WHO CARES WHO, JUST MAKE IT STOP:
THE CRITICALITY OF ATTRIBUTION AND NORMS IN SECURING THE CYBER DOMAIN

by
Joel T. Ahern

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts.

Baltimore, Maryland
December 2022

Abstract:

Security within the cyber domain continues to be an elusive target due to the rapid evolution of the domain and associated threats. Identifying the critical roles within security mechanisms to protect the cyber domain and the critical infrastructure it touches enables more effective means of security and appropriate management of resources. Examining high-profile malicious cyber events perpetrated against nation-states allegedly by nation-states, along with the peer competition space focusing on known malicious actors, enables a broad look at how the attribution of malicious actions and enforcement of normative behavior factor into security within the cyber domain. Exploring the current relationship between the public and private sectors and the potential for integrated defense identifies variances in problem framing, resource availability and allocation, and transparency. These factors demonstrate capabilities and limitations for creating effective and adaptable security within the cyber domain. While attributing malicious cyber actors enhances the ability to secure the cyber domain, it is not a critical aspect. The ability to identify and highlight actors has shown limited effect in deterring malicious events and often requires significant resource investment.

Similarly, the ability to enforce normative behavior within the cyber domain is limited in scope and effectiveness. Most nation-states lack the ability to enforce normative behavior against other actors, and actions such as sanctions, political pressure, or economic incentives have not been shown to deter malicious activity or enforce adherence to norms. Due to these factors' limited ability to increase security within the cyber domain, nation-states must look towards multi-faceted defensive approaches. A defense in depth focusing on identifying vulnerabilities, correcting vulnerabilities before exploitation, mitigating vulnerabilities after exploitation, and sharing information across sectors, is a more responsive and adaptable means of securing the cyber domain.

Official Readers:
Dr. Kathryn Wagner Hill
Dr. Michael J. Ard
Mr. Thomas Stanton

Table of Contents:

Introduction

The veteran detective had cultivated his investigation utilizing tried and true methods, building out networks of suspects and motivation for the crime. His months of turmoil, stress, and ignoring his family were finally about to be over. Maybe if he had a partner, he would have solved it sooner, but the department could not afford it. He believed he had solved the case. Giving his report a final review, he gathered his things and strode into the Chief's office, ready to present his findings and receive his congratulations. Upon arrival, the Chief welcomed the detective to a seat next to a younger man already in place near the desk. The detective began regaling his audience with a tale of how he had identified the perpetrator through superior intellect and determination and where he could be arrested upon approval for a warrant. Only the detective was not allowed to finish his tale; he was interrupted first by the Chief, who was curious about why he was still working on that case, and next by the younger man, who proclaimed it did not matter who committed the crime because he had already implemented a solution to prevent that crime from happening again. The veteran detective was shocked. Had he missed something, his world was spinning.

While this is an outlandish story about the evolution of solving crimes, it is not too far from how security within the cyber domain can be approached. This is not to say finding out who perpetrated criminal or malicious acts is arbitrary or unnecessary, but as alluded to in the story, it takes a toll on limited resources such as manpower and time. Attribution and enforcement are important to solving any crime but are they critical aspects of providing security within the cyber domain? Does the lack of ability to enforce cyber norms create significant security issues within the cyber domain? Is attribution of malicious cyber actors a critical aspect of the security mechanisms within the cyber domain?

This research examines the criticality of the roles of attribution of malicious cyber activity and enforcement of normative behavior within the cyber domain to answer these questions. This research demonstrates the answer to these questions as being, that neither are critical to security within the cyber domain but they are provide enhancing efforts to increasing security. While these attributes, enforcement, and attribution, are enhancing aspects of providing security within the cyber domain, they are not essential, nor will a deficiency in either create significant security issues. However, non-state actors will have increased influence within the international power dynamic due to their ability to leverage the cyber domain and the limited ability to punish violators of cyber normative behavior. This increase in influence will potentially disrupt power balances resulting in security issues outside of state-to-state conflict. This disruption will appear similar to that caused by "traditional" terrorists within the physical domain but will have a greater depth and reach due to the impacts on state and private sector security. These disruptions or non-conformist activities/events will force nations to continue enhancing security measures and integrating more fully with the private sector to ensure integrated protection within the cyber domain.

This research examined historical events within the past ten years that have seen either a non-state or state-sponsored actor disrupt a state actor via the cyber domain. Disruption in this context is creating result that prevents an entity from executing operations or efforts for an undetermined period of time, but does not prevent the entity from recovering from the event. This research will also utilize the current narrative of establishing cyber norms being discussed at the 2019 G7 conference in France, which has gained acceptance, to frame how the leading powers view the cyber threat and its overall impact on international security.

In order to establish a common understanding within the examination of the importance and roles of attribution of malicious cyber events and enforcement of cyber norms, we need to define these terms. The US Commerce Department defines malicious cyber activity as "activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon."[1] While this definition is backed in United States federal law, it can be translated to a broader definition of any activity that seeks to corrupt or disrupt networks, systems, or infrastructure within the cyber domain. Therefore, malicious cyber actors are the entities perpetrating these activities, and malicious cyber events are the encapsulated circumstances surrounding the activity. Cyber norms are acceptable or expected behavioral actions or interactions within the cyber domain. Normative behavior in this regard would be such as to maintain homeostasis or progressive evolution within the cyber domain or an avoidance to disrupt or corrupt the networks, systems, or infrastructure relating to the cyber domain. Attribution is the ability to determine the source or actor responsible for an action or event.

[1] U.S. Department of Commerce, National Institute of Standards and Technology, Computer Security Resource Center Glossary. "Malicious Cyber Activity." https://csrc.nist.gov/glossary/term/malicious_cyber_activity

Every aspect of security within the modern world has grown more complex as a direct result of the cyber domain and the interconnectedness it brings. The internet of things, the ever-growing network of interconnected devices updating and sharing data, has created a world in which nearly every aspect of life is regulated, captured, analyzed, or shared in an effort to increase knowledge and collaboration for improving technology.[2] The influence of the cyber domain has created shifts in the instruments of national power, impacting how nation-states, non-state actors, and everything in between interact. These shifts have also skewed the balance of power perceived in traditional dynamics, something not uncommon in the modern hybrid world of today. Diplomacy, Information, Military, Economic, Finance, Intelligence, and Law Enforcement (DIMEFIL) powers each have evolving roles in national power as the cyber domain reshapes the security landscape. While the DIMEFIL instruments of national power are forced to evolve, they are not necessarily strengthened within the cyber domain; in reality, their prominence is questioned as the cyber domain continues to influence a more asymmetric standard in the global power dynamic. How are these instruments of national power used to enforce normative behavior within the cyber domain? Additionally, the vulnerabilities of these instruments of national power that have been exposed within the cyber domain can have critically devastating impacts on critical infrastructure if a concerted effort is not placed on integrated defensive measures.

Within the United States, critical infrastructure is defined as "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that

[2] Ornes, Stephen. “The Internet of Things and the Explosion of Interconnectivity.” Proceedings of the National Academy of Sciences of the United States of America 113, no. 40 (2016): 11059–60.

their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[3] This definition can be translated similarly to other nation-states as well as private entities, as those assets, systems, and networks that would have devastating impacts on critical elements of that nation or entity's ability to function. Critical infrastructure vulnerability and the cyber domain are inherently linked as more of the world's infrastructure has become reliant upon digital means such as operating systems, programs, and artificial intelligence (AI) to efficiently manage physical and virtual systems. Weighing the desire for increased efficiency and reduction in physical labor or manpower with security is the crossroads for the future of critical infrastructure.

The level of risk a nation or private entity is willing to accept in gaining efficiency through reliance upon mechanisms within the cyber domain is often evident in their security posture and focus. Understanding the nature and types of threats to critical infrastructure as it relates to the cyber domain is an essential element in security.

To contextualize the potential level of threats within the cyber domain, the United States over the last two Presidential administrations has paid substantially more attention to the growing threat within the cyber domain and potential lack of viable security options. The 2019 National Defense Authorization Act established the Cyberspace Solarium Commission to identify strategic level way ahead for cybersecurity and potential impacts of malicious actions on security and critical infrastructure.[4]

[3] Cybersecurity & Infrastructure Security Agency. Critical Infrastructure Sectors. Updated October 29, 2021. https://www.cisa.gov/critical-infrastructure-sectors.

[4] Cyberspace Solarium Commission. March 2020. https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view

Additionally, several Executive level federal organizations have been created to provide guidance and recommendations, foster information sharing and integration with the private sector, and mange strategic level efforts for security and deterrence within the cyber domain. These federal entities include the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), the Office of the National Cyber Director, and the Deputy National Security Adviser for Cyber and Emerging Technologies. Multiple Executive Orders and attempts at legislation have also been implemented over the past six years, including the recent Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), aimed at more effective and efficient public-private sector integration.

The Cybersecurity Solarium Commission's final report identifies three layers of deterrence and six pillars supporting implementation. The layers of deterrence are Shaping Behavior, Denying Benefits, and Imposing Cost, and while each enables the overall deterrence strategy it is worth noting they are focused on deterrence all forms of malicious actors to include peer competitors, non-state actors, state-influenced actors, extremists, and criminals.[5] While this research does not focus on extremists and criminals, there are cross over considerations as the cyber domain blurs the lines between state and non-state actors.

The six pillars are broken down within each layer of deterrence. The pillars within the Shaping Behavior layer of deterrence are "building partnerships" and "leveraging non-military instruments."[6] This layer is more carrot then stick in using

[5] Cyberspace Solarium Commission. March 2020.
[6] Ibid.

cooperative means to achieve end states with external partners. The pillars within the Denying Benefits layer of deterrence are "securing elections", "protecting critical infrastructure", and "ensuring continuity of the economy."[7] These first two layers of deterrence and five pillars would benefit greatly from public-private sector integration. The pillar within the Imposing Cost layer of deterrence is "generate cyber capabilities and capacity."[8] This third layer can appear to have bleed over into offensive cyber which this research will not cover, but it does demonstrate a persistent need to grow and build resources within the human and digital terrain. Education within the cyber domain has also been a point of focus for the federal government, with agencies such as the CISA making concerted efforts to increase the level of education and talent within their workforce. Education and understand must also extend beyond the federal workforce, to the private sector, and the population at large in order to effectively secure the vastness of the cyber domain.

This research will examine the roles that attribution of malicious cyber events and the ability to enforce cyber norms play in securing the cyber domain through what is believed to be a logical progression. First, this research will look at the current stance of the international community regarding the need for establishing cyber norms, mainly through the United Nations and their Open-Ended Working Group. This chapter will focus on state-to-state relations within the cyber domain and how the establishment of normative behavior factors into these dynamics while also discussing the role of non-state actors in this regard. Non-state actors are those entities that are not directly or officially a

[7] Ibid.
[8] Ibid.

part of an established government but may be state-sponsored, completely independent of state influence, and anything in between. This includes the private sector entities such as global corporations as well as malicious actors, as they all provide influence as components within the cyber domain. Further examination in this chapter will focus on implementation issues surrounding established cyber norms, such as non-adherence from state and non-state actors and the complexity added by pseudo-conforming actors. These pseudo-conforming actors potentially have the outward appearance of adhering to cyber norms but whose actions within the cyber domain do not follow suit. Additionally, this chapter looks at attribution of non-conformist and malicious actors within the cyber domain by identifying the importance of the "Who" of malicious cyber actions in relation to the "What" or "Why."

The second chapter will focus on state actors and two schools of thought regarding the attribution of malicious cyber events. These viewpoints are a defense-in-depth model and an attribution-focused model. Defense in depth focuses on identifying vulnerabilities within a system and preventing, stopping, or mitigating exploitation of the vulnerability through adaptation and feedback loops. The attribution model focuses on identifying the source or actor responsible for the malicious event in an effort to determine why it occurred and how to stop it from happening again. This research examines three high-profile malicious cyber events alleged to be perpetrated by nation-states against nation-states, their impact on security within the cyber domain, and the response from the victim. Additionally, this research examines three peer competitors to Western nation-states within the cyber domain, their ties to malicious actions, and the limited role of attribution and enforcement of cyber norms within this peer competition.

The third chapter examines the public and private sectors' roles within the cyber domain as it relates to security. Looking at the impacts of the United States domestic policy on international security, and understanding how security within the cyber domain transcends borders allows for an examination of policy and private sector integration. This research examines the perceived roles of both the public and private sectors regarding security within the cyber domain and the potential impacts to critical infrastructure should security across both sectors not be adequate. Additionally, this research demonstrates the potential and existing impacts of malicious cyber events on the economic and political landscape, focusing on state-to-state and state-to-private sector relations.

Chapter 1:

Setting the Cyber Stage

Imagine a secure room, inside a secure building, within an ultra-secure facility. Within this room is an ultra-secure computer system, so secure it is not connected to any external systems. Any device it will come into contact with is isolated and cleared before entering the same room. All this for fear of it being compromised through the internet or other digital means. This computer's sole purpose is to operate critical equipment monitoring and regulating the temperature of machines attempting to enrich uranium. It would go without saying that the security and maintenance surrounding this computer and the associated mechanisms would be top tier and the highest priority. Now, what if the computer fails to regulate the temperature of that machine? Not only does it fail to regulate the temperature, but it also fails to recognize that it has failed to regulate the temperature. The computer does not even know anything is wrong and continues to enable the machines to conduct their processes as normal, ultimately leading to a failure in the process and damage to the mechanism as a whole. Now, what if the failure was blamed on a cyber-attack? How could a cyber-attack be responsible for this failure and potential disaster if the computer and its systems were completely isolated from the internet?

