International Journal of

INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Cybersecurity Against Emerging Threats in the Future of Cyber Warfare

[1]Zina Balani, [2]Naska Ismael Mustafa

Submitted: 17/07/2023 **Revised**: 07/09/2023 **Accepted**: 24/09/2023

Abstract: In today's technological landscape, cyber warfare has emerged as the most critical global issue. Cybersecurity experts predict the onset of cyber warfare, surpassing conventional military operations and having the potential to disrupt essential industrial management programs. The cyber revolution predominantly targets smaller governments and groups resembling terrorist pirates, employing similar tactics. These entities exhibit malicious intent by attempting to breach passwords and compromise both factory automation systems and military infrastructure. This study investigates the potential of combining firewalls and Intrusion Detection Systems IDS as a comprehensive cybersecurity strategy for the future of cyber warfare. Firewalls, as a primary line of defense, operate as barriers between networks, monitoring and controlling incoming and outgoing traffic. On the other hand, IDS functions as vigilant detectors, identifying anomalous activities or unauthorized access within a network.

Keywords: *Firewalls, cyberweapon, cyber-attack, malicious, automation, IDS, cyber warfare*

1. Introduction

In today's world, we are reading a lot of news about cyber events, especially when computer technology is involved on the battlefield. Due to its complexity, it is challenging to define both cyber and warfare. There is no single definition for "cyber"; if you've heard about it, it generally refers to cybersecurity. On the other hand, warfare means achieving victory without direct combat, avoiding the use of guns and bombs against the enemy. Cyberwarfare represents a revolution and the military's greatest challenge, operating in the sixth dimension and becoming a crucial aspect of warfare development. In modern militaries, cyberwarfare utilizes technology to steal information or understand the enemy's strategies, gaining the ability to access and potentially disrupt all military systems. Similar to nuclear warfare, cyber warfare's impact is far-reaching in a way that defies measurement. In the future, cyber will be increasingly used to control both military and civilian domains, including aspects like gas, electricity, health, transportation, and banking [1-3].

During the 1970s, the United States advanced its development of information technology to formulate policies and strategies for cyberspace. They aimed to establish control over international cyberspace activities in the future. As a result, cyberspace has evolved into a new political platform with military and economic implications, among others [4].

Cyberspace developed alongside the growth of network and computing environments in the 1990s. It was notably utilized in warfare, even dating back to World War II. For instance, German bombers used radio frequencies to direct attacks against Britain during the "beams war," transmitting signals from their point of origin [5].

Between 1999 and 2004, groups of Chinese attackers developed cyberattacks against Indonesia, Taiwan, and the United States in response to political incidents. During this period, the Hezbollah group initiated the hijacking and subsequent shutdown of its web pages in 2006 [6].

In December 2009, two Chinese educational institutions carried out attacks on Google's email accounts, targeting over 30 American companies and institutions, particularly those associated with the U.S. administration. The FBI reported that China had established a "cyber army" [1, 7].

The true history of cyber warfare began in mid-2010 with the emergence of Stuxnet, the first recognized digital weapon and a pioneering example of real-world cyber warfare. Stuxnet, a malicious computer worm capable of self-replication, was designed to target Programmable Logic Controllers (PLCs), specifically those used in Iran's nuclear centrifuges. It successfully managed to disable a significant portion of these centrifuges, which numbered in the thousands [8].

By the middle of the 21st century, digital technology had become deeply embedded in various aspects of political and economic life, including industrial operations, manufacturing, government functions, and military oversight. The array of harmful programs in the realm of information technology is as diverse as the legitimate uses of this ubiquitous technology, leading to the conflation of various threats in discussions about cybersecurity. The majority of malicious activities in cyberspace are driven by

1Department of Computer Engineering Lebanese French University Erbil,Iraq
zina.0174810@gmail.com
2Department of Information Technology Choman Technical Institute Erbil, Iraq
naska.324290@gmail.com

economic motives. Beneficial actions encompass commercial activities such as email spam, manipulation of search engine results, theft of electronic credentials or bank accounts, as well as the acquisition of sensitive government data. The crux of the cyber revolution argument lies in the continuous targeting of intellectual property and trade secrets, potentially empowering aggressors to undermine more prominent targets [9].

The attack referred to as Operation Aurora took place in China between mid-2009 and early 2010. It constituted a series of cyber-attacks aimed at the top 100 most significant companies, including Google, Adobe, Juniper, and others. Advanced malware was employed to steal critical intellectual property. Following this attack, Google indicated that it might withdraw from China and close its office there if an uncensored version of its search engine wasn't operational in the country (which was seen as a significant frustration). Details about the attack have not been fully disclosed, but it was primarily aimed at accessing Gmail accounts managed by individuals in China [8].

Cyber warfare surpasses the traditional realm of wartime military operations, extending its reach to disrupting essential industrial control systems. The cyber revolution typically involves small groups backed by governments or even terrorist hackers who employ similar malicious techniques to those used for password cracking, but instead target factory automation and military infrastructure [9].

2. Attack Modeling

Cyber-attack modeling, although not yet realized, offers the potential to save time, resources, and costs for systems. Attack modeling methods used to analyze cyber-attacks can be classified into Attack Graphs, Attack Vectors, Attack Surfaces, the Diamond Model, OWASP's Threat Model, and the Kill Chain. In this paper, we will discuss three cyber-attack modeling techniques: the Diamond Model, the Kill Chain, and the Attack Graph. The Diamond Model was chosen for its simplicity, consisting of only four major components. Kill Chains have been employed by the US Department of Defense for many years in both cyber defense and warfare. On the other hand, Attack Graphs or trees are traditional methods rooted in the fundamental search capabilities of computer systems. The modeling of cyber-attacks and the anticipation of risks pose significant challenges in protecting corporate systems [10].

A. Diamond Model

The Diamond Model, one of the emerging models for cyber-attacks, is expounded upon in this analysis. Attackers target victims based on two primary forces, differing from the stepwise approach of Kill Chains or Attack Graphs. This model encompasses four key elements: attack, infrastructure, capability, and victim. Moreover, this model is augmented with meta-properties such as timestamp, phase, result, directions, methodologies, and resources [10].

B. Kill Chain

The Kill Chain is a form of attack modeling that depicts attacks as a sequence of actions. The US Department of Defense defines the Kill Chain as a method of attacking a target. They outline the Kill Chain within distinct stages: Discover, Fix, Track, Target, Engage, and Assess. In the realm of Cyber Security, the Kill Chain is employed to outline the steps of an attack along with a corresponding countermeasure framework. The Kill Chain is divided into seven stages of attack: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Action and Objectives [10].

C. Attack Graph

Attack Graphs are conceptual diagrams used to analyze how a target might be attacked. They are essential for assessing cyber vulnerabilities within computer systems or networks. An Attack Graph is a tree-structured diagram featuring multiple levels of offspring stemming from a singular root. This modeling approach is a traditional method employed by many to uncover vulnerabilities, to establish an effective defense through systematic system analysis. Attack Graphs consist of nodes and can be intricate in nature, working in tandem during a specific attack. This type of attack diagram proves beneficial in numerous aspects of computer system security, including intrusion detection, forensic analysis, risk assessment, and cyber defense. An Attack Graph assists a system manager in determining [10]:

- Network vulnerabilities

- Possible attack scenarios

- A series of actions to counteract attackers targeting their objective

The primary purpose of an Attack Graph is to aid in identifying potential system attacks [10].

3. Cyber Warfare

1. Countries In Cyber Warfare

- The goal of the country's cyber management is to identify and safeguard numerous covert access points across the nation, either for espionage or countering cybercrime. The following are key active countries in cyber warfare [8]:

- United States of America: The United States, as one of the most technologically advanced countries globally, is highly susceptible to cyber-attacks and heavily relies on the Internet for conducting modern business operations. In the US, various adversaries consistently seek classified information, exploit vulnerabilities that undermine national security, and employ them for their advancement. The United States has a robust cyber defense strategy. Alongside defensive measures, some significant attacks are attributed to the country, including the development of highly dangerous and intricate malware attacks [8].

- China: China has recently been characterized as a prominent player in the realm of hacking by mainstream media. The assessment of China's cyber capabilities is often viewed from a strategic standpoint, with discussions about its potential impact on global power dynamics. Many attacks reported in the media are attributed to China, and there is a deliberate use of cyber warfare to counteract the United States' influence [11].
- Russia: Russia has been subjected to numerous Denial of Service (DOS) attacks. Weapons such as "Ouroboros," responsible for disrupting Ukrainian government computers in 2014, and another disruptive hacking effort named "Sandstorm," which targeted the Ukrainian power grid in 2015, have been linked to malware attacks. Some sources suggest that these attacks may be attributed to Russia. The Russian Hacking Group is also alleged to have exploited vulnerabilities in Microsoft OS and targeted communication companies, Ukraine, the European Union, and various software monitoring tools. The veracity of these claims remains unconfirmed [8].

2. *War With Cyber Weapons*

A. Cyberspace

In the context of systems operating in cyberspace, a clear comprehension of battlespace information is vital. Utilizing cyberspace within battlespace necessitates an intelligent system capable of employing automated analysis to select metrics. Once battlespace knowledge is amalgamated, individuals within the organization must decide what to measure and how to measure it. In such instances, these individuals must possess experience and a comprehensive understanding of strategies [12].

B. Reality of cyberweapon

Stuxnet stands as a prime example of a cyber weapon designed and employed for cyber warfare. Contrary to the perceptions of many non-technical individuals, the creation of an attack similar to Stuxnet is more achievable than one might expect. This underscores the crucial role that cyber warfare occupies. Stuxnet is a sophisticated assembly of malware that was discovered inadvertently in 2010 by an antivirus researcher. The detailed analysis commenced that year and has persisted since. Current conjecture suggests that the malware first emerged in 2009. In 2012, the involvement of the US in the Stuxnet attack became apparent through research conducted by the press.

Stuxnet operates as a covert control system capable of disrupting the physical processes under the supervision of a specific Siemens duration management system. The bulk of its malicious activities involves the insertion of code into an executable system (a DLL named s7otbxox.dll), followed by self-upload and concealing from detection. This classic "DLL injection/interpreter attack" functions as a conduit for data exchange between a Programmable Logic Controller (PLC) and the SIMATIC supervisory system. Think of it as an intermediary script where the embedded code observes and manipulates all data transmitted between the PLC and the control system. This code enables execution on a targeted PLC (including memory content checks, CPU type verification, process type control, and authorization of specific target controllers). Upon identifying a target, the code is directly inserted into the PLC's Ladder Logic (LL). This type of code has a direct impact on the physical process. By default, LL code can be employed to manipulate the physical processes [13].

C. Attack with Flame

The virus, which took nearly two years to detect, was eventually uncovered and named "Flame." This virus can spread to other computers through local Internet connections or pen drives. In 2012, the renowned antivirus company Kaspersky Lab identified this program. The virus was attributed to government-sponsored cyber espionage in Iran and various other Middle Eastern nations. It possesses the ability to gather diverse information from a computer, including personal details, manipulate computer systems, browse the internet, log online user activities, access banking services, and obtain passwords. The revelation indicated that nations were embarking on the use of malicious software to amass information from countries of interest [8].

D. Espionage

Espionage entails infiltrating a target system to extract sensitive or classified data. This process can be either social or technical in nature. This field of activity is historically significant and is referred to as human intelligence and signal intelligence in the realm of secret services. While a certain degree of technical complexity is required for espionage, it is typically less demanding than confronting sophisticated barriers. The primary objective is not to accomplish the target itself, but rather to gather data that can be employed to design more precise tools or strategies. Notably, a significant portion of political cybersecurity incidents involve espionage. Due to the often dubious identity of the attacker, assigning an accurate name for such operations proves challenging. For instance, "Titan Rain" is the codename used by the United States government to reference a series of attacks on military and governmental computer systems in 2003, spanning several years. It is believed that Chinese hackers managed to breach numerous firewalls within defense contractors such as the Pentagon, the State Department, Homeland Security, and Lockheed Martin. Uncertainty prevails regarding whether the Chinese security agency was complicit in the intrusion or if the infiltrator intended to mask their true identity by using a Chinese-based computer [14].

4. Methodology

1. Combining Firewalls and IDS for Enhanced Cybersecurity Against Cyber Warfare

In the ever-evolving landscape of cyber warfare, a multi-layered defense approach is crucial to effectively counter emerging threats. Combining firewalls and intrusion detection systems (IDS) offers a powerful methodology for bolstering cybersecurity by providing both preventive and proactive detection capabilities. This methodology aims to create a synergistic defense mechanism that addresses known and unknown threats in the future of cyber warfare. Figure 1 illustrates the collaborative approach of combining firewalls and intrusion detection systems (IDS) to fortify cybersecurity against evolving cyber warfare threats. The diagram depicts the key components and interactions of this integration.

2. Firewalls as the First Line of Defense:

Firewalls are deployed at network perimeters to regulate incoming and outgoing traffic based on predefined rules. This initial layer serves as a gatekeeper, blocking unauthorized access attempts, malicious payloads, and known threats. By filtering traffic and enforcing access controls, firewalls significantly reduce the attack surface and prevent many common cyber attacks.

3. Intrusion Detection Systems (IDS) for Real-time Monitoring:

IDS continuously monitors network traffic and system activities, analyzing patterns and behaviors to detect potential intrusions and anomalies. This real-time analysis goes beyond the static rules of firewalls, allowing for the identification of zero-day attacks, sophisticated tactics, and evasive techniques. IDS raises alerts when suspicious activities are detected, enabling timely responses to mitigate threats.

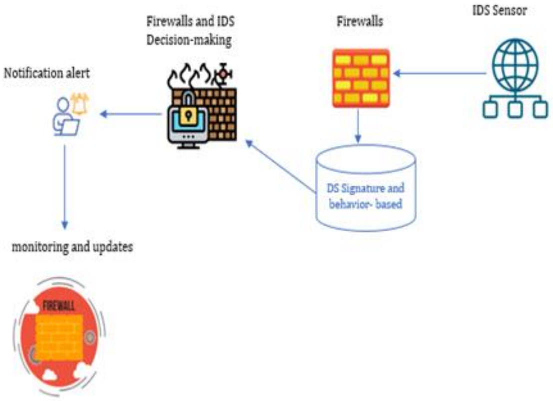


Fig 1: Synergistic Integration of Firewalls and Intrusion Detection Systems (IDS) for Enhanced Cybersecurity

2. Ethics In Cyber Ware

Computer technology has advanced to a level where it necessitates not only guidance but also a comprehensive ethical framework. Consequently, cyberwarfare must be governed by ethical policies that justify its application. One of the proposed policies is a "no first use" principle for cyber-attacks, similar to the approach taken with other hazardous weapons. Another suggestion is that cyber-attacks should only be employed as responses to cyber-attacks, with the response being proportional to the initial attack. Additionally, a commitment might be made to abstain from using cyber weapons due to their potential for widespread use. While employing cyber weapons, further policies could demand specific signatures to ascertain accountability for the attacks and their intended targets, or to ensure that attacks can be readily reversed. Moreover, there is a need to establish policies regarding the classification of participants in cyber warfare, whether they are soldiers, spies, civilians, or fall under other categories [15].

In the context of military operations, conducted for civilian safety or national security, states frequently adhere to specific regulations to prevent the use of dangerous weaponry, minimize harm to civilians, and safeguard essential infrastructure like hospitals. Such regulations, often referred to as the law of armed conflict, were established to combat the horrors of warfare and address issues arising both mentally and physically during warfare. Given the inclusion of cyber warfare as a viable option, it becomes imperative to either adapt or reinterpret existing laws to accommodate their unique characteristics or formulate entirely new regulations suited to the distinct nature of cyber warfare.

Furthermore, it's essential to recognize that traditional military law, typically governing warfare involving conventional weapons, primarily addresses the conduct of war between states. In the realm of cyber-war, we might face adversaries who appear to function like state-sponsored entities but are driven by the motives of individuals or small groups. The concept of Jus ad bellum, which encompasses the right to wage war, becomes relevant here. This principle is associated more with martial law than with specific organizations, including terrorist groups or other entities. The criteria for Jus ad bellum include right authority, right intentions, likelihood of success, proportionality, and just cause. The idea of the "right to fight" holds more global applicability in the context of martial law [16].1) *Right Authority:* The rule of law that permits us to act is based on a combination of legislative, national, and international agreements, treaties, and various other organizations.

2) *Right Intention:* A good motive in war states that we can use or threaten another government against one another.

3) *Probability of Success:* The rule of the probability of success indicates that power cannot be used for a meaningless war effort.

4) *Last Resort:* last resort principles specify that power can be used only when negotiations have failed, or seem to be ineffective

5) *Proportionality:* The proportional principle says that the benefits of war should be greater than the damages that result.

Taddeo tries to overcome the challenges of cyber warfare efforts by introducing three principles that make up the "Just Cyber War". These principles are in line with the concept of knowledge. Taddeo defines this as a place where inanimate objects, metaphysics, and light are morally evaluated [17].

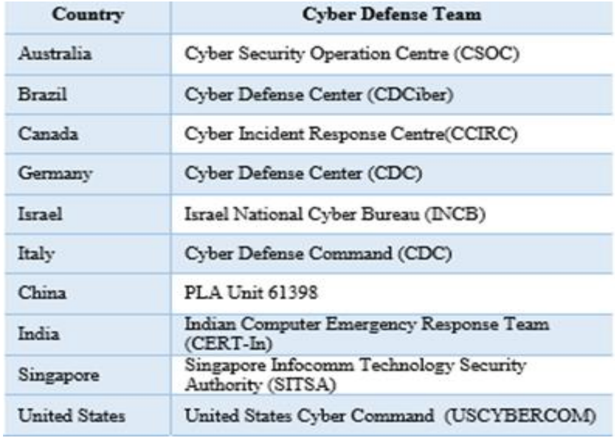
- The cyber war must be fought only for these wars which interfere with or undermines the influence of Integration.
- Cyber wars must be fought to protect the environment.
- The cyber war should not be banned to improve the efficiency of nature.

Point 1 represents the idea that cyber warfare should be able to remove the negative pressures on inflation. The following two points reflect the view that cyber warfare should only be used to restore post-traumatic Illness, while not improving health beyond its normal range. Cyber war can be ethically justified as long as the Info sphere protects your health [17].

3. Countries' Defense System

By being uncovered to developed threats, management around the world has enriched their security enclosure and, in this course, some countries have created significant progress in knowing new types of appropriate threats and have created a completely new cyber defense team that is capable to defend and offend when require. Table.1 describes some of the best cyber defense teams [8].

TABLE I. CYBER DEFENSE IN COUNTRIES



Country	Cyber Defense Team
Australia	Cyber Security Operation Centre (CSOC)
Brazil	Cyber Defense Center (CDCiber)
Canada	Cyber Incident Response Centre(CCIRC)
Germany	Cyber Defense Center (CDC)
Israel	Israel National Cyber Bureau (INCB)
Italy	Cyber Defense Command (CDC)
China	PLA Unit 61398
India	Indian Computer Emergency Response Team (CERT-In)
Singapore	Singapore Infocomm Technology Security Authority (SITSA)
United States	United States Cyber Command (USCYBERCOM)

5. Future Work

The goal of the country's cyber administration is to identify and safeguard numerous covert access points to counter-espionage or cybercrime. Cybersecurity holds paramount importance for military operations across land, sea, sky, and space. The development and successful deployment of potent cyber weapons are closely linked to technical vulnerabilities in security. Constructing security on a contemporary foundation that exclusively involves software can impede the swift evolution toward the ongoing landscape of cyber warfare. In forthcoming endeavors, we will present methodologies and techniques aimed at mitigating cyber-attacks.

6. Conclusion

The increasing discussion about cyber warfare would not come as a surprise to those who have followed the news in the last decade. Utilizing cyberspace as a battlefield involves an intelligent system that enables the selection of metrics through automated analysis. Numerous nations have simultaneously developed strategies for cyber warfare as part of their defensive measures against potential attacks. The case of Stuxnet clearly demonstrates the programming and usage of cyber weapons for cyber warfare purposes. However, espionage entails clandestine efforts to infiltrate secure systems with the goal of extracting sensitive and safeguarded information. this study investigates the potential of synergizing firewalls and Intrusion Detection Systems (IDS) as a comprehensive cybersecurity approach for the impending era of cyber warfare. Firewalls, functioning as primary defense mechanisms, establish a barrier between networks while overseeing and managing incoming and outgoing data flow. On the contrary, IDS operates as a vigilant sentinel, discerning unusual activities or unauthorized network access. By amalgamating these two distinct technologies, a robust defense stance can be fortified. This collaborative strategy harnesses the preventive prowess of firewalls and the real-time threat identification capacity of IDS. Beyond technical implementation, the study also underscores the necessity of organizational frameworks, training, and ongoing adaptation to the evolving threat landscape.

References

[1] Andress, Jason, and Steve Winterfeld. Cyber warfare: techniques, tactics, and tools for security practitioners. Elsevier, 2013.

[2] Carr, Jeffrey. Inside cyber warfare: Mapping the cyber underworld. " O'Reilly Media, Inc.", 2011.

[3] Christian Czosseck, and Kenneth Geers, eds. The virtual battlefield: perspectives on cyber warfare. Vol. 3. Ios Press, 2009.

[4] Gazula, Mohan Buvana. Cyber warfare conflict analysis and case studies. Diss. Massachusetts Institute of Technology, 2017.

[5] Poirier, William J., and James Lotspeich. Air Force cyber warfare: now and the future. AIR UNIV MAXWELL AFB AL AIR FORCE RESEARCH INST, 2013.

[6] Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. Introduction to cyber-warfare: A multidisciplinary approach. Newnes, 2013.

[7] Hjortdal, Magnus. "China’s use of cyber warfare: Espionage meets strategic deterrence." Journal of Strategic Security 4.2 (2011): 1-24.

[8] S. K. Sahu, A. Anand, A. Sharma, and N. Nautiyal, "A review: Outrageous cyber warfare," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 70-74.

[9] Lindsay, Jon R. "Stuxnet and the limits of cyber warfare." Security Studies 22.3 (2013): 365-404.

[10] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, "Cyber-Attack Modeling Analysis Techniques: An Overview," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, 2016, pp. 69-76.

[11] Hjortdal, M., China’s use of cyber warfare: Espionage meets strategic deterrence. Journal of Strategic Security, 2011, pp.1-24.

[12] Bryant, Adam, and Michael Grimaila. "Developing a Framework to Improve Information Assurance Battlespace Knowledge." ICIW2007-2nd International Conference on Information Warfare & Security: ICIW2007. Academic Conferences Limited, 2007.

[13] McGraw, Gary. "Cyberwar is inevitable (unless we build security in)." Journal of Strategic Studies 36.1 (2013): 109-119.

[14] Eidman, Christopher R., and Gregory S. Green. Unconventional cyber warfare: cyber opportunities in unconventional warfare. NAVAL POSTGRADUATE SCHOOL MONTEREY CA, 2014.

[15] Rowe, Neil C. "Ethics of cyberwar attacks/Chapter in Cyber War and Cyber Terrorism." Monterey, California. Naval Postgraduate School, 2007.

[16] Andress, Jason, and Steve Winterfeld. Cyber warfare: techniques, tactics, and tools for security practitioners. Elsevier, 2013.

[17] Robinson, Michael, Kevin Jones, and Helge Janicke. "Cyber warfare: Issues and challenges." Computers & Security 49 (2015): 70-94.

[18] Dasi , S. ., & Rao, G. M. . (2023). Design and Analysis of Metamaterial Absorber using Split Ring Resonator for Dual Band Terahertz Applications. International Journal on Recent and Innovation Trends in Computing and Communication, 11(1), 128–132. https://doi.org/10.17762/ijritcc.v11i1.6059

[19] Prof. Sharayu Waghmare. (2012). Vedic Multiplier Implementation for High Speed Factorial Computation. International Journal of New Practices in Management and Engineering, 1(04), 01 - 06. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/8