electronics

MDPI

Article

A Study on Designing Cyber Training and Cyber Range to Effectively Respond to Cyber Threats

Yongjoo Shin [1,†], Hyukjin Kwon [2,†], Jaeyeong Jeong [3,4] and Dongkyoo Shin [3,4,*]

[1] Center for Military Analysis and Planning, Korea Institute for Defense Analyses, Seoul 02455, Republic of Korea; keen56@kida.re.kr
[2] Department of Protection and Safety Engineering, Seoul National University of Science and Technology, Seoul 01811, Republic of Korea; kwonhj@seoultech.ac.kr
[3] Department of Computer Engineering, Sejong University, Seoul 05006, Republic of Korea; jaeyeong@sju.ac.kr
[4] Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul 05006, Republic of Korea
* Correspondence: shindk@sejong.ac.kr
† These authors contributed equally to this work.

Abstract: As cyberattacks become increasingly sophisticated with advancements in information and communication technology, the impact of cyberspace threats is growing in both civilian and defense sectors. The utilization of cyber capabilities in operations is on the rise, prompting major nations to continuously enhance their cyber capabilities. This study aims to establish a systematic approach to cyber operations training and propose a framework for the development of cyber training. A hybrid cyber training system is designed as a plan for temporal and spatial integration to simultaneously combine simulation-based training with real-world target training. To develop this concept, a literature review was conducted, expert consultations were held, and data were collected and analyzed through visits to relevant organizations and units. Additionally, the fundamental components of cyber training were examined from environmental, scenario-based, and operational perspectives, leading to the presentation of a development direction for effective cyber training. This study is anticipated to enhance response capabilities to evolving cyber threats and attacks, improve cyber operational proficiency, and secure cyber power to achieve dominance in cyberspace.

Keywords: cyber range; cyber operations training; cyber exercise; hybrid cyber training; cyber training scenario

Citation: Shin, Y.; Kwon, H.; Jeong, J.; Shin, D. A Study on Designing Cyber Training and Cyber Range to Effectively Respond to Cyber Threats. *Electronics* **2024**, *13*, 3867. https://doi.org/10.3390/electronics13193867

Academic Editor: Hung-Yu Chien

Received: 31 July 2024
Revised: 19 September 2024
Accepted: 26 September 2024
Published: 29 September 2024

1. Introduction

With the rapid development of advanced information and communication technologies, cyberattacks have become highly sophisticated, and the effects of cyberspace are expanding in both civilian and defense domains. Many countries continue to make efforts to expand their cyber capabilities. For example, the United States continues to invest in cyber exercises and cyber range to secure cyberspace dominance. However, the lack of a concept of scenario-based cyber training for cybersecurity has created difficulties in conducting effective cyber activities. In particular, despite the fact that rapidly developing information and communication technologies are being utilized for cyberattacks, there are insufficient cyber training infrastructures for cyber activities that can effectively respond to them. There is a lack of content and facilities for team- and institutional-level cyber training and on-the-job training that can enhance the expertise of cyber professionals and develop them into cyber professionals [1]. In addition, there is no integrated cyber training system that can verify cyber activity scenarios and countermeasures for effective cyber training [2].

Cyber training is conducted by establishing a network environment in the business cyberspace or simulation environment, which is the real system to be trained; injecting a scenario in which a cyberattack or defense can be performed; and providing all the

necessary conditions for participants to conduct cyberattack and defense training. The components of the cyber training are categorized as Environment, Scenario, and Operation. The cyber training Environment is the network and system to be trained in the cyber range and is increasingly being built using virtualization technology rather than physical systems due to space and cost issues [3,4]. A training scenario is a training content that can perform a cyberattack or defense in the environment of a cyber range. It is a task to be performed by trainees participating in the training and conducted in a problem-solving format or a series of processes for actual execution. The training operation is related to the actual training after the training scenario is injected into the environment of the cyber range, and the training participants are divided into Red Team, Blue Team, Green Team, and White Team according to the roles they play [5].