Though it may seem like science fiction, this scenario is the general premise of the STUXNET attack on the Iranian uranium enrichment processes at its Natanz nuclear facility.[9] STUXNET is a computer worm that does not simply disable or hijack a computer or system; it infiltrates and targets specific files and mechanisms in order to inflict failure within the system without highlighting the system is failing. It is in every sense of the word a targeted cyber weapon.[10] While the STUXNET attack did not ultimately cause a disaster in terms of lives and infrastructure lost, it does highlight the question of who conducted the attack and why. While it has been rumored that the worm's origin was a collaboration between the United States and Israel, it has not been confirmed or adjudicated. The why is relatively clear, to disrupt or degrade the Iranian nuclear program. Outside of the "who done it" aspects of the attack, an important question to ask is, if this was perpetrated by another nation-state, who would hold them accountable? Is this type of event and actions within the cyber domain something that requires oversight and governance? The seemingly obvious answer to these questions is yes, which is why several nations worldwide are focusing on the establishment and acceptance of international cyber norms.

As the world continues to evolve and technology plays a more significant role in every aspect of life, the cyber domain has taken an important place in discussions surrounding international affairs. Among the top concerns regarding the cyber domain is the role it plays in security issues and subsequently international politics. From maintaining national security and sovereignty to regulating international cooperation and interoperability, security matters within the cyber domain have significant and vital

[9] Kelly, Michael B. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought", Business Insider, November 20, 2013, https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

[10] Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", Wired, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet.

impacts on international affairs. Within these security discussions, the need for establishing international cyber norms is a leading topic for policymakers and private sector entities operating within the cyber domain. Establishing cyber norms has been a topic of interest at several international summits, including the United Nations and G7 conferences.[11] Is it critical to international security to establish internationally recognized cyber norms, and if so, what security shortfalls will be present should these norms not be either established or adhered to? This thesis will explore the thought process that the establishment of international cyber norms is enhancing to the overall security within the cyber domain; however, it is not critical. To date, there has not been a malicious cyber event that has caused damage or disruption significant enough to reach a threshold whereby retaliatory actions would be required by the international cyber community.

Additionally, state and non-state actors will continue to conduct protective measures to ensure minimal disruption to their interests within the cyber domain. However, it is important to note that the cyber domain is ever-evolving and doing so a what can be described as lightspeed. My focus will be drawing on the link between state and non-state actors within the cyber domain and how regulator actions must consider both of these parties as well as their relationship.

While international organizations and individual nation-states continue to work through the process of establishing cyber norms that are palatable to a broad audience, discussions continue to evolve regarding the implementations and enforcement of these norms. Additionally, after the norms are established, implemented, and a means for

[11] G7, Foreign Ministers Meeting. "Dinard Declaration on the Cyber Norm Initiative." Biarritz, France. 6 April 2019.

enforcement is emplaced, there is still the question of how to control non-state actors who choose not to abide by the established norms. Attribution and enforcement are challenging to accomplish between nation-states and become incredibly complex when the actions within the cyber domain are conducted by an entity outside the traditional bounds of state sanctions. The complexity only increases as non-state actors and state-sponsored entities become nearly impossible to differentiate between. Looking at how the lack of enforceable cyber norms creates issues from an international security standpoint, this inability to moderate or enforce international norms within the cyber domain will lead to security issues within national and international communities but will not be detrimental to overall security. Non-state actors will have increased influence within the international power dynamic due to their ability to leverage the cyber domain, including ease of access and resource availability. This increase in influence will disrupt the normative power balance with world powers and create security issues outside of the traditional state-to-state conflict.

Additionally, this disruption will extend beyond what has been seen in the physical domain with "traditional" terrorists and force nations to enhance security measures and integrate with the private sector to succeed in these endeavors. To address this theory, this thesis will examine historical events within the past ten years that have seen either a non-state or state-sponsored actor disrupt a state actor via the cyber domain. This thesis will also utilize the current narrative of establishing cyber norms that have been discussed at several the G7 leadership meetings and conference such as the 2019 Foreign Ministers Meeting in France, which has gained acceptance, to frame how the leading powers view the cyber threat and its overall impact on international security.

I. Norms in International Politics

In establishing international cyber norms, a collective effort must be placed behind ensuring that security is at the forefront of every discussion. While sovereignty and interoperability are significant factors to be considered within these cyber norms, security is of the utmost importance as it impacts sovereignty, interoperability, and trust both nationally and internationally. Without security, nations lose faith in one another, and citizens lose faith in leadership, leading to detrimental effects across the political, economic, and military realms. The United Nations (UN) role in establishing these cyber norms is that of a mediator. The UN must have a vested interest in providing equity to all members' concerns and claims in helping to determine a shared understanding of the security and other issues that impact the international community stemming from the cyber domain. From this shared understanding, common ground can be found in determining the most significant issues facing the international community regarding the cyber domain and marking them as hard lines to be addressed with the norms. It is essential that these norms need to address actions within the cyber domain as they relate to designated conflict and times of non-conflict.

The UN's cybersecurity Open Ended Working Group (OEWG), established in 2019, has sought to tackle the establishment of cyber norms from an international perspective focusing on cyber actions within declared conflict.[12] The results of about two years of work were all member nations within the UN agreeing to a form of international

[12] Hurwitz, Roger. "The Play of States: Norms and Security in Cyberspace." *American Foreign Policy Interests* 36, no. 5 (September 2014): 322–31.

cybersecurity. A key point in the agreement is the term "voluntary" norms, as the agreement is not legally binding.[13] Topics discussed within the conflict realm were offensive and defensive cyber actions, including the defend forward thought process and the interpretations of its relations to offensive actions. Additionally, addressing espionage as it relates to actions leading up to and during conflict as well as its role in periods of non-conflict.[14] While this agreement should have marked a significant step forward in cybersecurity and normalization of the cyber domain for international relations, the general consensus appears that there was not a need for a significant change in the current mentality and actions already occurring within the international cyber domain. The reasoning behind these thoughts is that, as it stands, there has not been an action executed within the cyber domain that has crossed a threshold of destruction of personnel or infrastructure. While we can cite the Stuxnet, Solar Winds, and Microsoft attacks as malicious actions that had significant impacts on state and private infrastructure, none has achieved the damage level that would typically be achieved through malicious actions within the physical domain. Attribution is a factor in examining these actions that will be addressed later. Still, the lack of attribution for the previously mentioned attacks also disabled the responses of the affected states to cross the threshold of causing an escalation of force either within the cyber or physical domains.

[13] United Nations General Assembly. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report. 10 March 2021.

[14] Ibid

II. Establishing Cyber Norms for State Actors

In addition to international organizations such as the UN, significant attention must be paid to the relationships and efforts of China, Russia, and the United States. As the leading three nations within the cyber domain, these three nations' historical tensions and failures to agree to international norms in other domains are cause for concern related to establishing international cyber norms. Their roles within all aspects of international affairs and the associated weight of their actions are critical to consider when discussing establishing cyber norms. Should one of these nations deem it not in their best interest to enable the establishment of international cyber norms, it would be a significant roadblock in continuity and consensus within the cyber domain. Fortunately, all three nations have a vested interest in the establishment of international cyber norms, mainly as a mechanism to help keep the other major players in check.[15] The issue of espionage, both within the cyber domain and concerning cyber capabilities, is a leading factor in the big three's interest in supporting the establishment of international cyber norms. Again, this will be discussed more in the attribution section, but the opposing viewpoints on the establishment of norms to regulate cyber-related espionage are; those in favor view it as means to prevent these actions and hold those conducting the actions accountable within the international community, while those against are concerned that should norms be emplaced regarding espionage nations will not simply stop conducting this action, but

[15] McKune, Sarah, and Ahmed Shazeda. "The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda." *International Journal of Communication (19328036)* 12 (January 2018): 3835–55.

rather execute it in ways that are more difficult to uncover and potentially expose the nation to more significant unknown threats.[16]

III. Cyber Norms and Non-State Actors

The primary focus for the establishment of cyber norms has stayed within the concept of state-to-state interactions. However, this is lacking in both depth and scale of what needs to be addressed and established. Nation-states do not hold the dominant or leading-edge position within the cyber domain. Private corporations have the drive, flexibility, and capacity to evolve within this domain much faster than traditional nation-states.[17] When looking at non-state actors specifically within the cyber domain, we must look beyond the traditional mindset of malicious actors such as terrorists.

Private corporations that operate within the cyber domain, such as software and social media corporations, must be viewed as critical links to the establishment of cyber norms, and vital contributors to security within the cyber domain must be discussed. Placing these private corporations into the discussion provides added context and thought origin that can often be overlooked by traditional nation-states. Additionally, these private corporations and non-state actors have a vested interest in the potential security that comes along with the establishment of cyber norms. This protection considers corporate and state-sponsored espionage, theft of intellectual property, and the economic

[16] Bey, Matthew. "Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition." *The Cyber Defense Review* 3, no. 3 (2018): 31-36.
[17] Hurel, Louise Marie, and Luisa Cruz Lobato (2018) "Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs." Journal of Cyber Policy. 3:1, 61-76.

impacts associated with a potentially more open and dynamic trade sector should security be increased as a result of these norms. The private sector has also spent significant resources on defensive measures that can be useful to the state entities with little additional capital investment from either side. This overall increase in security along with norms provides a defense in depth within the cyber domain, similar to deterrence within the physical domain.

While it may appear that the benefits associated with the establishment of cyber norms outweigh any reason to protest the establishment, there are still two sides to this argument. As mentioned previously, the establishment of cyber norms would potentially create a more cohesive and secure cyber domain for the nation-state and private sector alike. Limited malicious actions while enabling freedoms and deterring actions that would have significant political or economic impacts are generally viewed in a positive manner. However, the other view does not necessarily stand in opposition to the potential positives associated with the establishment of cyber norms but rather simply asks does it really change anything. Under current conditions, with the majority of nations and non-state actors mainly conducting actions within the cyber domain that best suit their own interests, there has not been a significant event that has disrupted or had lasting impacts on the security of any one nation, private organization, or collective within either sector.[18] While there have been occurrences of malicious actions impacting critical infrastructure such as the attacks previously mentioned, as well as the events surround the 2007 Estonian "blackouts," that saw a combination of actions to include

[18] Iasiello, Emilio. "What Happens If Cyber Norms Are Agreed To?" *Georgetown Journal of International Affairs* 17, no. 3 (2016): 30-37.

denial of service attacks to disrupt web traffic and cell service, there was no actual loss of life or significant damage to critical infrastructure.[19] This viewpoint also asks what is to gain from the establishment but making it more difficult to identify malicious or intrusive actions.

It is worth noting that the majority of the focus within the prevailing discussions has been placed on nation-states and private-sector corporations, while little has been paid to malicious non-state actors. This is due to a delineation between malicious cyber actions and cyber-terrorism.

IV. Implementation Issues

Once the international cyber norms are agreed upon and established, implementation is the next step. This step, especially under the framework of the UN, is mainly observatory in nature as the nations that have agreed to the norms must implement them within the established cyber structure of their nations and attempt to hold themselves and other nations accountable. From a state-to-state relationship, these nations must first look inward to hold themselves and their citizenry accountable for abiding by the established norms. Nations have the ability to hold their own citizens legally accountable for actions within the cyber domain, and aligning normative behavior in the cyber domain with the existing legal framework in the physical domain is beneficial in providing structure and support to enforcing the established norms. This accountability cannot be accomplished solely through government processes; nations

[19] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007.

must look outside of their own structure to other private sector actors within the cyber domain.

Incorporating the private sector in implementing these established cyber norms will be critical as the private sector holds a significant amount of weight within the cyber domain. Moreover, incorporating the private sector in the implementation of norms has the added benefit of more effectively reaching audiences and influencing cooperation beyond a single nation's borders. Private corporations such as Microsoft have a vested interest in ensuring compliance within normative behavior within the cyber domain, so much so that they are one of the leading figures in the establishment and implementation of international cyber norms.[20] Additionally, incorporating private-sector entities into the implementation phase, assuming they also participated in the establishment phase, provides a depth and breadth of expertise, influence, and flexible response to the changing environment. The feedback mechanism necessary to ensure implementation, accountability, and adjustment can potentially occur much faster within the private sector than through government channels. This efficiency in feedback can enable increased security and forward-thinking regarding an adjustment of the implementation strategy, as well as potentially be utilized as a "beta" version of a nation-state's planned implementation strategy.

The importance of state and non-state actors communally approaching the implementation process provides critical continuity and cooperation that, if not synchronized, could potentially create a separation in execution that would negate or

[20] Hurel, Louise Marie, and Luisa Cruz Lobato (2018) “Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs.” Journal of Cyber Policy. 3:1, 61-76.

confuse the entire cyber norm process. This shared vision and cooperation between the state and non-state actors are critical in all phases of the cyber norm process. However, it must be understood that while state and non-state actors may have a common goal of increased security within the cyber domain, they will most likely have diverging interests as the cyber domain continues to evolve. This will be a common theme during the attribution discussion as well.

Upon establishment and implementation of the international cyber norms, the most difficult processes occur. Enforcing the norms is difficult as there are currently no legal ramifications available to the UN for those who violate the norms. The nation within which the action originated must be the judiciary body if any recourse is to occur. While legal recourse is limited, other means of political and economic sanctions can be utilized as reactionary measures to violations. Another factor in the difficultly associated with enforcement is attribution. Nation-states rarely take credit for malicious or intrusive actions within the cyber domain, mainly for fear of retaliation or an escalation to conflict within the physical domain. For these reasons, those who conduct these types of actions or attacks are meticulous in their planning and execution to ensure there is little to no chance of attributing the action to the nation. This obviously makes enforcement extremely difficult as it would require attribution of almost absolute certainty. It also highlights the need for increased capabilities relating to attribution, as nations and other entities will not simply stop conducting these types of actions even with the establishment of cyber norms. This increase in capabilities for attribution must be viewed in the sense of increased security. Suppose a nation or non-state actor knows they have a limited chance of successfully conducting malicious or intrusive cyber actions without attribution. In that case, it should act as a deterrence for conducting the actions. While this increase in attribution capabilities will not deter all malicious or intrusive actions, it should provide enough incentive for abiding by the established cyber norms.[21]

Conversely, there is a school of thought that it is arbitrary to know the "who," but rather, it is more important to know the "what" in order to apply appropriate defensive measures and start the process of recovering from the event. This line of thinking deems it less important to know who conducted the attack as the more relevant information is that an attack or event occurred, what the target was, and the damage inflicted. Knowing the event occurred enables the "victim" to identify how they were compromised as well as what was potentially compromised. Knowing these facts enables those on the receiving end of a malicious event to implement measures to prevent similar events from occurring in the future, as well as analyze the information or infrastructure that was potentially compromised for further threats or recovery. By knowing how they were compromised and what was compromised, the organization can identify why the event occurred and create an analysis of what other information may have been targeted or may be targeted in the future. This again enables the organization to implement updated security measures to prevent future compromises or intrusions.[22] All of this can be accomplished without knowing who initiated or committed the event. This is a defensive

[21] Goel, Sanjay. "How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race." *Connections (18121098)* 19, no. 1 (Winter 2020): 87–95.

