DÜZCE UNIVERSITY | FACULTY OF AKÇAKOCA BEY POLITICAL SCIENCES

JEP
Journal of Economics and Political Sciences

Araştırma Makalesi ● Research Article

Trust Amidst Threats: A Defender's Approach to Navigating the Cybersecurity Dilemma

Juma Mdimu RUGINA *

PhD Student, Social Sciences University of Ankara, Institute of Social Sciences, Political Science and International Relations, Ankara, Turkey. ORCID: 0009-0008-5435-998X

ARTICLE INFO

Article History:
Received: 02.12.2023
Accepted: 21.12.2023

Keywords: Cybersecurity, Digital Networks, Defenders' Perspective, Cybersecurity Dilemma

ABSTRACT

This paper is based on the defenders' perspective on a crucial point often overlooked in cybersecurity: not every cyber intrusion is meant for attacking purposes. Some intrusions are truly defensive, providing justifications for a nation to protect its networks. The paper aims to reveal the strategies, challenges, and subtleties defenders use to build trust among nations while defending their digital networks against cyber threats. It discusses the enduring nature of defenders' creativity, skilled adversaries, the obstacles presented when gathering useful threat intelligence, and the importance of having capable network architecture and defenders. The main argument is that achieving maximum network security sometimes requires intruding into other nation's networks, especially for advanced defenders like well-funded intelligence agencies. Top-tier defenders enhance their cybersecurity by infiltrating the digital networks of potential adversaries and the networks of targets for those adversaries. Through these intrusions, they acquire valuable information that may be inaccessible through other means. Therefore, conducting network intrusions becomes exceptionally beneficial for advancing a state's cybersecurity posture.

1. Introduction

International hacking incidents, marked by their increasing frequency and sophistication, have pushed Cybersecurity to the forefront of global concern. Particularly in an era defined by exceptional technological advancement and interconnectedness, the digital domain has become a theater of rising intrigue and complexity. As nations compete for dominance and security in Cyberspace, a complicated tension unfolds-one that encapsulates the delicate balance between fostering trust among nations and safeguarding against the persistent onslaught of cyber threats (Val Sánchez & Akyesilmen, 2021). This tension lies at the heart of the cybersecurity dilemma term that encapsulates the complex interplay between the ever-present necessity to secure digital assets against cyber-attacks and the imperative to build and maintain trust.

The cybersecurity dilemma demonstrates the intricate tension between the pursuit of trust and the imperative of safeguarding against cyber threats. The pursuit of trust requires transparency, open communication, and collaboration while the defense against threats demands secrecy, vigilance, and

* Sorumlu yazar / Corresponding Author.
e-posta: jumamdimu@gmail.com
Atıf: Rugina, J. M. (2023). Trust Amidst Threats: A Defender's Approach to Navigating the Cybersecurity Dilemma, *Journal of Economics and Political Sciences*, 3 (2), 78-92.

protection of critical assets (Kesan & Hayes, 2014). This puzzle has profound implications for international relations, as the digital realm transcends geographical borders and challenges traditional norms of conflict and cooperation (Liaropoulos, 2016). Scholars have noted that the cybersecurity dilemma not only has direct consequences for national security but also forms diplomatic discourse and bilateral relations. Understanding how nations circumnavigate this dilemma is critical in a time where Cyberspace is an integral dimension of statecraft.

In this scenario, trust-building emerges as a cornerstone of international Cybersecurity efforts. Existing literature highlights several strategies employed to promote trust among nations. Information sharing, Diplomatic engagement, and collaboration in joint cyber defense initiatives are prominent approaches (Sabillon et al., 2016). Scholars argue that transparency and open communication are central to fostering trust, serving as the basis for meaningful cooperation and conflict prevention in the digital era.

Edward Snowden's disclosures[2] and other multiple case studies have shed light on instances where trust among nations was compromised due to cyber incidents. Notable breaches, attributed or suspected to state-sponsored actors, have led to diplomatic tensions and strained relationships, particularly among major powers (Samuel-Azran, 2013). Such incidents underline the fragility of trust in the digital realm, where attribution challenges and escalating consequences can undermine even well-established relationships. These cases emphasize the urgency of merging trust-building efforts with effective cyber defense strategies.

Within this dynamic setting, defenders hold a key role. Entrusted with navigating this complex tension-carving a path that upholds trust while concurrently countering threats in protecting national interests and global security. However, the question that emerges is a fundamental one: How do defenders balance the seemingly conflicting imperatives of fostering trust among nations and defending against cyber threats in an era characterized by international hacking?

This study delves into a comprehensive exploration of this question, examining the challenges, strategies, and viewpoints that define a defender's approach to navigating the cybersecurity dilemma. By revealing the complex strategies employed to reconcile security and trust, this study sheds light on the intricacies of an evolving landscape where technological competency and diplomatic finesse interlink. By conducting a comprehensive analysis of these strategies, this study contributes to a deeper knowledge of the subtle equilibrium between threats and trust, a balance that holds the potential to shape the future of international Cybersecurity. Furthermore, the study investigates the key aspects of this dilemma, exploring its implications for international relations, instances of trust erosion, existing strategies for trust-building, and frameworks for understanding defenders' approaches.

1. Methodology

This study utilizes analytical, comparative, and descriptive methodologies to scrutinize the defensive strategies employed in addressing cybersecurity challenges. The research relies on remote content analysis of both primary and secondary sources, encompassing scholarly articles, authoritative books, expert testimonies, official statistics, publicly available information, and media interpretations. Government documents and official doctrines, along with insights from state-run Daily Graphic newspapers, are pivotal sources for capturing the perspectives of leaders and government figures. The primary goal is to qualitatively explore the intricate dynamics involved in a defender's approach to navigating the complexities of the cybersecurity landscape.

To offer a comprehensive analysis, the paper systematically gathers, assesses, and synthesizes data from various sources. It delves into case studies spanning Cybersecurity operations from 1990 to 2023, providing a historical context for understanding contemporary Cybersecurity endeavors employed by different nations.

