sustainability

MDPI

Article

Cyber-Resilience Evaluation Methods Focusing on Response Time to Cyber Infringement

Se-Ho Choi [1], Jaepil Youn [1], Kookjin Kim [1,2], Seongkee Lee [3], Oh-Jin Kwon [4] and Dongkyoo Shin [1,2,*]

[1] Department of Computer Engineering, Sejong University, Seoul 05006, Republic of Korea; yeonwoo@sju.ac.kr (S.-H.C.); jpyoun@sju.ac.kr (J.Y.); kjkim@sju.ac.kr (K.K.)
[2] Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul 05006, Republic of Korea
[3] R.O.K Agency for Defense Development, Seoul 05771, Republic of Korea; seongkeel@add.re.kr
[4] Department of Electronics Engineering, Sejong University, Seoul 05006, Republic of Korea; ojkwon@sejong.ac.kr
* Correspondence: shindk@sejong.ac.kr

Abstract: Though multilevel, in-depth information protection systems are employed to defend against unknown cyber threats, vulnerabilities in these systems are frequently exploited by cyberattacks. As a result, it becomes challenging to comprehensively counter these attacks within a constrained time frame. When a cyberattack is detected, immediate measures are necessary to prevent widespread damage and maintain the system's regular functioning. Possessing sustainable cyber-resilience capabilities, which can promptly restore the system to its pre-attack state, is crucial. In this paper, a cyber-defense activity optimization procedure is introduced, drawing on the failure recovery time of the information system, aiming to enhance both the response and recovery phases of cyber resilience. Through training, the response time for various types of cyberattack was determined. Notably, a decrease in response time by 17.8% compared to the baseline was observed. By optimizing response times and integrating them with sustainable cyber-resilience assessment activities, a robust framework is presented for evaluating an organization's overall cyber-defense stance. Research on the cyber combat capability index, dissecting the response time for each distinct cyber-defense activity, is planned for future endeavors.

Keywords: cyber resilience; infringement response time; cyber-defense activity; recovery time objective

Citation: Choi, S.-H.; Youn, J.; Kim, K.; Lee, S.; Kwon, O.-J.; Shin, D. Cyber-Resilience Evaluation Methods Focusing on Response Time to Cyber Infringement. *Sustainability* **2023**, *15*, 13404. https://doi.org/10.3390/su151813404

Academic Editors: Muntasir Billah, Golam Kabir, Subhrajit Dutta and Harris Wu

Received: 5 July 2023
Revised: 16 August 2023
Accepted: 28 August 2023
Published: 7 September 2023

1. Introduction

Individuals are consistently connected to the Internet via diverse devices, including smartphones and Internet of Things (IoT) equipment, which are readily accessible. Cyberspace has evolved as an infrastructure, coexisting with people globally, reminiscent of the boundless nature of space. However, a fully reliable information protection system, adaptable to the swift shifts in infrastructure, has not been established. As a result, malicious activities persist in cyberspace. Furthermore, the magnitude and intensity of damages have been escalating, often bolstered by certain organizations and governments. Notably, entities, encompassing public institutions and private corporations, are confronted with tangible challenges when countering emerging, sophisticated cyber threats [1]. Since 2013, efforts have been undertaken by private companies to holistically incorporate and manage diverse security measures. These efforts involve perpetually countering cyberattacks and formulating and refining information protection policies through an information security management system (ISMS). Yet, the proficiency in real-time detection, analysis, and response to threats is found lacking [2].

In such a landscape, addressing every cyberattack within a limited time frame becomes unfeasible. The efficacy of investigation, analysis, and response largely hinges on the

competencies of individual entities and organizations. For effective countering, a cyber-resilience strategy needs to be embraced, championed by a proactive and cohesive approach. Once a cyberattack is detected, standardized methodologies and procedures optimized for cyber defense are mandated across information security policy management, malicious code mitigation, and system recovery. Swift responses, facilitated by these measures, can curtail the proliferation of damage during system operation. Furthermore, achieving sustainable cyber resilience capable of reverting systems to their pre-attack state swiftly becomes feasible.

The subsequent sections of this paper are delineated as follows: Section 2 encapsulates research trends encompassing cyber resilience, cyberattack response durations, and recovery timelines. Section 3 introduces procedures for refining cyber-defense activities and gauging response durations. In Section 4, the response durations for varied cyberattacks are scrutinized by juxtaposing them against actual cyberattack response training outcomes, and Section 5 delineates the conclusions and trajectories for future research.

2. Related Work

This chapter provides a summary of the introduction and prevailing trends in cyber resilience and the study concerning the time taken to recognize and respond to a cyberattack.

2.1. Cyber Resilience

Cyber resilience refers to an organization's capability to maintain its targeted performance despite a cybersecurity breach. At the World Economic Forum in Davos in 2012, cyber resilience was defined as the capacity of systems and organizations to endure cyber events, gauged as a blend of average downtime and recovery time [3]. This framework for cyber resilience is composed of five stages: identify, protect, detect, respond, and recover [4].

Cyberattacks are imminent threats, not merely distant possibilities. While it is widely held that maintaining updated software offers optimal information protection [3], the 2022 Ponemon report revealed that only 18% of cyberattacks resulted from software vulnerabilities. It is crucial to acknowledge that cyberattacks are executed across diverse platforms, and attackers continually innovate new means of breaching organizations; such intrusions have become routine [5].

Environments characterized by complexity and uncertainty, including cloud systems, IoT, blockchain, and globalized supply chain operations, are increasingly vulnerable to cyberattacks. An effective response necessitates the adoption of a proactive and cohesive cyber-resilience strategy. Notably, most breaches often go undetected internally and are brought to light only after being flagged by concerned organizations or the attackers themselves. Recognizing and swiftly responding to such cyberattacks using standardized protocols and reverting to a pre-attack state is paramount [3]. Consequently, cyber resilience is delineated as an organization's capacity to mitigate and recover from the detrimental impacts of both anticipated and unforeseen threats via defensive maneuvers in cyberspace [3].

The menace of cyber threats is not novel, but its magnitude and unpredictability are burgeoning daily. Detecting and thwarting cyberattacks proactively is challenging, and countering a specific cyberattack with established defense technologies is not straightforward [6]. Cyberattacks are evolving from isolated incidents to persistent, relentless campaigns. No singular remedy exists that is suitable for all infrastructures, and frequently, no unified approach prevails to defend against cyberattacks [7]. Rather than perpetually deploying security safeguards, enterprises ought to discern their paramount assets and evaluate their correlation with prevailing cyber-defense initiatives. A paradigm shift is warranted to propose strategies to stakeholders, underscored by cyber resilience, ensuring swift response and mission assurance.

A disparity in the evolution of defensive and offensive software has been highlighted by DARPA, as depicted in Figure 1. Due to the amplifying intricacy of the systems under safeguard, the complexity of software safeguarding a network has been observed to surge exponentially. However, the size of software code employed in a successful assault has remained relatively unchanged [8]. A defense system is mandated to counteract every conceivable attack, while attackers need only channel their efforts at the defense's most vulnerable point.