[22] Steffens, Timo. *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage.* 1st ed. 2020. Berlin, Heidelberg: Springer Berlin Heidelberg, 2020.

mindset and does not attempt to incorporate deterrence or enforcement into the security apparatus within the cyber domain.

V. Attribution, Prevention, and Feedback Loops

It must be considered what the ability to attribute actions within the cyber domain provides to the larger security discussion. Does the ability to attribute these actions provide substance to the overall security mechanism to include increased deterrence, or is it simply an information-gathering endeavor? A focus must also be paid to the differences between individual and group attribution, as the majority of actors within the cyber domain do not have the bandwidth to focus on single actors whose actions may not reach the threshold of what is deemed unacceptable to these state and non-state actors. Along these same lines of thought is providing weight to attribution objectives such as identifying actors or organizations or identifying motives, influences and tactics, techniques, and procedures. While these objectives and motives for attribution may differ from actor to actor, the normative behavior within the cyber domain, or lack thereof, can potentially be telling factors that may lead to attribution or influence reaction to an event.

Understanding the differences, roles, and interpretations between attribution, prevention, mitigation, and deterrence provides significant context to the larger discussion regarding security within the cyber domain. While it may appear that attribution is an action that occurs at the end of a linear process of dealing with malicious cyber actions, it actually articulates that the process is cyclical. Considering attribution as a type of feedback mechanism to help mitigate future events while also providing evidence for the enforcement of laws and norms. This does not necessitate that the ability to attribute malicious cyber actions or events provides security but that it is simply a mechanism in the larger security architecture. However, attribution of malicious cyber actions or events should be more than simply providing feedback on an event to improve security measures. Attribution should enhance the defend forward mechanism by enabling the organizations and nations the ability to apply pressure through legal, economic, or political channels to prevent future malicious events, hold those conducting them accountable, and demonstrate that there are repercussions for actions within the cyber domain. Thinking of attribution through this holistic lens, with the addition of private sector influence, adds weight to the need for attribution and the mechanisms to conduct the corresponding actions. In this light attribution is seen as enhancing to the security mechanisms associated with defending the cyber domain.

Prevention, mitigation, and deterrence, as opposed to attribution, focus on the "left of boom" for actions and are steps in the security mechanism to enable the entity being protected, or targeted, to continue operating with little to no interference. While these actions are certainly influenced by the data collected after an event has occurred and can be bolstered by successful attribution of malicious events, they can and should also operate outside of the post-event analysis with an eye towards the future threat.

While examining the post-event analysis, organizations must consider the cost-benefit analysis first of conducting attribution and second about making a public declaration of the findings. This cost analysis must consider the established cyber norms and how this action impacts the security of other actors within the cyber domain. What is more important for security; attribution, which can lead to a means of enforcement and hold individuals, organizations, and nations accountable for their actions, or the defensive measures themselves that would prevent the malicious actions from having an impact?

In order to examine why the establishment of international cyber norms would only be enhancing to international security, we must look at the major nation-state players within the cyber domain. The United States, Russia, China, and Iran are the predominant nation-states operating within the cyber domain. Focusing on the interactions between these nations is important to understand the weight and significance, or lack of significance, the establishment of international cyber norms truly carries. Examining the STUXNET attack on the Iranian nuclear program alleged to be carried out by the United States and Israel, how China views cyber espionage, and the malicious cyber events that targeted Estonia allegedly with Russian influence are gateways to understanding the larger security context within the cyber domain and the potential influence cyber norms could have.[23]

The STUXNET attack on the Iranian nuclear program highlights the role attribution plays in adhering to the international cyber norms. It is alleged that the United States and Israel were responsible for the attack that could have potentially resulted in catastrophic damage to infrastructure, loss of life, and second-order effects associated with a nuclear accident or meltdown. The intent of the attack, or intrusion, was to essentially interfere with the computer system used to manage safety protocols while

[23] Kerr, Paul, John Rollins, and Catherine Theohary, "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability," Congressional Research Service, December 9, 2010, 6-8.

causing other systems to overact such as excess spinning of centrifuges, and inevitably overheat and fail.[24]

Chinese cyber-espionage activities have been undeterred in recent years, and they are only accelerating their efforts within the cyber domain, conducting intrusions on nation-states and private corporations alike. China's "Three Warfares" specifically addresses means to offset any anticipated sanctions against the government from the international community for actions conducted within the cyber domain.[25]

The alleged Russian-influenced attack on Estonia that saw the governmental and financial websites go "dark," is another example of the limited capacity these norms can influence security. In response to Estonia removing Soviet-era statues from city centers, Russian-influenced hackers significantly disrupted the Estonian government and private sector cyber services rendering the nation unable to conduct a majority of its government and private business.[26] Unlike STUXNET and Chinese cyber espionage, this event was supposedly conducted by surrogates instead of a nation-state. Addressing the issue of surrogates or non-state actors begins to degrade the validity of the security provided by international cyber norms, as there is limited ability to hold non-state actors accountable for actions within the cyber domain if the nation in which they originated the event does not abide by the norms.

[24] Kelly, Michael B. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought", Business Insider, November 20, 2013, https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

[25]Iasiello, Emilio. "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities." Journal of Strategic Security 9, no. 2 (2016): 45-69.

[26] Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007.

VI. Conclusions

Viewing the establishment of international cyber norms within a similar construct as nuclear non-proliferation can aid in contextualizing the problem set. Nations collectively viewed nuclear non-proliferation as critical to increased international security, and while there have been some outliers with this stance, mutually assured destruction is not a desired end-state. The same can be said about malicious actions within the cyber domain; collectively, nations and other actors within the cyber domain would find it beneficial to prevent the proliferation of malicious actions and events within the cyber domain, and with adherence to cyber norms, security would naturally increase. However, just as state and non-state actors still seek to gain access to nuclear material despite the "Treaty on the Non-Proliferation of Nuclear Weapons," entities will continue to seek out ways to conduct malicious actions within the cyber domain.[27] It is still individual nations' and private organizations' responsibility to provide themselves with security within the cyber domain. The collective nature of international cyber norms would enhance this security and potentially provide a mechanism for accountability should attribution succeed. It is critical to highlight cyber norms and successful attribution as enhancing and not critical to improved security within the cyber domain, as they are a piece to the security puzzle not the key to solving it. Collective security measures would appear to be more beneficial than costly for most parties. However, there are costs associated with anything collective in nature. A cost worth highlighting is the potential need for collective reaction, such as how the Westphalian system of order

[27] "United Nations: Security Council Resolution on Security Assurances for Parties to the Treaty on the Non-Proliferation of Nuclear Weapons." International Legal Materials 7, no. 4 (1968): 895-96.

inevitably led to the scale of what would be World War I.[28] While this example should not be a significant dissuading argument, there is always the potential for escalation of collective response within the cyber domain as well as the transition into the physical domain for reactionary measures. Conversely, the collective nature of international cyber norms may, in fact, prevent the escalation of retaliatory actions from crossing into the physical domain or beyond an acceptable threshold within the cyber domain for the fact that there are other options. As previously mentioned, the ability to leverage political, social, and economic reprisals against the violator of the established norms has the potential to enhance security within the cyber domain, but as will be discussed in coming chapters the impacts of these efforts may be overestimated.

[28] Kissinger, Henry. 2014. World Order. New York: Penguin Press.

Chapter 2:

Deterrence, Defense, and Competition

As the world continues to increase its interdependence with the cyber domain, it is evident that the security apparatuses aimed at keeping our nations safe must significantly evolve to match the complex and integrated environment. Through the efforts of the United Nations through the Group of Governmental Experts (GGE) and cybersecurity Open-Ended Working Group (OEWG), it is understood and generally agreed upon by all representative nations that the establishment of normative behavior within the cyber domain is essential for international security. To have a common understanding of the cyber domain, we will identify cyber as cyberspace and utilize the definition of a domain as "a sphere of knowledge, influence, or activity."[29] Cyberspace in this context is "a global domain within the information environment consisting of the interdependent network information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[30] While specialists within the cyber domain across the international community continue to identify and implement security mechanisms, identifying the critical components of cybersecurity and the weight of their role in effective security across international borders has become an important topic for discussion. Among these components, attribution of malicious behavior and enforcement to adherence to cyber norms have become focal points. The cyber norms are those outlined in the OEWG on

[29] "Domain, N." Merriam-Webster, 2022, www.merriam-webster.com/dictionary/domain.

[30] United States. Department of Defense. *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms*. Department of Defense. 8 November 2010 (as amended through 15 February 2016).

developments in the field of information and telecommunications in the context of international security's final substantive Report from March of 2021, highlighting the acceptable and non-acceptable actions of nation-states within the cyber domain specifically regarding state sovereignty and protection of critical infrastructure.[31] Malicious events within the cyber domain are those events or actions that deviate from the established norms and have the intent to degrade, disrupt, damage, or otherwise harm an entity through actions taken within the cyber domain. Within this context, attribution is identifying the actor(s) responsible for supporting or conducting malicious events within the cyber domain.

Examining nation-states' ability to accurately attribute malicious behavior to its source actor within the cyber domain as well as enforce adherence from non-conformists to these normative behaviors is a starting point in this discussion. The larger question related to this examination is how a nation-state's ability to attribute malicious behavior and enforce cyber norms impacts its overall security. As critical as attribution and enforcement are to the discussion of security within the cyber domain, a nation-state's inability to enforce cyber norms upon potentially malicious actors does not drastically increase the threat within the cyber domain. Other preventative measures such as defense-in-depth and defend-forward mechanisms will provide more salient security solutions within the cyber domain. Defense-in-depth requires the layering of defensive mechanisms in an attempt to identify and correct vulnerabilities before they are exploited, correcting vulnerabilities that external actors have already exploited, and consistently

[31] United Nations. General Assembly. *Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.* United Nations General Assembly Conference Room Paper. 10 March 2021.

developing and implementing more effective defensive mechanisms to safeguard the cyber domain and its infrastructure. Defend-forward is an idea that in an effort to defend itself, the entity must seek out those who would conduct malicious events and prevent them from doing so by removing their capability or capacity.

Two perspectives need to be examined regarding security within the cyber domain. One perspective examines cyber-related security issues in a state-to-state context, similar to the construct of how conventional diplomatic, military and economic efforts are applied. The other perspective examines cyber-related security issues in a state to non-state entity context, potentially sharing applications of irregular warfare from a military mentality while implementing diplomatic and economic efforts through third-party entities. However, these two perspectives become blurred within the cyber domain as the lines between state actors, state-sponsored actors, and third-party entities grow increasingly more complex. This complexity further highlights the criticality of attribution and the need for expanding security mechanisms and approaches within the cyber domain.

Examining two distinct categories will provide the determination that security measures beyond attribution of malicious actors and deterrence through enforcement of cyber norms are essential to international security and its relationship to the cyber domain. The first category is high-profile malicious cyber events such as Moonlight Maze, STUXNET, and the 2007 Estonia event. These events demonstrate the growing complexity of not only security within the cyber domain but also the growth of hybrid relationships between state and non-state actors. The second category to be examined is nation-state threat actors, highlighting the roles and actions of China, Russia, and Iran.

While all three categories have become interwoven from international and cyber domain security perspectives, exploring them independently and collectively will provide further evidence that attribution and enforcement do not play a significant role in deterrence. By highlighting their lack of importance in the deterrence of malicious cyber activities, it forces nations to expand their cyber security mindset beyond what attribution and enforcement provide in terms of deterrence to potentially more proactive measures.

To demonstrate the role of attribution and enforcement of cyber norms within the international security continuum, I will examine two schools of thought regarding their importance through a literature review, followed by an exploration of research highlighting significant high-profile cyber events and the current landscape of cyber peer competitors outside of the United States. The literature review examines one school of thought that attribution of malicious cyber activities is critical to increasing security within the cyber domain, while the other school believes that while attribution is important increasing security, it is more vital to focus efforts on defensive measures and corrective actions to prevent or counter malicious cyber events then be concerned with the actor who perpetrated the event. The following research utilizes an examination of high-profile malicious cyber and the current cyber domain peer competitor landscape to highlight the limited role that attribution plays in the greater security continuum within the cyber domain. These events and actors are known quantities within the cyber domain, yet they continue to operate outside of normative behaviors within the cyber domain regardless of deterrence or enforcement attempts.

I. Attribution and Enforcement versus Defense-in-Depth

The relationship between the cyber domain and national security has matured to a point where they are interwoven at the molecular level, one having critical impacts on the future of the other. Understanding the vulnerabilities, malicious actors, and responses within the cyber domain now plays a prominent role in the decision-making process of world leaders and has ascended to inclusion in daily conversation regarding national security. As the expansion of the Internet of Things (IoT) increases at an exponential rate to include critical infrastructure, Department of Defense capabilities, the preponderance of the private sector, and a litany of other touch points that impact daily life, the need for security within the cyber domain has kept pace. In order to provide the necessary security, experts and scholars continue to examine the best means to keep pace with the growing threats. While it is a common understanding of the criticality of security within the cyber domain, the roles of attribution of malicious activities and enforcement of normative behavior are still up for debate.

Establishing acceptable or normative behavior within the cyber domain is viewed as a positive and widely accepted endeavor that will provide boundaries and expectations for the international community. However, how are these norms enforced, and what are the appropriate mechanisms to identify or attribute behaviors that do not operate within the established norms? While these questions continue to be answered, another question arises: Is it critical for security within the cyber domain to attribute malicious behavior and subsequently enforce adherence to the norms through the punishment of those who deviate from them? One school of thought believes that attribution of malicious behavior is critical to deterring similar actions, increasing the overall level of security within the cyber domain. In contrast, another believes it is beneficial but not critical to providing security within the cyber domain, as efforts are better spent elsewhere in correcting or preventing malicious actions.

