International Journal of Cyber Operations and Cyber Security Governance
Volume 1 Issue 1, 2026

# Improving Cyber Resilience: Converging Cyber Defence and Security

**E. RamaDevi, Krithika**

[1,2]Assistant Professor
Department of Management Information Systems

**Article Info**
Received: 22-11-2025 Revised: 13-12-2025 Accepted: 08-02-2026 Published: 18-02-2026

**Abstract**
Information and operational technology security are closely related to cyber security, which is defined by its varied variety of methodologies, tools, and ideas. An offensive information technology strategy with the goal of accomplishing antagonistic goals is what sets cyber security apart. However, customers and security experts alike may get confused due to the loose and unregulated usage of the term "cyber security," which is often confused with information security or IT security. Despite their interdependence, the merger of these fields obscures significant distinctions among them. The authors of this paper make a bold proposal to those in charge of security: restrict the term "cyber security" to describe only those practices that are defensive in nature and heavily reliant on IT and operational tech environments and systems. Cyber defence is an important tool for computer network security because it prevents malicious attacks, safeguards critical infrastructure, and guarantees the integrity of data for many different types of businesses, government organisations, and linked networks [3]. With an emphasis on how the concept of cyber resilience came to be, this research mostly looks at how cyber defence and security interact with one another. In this study, we provide a novel theoretical framework for comprehending cyber resilience, which clarifies the intricate relationship between the aforementioned fields. Moreover, the authors of this model take a close look at the strategies and procedures that are vital to strengthening cyber defences and security in light of the growing number of cyber threats. A look at the past, present, and future of CRRT and MACS is presented in this article. More strong resilience and unified defence against the ever-changing threat landscape is possible at the EU level via the innovation policy.

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

## 1 Introduction

Cybersecurity, on the other hand, is a phrase with its roots in the military that has evolved over the last decade. However, it seems to have expanded into other areas as of late, which has somewhat distorted its core. Ensuring the security of information is simply one aspect of cybersecurity. To further protect digital assets, there is OT security and IT security. When it comes to cyber defence, it's all about taking comprehensive actions. We need to identify important objects and confidential data, find ways to make attacks more expensive, develop reliable attack detection methods, and plan quick countermeasures. Only then can we hope to minimise the appeal of vulnerable attack channels [2].

Technical testing are also used in this field of cyber defence to identify potential attack vectors and vulnerabilities [3]. Recognising, preparing for, and responding to evolving cyber threats is the foundation of EU cybersecurity. The European Union is also trying to ramp up its efforts to strengthen its key infrastructure,

society, and institutions and to increase its capacity to identify and comprehend harmful activity. To better withstand and recover from cyberattacks, this is crucial for the European Union. Consequently, cooperation between member states is crucial, as is the formation of a relationship among the European Union, its member states, partner nations, and NATO.

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.

### 1.1 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

Cyber resilience in the modern information communications ecosystem is a multifaceted topic, and this research takes a methodical, model-driven approach to exploring it all. The construction of the Conceptual Cyber Resilience Model included the use of all these procedures and approaches.

### 2.1 Analysis of Cyber Défense

An in-depth examination of the studied environment is the first step in this inquiry. Next, cyber-defense analysis is performed on this environment to identify potential threats. In order to prevent such assaults, this research lays the groundwork for developing and executing suitable security measures. The purpose of this study is to provide a new angle on cyber resilience in the context of today's information and communication landscape.

### 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

Cyber resilience in today's information and communication landscape is the goal of this research, which aims to provide viewpoints on cyber defence and security. The end result is a novel theoretical model of cyber resistance. This paradigm offers new perspectives on cyber defence and includes European Union Cyber Rapid Response Teams (CRRTs) as one potential answer to the problem of cybercrime [6]. These are the CRRT, and they assist each other out by trading off personnel, processes, and tech.

### 2.4 Cyber Défense Focus

This research highlights the importance of cyber defence in preventing, detecting, and responding quickly to cyberattacks and threats. The goal is to safeguard confidential data and guarantee the stability of the infrastructure. Organisations and entities must prioritise cyber defence in light of the growing number and sophistication of cyber threats. This will ensure that all processes and activities can take place safely, free from the constant fear of cyberattacks [15]. Cyber

defence also improves the effectiveness of spending and resources allocated to security, especially in key sectors.