[2] The information he disclosed unveiled a multitude of worldwide surveillance initiatives, a significant portion managed by the NSA and the intelligence alliance known as the Five Eyes, operating in collaboration with telecommunications firms and governments in Europe.

Employing a meticulous combination of extensive literature reviews and insightful discourse analysis, the study investigates the strategic maneuvers, nuanced aspects, and perceptual insights held by key stakeholders, including intelligence services, within the realm of Cybersecurity.

2. Defender's Strategies in Navigating the Cybersecurity Dilemma

In the complicated settings of international cybersecurity, defenders are tasked with employing a multifaceted array of strategies to navigate the complex web of challenges integral in the cybersecurity dilemma (Wendt, 2020). One strategy that emerges as paramount is the practice of proactive diplomacy and strategic communication. This approach underscores the vital importance of establishing transparent communication channels among nations, fostering an environment of openness and cooperation that stands as a counterpoint to the shadowy realms of cyber threats.

At the core of this strategy lies the importance of building communication bridges that exceed geographical boundaries and political differences. Transparent communication channels provide a platform for defenders to share insights, information, and intentions. This sharing, in turn, engenders a culture of understanding and collaboration that is essential for countering the prevailing atmosphere of mistrust. By engaging in proactive diplomacy, defenders strive to cultivate an environment where nations feel compelled to interact, cooperate, and share rather than resort to isolated strategies driven by suspicion (Johnston et.al, 2005).

A pivotal element of proactive diplomacy is the astute utilization of diplomatic channels to address cyber incidents and mitigate potential fears. Diplomacy serves as a conduit through which defenders can openly engage in discussions about cyber incidents, attributions, and intentions. When incidents occur, defenders leverage diplomatic channels to facilitate discussions that defuse tensions, clarify intentions, and establish a foundation for effective response and resolution. This deliberate approach to addressing cyber incidents through diplomatic means reflects a departure from the traditional 'tit-for-tat' retaliatory approach, favoring instead a measured and rational discourse that seeks to de-escalate rather than inflame cyber-related conflicts (Heath & Lane, 2019).

Furthermore, the emphasis on assuaging fears is an integral aspect of proactive diplomacy. Recognizing that fear can proliferate in the absence of information or understanding, defenders employ strategic communication to provide reassurance, dispel confusion, and strengthen the importance of shared security goals. By demonstrating transparency in their intentions and actions, defenders work to build a climate of trust, wherein nations are more inclined to view one another as allies in the shared mission for cybersecurity rather than adversaries to be feared (Lindsay, 2021).

In essence, the strategy of practical diplomacy and communication exemplifies an attempt to rewrite the narrative of international cybersecurity (Theohary, 2018). Through transparent communication channels and diplomatic engagement, defenders struggle to restructure the dialogue from one marked by mistrust and suspicion to one characterized by shared objectives and cooperation. As they pioneer this path, defenders work towards a future where the cybersecurity dilemma is navigated not through escalating conflicts but through enlightened discourse and joint action.

2.1. Enhancing Cyber Resilience

In the ever-evolving realm of international cybersecurity, defenders are compelled to adopt a multifaceted arsenal of strategies to effectively navigate the intricate landscape of challenges presented by the cybersecurity dilemma. Among these strategies, the imperative to enhance cyber resilience emerges as a cornerstone approach. This strategy encapsulates the proactive efforts undertaken by defenders to fortify their digital infrastructure against the relentless tide of cyber threats, while simultaneously showcasing their capacity to rebound from the disruptive aftermath of cyberattacks - a testament to their commitment to safeguarding both the security of nations and enhancing global trust (Lindsay et al, 2015).

Central to the strategy of enhancing cyber resilience is the strategic investment in robust cyber defense mechanisms. This involves allocating resources to develop, implement, and continually refine cutting-edge

cybersecurity technologies, methodologies, and practices. By doing so, defenders strive to create an intricate web of safeguards designed to thwart malicious actors and prevent cyber incidents from escalating into catastrophic breaches (Falco & Rosenbach, 2021). This proactive approach transcends mere reactive responses, signaling a shift towards a more anticipatory and adaptive posture in response to continually changing cyber-attacks.

The demonstrable ability to swiftly recover from cyberattacks constitutes another vital facet of this strategy. In a landscape where adversaries constantly probe for vulnerabilities, defenders acknowledge that no system can be entirely impervious to attack. However, what sets them apart is their tenacity and readiness to recuperate from the aftermath. By showcasing their capability to restore functionality, regain control, and contain the damage following a cyber-incident, defenders not only mitigate the impact of attacks but also send a powerful signal of resilience and determination (Aoyama, 2019).

This demonstration of swift recovery is not solely about technological prowess-it also speaks to the broader concept of trust-building. In a time where the cybersecurity dilemma fosters apprehension and uncertainty, defenders wield their resilience as a means to bolster trust among nations. By displaying their capacity to swiftly manage and rebound from cyber incidents, defenders send a resounding message: a commitment to cybersecurity is not just rhetoric, but a demonstrated reality. This calculated display of resolve reinforces the foundation upon which trust can be built, positioning defenders as reliable partners in the collective effort to navigate the challenges of international hacking.

2.2. Bilateral and Multilateral Agreements

In the complicated domain of international cybersecurity, defenders are presented with a multifaceted array of strategies to effectively navigate the challenges posed by the complex web of the cybersecurity dilemma (Wendt, 2020). Among these strategies, the pursuit of bilateral and multilateral agreements emerges as a pivotal approach, embodying the quest for collaboration, information sharing, and collective defense against the ever-evolving menace of cyber threats.

Central to this strategy is the exploration of collaborative agreements designed to foster information sharing and collaborative action. Recognizing the transnational nature of cyber threats, defenders engage in diplomatic negotiations to establish frameworks that facilitate the exchange of intelligence, insights, and early warnings regarding potential cyber incidents (Riordan, 2018). This proactive sharing of information enables nations to collectively identify emerging threats, assess their implications, and collectively design strategies to counteract them. By breaking down barriers to information flow, defenders strive to build a collective intelligence network that transcends national boundaries-a united front against the uncertainties of the cybersecurity landscape.