II. Attribution- Key to Deterrence

Understanding the "Who" and "Why" of malicious cyber activities is often viewed as a critical component of providing security within the cyber domain. If those seeking to secure the nation from attacks or other malicious activities within the cyber domain can identify both the entities responsible and the reasoning behind their actions, they can devise a robust way ahead to mitigate the current malicious activity, secure the vulnerability attempting to be exploited, and prevent future events of similar nature from occurring or impacting national security.[32]

Attribution seeks to enable security by not only identifying the malicious actor but exposing the identified actor to the broader, potentially international, community for their actions.[33] Exposing the malicious actor is believed to deter future actions from the identified actor or influence other actors from attempting similar activities for fear of exposure. Knowing the actor and the action enable a more detailed view of the security issue and can potentially identify other security issues that may need correction.

[32] Healey, Jason. *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*. Atlantic Council, 2012.

[33] Mejia, Eric F. “Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework.” Strategic Studies Quarterly 8, no. 1 (2014): 114–32.

Additionally, identifying the malicious actor provides information that enables security experts to formulate appropriate responses.

Attribution also enables states to formulate the appropriate response to a malicious event or attack. Due to the cyber domain's complexity, it is increasingly important to respond appropriately to malicious activities or attacks. In the physical domain, a malicious action against a state that causes physical damage to personnel or infrastructure is often met with a physical and equal response. This causal relationship leads to most conflicts between state actors and those who wish them harm. Within the cyber domain, the relationship between action and response is not as clear, but attribution can provide the justification for kinetic or non-kinetic responses. Nation-states must also weigh their response depending on the malicious actor. Direct engagement through diplomatic, economic, or military means can be justified should the actor be another nation. However, should the malicious actor be a non-state actor, and attribution cannot link state sponsorship, a physical military response is often removed from the equation, and social, political, or economic means must be leveraged to achieve the desired end-state.

III. Defense First

The other school of thought generally agrees that attribution can provide positive input to security and deterrence but is not critical to defending the nation from malicious activities and attacks within the cyber domain. Instead, the focus should be on identifying a malicious action and taking the appropriate steps to mitigate and correct the event. Instead of attempting to put the puzzle together in hopes of better understanding the "Why" by finding the "Who," it is more critical to correct the damage the malicious activity created, identify and correct other vulnerabilities that may be exploited in a similar manner, and continue to provide defensive security measures across the continuum of the cyber domain.

Aside from the amount of time and effort that must go into attribution that could otherwise be focused on identifying and correcting vulnerabilities, some believe that attribution is unnecessary as it does not provide significant output from its labor.[34] When it comes to state-sponsored or state-initiated malicious activities within the cyber domain, attribution does not necessarily increase security or deter future malicious actions, as proven by the actions of Russia, China, and North Korea. Although the United States has identified and publicized that these nations, and entities they sponsor directly and indirectly actively execute malicious activities within the cyber domain against the United States, it has done little to discourage or prevent future malicious events. [35] The malicious activities of these nation-states range from espionage, such as China's efforts to gain access to private corporations' intellectual property or defense department secrets, to attacks on critical infrastructures, such as Russia taking control of and shutting off the Estonian government's internet in 2007.[36] While these actions are widely known and attributed to the nations that executed them, little has come from this attribution in terms of limiting future malicious actions outside of general condemnation from the

[34] Peters, Allison, and Pierce MacConaghy. "Unpacking US Cyber Sanctions." Third Way, 2021.
[35] Iasiello, Emilio. "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities." *Journal of Strategic Security* 9, no. 2 (2016): 45-69.
[36] Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007.

international community and some political and economic sanctions that appear to have done little to damage the perpetrator.

This school of thought may appear to be reactionary in nature, but it is not negating the responsibility to seek out potential threats and vulnerabilities to be mitigated actively. It also does not wholly dismiss attribution's role in the more significant security construct. Instead, it believes its impacts are limited in increasing security within the cyber domain.

A central point of difference between these two schools of thought is the means of achieving security and deterrence. In the "attribution is critical" school of thought, deterrence is achieved through identifying and exposing malicious actors, which in turn increases security within the cyber domain. In the "attribution is not critical" school of thought, deterrence is achieved primarily through consistently seeking to improve security and prevent attacks through good collective and individual practices. The criticality of the role attribution plays in the larger security conversation within the cyber domain is what needs to be examined and determined.

Examining high-profile cyber events and the peer competitor space within the cyber domain is a practical starting point for examining how attribution and enforcement of cyber norms factor into the larger context of security within the cyber domain and the impacts they have on international security. The examination of high-profile cyber events provides the background for how actions within the cyber domain, specifically actions that are counter to establish normative behavior, impact the physical domain from a security perspective while highlighting the limited importance of attributing these actions in the broader scope of international security. This is not to say that attribution is irrelevant in these malicious events, but that it does not play a significant role in degrading or deterring entities from conducting future actions of a similar nature. Examining the peer-competitor space within the cyber domain, those nation-states who possess the ability to create the largest impacts within the domain, highlighting their interactions with peers, adversaries, and those in undefined status further reduces the importance of attribution and identifies the limited capability of the international community in enforcing the established cyber normative behaviors even if the perpetrator is identified.

IV. High-profile Malicious Cyber Events

The threat of malicious activities within the cyber domain has been a reality since the creation of interconnected computer systems stemming from advancements based on the Advanced Research Projects Agency Network (ARPANET).[37] These malicious activities can range from individuals stealing internet time from universities in the early days of the internet to cyber-attacks aimed at destabilizing networks or destroying infrastructure; subsequently, the security mechanisms aimed at preventing or correcting these activities must encompass the same diversity and adaptability in order to be successful. A critical part of success in adapting security measures within the cyber domain is understanding historical malicious events by placing them into context regarding impact severity and means of resolution. Events such as Moonlight Maze, STUXNET, and the 2007 Estonian cyber-attack demonstrate the growing complexity of

[37] Shires, James, and Max Smeets. "ARPANET: WHERE DID IT ALL START AGAIN?" CONTESTING "CYBER." New America, 2017.

malicious cyber events and the roles that attribution, enforcement of cyber norms, and defensive cyber actions play in ensuring security on an international level. While non-state actors also contribute to the growing catalog of high-profile malicious cyber events, the focus of examining these events is within the context of nation-states' actions, even if they are only alleged.

Moonlight Maze was the name given to the FBI lead task force investigating a significant data breach in 1999. The investigation uncovered that an attack had occurred, resulting in the extraction of classified information from the United States government and civilian institutions, including the US Department of Energy, Department of Defense, and NASA. Additionally, the investigation revealed the attack had been occurring since 1996 and was eventually linked to Russian involvement though individuals were never identified.[38] Moonlight Maze provides a significant point in the evolution of the cyber domain, setting the tone for understanding cyber espionage and nation-state response to these types of attacks. While the United States investigation was able to determine with a high degree of confidence that the attack originated from within Russia, it could not identify the group or individual responsible nor hold them accountable. However, this event did enable the United States to begin examining how it would react to malicious activity within the cyber domain, laying the foundation for future cyber security frameworks. Despite not being able to attribute the source of the malicious activity, the United States was able to begin taking corrective action to improve its overall security within the cyber domain.

[38] Doman, Chris. "The First Cyber Espionage Attacks: How Operation Moonlight Maze made history." Medium, 7 July 2016.

In 2010, Iran was the victim of a significant malicious cyber event targeting its nuclear enrichment program. The Stuxnet worm targeted centrifuges within Iran's Natanz uranium enrichment facility, ultimately rendering a significant number of them inoperable and potentially setting back Iran's nuclear program for decades.[39] An important aspect of understanding the impact of the Stuxnet worm event on international security is the lack of confirmed attribution of the perpetrators of the attack. While it has been widely reported that the United States and Israel collaborated in the planning and implementation of the Stuxnet worm as a part of the larger Operation Olympics Games, a campaign aimed at utilizing cyber means vice conventional military strikes to disrupt Iran's nuclear program, it has never been officially acknowledged or legally attributed to either nation.[40] Regardless of the intent behind the Stuxnet worm, the focus of understanding this event in our context is that despite the lack of attribution, establishing countermeasures to the worm and subsequent preventative measures to reduce the likelihood of success of future attacks still occurred. Analyzing the assumed mechanism for introduction to the closed systems at the Natanz facility and the impacts of the Stuxnet worm provided greater information for improving security than may have been provided by identifying the perpetrators. Additionally, the Stuxnet worm is an important event to note as it demonstrated the potential ability of a malicious actor to impact or damage critical infrastructure within the physical domain through cyber means.[41]

[39] Kaminski, Mariusz Antoni. "Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the developments of Iran's nuclear programme." Security and Defence Quarterly Volume 29 (February 2020): 64-71.

[40] Broad, William, John Markoff, and David Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." The New York Times. January 15, 2011.

[41] Kerr, Paul, John Rollins, and Catherine Theohary. "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability." Congressional Research Service. December 9, 2010, 6-8.

In 2007 Estonia experienced a significant malicious cyber event that impacted every aspect of connectivity within the nation. A botnet had been introduced, purportedly by a foreign actor, to the nation's internet and attacked the functionality of everything from banking services to government communications systems.[42] Two aspects of this event are important to understand its significance in the international context of malicious cyber events. First is the timing of the event in relation to the Estonian government's decision to move a Soviet-era statue commemorating the Soviet lives lost in the region during World War II. The second is that Estonia is a member nation of NATO and the European Union.[43] The assumption that the denial-of-service (DoS) attack was executed by a foreign entity combined with the ethnic-Russian protests regarding the removal of the Soviet-era statue would lead Estonian officials to believe that the Russian government was involved.

Additionally, as a member of NATO being attacked by a foreign entity, Estonia had the ability to invoke its right to request collective defense. If Estonia had invoked collective defense to mount a military response in the physical domain to the attack, it would have required definitive attribution of the malicious actor or actors to ensure the response was proportionate and legal. These efforts may have been able to enforce the responsible entities to capitulate to established cyber norms through the use of force or diplomatic means.

[42] Kostadinov, Dimitar. "Estonia: To Blackout an Entire Country - Parts 1. " InfoSec Institute. October 8, 2013.

[43] Davis, Joshua. “Hackers Take Down the Most Wired Country in Europe.” Wired. August 21, 2007.

V. Peer Competitors

In the current spectrum of cyber competitors, the United States, China, Russia, and Iran can be assumed to be the leading state actors. These nations are also significant players within the political and military domains, keying in on the interconnectedness of the cyber domain and international security. Examining the peer competitor spectrum links to malicious cyber events highlights China, Russia, and Iran as the leading contributors to state-led and alleged state-sponsored malicious cyber events. While the United States is not excluded from this group in regards to malicious events, outside of its suspected involvement in Stuxnet, it has not been identified as a major contributor to malicious cyber events or increased security issues within the cyber domain. China, Russia, and Iran have consistently been identified as perpetrators, either directly or through proxies, of malicious cyber events in attempts to further their own political agenda or degrade international competitors or advisories. Despite the international community's growing awareness and response to these nations' actions, including political and economic sanctions, they continue to execute their cyber agenda.[44]

As China continues to attempt to evolve into an influential world power in almost every facet of modern society, they have leveraged the cyber domain to accomplish a large portion of this evolution. Unsurprisingly, China seeks internet sovereignty, making the state the focal point regarding control of the internet. Since the early 2010s, China has publicly pushed for other nations to take a similar stance, garnering support from

[44] Bartlett, Jason, and Megan Ophel. “Sanctions by the Numbers: Spotlight on Cyber Sanctions.” Center for a New American Security, 2021.

allies but drawing disapproval from the United States and its western allies.[45] A state-controlled internet remains on par with the Chinese government's agenda in most of its economic endeavors and is seen from within as a natural course of action to maintain national security in a rapidly evolving critical domain. Externally, the Chinese government appears to be utilizing its control of cyber capabilities and international telecommunications assets to perpetuate and improve upon the art of espionage. The United States has accused China of conducting cyber espionage against the private and public sectors resulting in the theft of intellectual property and classified information. The alleged thefts have reportedly enabled the Chinese government and its subsidiary companies to grow exponentially with minimal research and development investment. All in the name of their strategic interests.[46] China views the ability to grow at pace with the evolving domain and control of the associated assets as critical to their national security and has developed strategies and policies to mitigate any potential international sanctions due to their means of achieving success.[47]

Russia remains a hotbed for cyber developments directly and indirectly. Their alleged use of state-sponsored malicious entities demonstrated by the 2007 Estonia event has created a rising tide of defensive measures within the neighboring regions as well as with western competitors. These efforts, combined with developing tactics for hybrid warfare, fusing deliberate offensive cyber operations in support of military actions in foreign nations such as Ukraine, have reshaped the way the majority of the world views

[45] Kolton, Michael. “Interpreting China’s Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence.” The Cyber Defense Review 2, no. 1 (2017): 119–54.
[46] Iasiello, Emilio. “China Arctic Cyber Espionage.” The Cyber Defense Review 6, no. 3 (2021): 121–28.
[47] Iasiello, Emilio. "China’s Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities." Journal of Strategic Security 9, no. 2 (2016): 45-69.

the cyber domain.[48] While Russia has shown signs of losing its place as a leading world power, it can leverage its cyber capabilities to influence nations and corporations throughout the globe, as demonstrated by its alleged meddling in the United States Presidential elections and ransomware attacks on critical infrastructure such as gas and oil pipelines. [49] Russia's use of state, state-sponsored, and state-influenced entities all appear to be aimed at destabilizing opposition and influencing the international community in favor of Russian strategies.

