences that come with that. New IHL with specific language on these topics, as well as the other issues outlined throughout this paper, would be a good start in implementing policy that addresses modern technology.

The first step to getting anywhere near a solution is a sense of international urgency to address this problem. Cyberattacks are all very similar in that they exploit lack of preparation in a way that conventional weapons do not always have to do. The better prepared states are, both individually and as an international community, the less concern there needs to be about cyberattacks. The most difficult hill that must be climbed is consensus on what cyberattacks are and how they ought to be handled; this has thus far prevented any notable changes in international law. While a daunting task, it is important. Technology is moving at a speed that is almost impossible to keep up with, and the longer we wait, the harder it will be to make the changes we so desperately need. The digital age is upon us, I just do not know if anyone told the leaders of the world.

Works Cited

Buchanan, Ben. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press, 2022.

Efrony D, Shany Y. A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *American Journal of International Law*. 2018;112(4):583-657. doi:10.1017/ajil.2018.86

Fention, Hensey III, Proportionality and its Applicability in the Realm of Cyber Attacks, 29 *Duke Journal of Comparative & International Law* 335-359 (2019)

Greenberg, Andy. "The Untold Story of Notpetya, the Most Devastating Cyberattack in History." *Wired*, Conde Nast, 22 Aug. 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hansler, Jennifer. "Top US Defense Official Says Iran Could Produce 'one Bomb's Worth of Fissile Material' in 'About 12 Days' | CNN Politics." *CNN*, Cable News Network, 28 Feb. 2023, www.cnn.com/2023/02/28/politics/kahl-iran-nuclear-deal/.

Jenkinson, Andrew. Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyber Warfare. CRC Press, 2022.,

Knake, Robert K. *A cyberattack on the US power grid*. Council on Foreign Relations., 2017.,

Libicki, Martin C, and Project Air Force (U.S.). Cyberdeterrence and Cyberwar. RAND, 2009

Lika, Reyner Aranta, et al. “Notpetya: Cyber attack prevention through awareness via Gamification.” *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2018, https://doi.org/10.1109/icscee.2018.8538431.

Lindsay, Jon R. (2013) “Stuxnet and the Limits of Cyber Warfare”, Security Studies, 22:3, 365-404, DOI: 10.1080/09636412.2013.816122

Mueller, Grace B., et al. “Cyber Operations during the Russo-Ukrainian War.” *CSIS*, www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war. Accessed 11 Dec. 2023.

Pascucci, Peter. "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution." Minnesota Journal of International Law, vol. 26, no. 2, Summer 2017, pp. 419-460. HeinOnline.

“Notpetya: The Cyberattack That Shook the World.” *The Economic Times*, economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the

“How Does the U.S. Power Grid Work?” *Council on Foreign Relations*, Council on Foreign Relations, www.cfr.org/backgrounder/how-does-us-power-grid-work. Accessed 11 Dec. 2023.

“Cyber-Attack against Ukrainian Critical Infrastructure: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, 4 Mar. 2021, www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.