The establishment of international cyber defense alliances represents a logical extension of this strategy. These alliances are built upon shared objectives, where nations pool their expertise, resources, and capabilities to craft coordinated responses to cyber threats. Through these alliances, defenders leverage the strengths of their partners to bolster their own cyber defense measures, effectively transforming individual efforts into a cohesive and powerful force against adversaries (Donaldson et.al, 2015). The examination of these alliances provides insights into the challenges and successes faced by defenders as they navigate the intricacies of forming and sustaining such collaborative frameworks.

However, the road to successful bilateral and multilateral agreements is not without its obstacles. Defenders must navigate diplomatic intricacies, differing national interests, and varying levels of technological capabilities. Trust-building, an essential element of these agreements, requires a delicate balance between disclosing enough information to foster cooperation while protecting sensitive data from potential misuse. Furthermore, the challenge of maintaining equity in resource contributions and decision-making within alliances adds another layer of complexity to this strategy.

Despite these challenges, the strategy of bilateral and multilateral agreements stands as a testament to defenders' commitment to tackling the cybersecurity dilemma collectively. By transcending geopolitical

rivalries and establishing platforms for collaboration, defenders aim to build a united defense front that leverages the combined strengths of nations. This approach signifies a paradigm shift from isolated defense efforts to a collective endeavor that reflects the interconnected nature of the digital realm. Through these collaborations, defenders contribute to rewriting the narrative of international cybersecurity, transforming it from a zero-sum game into a cooperative pursuit that serves the interests of all.

2.3. Norms and Rules of Engagement

Defenders are trusted with a diverse array of strategies to skillfully navigate the multifaceted challenges presented by the complicated web of the cybersecurity dilemma. Among these strategies, the establishment of norms and rules of engagement stands out as a pivotal approach, embodying the deliberate effort to shape structured and responsible behavior in the realm of cyberspace (Lucas, 2017).

At the heart of this strategy lies the development of international norms and guidelines that delineate acceptable conduct in the digital domain. These norms function as a set of guiding principles that seek to establish shared expectations for state behavior in cyberspace. Defenders recognize the necessity of crafting these norms to mitigate the potential for escalating cyber conflicts and to foster an environment of responsible and accountable actions (Jasper, 2018). By establishing a common understanding of what constitutes acceptable behavior, defenders aim to create a foundation upon which trust can be built, helping to alleviate the inherent uncertainty of the cybersecurity dilemma.

An essential aspect of this strategy involves the evaluation of the effectiveness of existing agreements and norms in promoting responsible state behavior. This evaluation is a nuanced effort that encompasses assessing the devotion of states to established norms, analyzing the impact of these norms on deterring cyber aggression, and identifying gaps or limitations that may hamper the attainment of a stable and secure cyber landscape (Goldsmith, 2022). Through this examination, defenders gain insights into the complicated dynamics of norm implementation, enabling them to refine their strategies and adapt their approaches to better address the evolving challenges posed by international hacking.

However, the process of establishing and upholding norms and rules of engagement is not devoid of complexities. Defenders must navigate the intricacies of diplomacy, accounting for varying national interests, cultural differences, and interpretations of acceptable behavior. The fluid and borderless nature of cyberspace also adds an additional layer of intricacy, as norms must be applicable across diverse technical and geopolitical contexts (Lavorgna, 2020). Striking the delicate balance between preserving sovereignty and fostering cooperation is an ongoing effort that necessitates thoughtful negotiation and international consensus-building.

3. Challenges Faced by Defenders

Defenders in the international cybersecurity domain confront a complex web of challenges that demand delicate navigation to strike a harmonious balance. One of the challenges they encounter is the fine-tuned art of balancing transparency with national security imperatives. While transparency is pivotal for fostering trust among nations, revealing too much could inadvertently expose vulnerabilities that adversaries might exploit (Lord, 2012). This conundrum requires defenders to tread cautiously, crafting communication strategies that convey a commitment to openness while safeguarding critical information.

Another vexing challenge centers around the equitable distribution of responsibilities within collaborative cyber defense efforts. The interconnected nature of cyberspace calls for joint action among nations, yet the allocation of responsibilities often hinges on intricate negotiations. Defenders must grapple with questions of burden-sharing and resource allocation, striving to ensure that the benefits and obligations are distributed fairly among participating parties (Hood, 2019). This pursuit of balance is essential to avoid perceptions of exploitation or free-riding that could erode trust in collaborative endeavors.

Addressing the labyrinthine issue of attribution in international cyber incidents constitutes yet another uphill battle for defenders. The anonymous and multifaceted nature of cyberattacks complicates the identification of culprits, leading to challenges

in formulating appropriate responses. Attribution gaps can lead to uncertainty, potentially escalating tensions between nations. Defenders must develop robust methods and protocols for accurate attribution to facilitate effective and proportionate responses while minimizing the risk of missteps that could escalate conflicts (Lindsay, 2015).

Among the most formidable barriers that defenders must surmount are the political obstacles that hinder the realization of trust-building initiatives. Geopolitical rivalries, differing interests, and historical tensions can all cast shadows over collaborative efforts to strengthen cyber relations. The dynamics of international politics can impede the establishment of meaningful norms, agreements, and alliances, obstructing progress in building mutual trust (Larson, 1997). Overcoming these barriers demands a nuanced approach, one that acknowledges the broader political landscape while seeking common ground for cooperation.

In this complicated digital domain, defenders often find themselves at the nexus of complex challenges that demand an adept blend of technical expertise, diplomatic finesse, and strategic acumen. Balancing transparency and security, orchestrating collaboration, attributing cyber incidents, and navigating political impediments are all crucial facets of the defender's journey to forge trust amidst the ever-present threats of the cybersecurity dilemma. It is through the collective efforts to overcome these challenges that defenders pave the way for a more secure and stable digital networks.

Securing a network is a significant undertaking due to the complexity of many networks, which may encompass thousands of computers, constantly changing user rosters, and diverse storage locations for valuable information (Skopik et.al, 2016). The approach to network defense is structured into a series of steps, outlining the actions security experts need to take when confronted with a network intrusion. The six steps in network defense are as follows:

- **Preparation**: Conducted before any intrusion occurs, this step involves setting the groundwork for defense.
- **Detection**: Identifying the intrusion signals the beginning of the defensive process.
- **Data Collection and Analysis**: These steps are ongoing throughout the defensive effort, focusing on gathering and interpreting relevant information.
- **Containment**: Defenders work to shield the network from internal intruders, preventing exploitation or attacks before they achieve their goals.
- **Decontamination**: In this step, defenders clean the network and implement improvements to enhance future security.

The initial step, preparation, underlines a fundamental concept: network intrusions take place on the defender's territory. Network administrators play a crucial role in deciding which software and hardware to install or allow on their platforms, with security considerations being paramount (Singh, 2011). Strategic decision-making in this regard helps reduce the potential vulnerabilities that intruders can exploit. Defenders are advised to validate the security of deployed software, deactivate unnecessary software, and eliminate links between unrelated network components (Case, 2016). Failing to adhere to these principles, as exemplified by an incident in an Ohio nuclear plant in 2003, can lead to vulnerabilities exploited by computer worms. By limiting intruders' possibilities, the defensive side can increase the difficulty of unauthorized access and enhance the likelihood of detection.

In the scenario where defenders are unable to prevent an intrusion attempt at the network perimeter, their primary objective becomes the prompt identification of a successful intrusion (Sengupta, 2020). This task, though often challenging, is crucial. The longer intruders go unnoticed, the longer they explore the network, establish a lasting presence, and achieve their goals.

Despite employing a variety of detection methods, the challenge remains substantial. Industry surveys indicate that, on average, intrusions are only discovered 146 days after they occur. Enhancing detection capabilities becomes a pivotal aspect of fortifying overall network defense (Steingartner et.al, 2021). A false sense of security can easily develop when intruders go undetected, leading defenders to perceive absence of an adversary's existence. However, this perceived achievement can be detrimental, allowing attackers to deepen their foothold in

the network, familiarize themselves with its design, and acquire additional access. Hence, a blend of sophisticated defense mechanisms and proactive defending is indispensable. Cybersecurity experts must not only remain vigilant against potential threats but also scrutinize their networks for any previously undetected intrusions (Gartzke & Lindsay, 2015).

While the challenges of detection may seemingly favor intruders, the advantage gained from extended time before discovery is not insurmountable. Cyber offensive and exploitation missions often require time to disclose. If attackers can briefly gain access to valuable secrets without extracting them from the network or launch malicious code that defenders successfully block before any harm occurs, the potential damage is significantly minimized (Mitnick & Simon, 2009). Therefore, the actions taken by defenders after detection, provided it is not excessively delayed, play a critical role in determining the impact of an intrusion.

Upon detecting intruders, defenders must embark on the crucial steps of collecting and analyzing data. These two processes are interdependent, with the process of collecting data informs analysis and vice versa. Given that there is no certainty regarding the entry point of the intrusion, defenders may need to backtrack during the investigation to identify it. Similarly, they must collect information about compromised computers and accounts within their network (Levine et al., 2003). Once this data is gathered, a prompt and thorough analysis is essential, employing various methods.

Significant intrusions typically yield a substantial volume of data, necessitating a dedicated team with diverse training to conduct a thorough examination and contribute to informing defensive actions. The investigation team employ log files to reconstruct events, including instances involving the use of USB drives, document openings, and website visits. Additionally, they deconstruct the malicious code to comprehend its functionality and potential impact. Defense team must ensure the relevance of the analyzed information and remain vigilant for false flags and misdirection.

Following the conclusions drawn from data collection and analysis, the next imperative step is containment. Various defensive actions can be employed to thwart the effects of malicious code and provide defenders with the opportunity to regain control. Updating automated defensive systems based on intelligence from the analysis is a primary containment measure. Alternatively, installing overlooked patches from software vendors may be effective. In more severe cases, the defense team may need to resort to extreme measures, such as disconnecting sensitive network connection segments until the threat is adequately mitigated (Yuan et al., 2014). Some responses, like halting physical processes such as industrial control system operations, may be more time-consuming and require input from non-technical decision-makers.

Upon successfully thwarting the intruders' efforts, defenders face the critical task of immediately decontaminating their network. The establishment of a recurrent incidence within a target network by intruders is a potent capability. Attackers regularly aim to sustain a secure beachhead or foothold to facilitate future operations without the need to re-enter the network.

Decontamination is a substantial undertaking that may involve taking networks offline for days, as exemplified by the State Department's actions in addressing its email system. In some instances, it may require discarding entire securing computer hardware to prevent intruders from re-establishing a presence beneath the operating system (OS) level, such as in the firmware or BIOS (Chevalier, 2019). Even without these extreme measures, decontamination involves thorough scans for malicious code and anomalous activity, conducted by both human investigators and automated tools. This process is typically measured in months rather than minutes and can be costly if not undertaken with proper preparation.

However, successful decontamination is insufficient unless defenders also prevent the recurrence of the next operation. Adaptation is a crucial component of decontamination, necessitating a detailed after-action investigation. Defenders must identify and implement changes to procedures, software, and network policies to address the identified threats (Sengupta et al., 2020). This may involve deploying more advanced automated tools, enhancing intelligence for existing

tools, revising network procedures like patching or remote connection policies, and potentially hiring and training new personnel. These changes may require broader organizational approval, considering both technical and non-technical, that have the potential to affect a substantial number of individuals within the institution. While the process may take a considerable amount of time, it is crucial because if an organization is deemed worth being attacking once, it is highly likely to be targeted again.

4. Not Every Intrusion is of Offensive Intentions

During the mid-2000s, the National Security Agency (NSA) encountered a formidable task: safeguarding numerous American computer networks from Chinese intrusions, which amounted to over 500 significant cases (Bronk, 2016). Offering a comprehensive account would scarcely scratch the surface of the vast, mostly concealed efforts undertaken by the NSA to certify the security of these critical digital networks.

In response to the intrusions attributed to a group known as BYZANTINE CANDOR[3], the defenders situated at the NSA center sought to enhance their comprehension of the threat (Buchanan, 2016). Executing a complex maneuver, the American defenders infiltrated the very infrastructure utilized by the foreign operators. This enabled them to observe the adversary's actions from these intermediary positions. However, the NSA's penetration extended even further. They successfully breached five computers employed by the Chinese operators for their activities. Effectively, they managed to hack the attackers, tracing the Chinese operatives back to their stronghold and obtaining high-quality sources of information covering a broad spectrum of the attacker's operations. The intelligence extracted from the process, when disseminated to network defense team and integrated into automatic platforms, yielded concrete value for future defense efforts. This pool of data encompassed insights into the attacker's forthcoming targets, including profiles of senior White House officers. Furthermore, it facilitated access to the source code and novel tools utilized by the Chinese in their actions, thus revealing the tactics they employed (Andress & Winterfeld, 2013).

This scenario encapsulates pivotal themes in network defense: an illustration of the resourcefulness of ingenious defenders, the determination of skilled adversaries, the challenge of procuring actionable intelligence, and the requirement for network architecture and defender skills at translating information into action. Beyond these aspects, a frequently overlooked yet pertinent insight surfaces concerning the cybersecurity dilemma: not all cyber intrusions are executed with offensive intentions (Buchanan, 2016). Legitimate defensive reasons exist for states to conduct intrusions into the networks of other states.

By infiltrating the networks of potential adversaries and their targets, proficient defenders can accumulate invaluable information-some of which might be unattainable through alternative means or inaccessible to other entities, such as corporations, due to legal limitations. This standpoint underscores the distinctive efficacy of network intrusions in advancing a state's cybersecurity.

Complementing active defense, penetration testing is an additional facet. Skilled intruders are enlisted or hired to simulate actual intrusion attempts, encompassing both social engineering and technical methods (Agbogun & Ejiga, 2013). Utilizing tools like Metasploit, these testers employ techniques akin to those employed by potential adversaries. The outcomes of these tests are subsequently shared with the broader network defense team, furnishing insights into both successful and unsuccessful methods. This practice provides defenders with a clear roadmap for enhancing network security by addressing vulnerabilities exploited by intruders. Additionally, this testing equips analysts with leads to potentially identify intruders who might have gained entry using similar tactics.

Reinforcing network defense hinges significantly on augmented detection capabilities. Succumbing to a false sense of

[3] BYZANTINE CANDOR is an advanced persistent threat unit associated with the People's Liberation Army. Allegedly involved in cyber hacking attacks linked to China, this group frequently exploits internal software features within authentic websites. By infiltrating the platforms of users accessing these sites, the collective has been implicated in illegally acquiring confidential information and trade secrets from diverse foreign organizations and businesses.

security due to undetected intrusions can be detrimental (Waters, 2005). Such complacency allows intruders the opportunity to deepen their penetration, explore network architecture, and broaden their access. Thus, a blend of highly sophisticated security strategies and proactive investigation is indispensable. Network defense experts must remain vigilant against emerging threats while simultaneously scrutinizing internally for potential vulnerabilities they might have overlooked.

5. How Network Intrusions can Help Defenders

Preventing a cyber-attack goes beyond just improving defenses; it requires states to develop network penetration capabilities, often conducted by signals intelligence agencies, as part of their defensive efforts (Amoroso, 2012). This development aims to establish deterrence, a concept that isn't precisely defined for cyber operations yet. However, more immediately, these intrusion skills have the potential to directly assist defense by collecting detailed and valuable information.

This perspective forms a crucial aspect of the cybersecurity dilemma argument within the network defense domain. Despite thorough preparation, timely indicators, and proactive human-led analysis, defense remains challenging, particularly when facing skillful attackers (Buchanan, 2016). This practical operational scenario leads to a strategic resort: to secure their vital networks comprehensively, states have a strong motivation to infiltrate the networks and operations of other states, even before becoming targets themselves (Rattray, 2001). This approach allows them to collect more information on how other nations could potentially attack, the infrastructure they use, and internal organizational procedures, targets, and techniques. This enhances performance in various aspects of the network security model, particularly in detection, preparation, and data collection and analysis. For certain countries, these attacks represent a significant, and perhaps even necessary, aspect of their security mission, at times initiated with genuine security intent.

Private citizens and corporations are prohibited from such intrusions in many jurisdictions, including the United States, due to risks of vigilantism and increased instability (Gill & Ziolkowski, 2013). Therefore, private actors' defensive options typically end within their own networks. However, these restrictions do not adhere to states, as there are minimal rules in the anarchic international system. While some states may opt to impose limits on their security agencies, these restrictions are internal and not imposed by external actors. Consequently, the cybersecurity dilemma, partly influenced by defensive intrusions, is mostly prominent in the realm of states and state-sponsored actors (Malagutti, 2016).

The most straightforward means for intrusions to fulfill a state's defensive objectives is by focusing on the infrastructure, networks, and operations of a potential attackers (Hutchins et.al, 2011). These operations can be categorized into different types. Some operations involve thorough signals intelligence collection involves forming a wide network to gather information on the political and military leadership or strategic priorities of the potential adversary as a whole, instead of focusing solely on their cyber capabilities. Such extensive collection efforts can contribute to defensive preparation, influence resource allocation, and provide early warnings about potential future attacks. Although these operations hold substantial defensive value, it is universally acknowledged by all parties that they also pose a direct threat, as no nation desires to risk the exposure of highly classifies level secrets (Gaitan, 2017). Moreover, they can also serve non-defensive purposes.

On the other hand, some operations are more narrowly focused, collecting information solely for defensive purposes. From the viewpoint of those carrying out the intrusion, these actions do not directly threaten, as their goal is not to harm the security or integrity of the other nation but rather to impede its attempts at computer system penetration (Lin, 2010). This type of data can take various forms but generally has an operational scope, enabling specific defensive countermeasures.

This defensive enhancement can manifest in various ways. For instance, infiltrating another nation to ascertain the whereabouts of its control and command platform for cyber operations facilitates the blocking of traffic to

and from that infrastructure (Kuipers & Fabro, 2006). Collecting data on the malicious code created by attackers enables defence team to produce tailored indicators of compromise. Comprehending the likely method of entry and potential targets of the adversary enables the defender to strategically position its defenses and reduce risks (Weinberger, 1985). Identifying a zero-day vulnerability that an adversary is about to exploit provides defenders with time to notify the vendor or take measures to defend their own networks.

Defenders can leverage information obtained from these penetrations to assess whether the attackers have gained entry, providing immediate operational value to defensive-minded collection (Porch, 2013). In the case of the US and its allies, there is sufficient indication that such information gathering activities occur and contribute to enhancing state defensive actions. The Snowden files have shed light on an interconnected and intricate set of U.S. programs designed to gather intelligence and utilize it to bolster the security of its information system. The process involves collecting data on potential threats, as well as details about the network from which the attack is likely originating. This entails stopping communications of possible adversaries, often through locations in the internet infrastructure, and targeting the devices processing those communications (Stellios et.al, 2018).

The acquired details can alert the NSA's located malicious code on computers, networks and servers worldwide. Acting on this information, one of the NSA's nodes can respond by deploying a response onto the Internet directed at the adversary. The responses can include delivering malicious code, resetting connections, and redirecting internet traffic (Kaur & Randhawa, 2020). Learning about the adversary's tools and tradecraft allows the NSA to develop and deploy specific countermeasures early on to neutralize the intended effects of an intrusion (Buchanan, 2016). The NSA can then interpret the adversary's intent and employ its countermeasures to reduce or eliminate the attempted attack.

This system boasts various capabilities, such as outright preventing incoming traffic, introducing unexpected delays to traffic, responding to attackers, and allowing an activity to appear finish without revealing that it did not reach the projected target, all contributing to a proactive defensive posture.

These defensive capabilities are actively utilized by the US against a diverse array of attacks. NSA documents reveal that the system has been employed to prevent significant threats from major adversaries like China and Russia, as well as against numerous non-state actors (Harber, 2009). Notably, it has successfully thwarted intrusion attempts, including one named BYZANTINE HADES[4] targeting four high-ranking American military leaders, where the defense team identified the attempt and averted any adverse consequences (Singer & Friedman, 2014).

Another American system, overseen by the Department of Homeland Security and referred to as EINSTEIN, strives to fulfill a comparable function for other government-protected networks, functioning like an anti-aircraft weapon by intercepting and neutralizing an attack before it reaches its intended destination. This system aims to amalgamate diverse sources of threat intelligence and disseminate them to other elements of network defense. While these protection systems from the NSA and Homeland Security are not infallible, as attackers may still succeed on occasion, they exemplify how intelligence gathering significantly enhances defensive endeavors. This underscores the investment made by the US and its allies in creating such competences.

Some may argue that this reasoning may apply mainly to sophisticated states, raising questions about the accessibility of these activities for other nations. Indeed, the cybersecurity operations of the US and its allies are extraordinary, and assuming that

[4] Hades serves as a codename for an extensive and continuous series of network infiltrations targeting U.S. military, government, and corporate systems. These operations can be categorized into three sub-groups: Byzantine Candor, Byzantine Foothold, and Byzantine Anchor. Initial information about these cyber intrusions surfaced in a Reuters report, referencing details found in leaked diplomatic cables published by Wikileaks. The cables imply a long-standing pattern of Chinese intelligence, military units, and associated private hacking entities infiltrating U.S. networks, engaging in the theft of sensitive proprietary data and other valuable information over an extended period.

the techniques used by the Five Eyes[5] are easily replicable by other states might be unwise (Spafford et.al, 2023).

Regardless of the actor, if intrusions conducted for defensive purposes were narrowly focused, the cybersecurity dilemma could be less pronounced if states focused solely on specific segments of other nations that are likely to present a threat, such as their cyber operations divisions or infrastructure. This approach might somewhat mitigate the overall threat (Rudner, 2013). While these are crucial targets, they are relatively limited and less surprising, given the historical targeting practices of intelligence services. However, two main factors push states toward broader targeting, even if their motives are primarily defensive. This broader targeting intensifies the cybersecurity dilemma.

Through gathering intelligence on the wider government and strategic apparatus of a potential adversary, a state can gain valuable defensive insights (Betts, 2009). The second factor that encourages broader targeting is the value a state can gain from discovering its potential adversary's operations in real-time. To accomplish this, a state might focus on networks of interest to their potential adversary, even if the state itself lacks significant intelligence interest in those networks (Hutchins et.al., 2011). In essence, nations have an incentive to focus on neutral or even allied nations in order to understand about the activities of their potential adversaries (Leeds, 2003). States that excel in this kind of analysis will target a broader range of networks, aiming to identify potential adversaries in action.

A natural question that may arise from the previous discussion is whether the advantage gained by a state through collecting defensive intelligence via secret cyber operations is limited by the need for secrecy (Rudner, 2013). While the requirement for secrecy does impose some constraints on the value of the intelligence, it is not overly limiting. In many states, there isn't a significant separation between the government and critical infrastructure. Some governments own or operate crucial utilities, and the private sector has a limited role for the development of military and intelligence capabilities or the composition of actions. When there's minimal division through collaboration between public and private sectors on critical matters, states can more readily establish protocols for discreetly sharing intelligence.

Moreover, in states where the private sector plays a significant role in critical infrastructure, efforts have been made to enhance information sharing. The United States is a notable example, with private entities managing substantial segments of the power grid, various defense contractors supporting intelligence and military activities, and a flourishing private financial sector (Schreier & Caparini, 2005). Due to numerous intrusions targeting these tactically crucial non-governmental organizations, the U.S. has instituted information-sharing agreements with private sector entities that are of interest to other states. The federal government has advocated for private sector companies to recruit more individuals with security clearances to manage classified information and has introduced temporary clearance programs to facilitate increased intelligence sharing. (Prieto, 2006). Although the shared information extends beyond intelligence obtained from penetrating other networks, these arrangements empower the U.S. government to have a greater influence on the defensive strategies employed to protect these corporations (Alberts et.al., 1999). They also enable the government to inform these strategies with actionable details, as well as data that it alone can lawfully acquire.