While Iran is often viewed in the context of cyber capabilities as more of a victim than a perpetrator, it continues to develop its own capabilities to remain relevant within the broader international community. Since the Stuxnet worm and a handful of other cyber-attacks, Iran has embraced the need for security within the cyber domain and understands its relationship to national security. However, they also appear to understand the importance of projecting power through cyber capabilities, utilizing their growing capabilities to control access to information similar to China, as well as influence and disrupt political or military foes, as demonstrated by their efforts in August 2012 against Saudi Aramco with a denial-of-service attack.[50] It appears that most of Iran's growth within the cyber domain is a forcing function of regional conflict and consistent tension

[48] Barrinha, André. "Virtual Neighbors: Russia and the EU in Cyberspace." Insight Turkey 20, no. 3 (2018): 29–42.

[49] Shad, Dr. Muhammad Riaz. "Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions." Policy Perspectives 15, no. 2 (2018): 41–55.

[50] Sulmeyer, Michael, Jon B. Alterman, Michael Connell, Michael Eisenstadt, Farideh Farhi, Thomas Karako, J. Matthew McInnis, Hijab Shah, and Ian Williams. "Cyberspace: A Growing Domain for Iranian Disruption." Edited by Kathleen H. Hicks and Melissa G. Dalton. Deterring Iran after the Nuclear Deal. Center for Strategic and International Studies (CSIS), 2017.

with the west. Regardless, they have developed and continue to integrate malicious cyber events into a broader geopolitical strategy.

VI. Conclusion

While state actors' political and diplomatic stances provide insight into their ends, ways, and means regarding efforts within the cyber domain, they also enable a potentially higher degree of attribution for malicious actions. Regardless, they continue to execute offensive and defensive operations, and malicious and growth-seeking endeavors, within the cyber domain with limited fear of consequences. The difficulty of attribution aside, there remains limited ability for the international community to take effective punitive measures against a state actor conducting malicious cyber efforts beyond sanctions. Contributing factors to these limitations appear to be that the malicious actors do not fear the current punitive measures that can be imposed upon them, and the malicious actions have yet to cross the threshold requiring a physical or military response. This is an important distinction to make, as understanding that a threshold exists even unofficially can create the assumption that attribution is not an essential aspect of security within the cyber domain until that threshold is crossed. The international community will continue to face growing security threats from malicious cyber events, potentially perpetrated by nation-states, regardless of their ability to attribute the event to the actor unless tangible and effective measures are undertaken to prevent the nations from operating with near impunity within the cyber domain.

State actors remain a critical component to the growth and execution of capabilities within the cyber domain. However, they are not always on the leading edge of cyber initiatives. Non-state actors such as private corporations, collective organizations, and individual citizens play an important role in the evolution of the cyber domain and its growing complexity. Subsequently, these types of entities also play an important role in determining the need for attribution of malicious cyber events and enforcement of cyber norms. If nations still struggle to deter or influence state actors from conducting malicious cyber activities, these efforts appear diluted even more when seeking to deter non-state actors. The rise of cybercrime such as ransomware, malware, and denial-of-service attacks gives credence to the limited role of attribution or the importance of enforcing cyber norms. For these efforts to be successful, it would require global adherence of nation-states to establish cyber norms and their willingness to punish their citizens for failing to adhere. Currently, this appears to be a political bridge too far.

Chapter 3:
This is Where We Are, This is Where We Are Going

The United States is no stranger to tensions between the private and public sectors. Private corporations and entities often resist government influence and often utilize mechanisms such as lobbying in efforts to prevent government regulations from interfering with business. The private sector's concerns regarding government influence are often justified, as they seek to remain agile and adaptable in the ever-changing and complex economic environment. The main perception is that increased government involvement would lead to increased bureaucracy, subsequently degrading the private sector's ability to evolve, causing impacts on revenue, status, and employment. The cyber domain is no different from any other economic forum in this regard, as private entities seek to unburden themselves from traditional lethargic processes and the bureaucracy that comes along with them in an effort to increase profit and be on the cutting edge of what is next. But where should the lines be drawn between public and private responsibilities and integration regarding security within the cyber domain? Weighing the private sector's priorities along with those of the public sector regarding security within the cyber domain is an important starting point in finding a resolution to this question.

On the surface, it would seem fairly evident that integrated efforts and synchronized cooperation between the public and private sectors regarding security within the cyber domain would be in the best interest of all parties. However, in addition to variances in priorities within the cyber domain, the evolving dynamics of international security weigh heavily upon the public-private relationship. These dynamics include the interconnectedness of state and non-state actors, the evolving role of state-sponsored or state-known malicious cyber activities, cybercrime, and the glide slope of effective security measures within the cyber domain. Examining the varying and interconnected priorities, evolving dynamics of international security, and the impacts of malicious cyber events from the perspectives of both the public and private sectors will provide an outline for integrated efforts and roles.[51] Additionally, this examination will provide further evidence towards the limited roles of attribution of malicious cyber events and attempts at enforcing cyber normative behavior and focus on a more definitive role of defense in depth and appropriate allocation of resources to provide security within the cyber domain.

I. Policy Perspective

The public sector's main priorities, more specifically national level governments, appear to center around the protection of critical infrastructure and the population. In the United States, efforts to increase security within the cyber domain have focused on critical infrastructure protection and integration with the private sector. In 2013, Executive Order 13636- Improving Critical Infrastructure Cybersecurity conceptualized the need to increase the ability of the nation's critical infrastructure to handle the growing threat from malicious cyber activity. In the executive order, the National Institute for Standards and Technology (NIST) was tasked "to lead the development of a framework

[51] McGhee, James E. "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy." Journal of Law & Cyber Warfare, vol. 2, no. 1, 2013, pp. 64–103.

to reduce cyber risks to critical infrastructure" in coordination with the private sector.[52] Once the Framework was complete and approved, the Department of Homeland Security would focus on the promotion of voluntary adoption of the Framework and oversight to adhere to regulations. A critical component of this executive order and subsequent Framework is communication and information sharing across the public and private sectors. Through efficient and timely communication and information sharing between the two sectors, coupled with a focus on protecting critical infrastructure, the nation's overall security would benefit.

In 2017, Executive Order 13800- Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure was released, focusing on the modernization of Federal information technology infrastructure and again on a partnership with the private sector with regards to bolstering the nation's security and protection of critical infrastructure as it relates to the cyber domain.[53] These executive orders have taken an interagency approach to incorporation with the private sector, calling on the Departments of Energy and Commerce to provide oversight and feedback on risks, gaps, and plans to mitigate their findings. These Executive Orders also addressed the criticality of international cooperation when addressing cybersecurity and responding to malicious cyber events and actions. Understanding that the threat of malicious cyber actors and requisite responses to malicious events are not constrained by borders, many nations have looked to international organizations such as the United Nations to promote cooperation and coordination in this regard. The United Nations' Group of Governmental Experts

[52] United States, Executive Office of the President Barack Obama. Executive Order Number 13636: Improving Critical Infrastructure Cybersecurity. 12 February 2013.
[53] United States, Executive Office of the President Donald Trump. Executive Order Number 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 11 May 2017.

(GGE) and cybersecurity Open-Ended Working Group (OEWG), which helped to formulate a path to the establishment of voluntary normative behavior within the cyber domain in 2021, can be viewed as Executive Orders 13636 and 13800 having moved the United States and subsequently their partners in a positive direction regarding security within the cyber domain.[54]

In 2021, Executive Order 14028- Improving the Nation's Cybersecurity, sought to continue to progress in improving the security of critical infrastructure from malicious cyber actors and again sought to incorporate the private sector interagency and academic perspectives into the formulation of a plan for action.[55] In addition to continued and improved information sharing and communication between public and private sectors, this Executive Order sought the establishment of standardized response and reporting procedures for malicious cyber events, coupled with standardized and integrated mechanisms for deterrence and defense of the cyber domain and critical infrastructure. The passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) in March of 2022, is another measure in identifying the need for integration of the public and private sector and takes information sharing a step further with resource and aid allocations from the Cybersecurity and Infrastructure Security Agency to the private sector in the event of a malicious cyber event or activity.[56]

[54]United Nations General Assembly. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report. 10 March 2021.

[55] United States, Executive Office of the President Joseph Biden. Executive Order Number 14028: Improving the Nation's Cybersecurity. 12 May 2021.

[56] Cybersecurity & Infrastructure Security Agency. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). https://www.cisa.gov/circia

The Cybersecurity Solarium Commission's final report in March of 2020 continued with the expansion of vision and focus from the United States' government towards securing the cyber domain. Evidenced by the amount of focus paid to the threat of malicious cyber activities and though process beyond the report, it can be determined that the United States will continue to seek a means of security with a government entity as the focal point or lead proponent of security implementation. The Cybersecurity Solarium Commission focus is on deterrence and leveraging various portions of national power to achieve the desired end state. While the report does discuss public-private integration and information sharing, it remains difficult to facilitate these activities even with the previously mentioned Executive Orders and CIRCIA.

The continuation of seeking improvement of the nation's overall security through the protection of critical infrastructure and cyber-related activities, as evidenced in the Executive Orders and integration with international partners and organizations, demonstrates a collective understanding that this problem cannot be managed by the Federal Government alone. These examples also demonstrate a preference to focus on defense through an integrated and multifaceted structure, seeking to prevent attacks or malicious events through improved security postures and mechanisms; adaptation stemming from shared knowledge and experiences; and interoperability and standardization of responsive processes.[57] Attribution and enforcement of cyber normative behavior are part of the process of improving and integrating defensive mechanisms. Still, these factors are not the primary focus as they can potentially spread already limited resources even thinner.

[57] Healey, Jason. The US Cyber Policy Reboot. Atlantic Council, 2012.

Two critical factors regarding the success of these efforts remain the private sector's willingness to participate and the public's trust in the government. These factors have been tested, most recently through the exposure of the Federal Government's actions after the passing of the Patriot Act, having collected data and information on American citizens through partnerships with the private sector. Additional evidence of mistrust between the populous, private sector, and government agencies are outlined in the criticism of the proposed Cyber Intelligence Sharing and Protection Act during the first Obama administration.[58] As the interconnectivity of modern life associated with the Internet of Things (IoT), perceived private sector profiteering, and potential decrease in privacy continues to test the public sector's ability to protect its infrastructure and population, attention must be paid to the delicate balance between public trust and private sector involvement.

II. Private Sector

While it is clear that the public sector seeks to take an integrated approach to managing and defending critical infrastructure within the cyber domain, the private sector does not appear to consistently echo these sentiments. Private sector fears of government overreach or top-down regulations restricting freedom of movement are at the center of debate for public-private integration within the cyber domain. These fears have led to multiple stances regarding security within the cyber domain from the private sector perspective. Some view security of critical infrastructure to be the sole responsibility of

[58] Paoletta, Patricia. "The Cybersecurity Overreach: A Few Harsh Words about the President's Cybersecurity Executive Order, along with a Better Solution." The Federalist Society, February 28, 2014.

the government, viewing their access to potentially classified mechanisms and international partnerships as solvent enough to maintain security for all. Others wish to maintain and enforce security within the cyber domain through internal and independent private sector endeavors, maintaining freedom from government regulation and the ability to adapt to evolving threats quickly. Lastly, there are those who see merit in collaborative efforts with the public sector focusing on information sharing, collective adaptation, and defense in depth. The main attributes influencing these stances are the various priorities within the private sector. The delicate balance between focusing on profit, protection of proprietary data and mechanisms, and protecting critical infrastructure and the populous, coupled with anxious feelings about excessive government influence and regulation, are driving factors.

Those who view security within the cyber domain as a purely governmental endeavor do so mainly within the context that the private sector should not be burdened with protecting critical infrastructure that does not relate to their stated mission or objectives. Resource constraints are a driving factor for both sides in this debate as private entities may not have the requisite personnel or capabilities to facilitate these endeavors, and the public sector would likely be spread too thin or miss critical events if required to focus on the problem set alone.[59]

A focus on profit and protection of proprietary data and mechanisms are often mutually linked in private sector lexicon. For this reason, many private sector entities do not wish to participate in public-private integration regarding security in the cyber

[59] Grant, Vaughan. "Critical Infrastructure Public-Private Partnerships: When Is the Responsibility for Leadership Exchanged?" Security Challenges, vol. 14, no. 1, 2018, pp. 40–52.

domain. Should a private entity develop a mechanism to increase security within the cyber domain, to include critical infrastructure and information technologies, it would be in the best interest of profit to retain that proprietary mechanism and market it, vice freely sharing with the public sector and other private entities. Additionally, suppose a private entity is required to disclose a malicious cyber event or activity against them through integrated public-private information sharing and communication. In that case, it may have a negative impact on profit and shareholders. Some within the private sector also see themselves as being more adaptable without the constraints of public sector involvement. Government bureaucracy is another issue that causes hesitation from the private sector. In addition to the often slow-moving processes of government affairs, legality factors into a critical role. The United States government must abide by the rule of law when implementing defensive measures within the cyber domain, and the process of offensive cyber measures appears to be even more regulated through several layers of checks and approvals. However, private corporations may be able to avoid certain aspects of United States law by having divisions or subsidiaries located outside of the United States that operate within the cyber domain on the entity's behalf. While this opens up a litany of ethical and legal questions, it does factor into the security calculus for some private sector entities.[60]

Others desire a holistic and integrated approach to security within the cyber domain within the private sector. Those with this mindset often see the resource constraints on both sides, the potentially limited scope of expertise, and the stove-piping

[60] Hoffman, Wyatt, and Ariel E. Levite. "THE CASE FOR PRIVATE SECTOR ACTIVE CYBER DEFENSE." PRIVATE SECTOR CYBER DEFENSE: Can Active Measures Help Stabilize Cyberspace?, Carnegie Endowment for International Peace, 2017, pp. 13–18.

of information as critical gaps that an integrated approach has the potential to overcome. These concerns often mirror those of the public sector, and efforts to adopt this approach can be seen through the support given to previous legislation, such as the Cybersecurity Information Sharing Act and the Cyber Intelligence Sharing and Protection Act.[61] Though this legislation was unsuccessful, due in large part to concerns about previous legislation, such as the Patriot Act, it demonstrated the presence of an appetite for continued public-private sector integrated defense, information sharing, and communication.