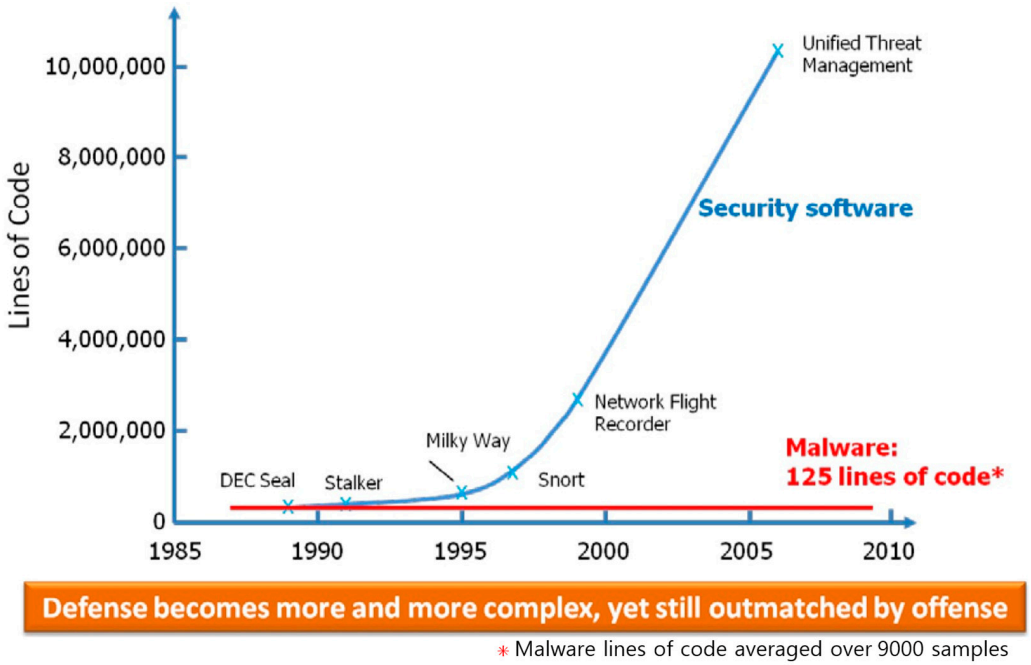

Figure 1. Size comparison of defensive and offensive software. Reprinted with permission from Ref. [8].

Huang et al. proposed a reinforcement learning (RL)-based cyber-resilient mechanism (CRM). This RL-CRM is designed to strategically respond to attacks from advanced persistent threats (APTs). When attacked, essential functions and performance are preserved to maintain their original function [9].

Babiceanu et al. proposed a cybersecurity resilience ontology combined with a software-defined networking (SDN)-based manufacturing testbed for use in capturing the requirements of the virtual manufacturing network design phase. Among these, Industrial Internet of Things (IIoT) system networks react to disruption events using available resilience mechanisms [10].

Haque et al. employed the R4 (robustness, redundancy, resourcefulness, and rapidity) resilience framework in its extended form to calculate cyber-resilience metrics for industrial control systems. Based on this, a qualitative cyber-resilience evaluation tool that employs this framework and a subjective survey method was proposed. This evaluation tool offers a comprehensive mathematical depiction of the elasticity calculation process [11].

Ligo et al. outlined both research and practical directions for formulating effective cyber-resilience countermeasures. They contended that for the development of new cyber-resilience measures, an apt definition of capabilities is pivotal. It was emphasized by the authors that a measure for cyber resilience ought to be defined post-restoration, following recovery efforts [12].

A system–theoretic process analysis for security through simulation (STPA-Sec/S) was proposed by Simone et al., marking a methodological bridge between STPA-Sec and quantitative resilience assessment grounded in simulation models. Once the systems–theoretic accident modeling and processes (STAMP) model, which addresses cyber threats and spots insecure controls within cyber–social technology systems, was expanded, it was

posited that cyber resilience can be quantitatively determined based on systems–theoretic modeling [13].

A follow-up investigation of cyber resilience was conducted as shown in Table 1. From these investigations, it was discerned that each study presented a somewhat distinct conceptualization of cyber resilience. This study recognizes, in alignment with the definitions, that cyber resilience is not an absolute defense against all cyberattacks. Cyber resilience is characterized as an organization's capacity to mitigate the adverse impacts of both foreseen and unforeseen threats via cyber-defense activities, aiming to revert to its pre-attack state in the minimal possible duration. Furthermore, cyber resilience is assessed contingent on the mean response time of the information protection apparatus and the quickest recuperation span following an information system disruption.

Table 1. Application plan in cyber-resilience study.

Study	How to Apply Cyber Resilience
Huang et al. [9]	Cyber resiliency is leveraged to uphold crucial functions and performance during vulnerability rectification.
Babiceanu et al. [10]	Restoration of software is approached from a security perspective, accentuating system responses to events.
Haque et al. [11]	Cyber resilience is qualitatively evaluated utilizing subjective survey techniques.
Ligo et al. [12]	Assessment of cyber resilience for autonomous entities is undertaken, barring recovery from outages.
Simone et al. [13]	Cyber resilience is applied based on cyberattack narratives, without giving precedence to specific scenarios.

2.2. Cyberattack Response

Ponemon, an IBM-sponsored lab, specializes in analyzing the cost of data breaches. Between March 2021 and March 2022, incidents of cyberattacks across 17 industries including healthcare, energy, and finance in 17 countries and regions were studied. Situations where data were leaked through irregular channels were examined, with results presented in Figure 2 [14].

Based on the survey, a cyberattack was recognized, on average, after 207 days, while a data breach was recognized and addressed in 70 days, leading to an entire life cycle of 277 days. For instance, if the initial cyberattack involving data leakage transpired on 1 January, 277 days up to 4 October were needed for recognition and response, indicating a lack of timely intervention [14].

In instances where cyberattacks leveraged stolen or compromised authentication data, 243 days were required for detection and an additional 84 days for response, totaling an extended period of 327 days. This duration is 18% longer than the typical time taken to detect and address a cyberattack. Cyberattacks executed via business emails were observed to have the second lengthiest life cycle for detection and response at 308 days. Moreover, attacks exploiting third-party software vulnerabilities took 284 days for detection and response, marking the fourth longest life cycle.

In a separate survey, average detection and response durations for cyberattacks from 2016 to 2022 were compared, with Figure 3 depicting the results [14]. A brief decline in average duration was observed in 2017, followed by a gradual rise through 2021. This trend suggests that as technologies for recognizing and responding to cyberattacks evolve, so too do the tactics and penetration methods of attackers. Consequently, innovative strategies are essential for countering these cyberattacks.