6. Conclusion

In an environment where there are ongoing threats and countries are dealing with vulnerabilities, cyber intrusions motivated by a defensive purpose not only appear attractive but also essential. Importantly, the presence of defensive-focused penetration in cyber activities marks a departure from the usual thinking in international relations and the security dilemma (Healey, 2019). Advanced states have valid defensive reasons for launching intrusions into other countries' networks. This can strengthen network defenses, collect useful information, and reveal potential future risks. Much of this

[5] The Five Eyes is a collaborative intelligence group consisting of Australia, Canada, New Zealand, US, and UK. These nations are participants in the UK-USA Agreement, a multilateral treaty fostering cooperation in signals intelligence. Additionally, colloquially, the term 'Five Eyes' can denote the collective intelligence agencies of these countries.

activity can stay hidden. When there's a perceived threat, and protecting networks is a constant challenge, engaging in defensive-minded penetrations might seem like a tempting and even essential step.

When dealing with regular military forces, it might be true that countries could enhance their defenses by placing troops in the territory of a potential enemy. This military unit could observe signs of an impending attack, get ready to defend, and stop the invasion before it even begins. However, unilaterally sending troops into another country is considered an invasion and a violation of sovereignty, even if the invading country argues that the troops were there for a defensive purpose. Defensive invasions with traditional forces are still invasions and often lead to an increased risk of escalation and conflict.

On the other hand, defensive-minded network intrusions are not invasions; they are intelligence efforts. Countries conducting these types of intrusions are collecting data about the competences of other nations, and they aim to do so discreetly. To some extent, gathering intelligence has been a widely accepted practice in international politics. In simple terms, all countries engage in espionage, and they are aware of this fact. However, there are still risks. When intelligence gathering becomes particularly menacing or can be easily misconstrued as an imminent attack, it can trigger the security dilemma.

It's clear that maintaining a delicate balance between building trust and dealing with threats is crucial for those defending networks. This study argues that to achieve overall security for networks, it's necessary to intrude into the networks of other nations. While numerous security measures provide a fundamental level of protection for most networks, the most advanced defenders, including well-equipped defensive agencies, go beyond these limits. Intruding into external networks can help improve defensive efforts.

However, there are challenges in achieving this balance. These include finding the right mix of transparency and security, identifying the sources of cyber incidents, assigning responsibilities in collaborations, and overcoming political obstacles. These challenges become even more complex with the advent of new systems that reshape the landscape of cyber threats and defenses. As the cyber landscape evolves, defenders must adapt their strategies.

Given these complexities, this study emphasizes the need for ongoing innovation, research, and international collaboration. The cybersecurity challenge is not static; it's a changing landscape that requires flexible responses. By promoting knowledge exchange, open communication, and sharing best practices, defenders can collaboratively build trust while effectively addressing the threats of the digital age.

Proactive diplomacy and communication, the pursuit of bilateral and multilateral agreements, the enhancement of cyber resilience, and the establishment of norms and rules of engagement-all share a common objective: to build a foundation of trust in an environment of uncertainty. The analysis of these strategies reveals that their effectiveness largely hinges on the establishment of consistent, transparent, and reliable lines of communication among nations. Through these strategies, defenders seek to transform the prevailing atmosphere of suspicion and mistrust into one characterized by shared objectives, cooperation, and collective security.

However, while these strategies strive to cultivate trust, they must also contend with inherent challenges that could potentially undermine these efforts. The interplay between transparency and national security concerns, the equitable distribution of responsibilities in collaborative efforts, the complexities of attribution, and the political barriers that hinder trust-building initiatives - all pose potential pitfalls that defenders must navigate with finesse. For instance, balancing the imperative of transparency with the necessity of securing national interests, requires a judicious approach and delicate diplomacy to information sharing that preserves both security and trust.

Moreover, the emerging technological landscape introduces an additional layer of complexity to the cybersecurity dilemma. The integration of quantum computing, artificial intelligence, and other transformative technologies has the potential to reshape the dynamics of cyber defenses and threats (Bonfanti, 2022). These technologies can accelerate the pace and sophistication of

cyberattacks while also providing innovative tools for defense team to detect, prevent, and respond to such attack.

References

Agbogun, J. B., & Ejiga, F. A. (2013). Network security management: solutions to network intrusion related problems. *International Journal of Computer and Information Technology,* 2(4), 617-625.

Alberts, D. S., Garstka, J., & Stein, F. P. (1999). *Network centric warfare: Developing and leveraging information superiority (p. 167).* Washington, DC: National Defense University Press.

Amoroso, E. (2012). *Cyber-attacks: protecting national infrastructure.* Elsevier.

Andress, J., & Winterfeld, S. (2013). *Cyber warfare: techniques, tactics and tools for security practitioners.* Elsevier.

Aoyama, T. (2019). Control Systems Security and Communication-Achieving Organizational Resilience through Exercise.

Betts, R. K. (2009). *Enemies of intelligence: Knowledge and power in American national security.* Columbia University Press.

Bonfanti, M. E. (2022). Artificial intelligence and the offence-defence balance in cyber security. Cyber Security: Socio-Technological Uncertainty and Political Fragmentation. London: Routledge, 64-79.

Bronk, C. (2016). Cyber Threat: The Rise of Information Geopolitics in US National Security: The Rise of Information Geopolitics in US National Security. ABC-CLIO.

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations.* Oxford University Press.

Case, D. U. (2016). Analysis of the cyber-attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388(1-29), 3.

Chevalier, R. (2019). Detecting and Surviving Intrusions: Exploring New Host-Based Intrusion Detection, Recovery, and Response Approaches (Doctoral dissertation, CentraleSupélec).

Donaldson, S., Siegel, S., Williams, C. K., & Aslam, A. (2015). Enterprise cybersecurity: how to build a successful cyberdefense program against advanced threats. Apress.