There is another component to these debates regarding public-private integration, that being the role of the general public. Often the government and private entities view their role as one to protect or capitalize upon the vulnerabilities of the general public. However, the general public, specifically within the United States, has a voice in this relationship, often demonstrating an aversion to government influence within the cyber domain. After the data collection scandal associated with the Patriot Act focusing on AT&T, the general public has become increasingly weary of the government and does not view increased influence within the cyber domain as an altruistic endeavor on the part of the government. This leaves portions of the government, such as the House and Senate, as direct representatives of the populous, in a potentially precarious position. Understanding the severity of the threat posed to critical infrastructure and to the population themselves is critical in convincing the public of the benefits of an integrated approach enabling defense in depth. The general public can also play an important role

[61] Tsukayama, Hayley. "Cispa: Who's for It, Who's against It and How It Could Affect You." The Washington Post. WP Company, April 27, 2012.

in the active defense of the cyber domain through programs such as bug bounties, a form of crowdsourcing and data mining for private entities in which the general public is financially rewarded for identifying zero-day vulnerabilities. A zero-day vulnerability is one that is unknown to the system or owner and, as such, can be exploited for malicious intent.[62] These efforts enable the private entity the opportunity to correct or mitigate them before a malicious action can occur, potentially saving them from financial or data losses. Bug bounty programs are an effective means of public-private integration for increasing security within the cyber domain that precludes direct government involvement.

The private has additional means of sharing and integrating with the public sector in the form of lessons learned. Zero-Trust Architecture (ZTA) is a solid example of innovation within the private sector matriculating its way into the government. ZAT is method of security within the cyber domain that forces a user to be authenticated or validated for each action or layer of access. This method differs from traditional security methods in that it continues to seek authentication during a user's time within a system instead of only for initial entry.[63] The Department of Defense as instituted the ZTA method recently and should the impacts on security should be monitored and disseminated. It makes sense for government agencies to adopt methods such as ZTA to improve security, as they are tapping into not only proofed ideas and mechanisms but

[62] Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. "Zero-Day Vulnerabilities in the Black and Gray Markets." In Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, 25–28. RAND Corporation, 2014.

[63] Odell, Laura A., Brendan T. Farrar-Foley, J. Corbin Fauntleroy, and Ryan R. Wagner. "Zero Trust: An Alternative Network Security Model." *In-Use and Emerging Disruptive Technology Trends*. Institute for Defense Analyses, 2015.

also determining interoperability with the private sector. Interoperability will be an important portion of any integrated efforts between the public and private sectors as it goes beyond information sharing and demonstrates the ability for mechanisms and systems to work in concert with limited friction.

III. Taking the Lead

There is no surprise that the dynamic between the public and private sectors regarding the cyber domain is rapidly and constantly evolving. Efforts, even integrated ones, towards securing the networks and infrastructure can appear disjointed and lacking unity of effort. This disjointedness can lead to significant inefficiencies and is a foundational reason for establishing an entity to take the lead in integrating the public and private sectors cyber security efforts. This leader should facilitate integrated efforts and act more in the capacity of organization and synchronization then a subject matter expert or implementer. While there should not necessarily be a prerequisite to be a subject matter expert, this entity should have foundational knowledge of the problem at hand, access to information and resources across multiple domains and agencies, and have the ability to enforce plans and facilitate follow through. The collaborative efforts between the public and private sector must extend beyond information sharing, and be inclusive of integrated defensive measures. For this reason, private entities must have some form of access to classified information or networks and the public sector must have a similar access to private entity information and networks. Additionally, these collaborative and sharing efforts must extend beyond regional or national boundaries to be the most effective. For these reasons it makes the most sense for a governmental entity to fill the leading role in the integration of public-private sector efforts to secure the cyber domain.

Focusing on the United States, the Executive Orders released by the past several Presidential administrations along with the CIRCIA and Cybersecurity Solarium Commission report, have attempted to focus integrated efforts regarding securing the cyber domain with a government agency as the lead. The agency identified through these Executive Orders has been the Department of Homeland Security (DHS), which makes sense from a governmental perceptive as many of the DHS's tasks are focused on securing the nation's critical infrastructure. While the DHS may be the best government agency suited to lead public-private integration of cyber defense as it has experience in collaborative public-private efforts during times of crisis, it still has hurdles that must be overcome for success given the private sector's overwhelming ownership of critical infrastructure. While the United States is not unique in this hurdle, nations without nationalized critical infrastructure face additional challenges in integration of the public and private sector cyber defense. The creation of the DHS Cybersecurity and Infrastructure Security Agency (CISA) is a step in the right direction of integrating efforts and having a focused governmental agency taking lead on securing the cyber domain. Additionally, the establishment of the Office of the National Cyber Director and the Deputy National Security Adviser for Cyber and Emerging Technologies under the Biden administration has re-enforced the federal government's role in managing and securing the cyber domain and protecting critical infrastructure.[64]

[64] "Cybersecurity: Kick-Starting the Officer of the National Cyber Director." United States Government Accountability Office. September 2022. https://www.gao.gov/assets/gao-22-105502.pdf.

Regardless of the entity responsible to assume the lead role, identifying the focus of this leadership position beyond integration and information sharing is critical to its success. Current endeavors and role players within the federal government may not be sufficient enough to secure the cyber domain and protect critical infrastructure, as they focus on responsive actions and are less prone to proactive measures of defense.[65] Expansion of integration into proactive measures is worth examining, but a determination must be made between offensive and defensive cyber mechanisms and their relationship to securing the cyber domain. This research does not explore offensive cyber, but an understanding of its role in deterrence and defense is inherent in the entire discussion of securing the cyber domain.

IV. Impacts of Malicious Cyber Events

The proliferation of asymmetric warfare and the increasing role of non-state actors within international affairs is mirrored in the evolving debate surrounding security within the cyber domain. This evolution is present in the dynamic nature surrounding threats and malicious activity within the cyber domain.[66] Two of the main focuses of threats are high-profile malicious events and what can be classified as cybercrime. While cybercrime is an exponentially growing threat within the cyber domain with potentially significant impacts on global security and international cooperation, the focus of this

[65] Schrier, Rob. "A Case for Action: Changing the Focus of National Cyber Defense." *The Cyber Defense Review* 4, no. 2 (2019): 23–28.

[66] While Ben Buchanan's "The Hacker and the State" provides valuable insight into the evolution of the relationships between intelligence agencies, states, and malicious actors within the cyber domain, it focus on offensive cyber and disruptive efforts were not points of focus for this research.

discussion will be on the link between high-profile malicious cyber events and perpetrators of cybercrimes, specifically the roles and linkage of state and non-state actors within the cyber domain.

As previously discussed, many within the private sector are hesitant or outright resistant to government inclusion in managing and defending within the cyber domain. This obstinance is potentially derived from the viewpoint that current cybercrime methods do not break their threshold for heightened concern. That is to say, they view government influence within the cyber domain as a more severe consequence than a certain level of loss in capital gains, data, or proprietary information. This would make it appear that the current level of data breaches, cyber intrusions, and other cybercrimes are not causing enough issues to make some within the private sector alter their mentality. However, the trajectory of current cybercrimes and associated malicious actions has drastically increased over the past decade and even more so since 2020.[67]

The impacts of malicious cyber activities span political and economic considerations. Politically, state-to-state relations can be severally impacted should a malicious cyber event be attributed to a known state actor. Even more precarious is the role of state-sponsored actors and state-influenced non-state actors in these relationships. With many of the high-profile malicious cyber events, attribution to the suspected perpetrator significantly impacted relations between the victim and the alleged perpetrator. Russia's actions in the Moonlight Maze event and China's growing cyber espionage agenda, and the resulting actions of the United States, are examples of how

[67] Peters, Allison, and Anisha Hindocha. "US Global Cybercrime Cooperation: A Brief Explainer." Third Way, 2020.

state relations can be strained or significantly degraded as a result of malicious cyber events and activities. In these instances, sanctions were the response of choice and more nations have given credence to them as appropriate responses to malicious cyber activity by state actors.[68] The effects of sanctions are felt on a political level, but often more importantly they seek to have economic effects.

Economically, malicious cyber activities can have varying impacts depending upon the target and type of event. Private sector entities may be able to recuperate and adapt after a malicious cyber event, but there will most likely still be economic ramifications in the near and long term. In the near term, immediate profit loss is factored in, along with public perception and potential loss of credibility. Long-term impacts can range from peer competitors gaining a competitive advantage to loss of client bases and partnerships, resulting in varying forms of economic losses. Within the public sector, similar events can result in the degradation of military advantages or capabilities, increased risk to forces, and loss of trust and confidence.

Collective defense must also be factored into the repercussions of malicious cyber activity as the cyber domain becomes recognized as a military operational domain.[69] How do malicious actions within the cyber domain factor into a nation or collective organization's calculus in supporting or defending allies or member nations? If malicious actions within the cyber domain are truly to be taken in the same vein as those in the physical domain, these entities would be required to collectively respond through military, diplomatic, or economic means. Where does the threshold lie for nations

[68] Peters, Allison, and Pierce MacConaghy. Unpacking US Cyber Sanctions. Third Way, 2021.

[69] Ilves, Toomas Hendrik. "The Consequences of Cyber Attacks." *Journal of International Affairs* 70, no. 1 (2016): 175–81.

belonging to collective organizations, such as the North Atlantic Treaty Organization (NATO), to be required to respond? These frameworks for collective response are continuing to be developed as the evolution of cyber domain defense matures, but intermediate efforts must be in line with those similar to the dynamics established for the physical domain. A hybrid approach of establishing a framework for collective defense for response to malicious activity within the cyber domain appears to be the most reasonable. Hybrid meaning approaching responses as they would to both military actions and criminal endeavors, as many collective organizations currently focus on cybercrime in their defensive efforts.[70] Establishing the mechanisms for support to the victim nation or entity, identification of vulnerabilities exploited, and mitigation of similar activities in the future would be enabled by a multi-faceted defensive approach while remaining in the legal domain of defensive cyber activities and responses.

This hybrid multi-faceted approach would still marginalize the necessity for attribution as many of these cases, such as the Colonial Pipeline incident and Estonia 2007, the perpetrator is known yet this fact brings little reprieve to the victim. However, attribution does enable execution of follow-on actions for the collective organization to pursue economic, diplomatic, or other means of enforcement or reprisal. The normality of response to malicious actions occurring within the cyber domain transcending into the physical domain appears to growing, even if only from a willingness to pursue alleged

[70] ILVES, LUUKAS K., TIMOTHY J. EVANS, FRANK J. CILLUFFO, and ALEC A. NADEAU. "European Union and NATO Global Cybersecurity Challenges: A Way Forward." *PRISM* 6, no. 2 (2016): 126–41.

criminal activity to prosecution. This highlights to importance and interconnectedness of the cyber domain into all facets of international relations and statecraft.[71]

V. Conclusion

Through all of the discussions on integrated defense, isolated response, and the rising threat of malicious activities within the cyber domain, it remains constant that while attribution of the malicious actor and enforcement of cyber norms play enhancing roles within the defense of the cyber domain, they do not play a critical role. Limitations on capability and capacity regarding security within the cyber domain regardless of sector or nation are significant factors in the necessity to focus on a multi-faceted defensive approach. Understanding the current limitations on resource availability relating to cybersecurity, focus should be paid to a defense in depth and adaptation as they appear to provide a greater cost to risk ratio in defending the cyber domain.

Many of the state and state-sponsored malicious cyber actors are known to the international community, yet the ability to attribute malicious actions to these actors does not significantly improve security within the cyber domain. International and multinational legal frameworks are not currently equipped to provide the level of punitive measures necessary to deter or dissuade malicious cyber activities. Due to this discrepancy attribution will not play critical role in securing the cyber domain. This is

[71] Maness, Ryan C., and Brandon Valeriano. “The Impact of Cyber Conflict on International Interactions.” *Armed Forces & Society* 42, no. 2 (2016): 301–23.

not to say that nation-states or private sector entities should not factor attribution into their defensive mechanisms. While not playing a critical role in increasing overall security within the cyber domain, attribution does factor in considerable when discussing international relations and nation state response to cyber activity. In order for nation-states to engage with peers and competitors on corrective, legal, or other punitive measures they must have the ability to identify and attribute malicious actors within the cyber domain. Continuing to improve the ability to attribute malicious events to actors within the cyber domain with increased certainty will enable the nascent legal efforts as they mature.

Additionally, efforts to enforce cyber norms lack the bite of other punitive or legal methods in other domains, and have proven inadequate in deterrence as well. Legal frameworks are working to adapt to the demands and actions of the cyber domain, but are restricted in efficiency due to disjointed efforts and the trans-border nature of the cyber domain. It will likely become increasingly more difficult to bring punitive measures against non-state entities conducting malicious actions within the cyber domain while operating out of certain nation-states. Without structured agreements or enforceable legal frameworks, nation-states must rely upon political relationships to solve the evolving problem of malicious activity within the cyber domain. Even with the implementation of political and economic efforts such as sanctions, there does not appear to be enough backing to change the habitual malicious cyber actors' behaviors.

Nation-states and private sector entities should focus on a multifaceted approach to cyber defense and securing the cyber domain. Maintaining active defensive mechanisms, identifying gaps and vulnerabilities, and enacting mitigation efforts play more critical roles in the over security apparatus of the cyber domain. These efforts are not entirely responsive or reactionary in nature, but should not move so far left of the event to be misconstrued as offensive in nature. Transparency and public-private sector integration are important to these defensive measures due to the previous mentioned resource limitations. Adaptability and speed in correcting identified vulnerabilities or exploitations will provide more substantial deterrence than attribution or enforcing cyber norms as it creates more difficulty for malicious actors in the near term, which may be enough to dissuade some malicious actors.

The speed at which the cyber domain operates and evolves will outpace the ability for attribution to have significant impacts on security. Efforts to attribute malicious actors within the cyber domain may prove fruitful, but will most likely be at the cost of other defensive measures in a perpetually resourced constrained environment. While many nation-states and private sector entities are devoting more effort and resources to operations within the cyber domain, the one resource constraint that appears to be the most difficult to overcome is time. Adaptability and flexibility can mitigate the factors associated with time constraints, but they will most likely never be able to keep pace with the evolution of the cyber domain itself in real time.