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

The difficulty in preventing cyberattacks is rising as the severity of these threats grows as well. For this reason, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security" is the name of the initiative that Lithuania has proposed to the European Union Council on Defence. The project's overarching objective is to strengthen cybersecurity across the two continents. The main goal of the initiative is to form international cyber defence teams that can respond quickly to cyber threats. Unlike many other international cyber defence projects, this one prioritises the pooling of resources among participating states, rather than just exchanging information. The project's scope includes studying EU cyber security protocols, creating cyber defence technologies, and coordinating tabletop exercises (simulations of cyber crises). Croatia, Lithuania, Estonia, Poland, the Netherlands, and Romania are the six EU member states that have officially joined the initiative as of this writing, while seven more nations—Finland, Belgium, Italy, France, Spain, Greece, and Slovenia—are keeping tabs on its development [15].

## 3 Problem Solution

Conventional cybersecurity methods are insufficient in today's digitally linked society to ward off the ever-changing cyber threat scenario. An approach that goes beyond basic security and incorporates the idea of resilience is required by the modern paradigm; this approach must be comprehensive and include defence, prevention, and reaction. One basic technique is cyber resilience, which looks at how well digitally networked systems are able to handle attacks both during and after an incident. In contrast to recovery, resilience is an ongoing, long-term effort that must be part of an organization's or business's entire strategy [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.

### 3.1 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].

### 3.2 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.

### 3.3 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].

### 3.4 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].

### 3.5 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].

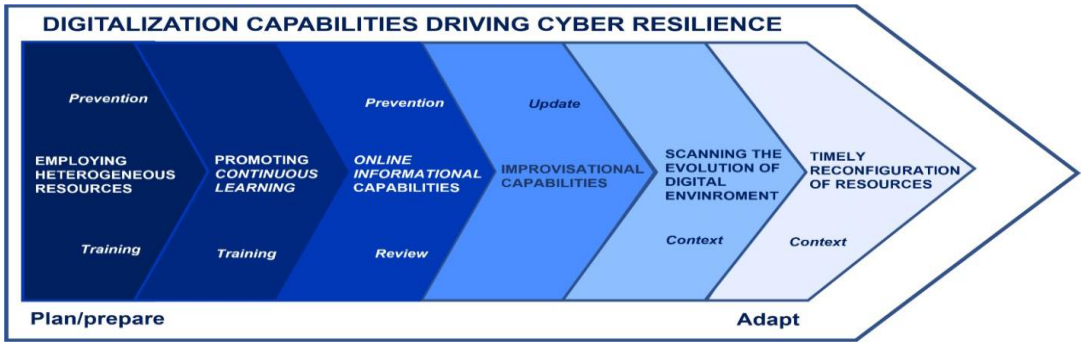



**Fig. 1: Cyber Resilience Model**

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].

### 3.6 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).

### 3.7 Creation, Performance, and CRRT Capability

Making A groundbreaking move toward establishing a robust cyber infrastructure has been the integration of the European Union's Cyber Rapid Response Teams (CRRTs) with the Mutual Assistance in Cybersecurity initiative. Among the EU's Permanent Structured Cooperation (PESCO)-approved initiatives, this one is among the most advanced. framework. The member states of the European Union (EU) with particular military responsibilities and capacities work together under PESCO to strengthen security and defence cooperation [10]. The significance of individuals willingly cooperating in the cyber domain is highlighted in the Declaration of Intent in the Field of Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity. It is essential to establish collaborative capabilities, share information, train together, assist with operations, conduct research and development, and share training [12]. Delegated specialists from CERT-EU, the European Union Agency for Network and Information Security (ENISA), and the Computer Emergency and Response Teams (CSIRTs) and Computer Crisis Response Teams (CRRTs) collaborate with other EU organisations to bolster ongoing cyber defences [8].

The CRRTs are a civil-military organization that works within the parameters set by the member states (MS). Its mission is to increase cyber defence awareness and collaboration within the European Union. We are also thinking about ways to improve our equipment, and we could create a standard Cyber Toolkit to help us identify and deal with cyber threats. In order to create this toolkit, which will strengthen the European

cyber security sector and encourage industrial collaboration among the participating MS, funding from the European Defence Fund and other EU sources is being considered [11]. A major step forward was the signing of the MoU in January 2020, and by 2021, the CRRTs had achieved full operational capability. In taking the lead on this initiative, the Ministry of National Defence of the Republic of Lithuania is showing the kind of teamwork that is needed to strengthen cyber resilience globally [11].

## 4 Discussion

Communication and information technology have become intrinsic to modern civilisations, allowing for the instantaneous dissemination of information in the form of text, pictures, and audio. Disruptions to the normal operation of these systems have evolved from minor technical issues into potential dangers to global security due to the increased interconnection and impact of the Internet of Things (IoT). In response, communities have established a wide range of strategies referred to as cyber security in order to protect themselves from online dangers. When it comes to cyber dangers, standardisation is king. Organisations should manage cyber risks in the same way they manage any other risk if they want to accomplish their goals. There are two very good reasons why government and business leaders should prioritise resilience. First, it aids in reducing the disastrous effects of a zero-sum game when it comes to cyber threats, where the only goal is to avoid network breaches at all costs. Second, it acknowledges that cyber resilience is a component of long-term strategy planning, expanding the discourse beyond the realm of IT and security [2]. Organisational leaders in both technology and strategy must engage in ongoing strategic communication to promote a comprehensive cyber resilience approach. Similar to "cybermedicine," this method improves preparedness, reduces duplication, and, in the end, increases efficacy and efficiency. Contrarily, conventional security measures are generally restricted to a single technological function—namely, to prevent unauthorised people from accessing a networked system—and are commonly seen as binary, with an outcome of "secure" or "not secure" [2].

Unpredictability is the biggest problem in cyber security. In 2002, former US Secretary of Defence Donald Rumsfeld magnificently described this difficulty, classifying it into three categories: "known unknowns," "known knowns," and the most terrifying, "unknown unknowns." Companies can't be ready for these dangers since they don't know about them [5].

By understanding what is considered typical behaviour for an organization and its users, emerging technologies may safeguard systems against significant dangers, offering a break from previous methods. Emerging abnormalities and risks may be detected by these technologies, unlike traditional rule-based and signature-based procedures. In addition to providing adaptive defence against sophisticated cyberattacks and insider threats, they are masters at handling ambiguity [11]. Cyber Rapid Response Teams for the European Union are nearing completion of their development phase. The project's EU representatives have met for lengthy meetings, during which they have exchanged ideas and laid the groundwork for a shared cyber toolbox. The nations that take part in this initiative will be better prepared to handle cyber incidents thanks to this toolbox. The conversations included both the general goal and the specific requirements of each individual. A thorough development plan was

also drafted, and participants discussed potential sources of financing for the toolbox. For the CRRT(s) initiative to be a long-term success, the toolbox is essential [8]. Research in the future will likely focus on finding better ways to make security information systems more resilient to cyberattacks and more flexible overall. To deal with the system's internal and external surroundings' "unknown unknowns," or unforeseen and unexpected occurrences, resilience is essential. Research in the future will focus on ways to facilitate mutual aid and collaboration in reacting to major cyber catastrophes, building on the fundamental step of establishing the Rapid Response Team. Joint training, the development of common skills, information exchange, and mutual operational assistance will all be part of these endeavours [7].
Essentially, in a world where threats are always changing and growing, it is essential for cyber resilience to change. In order to face the unknown threats posed by our interconnected digital world, organisations must adopt a proactive and collaborative strategy that recognises cyber risks as an essential part of their overall strategic goals [2].

## 5 Conclusion

This article has discussed the methods, procedures, and tactics needed to be cyber resilient in the modern, complicated digital world, especially in light of the ever-changing security threats. We have presented a novel Conceptual Cyber Resilience Model that incorporates both cyber and information security concerns into the field of cyber resilience. In order to respond to "unknown unknowns," or events that are neither predictable nor understood, our continuous research is focused on creating effective and efficient procedures that give security information systems agility. This means that these systems will be self-aware, able to change and adapt, and productive.

We have introduced a groundbreaking strategy for cyber defence and security at the European Union level [13] by outlining the development and implementation of the EU Cyber Rapid Response Teams and the Mutual Assistance in Cyber Security initiative as we have built this innovative conceptual model. By placing this effort within the larger framework of the Cyber Resilience Model, we have been able to better understand the critical roles that different players at different levels of the system hierarchy played in reaching the final objective.

### 5.1 Developments for Future

Management of cyber risk at the individual, network, and enterprise levels will be the focus of future studies. Cyber security and defence procedures may be made more efficient and successful with the help of the underlying Conceptual Model of Cyber Resilience, which is why it is of the utmost significance. There should be less "unknown unknowns," with the hope that they will be replaced by "known unknowns" and "known knowns." In order to improve our ability to deal with the constantly changing cyber threat scenario, this developmental trajectory is crucial.

## 6 References

Smith, S. (February 20, 2023). Striving for a cyber resilience definition grounded on science.... Volume 18, Issue 1, pages 379–386 of the International Conference on Cyber Warfare and Security. The authors of the cited 2020 work are Annarelli, Nonino, and Palombi. Understanding the management of cyber resilient systems. Publication: Computers & Industrial Engineering, Volume 149, Issue 10, Page 106829.

Thirdly, Enoch et al. (2022) cite Moon et al. as well as Lee, Ahn, and Kim. Cyber defence creation, enforcement, and assessment may be facilitated by a realistic framework. Publication: Computer Networks, Volume 208, Issue 10, by 108877.
4. Grieiman, V. (June 2023). Cyber Attacks: The Unknown Consequences. Volume 22, Issue 1, pages 223-231, European Conference on Cyber Warfare and Security.
In 2023, Dacorogna, Debbabi, and Kratz published a paper. Constructing cyber resilience via improved understanding of cyber risk through the use of a novel method for modelling data with large tails. Operational Research in Europe.
Sixth, Amini and Bozorgasl (2023). Sharing Cyber-Threat Data on the Cloud: A Game-Theoretic Approach. Computer Science and Engineering Research: An International Journal, Volume 11, Issue 4, Pages 2023–2023.
7. In a study published in May 2022 by Mallaboyev, Sharifjanovna, Muxammadjon, and Shukurullo. Concerns about the safety of data sent online. Section 241-245 of the Conference Zone.
In 2022, Ksibi, S., Jaidi, F., and Bouhoula, A. issued a study. Research on e-Health System Security and Cyber-Security Risk Management: A Synthesis, Analysis, and New Quantified Methodology. The book "Mobile Networks and Applications" has 21 pages.
In 2019, Efthymiopoulos was the author. An innovation, defence, and development framework for cyber-security at NATO. Tvaronavičienė, M., PlĎta, T., Della Casa, S., and Latvys, J. (2020) published an article in the Journal of Innovation and Entrepreneurship, volume 8, issue 1, pages 1–26. Managing the cybersecurity of vital energy infrastructure in national cybersecurity strategies: The United States, the United Kingdom, France, Estonia, and Lithuania as examples. Regional development insights, 2(4), 802-813.
Section 11. Barnes and Fandos's 2019 publication. His background raises eyebrows as the president's choice for head of intelligence under scrutiny. Section A16-L of the New York Times.
Shin, D. J., and Kim, J. J. (2022) were co-authors of the article 12. Exploration of the intersection of deep learning and cyber security technologies for identification and prediction purposes. Article number: 683 in the journal Symmetry.
The use of cyberspace for military purposes (Brantly, A., & Smeets, M., 2020). Military science handbook, pages 1-16.
14. In November 2019, Galineck, Steingartner, and Zebić published a paper. Among hybrid threats, a cyber fast reaction team offers an alternative. This is the fifteenth annual International Conference on Informatics (IEEE) (pp. 000043-000050).

In 2021, Annarelli and Palombi published a paper. Capabilities for digitalisation to promote long-term cyber resilience: a theoretical framework. Submitted to the journal Sustainability, volume 13, issue 23, page 13065.