Falco, G. J., & Rosenbach, E. (2021). *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity.* Oxford University Press.

Gaitan, J. P. (2017). Strategic Counterintelligence: An Approach To Engaging Security Threats To American Security (Doctoral dissertation, Johns Hopkins University).

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: offense, defense, and deception in cyberspace. *Security Studies*, 24(2), 316-348.

Gill, T. D., & Ziolkowski, K. (2013). Non-intervention in the cyber context. Peacetime Regime for State Activities in Cyberspace International Law. International Relations and Diplomacy. NATO CCDCOE, Tallinn, 217-238.

Goldsmith, J. (Ed.). (2022). *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment.* Oxford University Press.

Harber, J. R. (2009). Unconventional spies: The counterintelligence threat from non-state actors. *International Journal of Intelligence and CounterIntelligence*, 22(2), 221-236.

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, 5(1), tyz008.

Heath, T. R., & Lane, M. (2019). Science-Based Scenario Design: A Proposed Method to Support Political-Strategic Analysis (p. 59). RAND.

Hood, L. M. (2019). US-German Defense Burden-Sharıng Sınce 2014: Collectıve Defense Or Free Rıder? (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1(1), 80.

Jasper, S. (2018). US strategic cyber deterrence options (Doctoral dissertation, University of Reading).

Johnston, A. I., & Ross, R. S. (Eds.). (2005). *Engaging China: The management of an emerging power* (Vol. 10). Routledge.

Kaur, S., & Randhawa, S. (2020). Dark web: A web of crimes. *Wireless Personal Communications,* 112, 2131-2158.

Kesan, J. P., & Hayes, C. M. (2014). Creating a circle of trust to further digital privacy and cybersecurity goals. *Mich. St. L. Rev.,* 1475.

Kuipers, D., & Fabro, M. (2006). Control systems cyber security: Defense in depth strategies (No. INL/EXT-06-11478). Idaho National Lab.(INL), Idaho Falls, ID (United States).

Larson, D. W. (1997). Trust and missed opportunities in international relations. Political Psychology, 18(3), 701-734.

Lavorgna, A. (2020). Cybercrimes: Critical issues in a global context. Bloomsbury Publishing.

Leeds, B. A. (2003). Do alliances deter aggression? The influence of military alliances on the initiation of militarized interstate disputes. American Journal of Political Science, 47(3), 427-439.

Levine, J., LaBella, R., Owen, H., Contis, D., & Culver, B. (2003, June). The use of honeynets to detect exploited systems across large enterprise networks. In IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003. (92-99). IEEE.

Liaropoulos, A. (2016). Exploring the complexity of cyberspace governance: state sovereignty, multi-stakeholderism, and power politics. *Journal of Information Warfare*, 15(4), 14-26.

Lin, H. S. (2010). Offensive cyber operations and the use of force. J. Nat'l Sec. L. & Pol'y, 4, 63.

Lindsay, J. R. (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity,* 1(1), 53-67.

Lindsay, J. R. (2021). Cyber conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem. *Intelligence and National security,* 36(2), 260-278.

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (Eds.). (2015). China and cybersecurity: Espionage, strategy, and politics in the digital domain. Oxford University Press, USA.

Lord, K. M. (2012). *The perils and promise of global transparency: Why the information revolution may not lead to security, democracy, or peace.* State University of New York Press.

Lucas, G. R. (2017). *Ethics and cyber warfare: the quest for responsible security in the age of digital warfare.* Oxford University Press.

Malagutti, M. A. (2016). State-sponsored cyber-offences. Revista da EGN, 22(2), 261-290.

Mitnick, K. D., & Simon, W. L. (2009). The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers. John Wiley & Sons.

Porch, D. (2013). Counterinsurgency: Exposing the myths of the new way of war. Cambridge University Press.

Prieto, D. (2006). Information sharing with the private sector. Seeds of Disaster, Roots of Response. How Private Action Can Reduce Public Vulnerability, 404-428.

Rattray, G. J. (2001). Strategic warfare in cyberspace. MIT press.

Riordan, S. (2018). The Geopolitics of Cyberspace: A Diplomatic Perspective. *Brill Research Perspectives in Diplomacy and Foreign Policy,* 3(3), 1-84.

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and CounterIntelligence*, 26(3), 453-481.

Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, 5(5), 67.

Samuel-Azran, T. (2013). Al-Jazeera, Qatar, and new tactics in state-sponsored media diplomacy. *American behavioral scientist,* 57(9), 1293-1311.

Schreier, F., & Caparini, M. (2005). Privatising security: Law, practice and

governance of private military and security companies (Vol. 6). Geneva: DCAF.

Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., & Kambhampati, S. (2020). A survey of moving target defenses for network security. IEEE Communications Surveys & Tutorials, 22(3), 1909-1941.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know.* oup usa.

Singh, B. (2011). *Network Security and Management.* PHI Learning Pvt. Ltd.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, 60, 154-176.

Spafford, E. H., Metcalf, L., & Dykstra, J. (2023). *Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us*. Addison-Wesley Professional.

Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry,* 13(4), 597.

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials,* 20(4), 3453-3495.

Theohary, C. A. (2018). Information warfare: Issues for congress. *Congressional Research Service,* 7-5700.

Val Sánchez, K. V., & Akyesilmen, N. (2021). Competition for High Politics in Cyberspace: Technological Conflicts Between China and the USA. *Polish Pol. Sci. YB,* 50, 43.

Waters, L. A. (2005). Secrecy, deception and intelligence failure: explaining operational surprise in war (Doctoral dissertation, Massachusetts Institute of Technology).

Weinberger, C. W. (1985). US defense strategy. *Foreign Aff.,* 64, 675.

Wendt, D. W. (2020). Exploring the strategies cybersecurity specialists need to improve adaptive cyber defenses within the financial sector: An exploratory study (Doctoral dissertation, Colorado Technical University).

Yuan, W., Zhao, L., & Zeng, B. (2014). Optimal power grid protection through a defender–attacker–defender model. *Reliability Engineering & System Safety,* 121, 83-89.