Conclusion:

In the first chapter, this thesis identified the shared interest of nation-states to establish cyber norms as a means to enhance security within the cyber domain. Concurrently, these nation-states sought to focus on attribution of malicious cyber activities, linking these malicious actors as non-compliant to the cyber norms established by the United Nations Open-Ended Working Group. This chapter highlighted the issues surrounding implementing cyber norms for state actors and identified the compounding factors related to non-state actors. Many of the cyber norms can be viewed by nation-states as self-regulatory, meaning they must hold themselves accountable as well as those within their borders. While other nation-states or unified entities such as the United Nations can attempt to regulate nation-state deviation from cyber normative behavior through sanctions or potentially threats within the physical domain, they often lack the ability to attribute the malicious action or deviation from cyber norms to the nation-state. Non-state actors play a significant role in the inability to enforce cyber norms on nation-states, as they can act as a scapegoat with the nation-state blaming a non-state entity that is non-attributable. Regardless of whether these non-state entities are state-sponsored, state-influenced, or independent actors, the unwillingness or inability to enforce punitive measures upon those either deviating from norms or conducting malicious actions within the cyber domain is a significant hurdle to overcome. Even with this hurdle identified, the security of the cyber domain has not appeared to deteriorate significantly.

The second chapter of this thesis focused on state actors' defensive strategies for securing the cyber domain by analyzing two schools of thought. One focusing on attribution as the key to successful security, and the other focusing on a more multi-faceted approach to defensive measures. Key aspects of this chapter also focused on responses to high-profile malicious cyber events and peer nation-state competition in the cyber domain. These high-profile malicious cyber events were chosen as they were perpetrated against nation-states, allegedly by other nation-states. The nation-states chosen for examination in the peer competition were done so because of their proclivity for behavior that can be classified as either deviating from normative behavior or outright malicious behavior within the cyber domain. These studies highlight the issues of enforcement discussed in the first chapter of this thesis but also downplay the role attribution plays in securing the cyber domain. The nation-states identified in the peer competition spaces are known violators of deviating from normative behavior or perpetrators of malicious activities within the cyber domain. Yet, the behavior is often unchanged after attribution or attempts at enforcing adherence to norms. It is not to say that attribution of malicious cyber activity has no role in securing the cyber domain, but rather that it is enhancing vice essential or critical.

The third chapter of this thesis focuses on the roles of the public and private sectors in securing the cyber domain. Through examination of how each perceives their roles as well as the other sectors, the influence of national policy specific to the United States, and the impacts of malicious cyber events on the economy and political relationships, it can be reasoned that integration of the public and private sector regarding securing the cyber domain is in the best interest of all parties. Neither sector currently has the resources or influence necessary to protect critical infrastructure and secure the cyber domain alone. While this integration will require compromise from both sectors, potentially more so from the private sector, it will enable a more robust and enforceable security apparatus to protect the cyber domain.

The establishment of cyber norms is a good start and an important step in increasing security within the cyber domain. However, the limited ability of nation-states to enforce these cyber norms or bring substantial punitive measures against those who deviate from them diminishes the criticality of their role in security within the cyber domain. The lack of shared legal and political frameworks between even the members of the United Nations regarding the cyber domain prevents the enforcement of cyber norms and diminishes the responsiveness of the international community to malicious cyber events. Similarly, the lack of corrective behavior brought on or enabled by attribution of malicious cyber activity has limited the role of attribution in the overall defense of the cyber domain. It is evident that attribution alone does not increase security within the cyber domain, but its importance to the overall security mechanisms is often marred the ambiguity it must overcome. Though technical means to track and identify sources of malicious cyber activity have continued to increase, they still often lack the ability to prove beyond reasonable doubt that the identified actor did in fact conduct the malicious act. The ambiguity of the cyber domain is a leading factor in this difficulty. Capabilities such as virtual private networks (VPNs), Tor Browsers, and a litany of other tunneling applications and programs enable entities to maintain a degree of standoff from the action, the actor, or both and can cast doubt on the certainty of attribution. Additionally, the legal framework of many nation-states may not be willing to support the pursuit of malicious entities due to the ambiguity associated with absolute certainty of attribution. Political means may be better suited to support claims of attribution to enable justice or other punitive measures, but again the general ambiguity of the cyber domain may prevent nation-states from attempting to pursue malicious actors for fear of losing face in the international community.[72] The examples of the Moonlight Maze, Russia's actions against Estonia in 2007, and China known state-sponsored cyber espionage are premier in demonstrating the ineffectiveness of attribution and the limitations of attempting to enforce cyber normative behavior within the cyber domain. All of these examples have a known nation-state perpetrator conducting malicious cyber activities and the majority of the reprisals have been political and economic sanctions that had little impact on dissuading or preventing malicious behavior.

While both the establishment of cyber norms and the ability to attribute malicious actions within the cyber domain have their roles in securing the cyber domain, they are not critical roles or capabilities. Instead, the recommended best practice is a more robust defense in depth within the cyber domain. Actively identifying vulnerabilities, mitigating these vulnerabilities, responding to exploited vulnerabilities, and mitigating exploited vulnerabilities should be the priority efforts for security within the cyber domain. This recommendation is founded on understanding resource limitations from the private and public sectors regardless of integration. Attribution of malicious cyber events continues to be a resource-laden endeavor that can potentially divert time and effort away from the previously mentioned priority efforts.

[72] Johnson, Durward E., and Michael N. Schmitt. "Responding to Proxy Cyber Operations Under International Law." *The Cyber Defense Review* 6, no. 4 (2021): 15–34.

Additionally, the efforts to protect the cyber domain through a multi-faceted approach cannot be conducted in isolation. The public and private sectors must work in concert to protect critical infrastructure and influence behaviors that cross both borders and domains. Detailed and in-depth integration between the two sectors is recommended to provide a more deliberate, resource-appropriate, and dynamic approach to security within the cyber domain.

Since the release of its initial report, the Cyberspace Solarium Commission has proposed over one hundred policy and legislative recommendations to bolster the United States ability to secure the cyber domain. The Commission was tasked with answering two questions regarding cybersecurity: "What strategic approach will defend the United States against cyberattacks of significant consequences? And what policies and legislation are required to implement that strategy?"[73] The results of the Commission's findings focus on multi-layered deterrence of malicious cyber activity, specifically into three layers. The layers are described as "Shaping Behavior," "Denying Benefits," and "Impose Cost". Shaping behavior is framed as working with allies to promote normative behavior within the cyber domain. Denying benefits is enemy or advisory focused, ensuring the United States is not taken advantage of or exploited within the cyber domain. Impose cost focuses on ensuring the United States has the ability to retaliate for malicious actions.[74] These layers, aimed at deterrence can be summarized as establishing and enforcing normative behavior, defense in depth, and potentially some form of defend forward or offensive cyber.

[73] US Cyberspace Solarium Commission. Official Report. March 2020
[74] Ibid.

The Cyber Solarium Commission also suggested the creation of several positions within the Executive branch, to include the Office of the National Cyber Director, along with Congressional oversight and a push for private sector integration. In the case of the cyber domain, more agencies are not necessarily better as competition for personnel, funding, and other resources are already limited. The last two administrations have enabled efforts at bolstering the United States focus on cybersecurity, critical infrastructure, and actions within the cyber domain, but to what end? It appears that the United States may be looking at defense of the cyber domain in too similar of a light as they would conventional military operations. This can be problematic and if it were to viewed in a similar light it should be one that resembles asymmetric conflicts.

The cyber domain has created an asymmetric conflict space that shares similarities to previous conflicts associated with the Global War on Terror. In these conflicts, terrorist sought means of leveling the battlespace and mitigating Coalition forces significant military and resource advantages. These terrorists' efforts focused on improvised weapons such as Improvised Explosive Devices (IEDs) within a resource constrained environment to create standoff while continuing to inflict damage and instill fear in combatants and the civilian populace. Actions such as these forced Coalition forces to improve security by adding additional armor to vehicles and personnel. These efforts to improve security, while effective, created a larger, slower, more resource demanding force within increased survivability. Similarly, within the cyber domain, malicious actors continue to exploit the asymmetric nature of cyberspace. The very nature of the cyber domain enables all users similar availability to resources as long as capability is present with the user. Even more so in the cyber domain than in other conflict spaces, speed, agility, and resourcefulness are critical components to achieving success in any aspect of operations, malicious or otherwise. A more applicable example of conflict within the physical domain relating to the cyber domain would be the Vietnam War, specifically the actions of the Viet Cong against United States and South Vietnam forces. The Viet Cong, like malicious actors within the cyber domain, are light and agile, possessing superior knowledge of the terrain, defenses, and opposition reactions to contact. The United States, in both scenarios, appears to be a goliath incapable of being significantly impacted by advisories with few resources and underestimating their capabilities and capacity. In both scenarios the ability to act and adapt with significant speed determines the victor. Adding bureaucracy to cyber security will potentially have the same negative results as adding armor to ground forces in the Global War on Terror or massing troops in Vietnam. Creating a larger footprint with more channels will slow responsiveness to malicious events of all degrees but will not necessarily provide increased survivability or security.

Nation-states should focus on integration between the private and public sectors regarding securing the cyber domain. The roles and responsibilities must be deliberately identified and approached with a mindset of feasibility, supportability, and sustainability. Understanding capabilities and limitations within each sector will enable a comprehensive architecture for security mechanisms. Key to this understanding is the availability of resources and the overlap of national security measures. While one entity may have the resources to protect its own portion of the cyber domain, the nature and the interconnectedness of the cyber domain make this a collective issue. The connection of critical infrastructure across both sectors, multiple domains, and its transborder nature drives the demand for an integrated defensive strategy within the cyber domain.

While nation-states may seek to codify these relationships in writing through law or executive order, there needs to remain a certain level of autonomy and flexibility in these relationships to allow for adaptation on pace with threats within the cyber domain. In this regard, there must be private sector buy-in, as codifying an Act or Law that hampers innovation or detracts from revenue may dissuade private sector entities from providing efficient efforts to the overall security mechanisms.

Within the United States, there has been limited headway made toward integration through Executive Orders, as outlined in the third chapter of this thesis. However, codifying these efforts into law has remained elusive as the support from both the private and public sectors has not materialized collectively. Additionally, there will potentially always be a lingering distrust from public-private sector collaboration regarding security after the Patriot Act, and without another 9/11 level event, there may not be enough support to overcome that distrust from the populace. Thus, it will be incumbent upon key leaders and influencers in each of these sectors to integrate, share, and transcend boundaries that may prevent gaining the most out of the established and evolving security mechanisms.

Additionally, the relationships and dynamics between the federal agencies associated with cyber within the United States must be codified and enforced. Between the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Director, Office of the National Cyber Director, and the Deputy National Security Adviser for Cyber and Emerging Technologies, the relationship for integration with the private sector has continued to grow more convoluted. This complexity will emphasis the need not just for clear command relationships, but clear and effective relationships between commanders and leaders. While all three of these agencies have specific areas of focus, many of their undertakings cross into each other's spheres of influence. Adding to the potential confusion for the private sector is the nascency of these organizations, all having been formed within the past four years and all residing within the Executive branch. While these relationships and associated funding are being worked out within the Federal government, there remains a gap in the ability to facilitate communication between the public and private sectors regarding securing the cyber domain and threat vulnerability.

Attempts to mitigate the gaps in leadership and communication are currently being filled by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and CISA. CIRCIA was signed into law in March of 2022 and requires specified entities to report "cyber incidents and ransomware payments to CISA" so they may collect, analyze, and disseminate information and deploy appropriate resources to aid victims and help secure the cyber domain. It is important to note that the reporting criteria and enforcement are still being formulated with assistance from the private sector and others with a vested interest in protecting critical infrastructure, and currently, all reporting is voluntary.[75]

Considerable thought from the federal government has been made towards education as it relates to cybersecurity over the past two administrations. Educating private sector working professionals, government officials, future personnel, and

[75] Cybersecurity & Infrastructure Security Agency. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). https://www.cisa.gov/circia

everyone in between on the threats, mechanisms, and capabilities is a critical step in increasing overall security within the cyber domain. It is vitally important that at the user level, security mechanisms and threats are understood. The most secure and robust systems in the world can be rendered useless if a user fails to implement the appropriate security mechanisms for the system. If a person does not lock the doors to their homes, what good are having doors? The door may deter some actors, but truly motivated actors will continue to probe and identify the security is lacking.

In addition to educating the general population on cyber threats, educating sourcing the next generation of cyber professionals will be vital to growing the organization currently being constructed. CISA has taken a leading role on this initiative, making a concerted effort to recruit top tier talent and attempting to incentivize the work force comparable to other federal agencies in the intelligence and defense agencies. The need for these types of efforts have also been highlighted in the Cybersecurity Solarium Commission's report, demonstrating the federal government's intentions to grow a well-educated and talented cyber work force. It is worth noting that all of the organizations focused on cyber initiatives will potentially be competing with each other, as well as the private sector, for the same human capital and resources in addition to funding and access.

The federal govern is continuing to seeking means of adapting and learning from private sector lessons. Initial efforts should be made to move towards Zero-Tolerance Architecture (ZTA) in conjunction with multi-faceted defensive mechanisms. While federal departments are currently undertaking these efforts, wider dissemination and application of ZTA will enable increased security in the near term. However, implementation of ZTA will require additional resources specific to infrastructure and maintenance, which may discourage some entities from adopting the method.[76] ZTA differs from traditional security methods in that it continuously checks and verifies users' credentials while it is operating within a system. Traditional security methods usually only validate users upon initial entry into the system and provide unobstructed access within the prescribed system.[77]

Bureaucracy and distrust remain hindrances to efficient collaboration between the public and private sectors in securing the cyber domain. The incentive of resource allocation and aid to victims of malicious cyber activities may entice some private sector entities to participate in these information sharing efforts with CISA voluntarily, and they may not be enough to bring in the major player within the private sector. Additionally, the lack of prescribed funding for some of these newly formed offices and organizations may dissuade participation from the private sector for fear of exposing vulnerabilities or missteps and gaining little in return.

