Advancing Cyber Resilience: Bridging the Divide Between Cyber Security and Cyber Defense

Md Faisal Ahmed[1], Abul Hasan Molla[2], Md Riaj Uddin[3], Toufecur Rahman Chowdhury[4]

[1]Doctor of Management, International American University, Los Angeles, California.
[2]MBA in Business Analytics, International American University, Los Angeles, California.
[3]Bachelor of Business Administration in Marketing, Shahjalal University of Science & Technology, Sylhet.
[4]MBA in Marketing, Shahjalal University of Science & Technology, Sylhet.

Abstract

The field of cyber security is characterized by its diverse range of techniques, tools, and concepts, and it is closely interconnected with the security of information and operational technology. The distinguishing characteristic of cyber security is in the adoption of offensive information technology strategies with the intention of achieving adversarial objectives. Nevertheless, the broad and unrestricted utilization of the word "cyber security," frequently used interchangeably with information security or IT security, has the potential to create misunderstandings among both consumers and professionals in the security field. The merging of these disciplines obscures important differences between them, notwithstanding their interconnectedness.

This paper advocates for a significant suggestion aimed at security leaders: to limit the usage of the word "cyber security" to refer specifically to security practices that are closely intertwined with and dependent on information technology and operational technology environments and systems, solely for defensive objectives. In the context of computer network security, cyber defense plays a crucial role as a mechanism that addresses adversary acts, protects key infrastructure, and ensures information assurance for a wide range of enterprises, government agencies, and interconnected networks [3].

This study primarily examines the interplay between cyber security and cyber defense, emphasizing the development of the notion of cyber resilience. This paper presents a new conceptual framework for understanding cyber resilience, shedding light on the complex interplay between these several domains. Furthermore, in this model, the authors critically examine the tactics and measures necessary to enhance the resilience of cyber security and cyber defense in the face of escalating cyber threats. The article examines CRRT and MACS history, purpose, and future directions. At EU level, through the policy of innovation there is opportunity for more robust resilience and joint defense against the ever-changing landscape of threat.

Keywords: Cyber Resilience, Cyber Security, Cyber Defense, European Union, Rapid Response Teams

1 Introduction

However, cybersecurity is a term which originated from military circles but has undergone changes in the last ten years. Nonetheless, it seems that it has recently spread into different spheres, and this has resulted in partial deformation of its essence. Cybersecurity involves more than just ensuring that information is secure. Also included are OT security and IT security to shield digital assets. Defending effectively against cyber threats requires comprehensive actions to minimize the appeal of vulnerable channels of attack, identifying important objects and confidential data, instituting safeguards to make attacks more expensive, developing reliable means of attack detection, and planning quick countermeasures [2].

In addition, this is also another area of cyber defense where there are technical tests used to check for routes of attacks as well as weak points [3]. Cybersecurity within the EU builds upon awareness, resilience, and response for adaptive measures against dynamic menaces. Additionally, in a bid to further improve its capabilities of detecting and understanding malicious activities as well as building the resilience of its critical infrastructure, society and institutions, the EU attempts to intensify its efforts towards this end. This is essential in bolstering EU's resilience against as well as recovery after cyber-attacks. As such, it is essential that Member States work together as well as develop a partnership between the EU, its Member States, partner countries and NATO.

1.1 Problem of The Statement

The purpose of this paper is to explore the dynamics between cybersecurity, cyber defense, and cyber resilience in an era marked with evolving security threats and limited countermeasures. The paper will also shed light on the regulatory framework for the EU Cyber Rapid Response Teams and Mutual Assistance in Cyber Security, providing a new perspective on cyber security and cyber defense at the EU level.

1.2 Objectives

1. Focusing on change from conventional cybersecurity towards pervasive cyber resilience, based on strategic perspective and preparation for adaptable dangers.
2. A review of the evolution and functionality of the EU CRRTs and MA in CyS projects aimed at strengthening cyber event management as well as promoting collaboration within the EU.

2 Methodology

This study adopts a systematic and model driven approach in order to holistically address the complex terrain of cyber security and cyber defense and role in building cyber resilience in the current information communications ecology. All these steps and methods were applied in building the Conceptual Cyber Resilience Model.

2.1 Analysis of Cyber Défense

To begin with, this research entails a detailed analysis of the environment under study. This environment then undergoes cyber-defense analysis to establish possible risks against it. This analysis provides a basis for designing and implementing appropriate security strategies that could curb such attacks. In this context, the paper seeks to provide a different perspective towards cyber resilience in the modern information communication environment.

2.2 Model-Driven Approach

A modelling-based approach and technique is applied in developing the Conceptual Cyber Resilience Model. This way creates a logical framework for incorporating major issues in cyber-resilience, cyber-security, and cyber-defense.

2.3 Perspectives on Cyber Resilience

The aim of this study is to offer perspectives toward cyber security and cyber defense, aimed at achieving cyber resilience in the modern information communication environment. Eventually, this leads to the creation of a unique conceptual cyber resilience model. It constitutes an approach and insights on innovative model of cyber security that considers EU Cyber Rapid Response Teams (CRRTs) among a possible solution to cybersecurity [6]. These are the CRRT which serve as a form of helping one another by sharing human resources, operations, and technology.

2.4 Cyber Défense Focus

Within the scope of cyber defense, this study emphasizes the critical roles of prevention, detection, and timely response to cyberattacks or threats. The objective is to ensure the integrity of infrastructure and the protection of sensitive information. Given the escalating volume and complexity of cyber threats, cyber defense emerges as a crucial aspect for organizations and entities, fostering an environment where processes and activities can proceed securely and without the looming specter of threats [15]. Furthermore, cyber defense enhances the efficient utilization of security resources and expenditures, particularly in critical areas.

2.5 Cyber Rapid Response Teams (CRRTs) and Mutual Assistance in Cyber Security

Cyber threats are getting worse, and it is getting harder to stop them. That is why Lithuania has put forward a project to the EU Council on Defense called "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security." The goal of this initiative is to improve cybersecurity in both the United States and Europe. The project's core objective is the establishment of multinational rapid response cyber teams comprising cyber defense experts from participating countries.

A distinguishing feature of this project is its emphasis on resource-sharing among participating nations, surpassing many existing multinational initiatives in cyber defense that primarily focus on information exchange. The project encompasses research on legal procedures related to cyber security in the EU, the organization of tabletop exercises (cyber crisis simulations), and the development of cyber defense tools. As of the status, six EU countries have joined the project (Croatia, Lithuania, Estonia, Poland, Netherlands, Romania), with seven states observing its progress (Finland, Belgium, Italy, France, Spain, Greece, Slovenia) [15].

3 Problem Solution

In an increasingly interconnected digital world, traditional cybersecurity measures alone are no longer sufficient to protect against the evolving landscape of cyber threats. The contemporary paradigm demands a holistic strategy that encompasses defense, prevention, and response—a strategy that goes beyond mere security to embrace the concept of resilience. Cyber resilience, as a fundamental approach, evaluates the preparedness and capabilities of digitally networked systems to withstand threats not only during the event but also before and after. It is crucial to understand that resilience is not synonymous with recovery;

instead, it is a continuous, long-term endeavor integrated into overall business and organizational strategies [1].

3.1 Long-term View and Durability

Cyber resilience is based on its ability to keep going for a long time. A strong strategy includes long-term planning that thinks about what can go wrong and how to stop it before, during, and after a risk happens. You need to think about the long term to make sure that the strategies you use are complete and adaptable enough to work in different situations [2]. Approaches to strategy that look at all stages of a threat are naturally more resilient than approaches that only look at one point in time.

3.2 Broadening the Conversation

Leadership is the most important thing that can affect the direction and growth of cyber resilience. It is important to move beyond the usual conversations about information security and have a bigger conversation about how resilient whole networks are. Having a bigger picture view is important for making sure that the economy and society can handle problems. This is especially true now that new technologies like AI, the internet of things, and quantum computing are appearing and presenting new risks. It is very important for businesses to include the ability to change their plans to deal with new problems caused by quickly disrupting technology in their long-term planning [2].

3.3 System-Level Approach

There is a notable contrast between the access control component of cybersecurity and the strategic, forward-looking mindset that is encompassed by cyber resilience. The concept of cyber resilience necessitates the adoption of a comprehensive approach, which entails a shift in focus from singular enterprises to interconnected systems. In the context of networked settings, it is important to recognize that the presence of a vulnerability in a single node has the potential to compromise the overall security and resilience of the entire network. Hence, it is imperative to acknowledge the significance of resilience in the framework of public goods or commons, with a particular emphasis on the value of collaborations [2]. These relationships have the potential to go beyond commercial enterprises and encompass regulatory bodies, law enforcement agencies, and government officials, thereby exemplifying the shared need to establish and sustain cyber resilience.

3.4 Responsibility and Strategy

The concept of cyber resilience is inherently rooted in the principles of risk management, lacking a clearly defined initiation or termination phase. However, it undergoes a transformation because of the development of a strategic methodology and the execution of risk-transfer mechanisms. Leadership at the top echelons of both private sector and government entities carries the onus of acknowledging the importance of preventing and minimizing cyber threats. The integration of collaboration across stakeholders is crucial in order to enhance cyber resilience. However, it is the responsibility of organizational leaders to ensure that this collaboration is effectively included into the plan [9].

3.5 Known and Unknown Threats

Historically, cybersecurity strategies have mostly concentrated on addressing established threats, which continues to be an indispensable element of a comprehensive cybersecurity framework. Nevertheless, within the swiftly changing realm of cyber dangers, it is equally imperative to cultivate sophisticated capacities for predicting, apprehending, and gaining knowledge from unfamiliar hazards. Every security challenge, regardless of its familiarity or novelty, is associated with a distinct solution. Through the incorporation of values obtained from systematic evaluations of system security, these issues can be classified as "known knowns" (pertaining to information security), "known knowns" (pertaining to cyber security), and "unknown unknowns" (pertaining to cyber resilience) [4].

3.6 Cyber Resilience Model

Introducing the Conceptual Cyber Resilience Model is meant to create a structured way to understand and practice cyber resilience. There are three separate parts to the model this study presents: information security, cyber security, and cyber resilience. The information security dimension is made up of three main parts: availability, integrity, and confidentiality. These three parts are often called the "CIA triad." This part looks at threats and responses that have to do with the CIA triad. However, the cyber security dimension deals with more complicated threats that do not fit into the CIA triad. These include Advanced Persistent Threats (APTs) and how to protect against them. Lastly, the cyber resilience dimension includes threats that cannot be predicted or controlled, as well as the ways to deal with them [4].

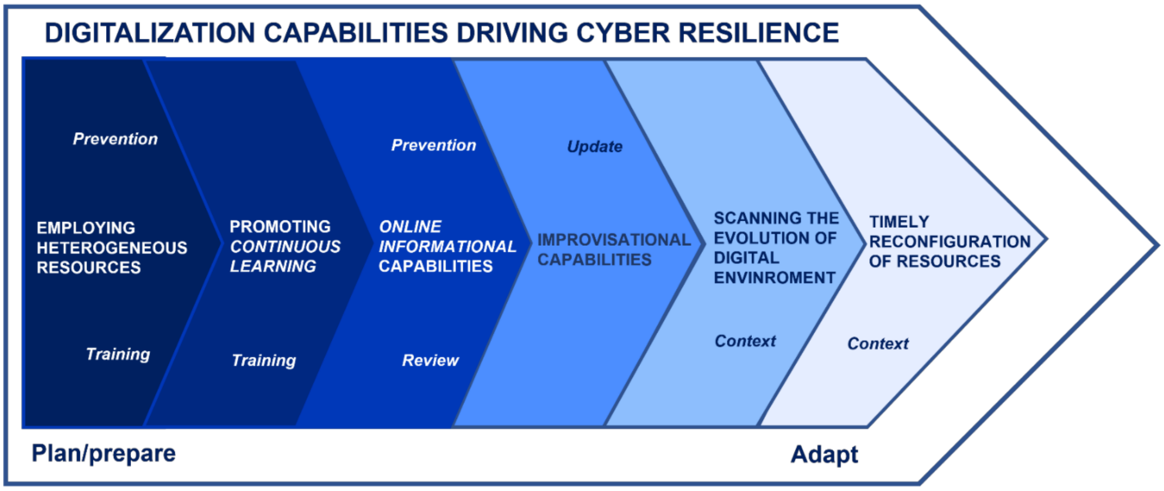
DIGITALIZATION CAPABILITIES DRIVING CYBER RESILIENCE
Prevention
EMPLOYING HETEROGENEOUS RESOURCES
Training
PROMOTING CONTINUOUS LEARNING
Training
Prevention
ONLINE INFORMATIONAL CAPABILITIES
Review
Update
IMPROVISATIONAL CAPABILITIES
SCANNING THE EVOLUTION OF DIGITAL ENVINRONMENT
Context
TIMELY RECONFIGURATION OF RESOURCES
Context
Plan/prepare
Adapt

Fig. 1: Cyber Resilience Model

In order to deal with problems that come up out of the blue, systems often support people's abilities to change how things are done, come up with new ways to organize things, and add new technology [14].

3.7 Transitioning to the Unknown Unknowns

As cyber risks get worse, systems need to change and employees need to be given the power to change current processes, organizations, and technologies. Systems must be able to adapt and respond quickly in order to deal with problems that come up out of the blue. One important part of cyber resilience is the ability to adapt to unplanned events. This makes sure that businesses can handle new situations well and keep their operational integrity (6).

3.8 Creation, Performance, and CRRT Capability

Making the EU's Cyber Rapid Response Teams (CRRTs) and the Mutual Assistance in Cybersecurity project work together is a very innovative step toward building a strong cyber infrastructure. This is one of the most advanced projects approved under the EU Permanent Structured Cooperation (PESCO) framework. The goal of PESCO is to improve security and defense cooperation between EU member states that have specific military obligations and capabilities [10].

The Declaration of Intent in the Field of Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity makes it clear how important it is for people to work together voluntarily in the cyber domain. Sharing information, training together, helping each other with operations, doing research and development, and building up joint capabilities are all important parts of it [12]. As part of their regular Computer Emergency and Response Teams (CSIRTs) and CRRTs, designated experts work together with EU organizations like the CSIRT Network, the European Union Agency for Network and Information Security (ENISA), and CERT-EU to support current cyber security efforts [8].

The CRRTs operate within the scope agreed upon by member states (MS), embodying a civil-military nature that fosters a culture of cooperation in the cyber domain and expands the concept of cyber defense within the EU. Equipment enhancements are also considered, with the potential development of a common Cyber Toolkit designed to detect, recognize, and mitigate cyber threats. Funding from the European Defense Fund and other EU sources is being explored to support the development of this toolkit, fostering industrial cooperation among participating MS and bolstering the European cyber security industry [11].

The successful signing of the Memorandum of Understanding in January 2020 marked a significant milestone, and the CRRTs reached full operational capabilities in 2021. The Ministry of National Defense of the Republic of Lithuania serves as the lead nation for this project, exemplifying the collaborative spirit required to enhance cyber resilience on a broader scale [11].

4 Discussion

Modern societies have become inextricably linked with communication and information technology, where people are interconnected through various technologies facilitating the exchange of text, images, and sound. This interconnectedness, including the expanding influence of the Internet of Things (IoT), has transformed deviations in the proper functioning of these systems from mere technical glitches into global security threats. Consequently, societies have developed a comprehensive array of activities and measures collectively termed cyber security to counter these threats.

The key to effectively addressing cyber risks lies in normalization. Cyber risks should be treated like any other risks that organizations must manage to achieve their objectives. Business and government leaders must adopt a resilience-focused mindset for two compelling reasons. Firstly, it helps mitigate the catastrophic consequences associated with an all-or-nothing approach to cyber risks, where the sole focus is on preventing network breaches. Secondly, it broadens the conversation beyond the confines of information technology or information security, recognizing that cyber resilience is an integral part of long-term strategic planning [2].

Promoting a holistic cyber resilience approach necessitates a continual strategic dialogue within organizations, involving both technology and strategic leaders. This approach, akin to "cybermedicine," enhances readiness, minimizes redundancy, and ultimately boosts efficiency and effectiveness. In contrast, traditional security measures are often seen as binary, where something is either secure or not, and are typically confined to a limited technical function aimed at keeping unauthorized users out of a networked system [2].

The most challenging aspect of cyber security is dealing with the unknown. Former US Secretary of Defense Donald Rumsfeld eloquently articulated this challenge in 2002, distinguishing between "known knowns," "known unknowns," and the most daunting category, "unknown unknowns." These are the threats that organizations are unaware of and, therefore, cannot prepare for in advance [5].

Emerging technologies offer a departure from traditional approaches, presenting the capability to protect systems from serious threats by learning what constitutes normal behavior for an organization and its users. Unlike conventional rule-based and signature-based methods, these technologies can identify emerging anomalies and threats that conventional approaches might overlook. They excel in dealing with uncertainty and provide adaptive protection against insider threats and advanced cyberattacks [11].

The development of the European Union Cyber Rapid Response Teams is progressing toward the final stages of its development phase. Representatives from EU member states involved in the project have engaged in extensive discussions, exchanging ideas and formulating plans for a common cyber toolkit. This toolkit will equip participating countries with essential cyber incident management capabilities. The discussions encompassed the unique needs of each participant and the overarching shared vision. Participants also addressed funding mechanisms for the toolkit and laid out a comprehensive development plan. The toolkit will serve as a foundational element in ensuring the lasting success of the CRRT(s) project [8].

Future research endeavors are poised to explore and establish efficient and effective processes for achieving agile cyber resilience in security information systems. This resilience aims to cope with unforeseeable and unpredictable events, often referred to as "unknown unknowns," in both the internal and external environments of the system as a whole. Following the establishment of the Rapid Response Team as a foundational step, upcoming research will emphasize the creation of opportunities and avenues for mutual assistance and cooperation in responding to significant cyber incidents. These efforts will involve information sharing, joint training, mutual operational support, and the development of shared capabilities [7].

In essence, the evolution of cyber resilience is crucial in an environment where threats continuously evolve and expand. It necessitates a dynamic and adaptive approach, one that views cyber risks as an integral aspect of an organization's broader strategic objectives, fostering a proactive and collaborative stance to safeguard against the unknown challenges of an interconnected digital world [2].

5 Conclusion

This paper has explored the strategies, processes, and mechanisms required to achieve cyber resilience in the face of emerging security risks in today's complex digital landscape. Within the domain of cyber resilience, we have introduced the innovative Conceptual Cyber Resilience Model, encompassing both information security and cyber security considerations. Our ongoing investigations are oriented towards the development of efficient and effective processes that imbue security information systems with agile characteristics, making them adaptable, aware, flexible, and productive in order to respond to unforeseeable and unpredictable events, often referred to as "unknown unknowns," within both internal and external system environments.

Throughout the construction of this novel conceptual model, we have elucidated the creation and execution of the EU Cyber Rapid Response Teams and Mutual Assistance in Cyber Security initiative, thereby introducing a pioneering approach to cyber security and cyber defense at the European Union level [13]. This initiative has been situated within the broader context of the Cyber Resilience Model, highlighting the crucial roles played by various actors at all levels of the system hierarchy in achieving the overarching goal.

5.1 Developments for Future

Subsequent research will extend into the realms of personal, network, and organizational cyber security management. The foundational Conceptual Model of Cyber Resilience holds paramount importance, as it serves as the conduit for incorporating knowledge and, subsequently, enhancing the efficiency and effectiveness of cyber security and cyber defense processes. The aim is to diminish the prevalence of "unknown unknowns," gradually transforming them into "known unknowns" and "known knowns." This evolutionary trajectory is essential for advancing our capacity to navigate the ever-evolving cyber threat landscape.

6 References

1. Smith, S. (2023, February). Towards a scientific definition of cyber resilience. In *International Conference on Cyber Warfare and Security* (Vol. 18, No. 1, pp. 379-386).
2. Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & industrial engineering*, *149*, 106829.
3. Enoch, S. Y., Moon, C. Y., Lee, D., Ahn, M. K., & Kim, D. S. (2022). A practical framework for cyber defense generation, enforcement and evaluation. *Computer Networks*, *208*, 108878.
4. Greiman, V. (2023, June). Known Unknowns: The Inevitability of Cyber Attacks. In *European Conference on Cyber Warfare and Security* (Vol. 22, No. 1, pp. 223-231).
5. Dacorogna, M., Debbabi, N., & Kratz, M. (2023). Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. *European Journal of Operational Research*.
6. Amini, M., & Bozorgasl, Z. (2023). A Game Theory Method to Cyber-Threat Information Sharing in Cloud Computing Technology. *International Journal of Computer Science and Engineering Research*, *11*(4-2023).
7. Mallaboyev, N. M., Sharifjanovna, Q. M., Muxammadjon, Q., & Shukurullo, C. (2022, May). INFORMATION SECURITY ISSUES. In *Conference Zone* (pp. 241-245).
8. Ksibi, S., Jaidi, F., & Bouhoula, A. (2022). A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach. *Mobile Networks and Applications*, 1-21.
9. Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, *8*(1), 1-26.
10. Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into regional development*, *2*(4), 802-813.
11. Barnes, J. E., & Fandos, N. (2019). President's Pick as Intelligence Chief Faces Questions About His Resume. *The New York Times*, A16-L.
12. Hwang, S. Y., Shin, D. J., & Kim, J. J. (2022). Systematic review on identification and prediction of deep learning-based cyber security technology and convergence fields. *Symmetry*, *14*(4), 683.
13. Brantly, A., & Smeets, M. (2020). Military operations in cyberspace. *Handbook of military sciences*, 1-16.
14. Galinec, D., Steingartner, W., & Zebić, V. (2019, November). Cyber rapid response team: An option within hybrid threats. In *2019 IEEE 15th International Scientific Conference on Informatics* (pp. 000043-000050). IEEE.

15. Annarelli, A., & Palombi, G. (2021). Digitalization capabilities for sustainable cyber resilience: a conceptual framework. *Sustainability*, *13*(23), 13065.