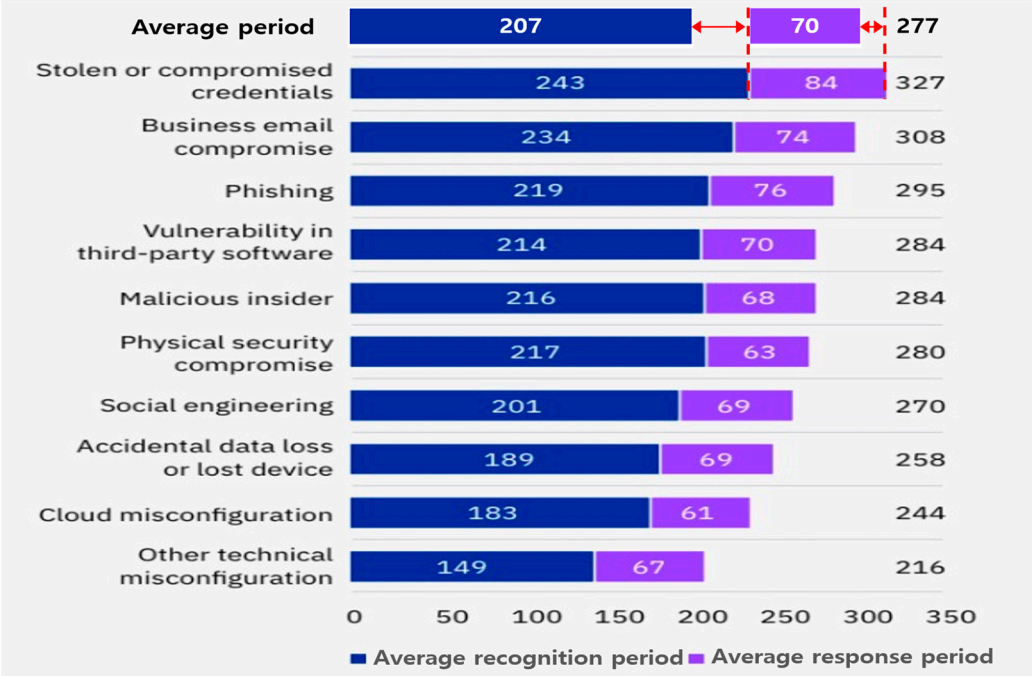

Figure 2. Time taken to recognize and respond to each type of attack. Reprinted with permission from Ref. [14].

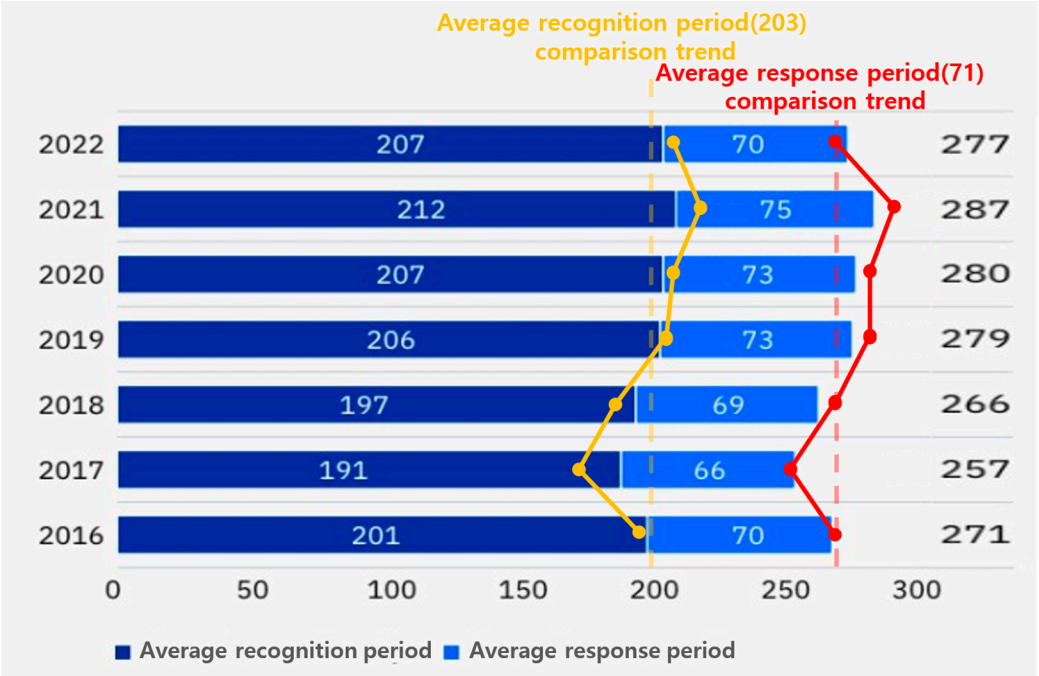

Figure 3. Average times to recognize and respond to cyberattacks by year. Reprinted with permission from Ref. [14].

2.3. Recuperation Times

Recuperation time is employed as a functional damage assessment metric within combat damage assessment. It designates the period necessary to either restore or replace the functionality of a specific target. Both the shortest feasible (minimum) and the most realistic extended (maximum) times to regain lost functionality are determined. Furthermore, a combat damage assessment may incorporate a judgment on recuperation time

contingent on the target's processing objective and accessible intelligence. For instance, while full restoration of a particular target's capabilities might be projected to take 10 days, achieving 50% of its original functions could require a minimum of 2 days. In specific scenarios, satisfactory performance might be sustained even with just half of the original functionalities restored [15].

3. Optimization of Cyber-Defense Activities and Measurement of Response Time

In this chapter, a procedure is proposed to optimize cyber-defense activities in response to cyberattacks. The optimal response time for each cyber-defense activity is derived based on the target recovery time of information systems and the recovery time of public institutions.

3.1. Optimization of Cyber-Defense Activities against Cyberattacks

A procedure to optimize cyber-defense activities is presented in Figure 4. Such a procedure is crucial for actions in the cyber-resilience response and recovery phases against cyberattacks.

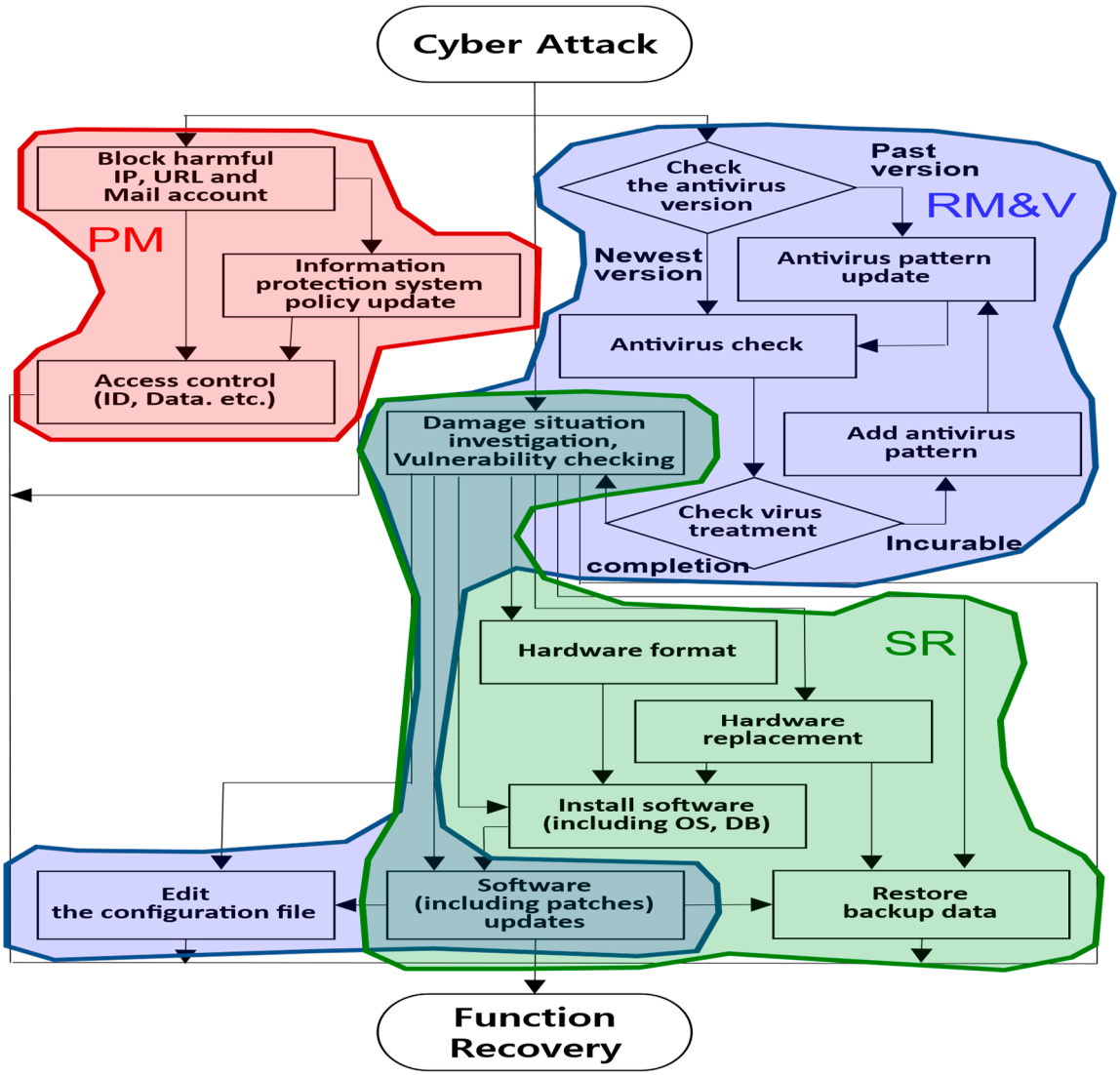

Figure 4. Procedures for optimizing cyber-defense activities against cyberattacks.

In the event of a successful malicious cyberattack, policy management (PM) updates, such as those related to information protection system policies, must be swiftly imple-

mented to mitigate further damage and safeguard against subsequent attacks. The remove malware and vulnerabilities (RM&V) in preparation for secondary additional attacks. Subsequently, actions like system restoration (SR) are necessary to bring the compromised function back to its normal state [16].

As depicted in Figure 5, the PM domain manages the security policies of the information protection system. This ensures the curtailment of damage spread and prevention of identical cyberattacks. To achieve this, malicious IPs/URLs and email accounts are blocked using firewalls and antihacking email measures. Detection policies of the intrusion prevention system (IPS), web firewall, and antivirus systems are updated with the most recent data. This helps in scrutinizing network packets for known cyberattacks, obstructing webpage forgery based on signatures, identifying malicious software, and isolating pertinent files. By employing extranet access management and a secure OS, different privileges can be assigned based on accounts, and data access can be regulated.

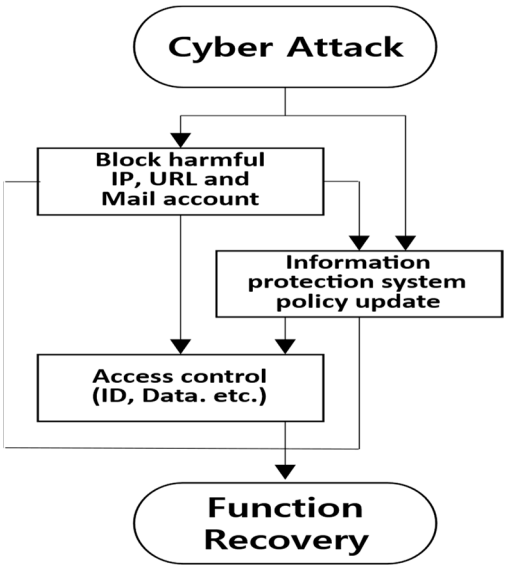

Figure 5. Cyber-defense activity in the PM field.

Figure 6 elaborates on activities in the RM&V domain. Here, the virus defense system identifies and eradicates malicious software and the potential paths that allow its installation. The premise assumes that a harmful IP/URL has already been obstructed in the PM sector. If separate individuals are assigned to handle malicious software removal and vulnerability management, a coordinated simultaneous effort can reduce the response time to breaches. To purge malicious software, virus defense system patterns are updated and inspected. If no detection occurs, a malicious software sample is secured, a fresh pattern is introduced, and the virus is neutralized. Following the elimination of malicious software, vulnerability inspection tools assess potential weaknesses. Before updating a vulnerable version of the web development program or database, the interplay with currently active application software must be verified and any vulnerability addressed. Should there be any adverse impact from application software, service access is either restricted until necessary modifications are made or user access is minimized to prevent malicious exploitation. Additionally, if a service exploited during the cyberattack is located within a fundamental file, the configuration file undergoes modification.

As illustrated in Figure 7, damage to cyber assets such as servers, storage, information protection systems, and networks is examined in the SR field to restore the hardware and software to their state prior to the cyberattack. For minor software errors, the latest version is installed. If the same error is encountered again, the relevant software is reinstalled (rebooting is required after deletion) and updated to the latest version. If a hardware issue arises, the related software is reinstalled after formatting, followed by a backup file

restoration. However, for appliances (equipment designed to function immediately upon powering on without the need for installing a separate OS or software), the backup file is restored after hardware replacement.

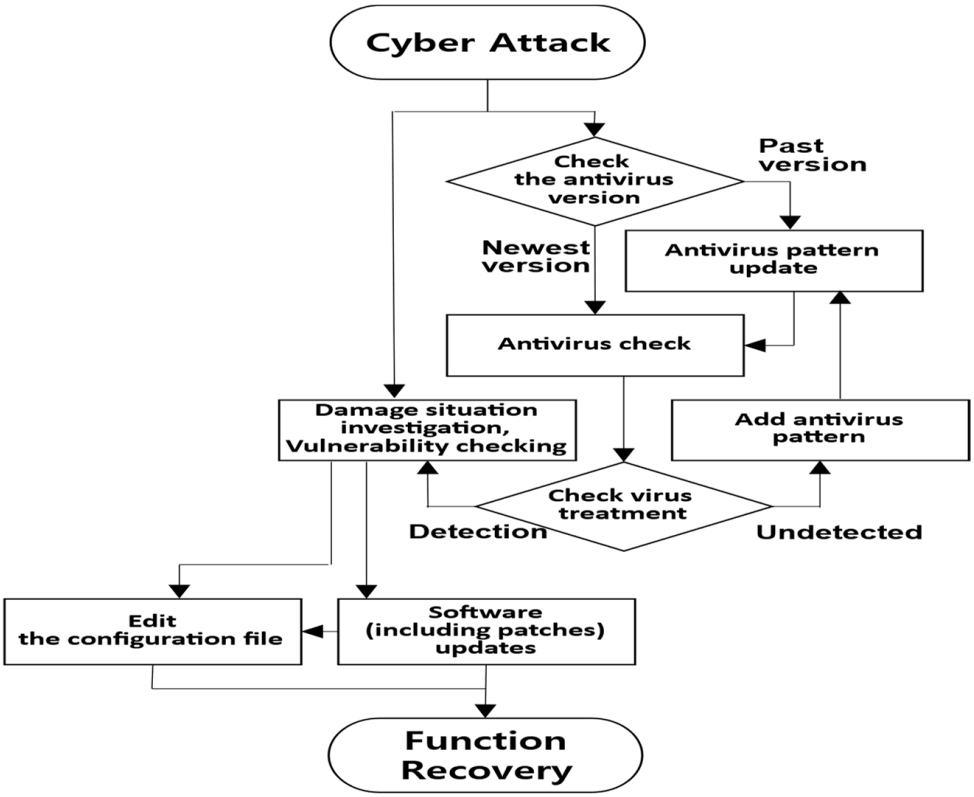

Figure 6. Cyber-defense activity in the RM&V field.

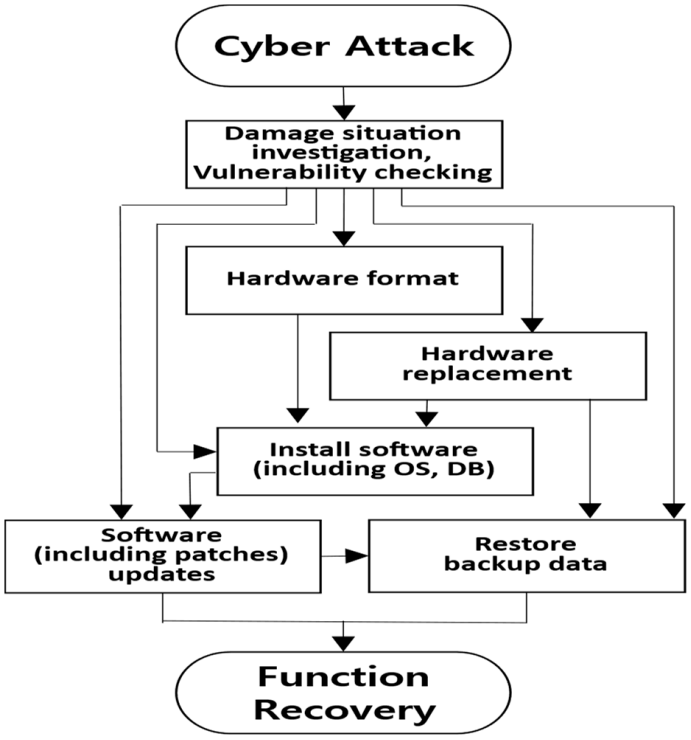

Figure 7. Cyber-defense activity in the SR field.

In this manner, the security policy is updated by PM using distributed processing (executing multiple tasks simultaneously) through information protection systems like firewalls and IPS based on the IP address information of the attack target. Moreover, RM&V and SR undertake countermeasure activities in sequence, such as installing and running software (OS, DB, etc.) on the physical target of the attack. Typically, PM and RM&V can execute cyber-defense activities simultaneously, but SR must commence its cyber-defense activities after RM&V has finished to prevent a secondary cyberattack. However, during hardware formatting and replacement, these three cyber-defense activities might be intermingled.

3.2. Target Recovery Time for Each Information System Resource

Failure-handling procedures for each information system resource document potential system failures of primary resources within the information system in advance. These procedures are recommended to serve as a reference to facilitate communication between system operating organizations and to estimate the probable cause of failure and the recovery time from major disruptions [17]. Individuals responsible for the information system should have the capability to address failures in the actual operational environment effectively. This capability can be enhanced through regular reviews and training on the failure-handling procedures for each resource.

The failure-handling procedure for each resource should be updated periodically based on improvements relevant to the actual operational environment and distributed to the appropriate individuals. Furthermore, the inspection sequence for identifying failures is drafted to prioritize checks on components that are more likely to be the sources of failures.

The National Information Society Agency (previously known as the National Computerization Agency) has provided the recovery time objectives for failure handling, which are listed in Table 2 [17]. Each agency should establish a suitable procedure and recovery time, tailored to the characteristics of the operating system resources, when addressing failures by resource.

Table 2. Time required for failover by the information system.

Type	Cause of Disability	Time (min.)
Web server	One bad web server disk	60
	Two or more bad web server disks	120
	Excessive share of resources (CPU, memory, disk) per process	5
	Operating system corruption	5
	Bad LAN card	30
Application software	Application software error	60
	Data error	60
	Batch job error	60
Database and middleware	Oracle process stopped/abnormal	10
	Oracle archive files full	10
	Oracle listener stopped/abnormal	10
	Oracle home directory full	10
	Oracle block corruption	60
	MQ process stopped/abnormal	10
	MQ config file change abnormal	10

The failure-handling procedure for each information system resource details the measures to be taken after the cause of failure for major resources has been identified.

Information system resources encompass servers, application software, networks, and databases. Both comprehensive solutions for addressing the disruptions and immediate response measures for situations where comprehensive solutions are unattainable are included. The target time for failover is defined as the duration until the cause of the failure is identified and normal operations are resumed.

3.3. Restoration Time for Each Failure of Public Institutions

Efforts are being made by public institutions to enhance their operational efficiency through the introduction of standardized failure handling, which is achieved by defining failure management policies within their information systems. Standards for types of information system failures and their resolutions are established to document the history of failures. Every quarter, the state of failure management is analyzed based on reports detailing the performance of the information system [18].

Drawing from the 2021 disability management data of public institutions overseen by this author, restoration times are compiled in Table 3 [18]. Unlike the data from the National Information Society Agency, the times incorporated here account for the duration needed to identify the root cause of the disability, ensuring that the quickest duration for identical disabilities is captured.

Table 3. Time taken for failure measures by information systems of public institutions.

Type	Cause of Disability	Time (min.)
Web server	Defective voltage regulator module	101
	Excessive share of resources (CPU, memory, disk) per process	85
	Bad memory card	81
	LAN card setting error	117
Application software	Application software error	185
	Batch job error	75
	Excessive antivirus memory usage	32
	Hang occurs	68
Database and middleware	DB forced restart	96
	Oracle archive files full	153
	Oracle listener log capacity full	90

3.4. Response Time for Each Cyber-Defense Activity

The process of rectifying damages sustained from a cyberattack, bringing the system back to its pre-attack state, mirrors the system restoration procedure post-information system failure. The time frames for each cyber-defense activity were established as follows.

Cyber-defense targets comprise cyber assets like information protection systems, overarching systems, networks, and PCs. The infringement response time, also known as the recovery time objective (RTO), is the period required to attain the desired operational level post-cyberattack. Relying on the 2021 data regarding restoration durations for each failure action from public institutions and the failure handling procedure of the National Information Society Agency for each information system resource, Table 4 outlines the response times for individual defense activities against cyberattacks. This takes into consideration both the RTO and the identified cause of the failure. Some defense activities sourced their data directly and employed default configurations provided by antivirus system manufacturers.

Table 4. Response time for cyber-defense activity.

Type	Response Activity	Time (min.)
Policy management	Block harmful IPs, URLs, and mail accounts	10
	Information protection system policy update	20
	Access control (ID, data, etc.)	10
Remove malware and vulnerability	Antivirus check	40
	Antivirus pattern update	60
	Add antivirus pattern	360
	Damage situation investigation, vulnerability checking	30
	Edit the configuration file	10
	Software (including patches) updates	60
System restore	Hardware format	30
	Hardware replacement	60
	Install software (including OS, DB)	1440
	Restore backup data	60

4. Cyber-Resilience Evaluation by Cyberattack Type

According to the Defense Cyber Crisis Response Manual of the Ministry of National Defense, response activities are initiated in the sequence of breach detection, initial action, analysis, and recovery when a cyberattack takes place [19]. Typically, cyberattacks can span multiple countries by utilizing concealment technology, or the attacker's identity might be concealed. The processes of investigation and analysis, which encompass identifying the cause, verifying additional damage, determining the response level, and pinpointing the attacker, might yield different outcomes based on the distinct capabilities of individuals and organizations [20]. Thus, a system is needed that suggests countermeasures when a specialized program is executed per the manual or when the gathered data are inputted in a designated format. The outcomes of the training conducted in the latter half of 2022 were juxtaposed with the cyber-defense activity optimization procedure delineated in Figure 4 of this paper. The objective was to validate the breach response time, emphasizing the cyber-resilience response and recovery phases of PM, RM&V, and SR, to the extent actions were feasible.

4.1. Defense Activity and Response Time against DDoS Attacks

On 30 September 2022 at 06:00, a DDoS attack targeting the homepage was identified, originating from both domestic and international IP addresses as well as internal IP addresses of public institutions. Continuous attacks caused a lag in website accessibility. Blocking harmful packets with an information protection system and addressing zombie PCs became imperative.

For cyber-defense activities, as illustrated in Table 5, from the PM perspective, the timeout setting value was decreased or a specific overlapping packet signature was identified to obstruct abnormal IP access to the homepage. Under RM&V, by collaborating with affiliated organizations, virus patterns were updated, treating PCs compromised by malicious code, or malware samples were procured from the infected PCs of public institutions.

During the live training, the session was sustained for a set duration by coordinating the timeout setting value with the user on the homepage server. In the IPS, normal service was restored at 06:45 by blocking packets in which the newline character (\r\n) of the Get request was showcased only once as a signature [21]. Subsequent to this, more virus patterns were solicited to remediate zombie PCs within public institutions compromised by malicious software, and by 17:15 (after 11 h and 15 min), no detrimental traffic associated

with the training was observed. The defense activities against DDoS attacks are depicted in Figure 8.

Table 5. Cyber-defense activities and response times to DDoS attacks.

Type	Response Activity	Time (min.)
Policy management	Block harmful IPs, URLs, and mail accounts	10
	Information protection system policy update	20
	Access control (ID, data, etc.)	10
Remove malware and vulnerability	Antivirus check	40
	Antivirus pattern update	60
	Add antivirus pattern	360

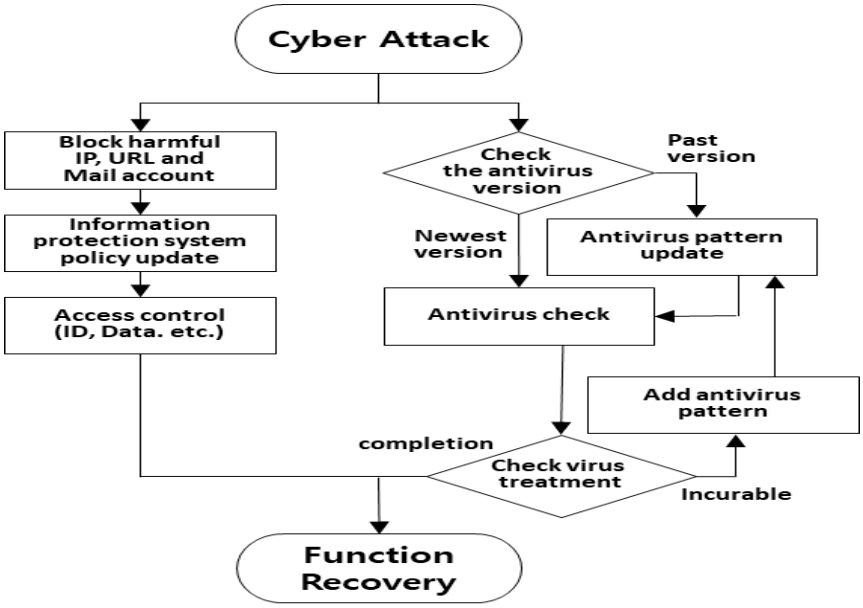

Figure 8. Connection diagram of defense activities against DDoS attacks.

Against DDoS attacks, the PM required 40 min, and the malicious code removal process (antivirus check + addition of antivirus pattern + antivirus pattern + antivirus check) consumed 500 min. Both the PM and malicious code removal are distributed processing response activities that can be executed concurrently. The combined duration was 8 h and 20 min, equivalent to the malicious code removal response time and 2 h and 55 min shorter than the real training response duration of 11 h and 15 min.

4.2. Defense Activity and Response Time against Homepage Alteration

On 30 September 2022 at 10:00, illegal access from a Chinese IP to an internal IP of a public institution was detected, and modifications to the pop-up window of the B homepage were confirmed. Changing the access rights to the homepage's source files, patching security for open-source bulletin boards, and restoring sources for pop-up windows became necessary.

As illustrated in Table 6, from the PM side, all access to administrator pages from external IPs was restricted, and access rights were checked. On the RM&V side, the webpage program was updated to its most recent version. From the SR perspective, the altered pop-up window was restored using backup data and was normalized.

Table 6. Cyber-defense activities and response times against homepage alteration.

Type	Response Activity	Time (min.)
Policy management	Block harmful IPs, URLs, and mail accounts	10
	Information protection system policy update	20
	Access control (ID, data, etc.)	10
Remove malware and vulnerability	Vulnerability checking	30
	Edit the configuration file	10
	Software (including patches) updates	60
System restore	Restore backup data	60

During the live training, the bulletin board was patched for security to its latest version, and control was established over both the upload file extension and external access to the administrator's webpage. By using backup data to restore the pop-up window's source, the homepage was returned to its normal state at 12:05, after an elapsed time of 2 h and 5 min. The defense activities against homepage modifications are depicted in Figure 9.

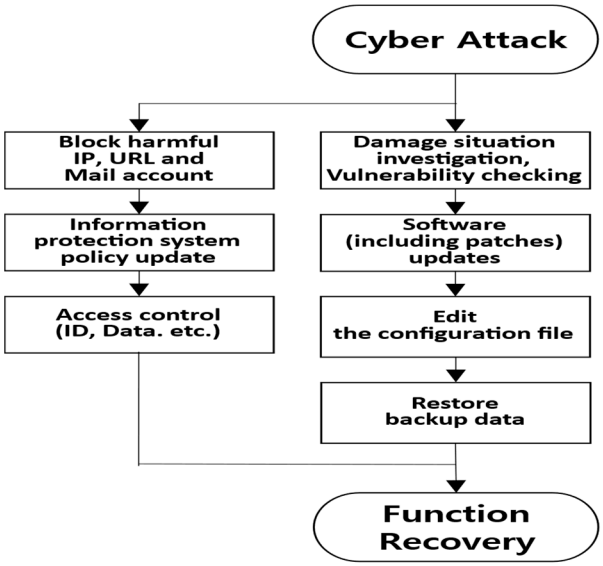

Figure 9. Connection diagram of defense activities against homepage alteration.

When comparing the cyber-defense activity optimization procedure and response time for homepage alteration, PM took 40 min, vulnerability removal 100 min, and the pop-up window source restoration 60 min. While PM and vulnerability removal could be executed concurrently as distributed processing response activities, vulnerability removal and SR were carried out sequentially. Thus, the entire process took 2 h and 40 min, which was 35 min longer than the actual training response time of 2 h and 5 min.

4.3. Defense Activity and Response Time for Information Protection System Interruption

On 30 September 2022 at 14:00, unauthorized access from a US IP to an internal IP of a public institution was detected, resulting in a down message being issued to the firewall operating in the WAN area. Although redundancy was configured, ensuring that external service support was uninterrupted, the firewall was rendered inaccessible. A forced reboot was attempted, but a normal startup could not be achieved. The CF memory (a nonvolatile memory that stores OS and policy information) was found to be defective, necessitating an urgent equipment replacement.

As detailed in Table 7, external IPs attempting direct access to the information protection system were blocked from the PM side. From the SR viewpoint, the damage status of the information protection system was assessed, replacement equipment was secured, and data backups were restored.

Table 7. Cyber-defense activities and response times for information protection system interruption.

Type	Response Activity	Time (min.)
Policy management	Block harmful IPs, URLs, and mail accounts	10
	Information protection system policy update	20
	Access control (ID, data, etc.)	10
System restore	Damage situation investigation	30
	Hardware replacement	60
	Restore backup data	60

In the actual training session, normal function was resumed at 17:05, after an elapsed time of 3 h and 5 min, by obtaining and replacing the necessary equipment and restoring the backed-up policy and configuration files. The defense actions against the disruption of the information protection system are shown in Figure 10.

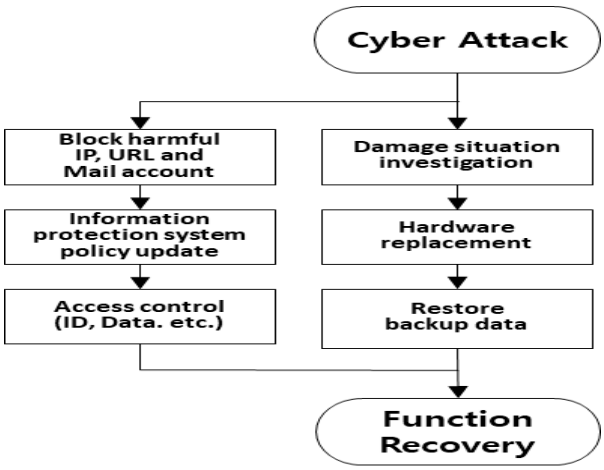

Figure 10. Connection diagram of defense activities against interruption of the information protection system.

In a comparison between the cyber-defense activity optimization procedure and the response time for the interruption of the information protection system, PM required 40 min and SR took 150 min. Both PM and SR, being distributed processing response activities, could be initiated concurrently. The total process took 2 h and 30 min, equal to the SR response time and 35 min shorter than the real training response time of 3 h and 5 min.

4.4. Cyber-Resilience Response Time Analysis

In the second half of 2022, among the training contents, three types of attacks were compared with procedures for optimizing cyber-defense activities. As depicted in Figure 11, an analysis of cyber-resilience response times revealed that PM exerted minimal influence on the response time for cyber infringements due to its distributed processing alongside other response components. It was confirmed, however, that RM&V and SR were processed sequentially and predominantly influenced the cyber-infringement response time.

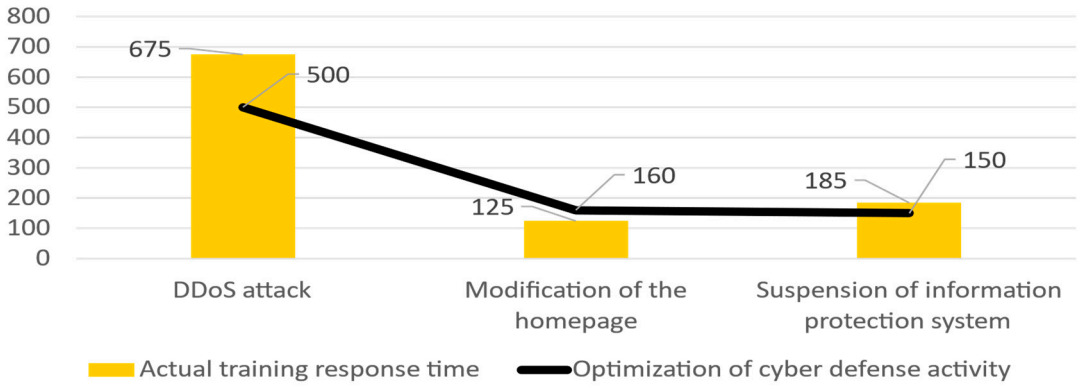

Figure 11. Cyber-resilience response time comparison result.

For cyber-defense activities to be executed smoothly, it is essential for all stakeholders to be familiar with them [22]. If response times, either verified through training or based on actual response activities, are consistently analyzed, cyber-defense activities are expected to become more nuanced than those presented in Table 4. Concurrently, response times will be updated, enhancing their accuracy and reliability [23].

5. Conclusions

While multilevel deep information protection systems are employed to guard against unidentified cyber threats [24], cyberattacks often test their effectiveness by exploiting gaps in these systems. Addressing this challenge requires an assessment of cyber-resilience capabilities, ensuring sustainability by refining cyber-defense activities and revisiting response procedures. A methodology and response procedure, designed to revert to the pre-cyberattack state in the shortest possible duration, is also indispensable as an optimal policy.

This paper introduces a novel method for evaluating cyber resilience, emphasizing the response and recovery phases based on the RTO of failure management. As illustrated in Figure 11, organizations that boast shorter response times using standardized measures stand a better chance of curtailing the damage from cyberattacks [25]. By reducing the overall response time by 17.8%, the ability to swiftly recover from cyberattacks was enhanced. An organization's cyber-resilience capabilities can be significantly fortified if its response and recovery procedures are ingrained prior to an actual cyberattack taking place. Enhancing response times through such continuous cyber-resilience assessment endeavors offers a valuable framework for assessing an organization's comprehensive cyber-defense stance [26].

Future endeavors aim to incorporate the extent of impact and urgency of cyber-defense activities, which will augment research on cyber battlefield management systems. Research centered on the cyber combat capability index is planned, which will support command decisions [27,28] by evaluating the operational status of cyber assets like information protection systems, systems, and networks, thereby visualizing damage in real-time during a cyberattack.

Author Contributions: Conceptualization, S.-H.C., J.Y. and S.L.; funding acquisition, D.S.; methodology, S.-H.C., K.K. and O.-J.K.; design of optimization process for cyber-defense activity, S.-H.C., J.Y. and S.L.; supervision, D.S.; validation, S.L.; writing—original draft, S.-H.C., K.K. and S.L.; writing—review and editing, O.-J.K. and D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by a National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No. 2022R1F1A1074773).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
ISMS	Information security management system
RL	Reinforcement learning
CRM	Cyber-resilient mechanism
APT	Advanced persistent threat
SDN	Software-defined networking
IIoT	Industrial Internet of Things
R4	Robustness, redundancy, resourcefulness, and rapidity
STPA-Sec/S	System–theoretic process analysis for security through simulation
STAMP	Systems–theoretic accident modeling and processes
PM	Policy management
RM&V	Remove malware and vulnerability
SR	System restore
IPS	Intrusion prevention system
RTO	Recovery time objective
DDoS	Distributed denial of service

References

1. Government of the Republic of Korea. *National Cyber Security Master Plan*; Government of the Republic of Korea: Seoul, Republic of Korea, 2019; p. 2.
2. Kim, K.H. *Overview of Information Security Management System Certification System and Development Direction*; Korea Internet & Security Agency: Seoul, Republic of Korea, 2017; pp. 3–7. Available online: https://m.blog.naver.com/ntower/221003396724 (accessed on 3 July 2023).
3. Ryu, J.G. *Respond to Cyber Security Incidents That You Don't Know When Not If*; IDG Summary, International Data Group KOREA: Seoul, Republic of Korea, 2018; Available online: https://www.itworld.co.kr/techlibrary/111004 (accessed on 3 July 2023).
4. Frank, D.; Phil, G. Five Key Technologies for Enabling a Cyber Resilience Framework. In *IDC White Paper*; IDC: Needham, MA, USA, 2020.
5. Segovia, M.; Rubio-Hernan, J.; Cavalli, A.R.; Garcia-Alfaro, J. Cyber-Resilience Approaches for Cyber-Physical Systems. *arXiv* **2023**, arXiv:2302.05402.
6. Lee, S.K.; Lee, S.H.; Kang, T.I.; Kwon, M.Y.; Lee, N.B. Resiliency of Mobile OS Security for Secure Personal Ubiquitous Computing. *Pers. Ubiquitous Comput.* **2018**, *22*, 23–34. [CrossRef]
7. *White Paper, The Cyber Resilience Blueprint: A New Perspective on Security*; Symantec: Mountain View, CA, USA, 2014.
8. Defense Science Board. *Resilient Military Systems and the Advanced Cyber Threat*; Department of Defense: Washington, DC, USA, 2013.
9. Huang, Y.; Huang, L.; Zhu, Q. Reinforcement learning for feedback-enabled cyber resilience. *Annu. Rev. Control.* **2022**, *53*, 273–295. [CrossRef]
10. Babiceanu, R.F.; Seker, R. Cyber resilience protection for industrial internet of things: A software-defined networking approach. *Comput. Ind.* **2019**, *104*, 47–58. [CrossRef]
11. Haque, M.A.; Shetty, S.; Krishnappa, B. ICS-CRAT: A cyber resilience assessment tool for industrial control systems. In Proceedings of the 2019 IEEE 5th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity), High Performance and Smart Computing (HPSC) and Intelligent Data and Security (IDS), Washington, DC, USA, 27–29 May 2019; pp. 273–281.
12. Ligo, A.K.; Kott, A.; Linkov, I. How to measure cyber-resilience of a system with autonomous agents: Approaches and challenges. *IEEE Eng. Manag. Rev.* **2021**, *49*, 89–97. [CrossRef]
13. Simone, F.; Akel, A.J.N.; Di Gravio, G.; Patriarca, R. Thinking in systems, sifting through simulations: A way ahead for cyber resilience assessment. *IEEE Access* **2023**, *11*, 11430–11450. [CrossRef]
14. Ponemon Institute. *Cost of a Data Breach Full Report 2022*; IBM Security: Armonk, NY, USA, 2022; pp. 14–18.
15. *Chairman of The Joint Chiefs of Staff Instruction 3162.02, Methodology for Combat Assessment*; U.S. Joint Chiefs of Staff: Washington, DC, USA, 2019; p. C-7.
16. Cyber Operations Department. *Guidelines for Performing Cyber Operations*; R.O.K Joint Chiefs of Staff: Seoul, Republic of Korea, 2021; pp. 25–37.

17. National Computerization Agency. *Guideline for Incident & Problem Management Information System, Office of Government Policy Coordination*; Ministry of Information and Communication: Seoul, Republic of Korea, 2005; pp. 20–31, 94–96. Available online: https://sysadmin.atlassian.net/wiki/spaces/sysadmin/pages/686915631/-2005+ITIL (accessed on 3 July 2023).
18. *2021 1/4–4/4 Information System Operation Result Report*; Public Institution: Seoul, Republic of Korea, 2021.
19. Cyber Response Force Team. *Defense Cyber Crisis Response Practical Manual*; R.O.K Ministry of National Defense: Seoul, Republic of Korea, 2021.
20. *Joint Education President 17-1, Joint Cyber Operations*; R.O.K Joint Chiefs of Staff: Seoul, Republic of Korea, 2017; pp. 6–11.
21. Internet Infringement Response Center. *DDoS Attack Response Guide*; Korea Internet & Security Agency: Seoul, Republic of Korea, 2021; p. 60.
22. Marsh. *Cyber Resilience: Twelve Key Controls to Strengthen Your Security*; Marsh: New York, NY, USA, 2022; pp. 19–20.
23. *Cyber Security & Operational Systems Resilience*; New Zealand's Financial Markets Authority: Auckland, New Zealand, 2022; p. 6.
24. National Security Office. *National Cyber Security Strategy*; National Security Office: Seoul, Republic of Korea, 2019; pp. 16–17.
25. Tsuji, D.; Fujita, J.; Matsumoto, N.; Tamura, Y.; Doenhoff, J.; Shigemoto, T. 3-layer modelling method to improve the cyber resilience in Industrial Control Systems. *SICE J. Control. Meas. Syst. Integr.* **2023**, 1–12. [CrossRef]
26. The Cyber Resilience Index: Advancing Organizational Cyber Resilience. In Proceedings of the 2022 World Economic Forum, Geneva, Switzerland, 18–19 July 2022; p. 14.
27. Youn, J.P.; Kim, K.K.; Kang, D.Y.; Lee, J.I.; Park, M.S.; Shin, D.K. Research on Cyber ISR Visualization Method Based on BGP Archive Data through Hacking Case Analysis of North Korean Cyber-Attack Groups. *Electronics* **2022**, *11*, 4142. [CrossRef]
28. Kim, K.K.; Youn, J.P.; Yoon, S.J.; Kang, J.W.; Kim, K.S.; Shin, D.K. Study on Cyber Common Operational Picture Framework for Cyber Situational Awareness. *Appl. Sci.* **2023**, *13*, 2331. [CrossRef]