Looking at overarching security impacts, it one can assume that defense extends beyond simply attribution and enforcement of normative behavior within the cyber domain. What should be encompassed within a multi-faceted defense is still being developed, but the Cybersecurity Solarium Commission's recommendations focus primarily on deterrence and utilizing multiple aspects of national power to achieve success. While deterrence and utilizing available aspects of national power are important

[76] Foltz, Kevin E., and William R. Simpson. "Zero Trust Technology Integration Issues." Institute for Defense Analyses, 2021.

[77] Odell, Laura A., Brendan T. Farrar-Foley, J. Corbin Fauntleroy, and Ryan R. Wagner. "Zero Trust: An Alternative Network Security Model." *In-Use and Emerging Disruptive Technology Trends*. Institute for Defense Analyses, 2015.

in the cybersecurity construct, the multi-layered approach recommended by the CSC needs to be expanded to include a defense in depth approach. Deterrence, active defense, attribution, and enforcement can make up a foundation for multi-faceted defense in depth within the cyber domain. Active defense should include some form of red cell, identifying vulnerabilities, mitigating risks, correcting identified vulnerabilities, identifying exploitation efforts or attempts such as leaks, hacks, probes, and compromises, mitigating vulnerabilities, and correcting gaps and vulnerabilities. Red celling a system is utilizing subject matter experts in a specified area of study or capability, and utilizing their expertise and experience to find flaws in a system or thought process. This process is important in securing the cyber domain, as can enable speed and agility with limited resources.

The main limiting feature of this research has been the evolving nature of the cyber domain. Every day there are different threats of varying degrees that security mechanisms must identify, solve, and adapt to maintain the desired security status. While fears of a catastrophic cyber events such as a "Cyber Pearl Harbor" have yet to be realized, this does not discredit this type of event from occurring in the future. This research's primary focus has been securing the cyber domain from current and evolving threats, but not necessarily threats that would cause reaction or retaliation to cross from the cyber to the physical military domain.

Additionally, the private sector's limited willingness to disclose information or impacts regarding cyber security issues or malicious events prevents further analysis of evolving threats and mechanisms to overcome them. This unwillingness to be totally transparent regarding cyber security and actions within the cyber domain is also true of the public sector. Classification of programs associated with the cyber domain such as security mechanisms, reactions, techniques, and procedures are a limiting factor in gaining access to the whole picture, and rightfully so as access to this type of information has potentially damaging impacts to national security if released to the public. Also, the military may not be disclosing issues or impacts for fear of greater threats or exposure of vulnerabilities that may impact national security.

While defense in depth or a multi-facet defense is the recommended method for securing the cyber domain, the impacts of offensive cyber could potentially be an area for continued research. Understanding the ramifications of conducting offensive cyber or establishing offensive cyber means as deterrence would enable a wider understanding of what it would take to secure the cyber domain in the face of evolving threats and state and non-state peer competition. Additionally, further research into nation-states threshold for retaliatory actions from malicious cyber events could potentially enable a more detailed risk analysis into the utilization of state-sponsored or influenced cyber operations. Looking at what nation-states would consider a "Cyber Pearl Harbor" event and their willingness to retaliate through the physical domain may prove helpful and has the potential to uncover similar risk calculus as nuclear deterrence.

The grey zone between offensive and defensive cyber operations is a contributing factor to the ambiguity of nation-states' actions within the cyber domain. If a nation-state perceives their actions as being defensive in nature, they may feel their actions are justified and are not at risk of running afoul any international norms or laws. However, other entities may perceive these same actions as offensive in nature and seek retaliation or some form of justice. Defending forward is an example of this potential grey zone, with a nation-state seeking to prevent a malicious cyber event from occurring by denying the assumed malicious actor the ability to conduct the act. These actions may appear as preventative and defensive in nature, but through disabling, disrupting, or defeating the other entities capability before it is employed is often viewed as offensive in nature. In the physical military domain, there is a clear delineation and definitions of offensive and defensive actions. An example would be the use of air strikes against enemy combatants perceived to be massing against friendly forces. This action can be defined as a defensive strike in order to prevent enemy combatants from harming friendly forces, and depending on the conflict and theater falls under a specific rule of engagement (ROE). Does this hold true within the cyber domain? If the entity conducting the assumed defensive action is doing so while adhering to international cyber norms and preventing non-adherence to those same norms, it could hold true. However, the assumption would require that all entities involved understand the norms, the battle or playing field, and the ramifications of their involvement and actions. Again, the ambiguity of the cyber domain and the limitations of attribution factor into the differences between cyber and other domains. It would be illogical and irresponsible for nation-states to treat the cyber domain as a theater of conflict, and as such must not take the same approach to defense within the cyber domain as they do in the physical domain.

Works Citied

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. "Zero-Day Vulnerabilities in the Black and Gray Markets." In Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, 25–28. RAND Corporation, 2014.

Barrinha, André. "Virtual Neighbors: Russia and the EU in Cyberspace." Insight Turkey 20, no. 3 (2018): 29–42.

Bartlett, Jason, and Megan Ophel. "Sanctions by the Numbers: Spotlight on Cyber Sanctions." Center for a New American Security, 2021.

Bey, Matthew. "Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition." *The Cyber Defense Review* 3, no. 3 (2018): 31-36.

Broad, William, John Markoff, and David Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." The New York Times. January 15, 2011.

Cybersecurity & Infrastructure Security Agency. Critical Infrastructure Sectors. Updated October 29, 2021. https://www.cisa.gov/critical-infrastructure-sectors.

Cybersecurity & Infrastructure Security Agency. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). https://www.cisa.gov/circia

Cyberspace Solarium Commission. March 2020. https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view

Davis, John A., and Charlie Lewis. "Beyond the United Nations Group of Governmental Experts: Norms of Responsible Nation-State Behavior in Cyberspace." The Cyber Defense Review, 2019, 161-68.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007.

Doman, Chris. "The First Cyber Espionage Attacks: How Operation Moonlight Maze made history." Medium, 7 July 2016.

"Domain, N." Merriam-Webster, 2022, www.merriam-webster.com/dictionary/domain.

Foltz, Kevin E., and William R. Simpson. "Zero Trust Technology Integration Issues." Institute for Defense Analyses, 2021.

G7, Foreign Ministers Meeting. “Dinard Declaration on the Cyber Norm Initiative.” Biarritz, France. 6 April 2019.

Goel, Sanjay. "How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race." *Connections (18121098)* 19, no. 1 (Winter 2020): 87–95.

Grant, Vaughan. “Critical Infrastructure Public-Private Partnerships: When Is the Responsibility for Leadership Exchanged?” Security Challenges, vol. 14, no. 1, 2018, pp. 40–52.

Healey, Jason. Beyond Attribution: Seeking National Responsibility for Cyber Attacks. Atlantic Council, 2012.

Healey, Jason. The US Cyber Policy Reboot. Atlantic Council, 2012.

Hoffman, Wyatt, and Ariel E. Levite. “THE CASE FOR PRIVATE SECTOR ACTIVE CYBER DEFENSE.” PRIVATE SECTOR CYBER DEFENSE: Can Active Measures Help Stabilize Cyberspace?, Carnegie Endowment for International Peace, 2017, pp. 13–18.

Hurel, Louise Marie, and Luisa Cruz Lobato (2018) "Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs." Journal of Cyber Policy. 3:1, 61-76.

Hurwitz, Roger. "The Play of States: Norms and Security in Cyberspace." *American Foreign Policy Interests* 36, no. 5 (September 2014): 322–31.
Iasiello, Emilio. "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities." Journal of Strategic Security 9, no. 2 (2016): 45-69.

Iasiello, Emilio. “China Arctic Cyber Espionage.” The Cyber Defense Review 6, no. 3 (2021): 121–28.

Iasiello, Emilio. "China’s Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities." Journal of Strategic Security 9, no. 2 (2016): 45-69.

Iasiello, Emilio. "What Happens If Cyber Norms Are Agreed To?" *Georgetown Journal of International Affairs* 17, no. 3 (2016): 30-37.

Ilves, luukas K., timothy J. Evans, Frank J. Cilluffo, and Alec A. Nadeau. “European Union and NATO Global Cybersecurity Challenges: A Way Forward.” *PRISM* 6, no. 2 (2016): 126–41.

Ilves, Toomas Hendrik. “The Consequences of Cyber Attacks.” *Journal of International Affairs* 70, no. 1 (2016): 175–81.

Johnson, Durward E., and Michael N. Schmitt. “Responding to Proxy Cyber Operations Under International Law.” The Cyber Defense Review 6, no. 4 (2021): 15–34.

Kaminski, Mariusz Antoni. "Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the developments of Iran's nuclear programme." Security and Defence Quarterly Volume 29 (February 2020): 64-71.

Kelly, Michael B. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought", Business Insider, November 20, 2013.
Kerr, Paul, John Rollins, and Catherine Theohary, "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability," Congressional Research Service, December 9, 2010, 6-8.

Kerr, Paul, John Rollins, and Catherine Theohary. "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability." Congressional Research Service. December 9, 2010, 6-8.

Kissinger, Henry. 2014. World Order. New York: Penguin Press.

Kolton, Michael. "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence." The Cyber Defense Review 2, no. 1 (2017): 119–54.

Kostadinov, Dimitar. "Estonia: To Blackout an Entire Country - Parts 1. " InfoSec Institute. October 8, 2013.

Maness, Ryan C., and Brandon Valeriano. "The Impact of Cyber Conflict on International Interactions." *Armed Forces & Society* 42, no. 2 (2016): 301–23.

Mazanec, Brian M. "Constraining Norms for Cyber Warfare Are Unlikely." Georgetown Journal of International Affairs 17, no. 3 (2016): 100-09.

McGhee, James E. "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy." Journal of Law & Cyber Warfare, vol. 2, no. 1, 2013, pp. 64–103.

McKune, Sarah, and Ahmed Shazeda. "The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda." *International Journal of Communication (19328036)* 12 (January 2018): 3835–55.

Mejia, Eric F. "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework." Strategic Studies Quarterly 8, no. 1 (2014): 114–32.

Moret, Erica, and Patryk Pawlak. The EU Cyber Diplomacy Toolbox: towards a Cyber Sanctions Regime? European Union Institute for Security Studies (EUISS), 2017.

Mueller, Milton, Karl Grindal, Brenden Kuerbis, and Farzaneh Badiei. "Cyber Attribution: Can a New Institution Achieve Transnational Credibility?" The Cyber Defense Review 4, no. 1 (2019): 107-22.

Mussington, David, and Stephanie MacLellan. "US Cyber Policy: Sources of and Impediments to Rapid Progress." Edited by Christian Leuprecht. *Governing Cyber*

Security in Canada, Australia and the United States. Centre for International Governance Innovation, 2018.

Odell, Laura A., Brendan T. Farrar-Foley, J. Corbin Fauntleroy, and Ryan R. Wagner. “Zero Trust: An Alternative Network Security Model.” *In-Use and Emerging Disruptive Technology Trends*. Institute for Defense Analyses, 2015.

Ornes, Stephen. "The Internet of Things and the Explosion of Interconnectivity." Proceedings of the National Academy of Sciences of the United States of America 113, no. 40 (2016): 11059–60.

Paoletta, Patricia. “The Cybersecurity Overreach: A Few Harsh Words about the President's Cybersecurity Executive Order, along with a Better Solution.” The Federalist Society, February 28, 2014.

Peters, Allison, and Anisha Hindocha. “US Global Cybercrime Cooperation: A Brief Explainer.” Third Way, 2020.

Peters, Allison, and Pierce MacConaghy. “Unpacking US Cyber Sanctions.” Third Way, 2021.

Raymond, Mark. "Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot." Strategic Studies Quarterly 10, no. 4 (2016): 123-49.

Schrier, Rob. “A Case for Action: Changing the Focus of National Cyber Defense.” *The Cyber Defense Review* 4, no. 2 (2019): 23–28

Shad, Dr. Muhammad Riaz. “Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions.” Policy Perspectives 15, no. 2 (2018): 41–55.

Shires, James, and Max Smeets. “ARPANET: WHERE DID IT ALL START AGAIN?” CONTESTING “CYBER.” New America, 2017.

Steffens, Timo. Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage. 1st ed. 2020. Berlin, Heidelberg: Springer Berlin Heidelberg, 2020.

Sulmeyer, Michael, Jon B. Alterman, Michael Connell, Michael Eisenstadt, Farideh Farhi, Thomas Karako, J. Matthew McInnis, Hijab Shah, and Ian Williams. “Cyberspace: A Growing Domain for Iranian Disruption.” Edited by Kathleen H. Hicks and Melissa G. Dalton. Deterring Iran after the Nuclear Deal. Center for Strategic and International Studies (CSIS), 2017.

Tsukayama, Hayley. “Cispa: Who's for It, Who's against It and How It Could Affect You.” The Washington Post. WP Company, April 27, 2012.

United Nations. General Assembly. Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations General Assembly Conference Room Paper. 10 March 2021.

United Nations General Assembly. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report. 10 March 2021.

"United Nations: Security Council Resolution on Security Assurances for Parties to the Treaty on the Non-Proliferation of Nuclear Weapons." International Legal Materials 7, no. 4 (1968): 895-96.

United States Cyberspace Solarium Commission. Official Report. March 2020.

United States. Department of Commerce, National Institute of Standards and Technology, Computer Security Resource Center Glossary. "Malicious Cyber Activity." https://csrc.nist.gov/glossary/term/malicious_cyber_activity

United States. Department of Defense. Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms. Department of Defense. 8 November 2010 (as amended through 15 February 2016).

United States, Executive Office of the President Barack Obama. Executive Order Number 13636: Improving Critical Infrastructure Cybersecurity. 12 February 2013.

United States, Executive Office of the President Donald Trump. Executive Order Number 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 11 May 2017.

United States, Executive Office of the President Joseph Biden. Executive Order Number 14028: Improving the Nation’s Cybersecurity. 12 May 2021.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", Wired, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet.