Defending The Defenseless In Cyber-War

Oluwatosin Amodu
Department of Information Security,
University of The Cumberlands, Kentucky, USA
oamodu23777@ucumberlands.edu

***Abstract*—Protecting against digital attacks has become increasingly important in the modern cyberwarfare environment. However, in the conversation about smart data exchange and security protocols, people's rights and safeguards are frequently ignored or devalued. This paper argues that while cybersecurity fortification methods are important, personal privacy and autonomy shouldn't suffer. Based on findings from recent studies by Pisharody et al., (2021) and Mtsweni & Thaba, (2022), this write-up emphasizes the necessity for a balanced strategy that gives security and fundamental human rights equal priority. It contends that to protect the weak and preserve democratic values, effective cyberwarfare protection requires strong legal and ethical frameworks in addition to technological fortifications. This article aims to contribute to a more thorough knowledge of cybersecurity that incorporates both technical skills and ethical considerations through a nuanced study of the potential and challenges in defending the helpless in cyber-warfare.**

Keywords—Cyber-warfare, Defense, Defenseless, Vulnerability, Resilience, Security, Safeguarding, Threats, Cyber-attacks, Vulnerable targets, Countermeasures, Mitigation, Resisting attacks, Cyber resilience, Empowerment.

I. INTRODUCTION

Successful cyberwar requires both offensive and defensive capabilities. Defending Cyberspace is crucial to protect military communications, sensitive data, and national security interests. Countries such as Vietnam, the Gulf Wars, and Israeli-Palestine have demonstrated remarkable success in defending against hostile forces seeking to breach their digital borders and compromise their infrastructure. China and Russia, on the other hand, have actively projected their defensive capabilities by executing strategic offensive cyber operations, enhancing their cyber defenses, and asserting dominance in cyberspace (Pisharody et al., 2021).

Moral hazard inevitably arises with the emergence of the National Cyber Force, which possesses the unprecedented ability to engage in defensive and offensive cyberwarfare. This force must operate within the boundaries of international law and adhere to ethical principles at the onset of any hostile act. Upholding international rules and preserving the sanctity of cyberspace is vital to preventing further escalation and ensuring a stable global cyber environment (Mtsweni & Thaba, 2022).

In today's interconnected world, economic growth and society heavily rely on information technology and advanced communication systems. A thriving cyber conflict landscape grants the defender increased power and leverage while minimizing the inherent risks associated with traditional warfare. However, the rise of ambiguous warfare techniques and the proliferation of modern cyber weapons introduce new challenges and risks for both offensive and defensive actors (Brantley, 2021).

While nations must build robust defensive capabilities, the preference lies in formulating strategic coalitions to combat the evolving threats. Cooperation and joint efforts among military organizations, intelligence agencies, and cybersecurity specialists play a vital role in restoring compromised capabilities and bolstering the resilience of critical networks. Furthermore, collaborative actions between civil society and public administration are necessary to navigate the complex landscape of cybersecurity, ensuring the protection of individuals, businesses, and overall national security interests (Leitzel & Hillebrand2022).

2. STRATEGIES FOR DEFENDING THE DEFENSELESS

Negotiation and coalition formation between different layers are necessary during real-time operation, and the price of anarchy may increase with attacker capabilities for these games. Approaches for defense can be categorized into the following two categories based on their purposes: diminishing the entrance of adversaries to the system (prevention approaches) and creating resilient systems (resilience approaches) (Buchler et al., 2018). Prevention can be unfeasible in certain situations and the resilience approach is more necessary. The resilience approaches can be applied to uncertain outcomes of attacks, making the outcomes of attacks less harmful. At a certain point, the better defense can improve the level of the attacker's costly operations more than the resilience value the attacker can retrieve after implementation in the defense system.

The determined operation of the resilience approach can be a potential strategy for cybersecurity in uncertain environments. Adsorption, isolation, the diversity of components, systemic defensive measures, and entanglement of upper layers (communication system and application system) and lower layers (physical and cyber systems) footprints are some of the effective defense approaches. In addition, a real-time template can be extracted and issued by machine learning first, and then compare messages against the real-time template to find some obvious hacking instructions or reduce alerts to proceed with the second defense mechanism. With this second approach, an alert about a loss of power shall be issued if messages do not fit to real-time message templates and inclusion of a margin for false positives will arise.

It is important to detect negative effects on the reliability and security of electrical power systems as early as possible and to diagnose and mitigate them. A defense-in-deep approach usually is followed for incorporating the attack detection, diagnosis, and mitigation strategies for cyber-physical electric power systems. More precisely, a computational approach from spatio-temporal data-driven detection and diagnosis of cyber-attacks can accomplish risk assessment and novel mitigation decisions. Models at different spatial and time scales can characterize the fundamental mechanism of the interaction between different aspects of the power systems with their backgrounds. These models provide fundamental limits and insights into detection, diagnosis, and mitigation in the face of adversary actions. The control system's capability regarding the self-configuration, self-healing, and reconfiguration properties can reduce the potential practical impacts of cyber-attacks, which can be attractive for adversaries.

Critical Infrastructure (CIs), including electric power grids, telecommunications, water supplies, and financial services, is indispensable for every modern country (Babu Mitikiri et al., 2023). Cyber-attacks targeting critical infrastructures can have debilitating effects on a country´s government, national defense, and economic power. A well-known CIS attack targeting Ukraine, on December 23, 2015, leading to the loss of electrical power to more than 230,000 Ukrainian customers, is a typical example of the kind of wide disruption that can occur due to a well-organized and precisely orchestrated cyber-attack (Agnarsson et al., 2015). In these cases, poor resilience and fast recovery capabilities can lead to a significant disaster, soft targets are even most vulnerable, leading to their excessive disruption or destruction by the adversary.

2.1. Enhancing cybersecurity measures

This review has shown that society is increasingly vulnerable to the virtual side of life, especially during the global COVID-19 pandemic. As reliance on technology and digital networks grows, the sophistication and frequency of cyber-attacks also increase. Businesses and individuals need to be vigilant and cautious. The regulatory framework on cyber security implementation emphasizes regulatory governance at all stages of development and throughout the system life cycle. Future directions suggest close engagement with the regulatory framework of human studies to train human behavior. Abbreviated training protocols will greatly facilitate the incorporation of game theory models. It is also important to continue to receive funding for cyber-encroachments, which are currently a small fraction of national spending on cyber security.

A strong cybersecurity infrastructure consists of a range of functional units, including governance and security testing. Companies that practice good governance provide clear roles and responsibilities, senior management commitment, constant monitoring of security features and policy compliance, regular reassessment of security controls, and continuous incident analysis. Regulatory agencies and private institutions offer clear guidelines on how to ensure different technical skills for individual companies and industry sectors. These principles include minimum privileges, multiple defenses, streamlined content, simplicity, secure defaults, secure start-up, and trusted external connections. They all emphasize leadership and security accountability (M. Borky & H. Bradley, 2018). In a formal cybersecurity strategy document, the Department of Defense (DoD) emphasizes the need for some of the cybersecurity principles suggested by other organizations. DoD's formal guidance focuses on identification and authentication. The DoD argument implies that breach detection is fifteen times more important than breach prevention. Breach detection becomes all the more important because attacks have become more sophisticated, focusing on social and human vulnerability. When a security mechanism is bypassed by exploiting a human error, DoD expects the system to raise an alarm on activity or behavior. There are several other measures that a company should adopt to develop a successful security governance infrastructure. The list includes but is not limited to (1) documentation, (2) periodic training, (3) regular risk assessments and (4) clear arrangements for third-party support in matters of confidentiality and security.

2.2. Educating vulnerable individuals

The best remedy to overcome this situation is awareness. Awareness, if not removes 100% of the cyber-attacks but minimizes it quite very much. NIST considerations recommend increasing cyber security awareness in children and older members of the family. It is because children in the house are being provided with unnecessary facilities, and some websites have the potential hazard of ripping personal information out of the user's web browsing. Sometimes, when these children are provided with Bluetooth-related devices get bugs in their device, and end up sharing it with their parent's iPhone (Huang & Zhu, 2018). In these kinds of accidents, it is not the child to be blamed but the parent who already knows that the child will somehow misuse the Bluetooth phone while playing games and browsing. Therefore, major threats of cyber-attacks will win the race to take place in the house due to the ignorance of the primary members of the family from the child to the eldest. Hence, these primary targets not only become the way how cyber-attacks start reaching organizations but are also ripe to manage any hacking threat in favourable conditions through ransomware attacks and threats.

The subject of cyber security is not new, and hence, it is understood that no entity on the Internet is 100% invincible or immune to cyber-attacks (Jing, 2022). According to NIST, the majority of the world's populous falls under the category of vulnerable. In simple words, web users along with netizens, who are not aware of the cyber security concepts can be very easily targeted and their online resources misused (Li & Zhu, 2024). One of the primary reasons for cyber threats turning into cyber-attacks is the ignorance of the end-user. To minimize the cyber security threats at the primary and end-user levels, we need to transform the unawareness into a state of knowledge to secure the surroundings.

2.3. Collaborating with international partners

Intelligence sharing is essential to identify vulnerabilities in the system in real-time to prevent attacks. Despite the existence of information sharing and analysis centers (ISACs), these entities can still be ineffective if no personal relationships exist between information stakeholders in the organization. Establishing cooperation agreements between countries can be a solid measure to enhance collaboration among intelligence agencies that aims to deepen trust between them, the utility of agents whose expertise in international cooperation and negotiation may be comparable to or exceed that of diplomats and military officers. Law enforcement organizations in leading countries will also continue to develop cooperation to share comprehensive information on cyber incidents and suspects for criminal purposes. Improving cybersecurity must also be addressed as one of the priorities of bilateral or multilateral negotiations and consultations. Policymakers should also foster the participation of more players in the formulation and improvement of international cybersecurity laws and global standards. (Feijóo et al.2020)

Gathering information from an adversary is a challenging task. In some cases, senior military officers and government officials must receive a daily update on where they see cyber defense, cyber operations, and cyber intelligence (Ho et al., 2022). This is typically referred to as the commander's cyber update brief. During the update, full-time staff members or contractors normally provide critical information to military leaders and government officials on potential incoming cyber threats, new malware, hostile tactics and procedures, or strong cyber defense practices (S. Reveron & E. Savage, 2020). Internationally, cybersecurity partnerships play a crucial role in global cyber defense and security. These partnerships can help develop strategies for cyber defense and promote policy coordination among governments. This multinational collaboration is a critical factor in order to tackle the increasing cyber threats. This chapter surveys the types of partnerships that constitute the full spectrum of cooperation on cybersecurity. Advantages, limitations, potential policy challenges, and the types of partnerships designed to strengthen cybersecurity and areas for further research are also analyzed (Papathanasaki et al., 2020).

3. Challenges faced in cyber-war

Such a complicated landscape is hard (even impossible in general) to fully understand and a fortiori to represent. It's more like a living and evolving organism in which one can only hope to understand a few connecting threads. A way to get more insight from the fuzziness of the whole is to reduce its complexity. Almost all approaches thus reduce the response to a game: relations in the variables may be endlessly not understood, but the overall evolution of each actor in the state space of his objectives can be reduced to a binary choice and therefore seen as a game against the others.

What makes responses to threats in cyberspace difficult is that their actors operate in an unbounded and dynamic environment that they seek to transform, for example, to deceive your own AI tools into thinking there are still threads. The variables of that large state space evolve largely independently of each other and at different rates: technical vulnerabilities, architecture changes, basic ideas behind configurations of the tools deployed, operational needs (thus processes), strategies in responses to anti-responses or to shift dependencies, detection technologies and use of that info, AI rule learning, raw capacities of the SOC (people, technology, or data storage), adversarial knowledge pool getting updates as well, feedbacks and constraints in global ecosystems (e.g. new legal measures on data privacy which shift towards non-technical solutions), beliefs and habits of humans, etc (Jing, 2022).

The defence and response strategies in cyber-war challenge the traditional approach in military operations in facing state and non-state network adversaries in complex battlefields. Dealing with ever-increasing threats and intercepts in cyberspace, Security Operation Centers (SOCs) face daunting hurdles in detecting and hunting adversaries while maintaining an uninterrupted supply chain, and managing the policies, traffic and devices under constant threat from misconfigurations or exploits. Attackers constantly use all available tools to update their TTPs (Unit 1), prepare zero-day exploits, send social-engineered phishing e-mails or fingerprints that defence systems do detect, and all. Strategies and tactical interactions in response must adapt to this rapidly evolving landscape (Li & Zhu, 2024).

3.1. Rapidly evolving cyber threats

Most recently, we have witnessed the COVID-19 crisis and world-scale remote working adoption gives rise to expanding cyber attacks (Papathanasaki et al., 2020). Mt.Gox, the company hosting the biggest cryptocurrency exchange platform at the time, found as many as 650,000 bitcoins were stolen, valued at around $8.75 million at the time of the thievery. These threats can include a target's search for unauthorized network access, which can be obtained through a variety of hacking methods. Threat intelligence services analyze malware and its traffic to recognize patterns of recognized threats, allowing organizations to prepare for safe use of the network and properties. Fraudulent networks are often combined with various identity thefts and fraud forms. Such malicious apps deceive end users into delivering personal information. Some malware is stealthy and prevents the user's tricks or views of its identity. Scammers often use malware to obtain unauthorized entry to computer systems providing financial information.

Cybersecurity contributes to preserving the Internet's confidentiality, integrity, and availability by protecting systems, consumers, and data (Ho et al., 2022). Technical and human controls are often included in cybersecurity strategies, but they are not always successful, particularly as players become a preferred target for cybercriminals due to the increasing sophistication and resulting difficulties in extricating attacks from the standard noise of cybersecurity activities (Khan et al., 2022). The internet's increased adoption has, without a doubt, had a major impact on regular infrastructure, posing a slew of challenges to network administrators, among others. One significant concern is the increase in cyber threats as criminals seek newer methods to exploit the expanded surface area given by the internet.

3.2. Limited resources for defense

Technical defenses include revival strategies and protection measures like high entropy for systems and algorithms that handle the access of outside software or data within the territory which (sometimes) protects the network in which they are contained. Policies and processes are the system components and the decision processes, autonomous action processes and, data-sharing processes that are characterised in terms of architectural components. Active defenses are those kinds of defenses where defense against a threat is actively operated (Li & Zhu, 2024). The techniques used in this kind are computer forensics and intrusion prevention systems.

The technology available for misuse as hacking tools has become more effective and user-friendly (Harsora & Khoyani, 2022). The success of a defense in war can include avoiding possible attacks, as well as reducing the effect of harm in the aftermath. Unsophisticated attackers are unlikely to exhaust all the defensive resources, but sophisticated attackers demand knowledgeable manpower. Defender efforts are being focused on repair after damage has been done, making it difficult for them to respond quickly during operations (Khan et al., 2022). There is a need for a new framework for cyber-warfare operations where efforts are shared between attack, defense, and recovery.

3.3. Lack of global cyber regulations

The are a few reasons why we face such a complex, and at times, confounding environment as mentioned earlier on above. Industries and companies within the same industry do not tend to share information regarding how they overcame a cyber-attack or inform others how they are working towards fighting off angles of possible cyber-attacks(Antonio Sotelo Monge & Maestre Vidal, 2021). The hole in collaboration has also obviously been affected by the mistrust between public and private companies. Government leaders and CEOs share the belief that companies share a love for “keeping a lid on” their affairs. A 2019 report conducted by the Wall Street Journal opines that tech corporations must not extend a hand to link up with authorities and thus have trust built consequently. Some prominent company executives admit that they seemed not to believe the United States authorities. The leaders of the agencies claim that the companies have to exhibit a tad more effort in taking up their advice. This worrying interferes with efforts aimed at ushering in more team-sharing inside countries and among these nations - hence bilateral and multi-path international cooperation. In other words, all countries entering into deals of close-knit cooperation must get together to formulate mutual trust. The implementation of laws should be allowed for recurring attacks guarded against. However, nothing is ideal.

It is widely agreed upon that one of the, if not, the most fundamental reasons why defending against potential cyberattacks is something of a challenge is because there currently exists, to a large extent, a lack of global cyber regulations(Harsora & Khoyani, 2022). Each country differs from the other in terms of internet and cyber regulations meaning that making the entire world be on the same page is an extremely difficult proposition. When it comes to Japan, for example, Japan's Basic Act on Cybersecurity, this act is founded on three core measures for each company to improve its protection policies. These are, first, establishing the ability to offer security measures to the necessary extent, and second promptly responding to and facilitating the tracking of cyber-attacks. Third, to be prepared for risk management. The controlling authorities of Japan have outlined these fundamental heterogeneity measures in much more detail than other places which suggests that the country takes its cybersecurity seriously. The individualistic approach is well and truly evident in Japan(Papathanasaki et al., 2020).

4. Conclusion

Requirements for cyber security continue to change and remain erratic. A single security investment weathers quickly as networks evolve and adversaries improve both their techniques and their cadence. Given that, a variety of approaches to security makes sense: the layering of the solution, attack signatures that confer and a broad understanding of network activity (so that outliers suggest nefarious behavior) from analyses. The problem is one of estimating who will be secure and who will not. Fortune 1000 companies back vulnerability databases but no large organization can boast a perfect security report card. Security deficit persists because things are far from understood on the applied organizational level (Maurushat & Nguyen, 2022).

DEFENDING THE DEFENSELESS (W. Reddie et al., 2023)To address these issues, two scholars, William Ascher and Emmanuel Jimenez propose adopting a more strategic mindset when it comes to defending our networks and data in cyberspace. Currently, organizations and countries operate with a tendency to “mow the grass” or focus narrowly on identifying, defending against, and counteracting any specific new threats that emerge. When it comes to cybersecurity In short, there’s a wide variety of tools and techniques that you can use to look for intruders and try to prevent them from getting into your organization. But there are far too many attacks and device vulnerabilities—to say nothing of human mistakes—that one could hope to keep with them all. Each new threat diverts effort towards understanding it and moving to prevent it. The broader strategic advance here is to target your efforts on keeping everyone alive (keeping the adversary out) rather than patching all the things.

Cyberspace provides a domain for conflict where military power is no longer a guarantee of relative advantage. Outspent and outnumbered adversaries find offensive actions attractive. In response, defense becomes more important. From an international security perspective, the fear is that, for example, terrorists or financially constrained states will be the threat actors. This fear of offense and fear of capability leads to various reactions: attempts to build monitoring networks, a growing remit for U.S. Cyber Command, and the possibility of pre-emptive action. All of these reactions integrate inconclusive or missing evidence and a failure to understand the second-and third-order effects of action (S. Reveron & E. Savage, 2020).

References

[1] Pisharody, S., Bernays, J., Gadepally, V., Jones, M., Kepner, J., Meiners, C., Michaleas, P., Tse, A., & Stetson, D. (2021). Realizing Forward Defense in the Cyber Domain. [PDF]

[2] Brantley, D. S. (2021). Evolving Cyber Warfare Strategies of the United States, Russia, China, and Iran. [HTML]

[3] Lancry A. S. Robalo, T. & Begum Bt Abdul Rahim, R. (2023). Cyber Victimisation, Restorative Justice and Victim-Offender Panels. ncbi.nlm.nih.gov

[4] Mtsweni, J. & Thaba, M. T. (2022). Building an integrated cyber defence capability for African missions. Journal of Information Warfare. researchgate.net

[5] Leitzel, B., & Hillebrand, G. D. (2022). Strategic cyberspace operations guide. Carlisle, PA: United States Army War College/Center for Strategic Leadership, 28. defense.gov

[6] Buchler, N., Genevieve La Fleur, C., Hoffman, B., Rajivan, P., Marusich, L., & Lightner, L. (2018). Cyber Teaming and Role Specialization in a Cyber Security Defense Competition. ncbi.nlm.nih.gov

[7] Babu Mitikiri, S., Victor Sam Moses Babu, K., Dwivedi, D., Lakshmi Srinivas, V., Chakraborty, P., Kumar Yemula, P., & Pal, M. (2023). Modelling of the Electric Vehicle Charging Infrastructure as Cyber-Physical Power Systems: A Review on Components, Standards, Vulnerabilities and Attacks. [PDF]

[8] Agnarsson, G., Greenlaw, R., & Kantabutra, S. (2015). The complexity of cyber attacks in a new layered-security model and the maximum-weight, rooted-subtree problem. [PDF]

[9] M. Borky, J. & H. Bradley, T. (2018). Protecting Information with Cybersecurity. ncbi.nlm.nih.gov

[10] Huang, L. & Zhu, Q. (2018). Dynamic Bayesian Games for Adversarial and Defensive Cyber Deception. [PDF]

[11] Jing, J. (2022). Applications of Game Theory and Advanced Machine Learning Methods for Adaptive Cyberdefense Strategies in the Digital Music Industry. ncbi.nlm.nih.gov

[12] Li, T. & Zhu, Q. (2024). Symbiotic Game and Foundation Models for Cyber Deception Operations in Strategic Cyber Warfare. [PDF]

[13] Feijóo, C., Kwon, Y., Bauer, J. M., Bohlin, E., Howell, B., Jain, R., ... & Xia, J. (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. Telecommunications Policy, 44(6), 101988. sciencedirect.com

[14] Ho, E., Rajagopalan, A., Skvortsov, A., Arulampalam, S., & Piraveenan, M. (2022). Game Theory in Defence Applications: A Review. ncbi.nlm.nih.gov

[15] S. Reveron, D. & E. Savage, J. (2020). Cybersecurity Convergence: Digital Human and National Security. ncbi.nlm.nih.gov

[16] Papathanasaki, M., Dimitriou, G., Maglaras, L., Vasileiou, I., & Janicke, H. (2020). From Cyber Terrorism to Cyber Peacekeeping: Are we there yet?. [PDF]

[17] Khan, N., J. Houghton, R., & Sharples, S. (2022). Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks. ncbi.nlm.nih.gov

[18] Harsora, D. & Khoyani, K. (2022). A systematic literature review of cyberwarfare and state-sponsored hacking teams. [PDF]

[19] Antonio Sotelo Monge, M. & Maestre Vidal, J. (2021). Conceptualization and cases of study on cyber operations against the sustainability of the tactical edge. [PDF]

[20] Maurushat, A. & Nguyen, K. (2022). The legal obligation to provide timely security patching and automatic updates. ncbi.nlm.nih.gov

[21] W. Reddie, A., E. Booth, R., L. Goldblum, B., Lakkaraju, K., & Reinhardt, J. (2023). Wargames as Data: Addressing the Wargamer's Trilemma. [PDF]