In this paper, based on the implications of cyber training trends and the opinions of cyber training participants and operators from the perspective of cyber training components, two directions were derived for the development of cyber training. First, a hybrid cyber training system should be established [6]. Since real-world and simulation-based training have opposite advantages and disadvantages, it is necessary to conduct and integrate both simultaneously rather than choosing only one. Temporal integration and spatial integration are proposed as means to realize a hybrid training system. The second is the composition of an integrated cyber range. Each organization establishes cyber training that reflects its characteristics in cyberspace, and the organization in charge of cyberattack and defense (cyber activity operation organization) establishes a cyber range that enables integrated cyber training and connects each cyber range with a network. This integrated cyber range can improve the ability to conduct cyber activities within each organization's specialized cyberspace, conduct cyber training at different scales depending on the participating organization, and share the capabilities and resources of each cyber range. Through the method presented in this study, it will be possible to ensure response capabilities similar to real-life situations by conducting balanced cyber training in real and virtual environments. In addition, it is possible to combine each specialized cyber range to configure various forms of cyber training that fit the training purpose. This will enable the effective operation of cyber ranges by supporting various forms of cyber training by combining modular training centers. It is expected that this method of conducting cyber training and operating cyber ranges will contribute to ensuring effective response capabilities against evolving cyber threats and cyberattacks, improving performance capabilities in cyber activities, and ensuring cyber power to ensure future cyberspace superiority. The contributions of this paper are summarized as follows:

- It enables real-life cyber training that links the real system and virtual space without compromising the availability of service provision in the real system.
- It saves the time and effort required to expand the cyber training field and provides a flexible cyber training field configuration plan based on a high-quality network.

The remainder of this paper is organized as follows. In Section 2, a theoretical review of cyber training is provided, with relevant terms defined and the purposes and types of cyber training categorized. Section 3 examines the current status and trends of cyber training conducted by the United States. The components of effective cyber training are discussed in Section 4. A hybrid cyber training system, designed as a plan for temporal and spatial integration to simultaneously combine simulation-based training with real-world target training, is proposed in Section 5. Section 6 describes the survey analysis conducted to determine the type of training preferred by each user. The study is concluded in Section 7.

2. Background Studies

In this section, terms related to cyber training, as well as the purpose and types/methods of cyber training, are categorized. In particular, the term "training" is considered confusing because various words are used not only in physical space but also in cyberspace. The terms related to training are defined through operational definitions and utilized in this paper. Additionally, the purpose and types/methods of cyber training are defined and categorized.

2.1. Exercise/Training Terminology

The definitions of terms related to exercises and training are not generally agreed upon [7]. Individuals and organizations use terms that are semantically similar but with subtle differences. In many documents, the words used to refer to exercises and training are also used in a variety of ways, with no specific rules or principles. Table 1 summarizes the various uses of these words.

Table 1. Terminology related to cyber training.

Terms	Description
Education	the action of process of teaching someone
Training	a process by which someone is taught the knowledge and skills
Practice	the activity of doing something again and again to become better at it
Drill	an activity that is done repeatedly to learn something
Exercise	the series of activities done to improve the capability of elements of process based on scenario
Rehearsal	an event at which a person or group practices an activity
Test	to measure someone's skills, knowledge, or abilities

"Education" is the activity of teaching knowledge and skills, focusing on teaching and learning. "Training" is the activity of learning and mastering new knowledge or skills learned through education, and it is executed and practiced through 'Execution/Practice' to master knowledge and skills. In addition, it is necessary to perform it repeatedly through "Drill" to effectively master it. "Exercise" is the process of reacquainting and practicing mastered knowledge and skills. "Rehearsal" is a comprehensive set of exercises that are performed in the exact same order before an event. As an activity to evaluate learning and mastery, "Test" is used to measure the level of mastery of knowledge and skills, identify deficiencies, and perform the drill again. The relationship between practice and training is summarized in Figure 1.

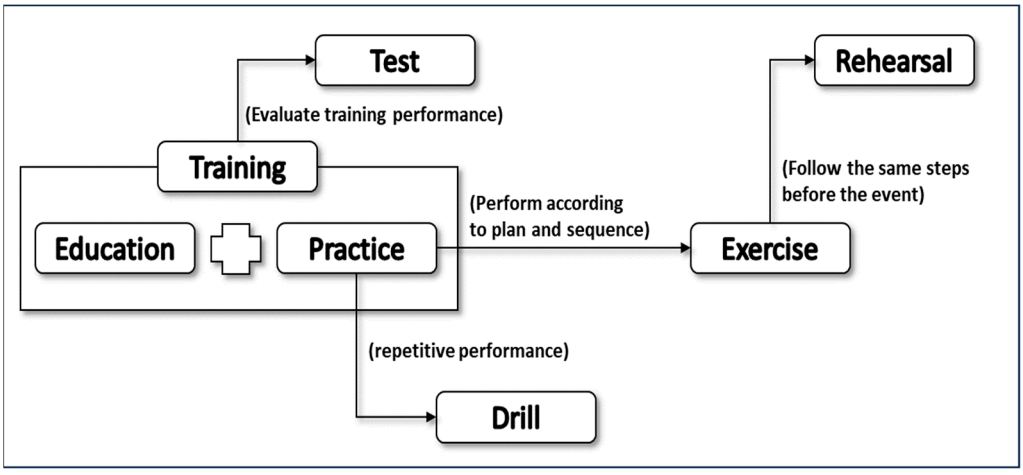

Figure 1. Relationship between training and exercise.

"Training" is composed of "education" and "practice". Basically, "training" is learning knowledge and skills through "education", and "practice" is practicing and refining the acquired knowledge and skills. If this method of training and refining is performed repeatedly, it becomes a "drill", and if it is performed according to a plan and procedure, it becomes an "exercise". If "exercise" is performed from beginning to end with the same procedure before the event, it becomes a "rehearsal". In addition, a "test" is performed to evaluate the results of "training".

2.2. Purpose of Cybyer Training

Cyber training is conducted for various purposes, which can be generally categorized into the performance intention perspective and the expected effect (outcome) perspective [8,9]. The performance intention perspective is categorized into five types, as shown in Table 2, depending on the intent of the cyber exercise. "Identification" emphasizes and identifies vulnerabilities or procedural flaws and information-sharing processes. "Testing mechanism and/or procedures" evaluates established tools, practices, procedures, etc., to ensure that existing systems are fit for purpose or that newly developed systems of practice are operating as intended. "Exercising mechanisms and/or procedures" is practicing using established mechanisms and procedures to ensure readiness in the event of an actual security incident. "Increasing communication and cooperation" identifies communication channels between actors with differing priorities in practice, such as public and private sector organizations or different national cybersecurity frameworks. "Developing policies and procedures" means that the purpose of conducting cyber training is to identify gaps in your current policy framework or bottlenecks in policies that prevent an effective response to a cyber incident. Through this process, it is possible to develop policies where none currently exist.

Table 2. Purpose of cyber training (aspect of performance intention).

Aspect	Purpose	Description
Performance Intention	Identification	Highlight and identify vulnerabilities, procedural deficiencies, and information-sharing mechanisms
	Testing mechanisms and/or procedures	Evaluate established tools, practices, procedures, etc., to ensure that existing systems are fit for purpose or that newly developed practices are functioning as intended
	Exercising mechanisms and/or procedures	Exercise using established mechanisms and procedures to ensure readiness in the event of an actual security incident
	Increasing communication and cooperation	Identify communication channels between actors with different real-world priorities, such as public and private sector organizations or different national cybersecurity frameworks
	Developing policies and procedures	Develop and produce new and efficient methods and response procedures through simulation exercises

Unlike the intention to perform, the purpose of cyber training can be categorized in terms of expected effects (training outcomes), as shown in Table 3. "Awareness" is to introduce cybersecurity to the general public (participants) and make them aware of the cybersecurity situation. "Hard skill/Technical" provides technical skills to those who need to perform specific procedures related to cyber incident management. "Soft skill/Non-technical" secures non-technical skills such as cooperation, communication, and decision-making to form a high level of cyber incident management capability. "Resilience" ensures a high level of resilience/recovery by assessing the organization's ability to adapt to unpredictable situations.

Table 3. Purpose of cyber training (aspect of expected effects and results).

Aspect	Purpose	Description
Expected effects and results	Awareness	Introduce cybersecurity to general individuals (participants) to create situational awareness
	Hard skill/Technical	Provide technical skills for those who need to perform specific procedures related to cyber incident management
	Soft skill/Non-technical	Acquire non-technical skills such as cooperation, communication, and decision-making to form a high level of cyber incident management capability
	Resilience	Achieve a high level of resilience/recovery by assessing the organization's ability to adapt in unpredictable situations

2.3. Types and Method of Cybyer Training

Types and methods of cyber training are divided into discussion-based and operation-based, as shown in Figure 2. Discussion-based cyber training focuses on procedural issues and improvements rather than seeking technical solutions in a simulation environment because participants discuss effective response procedures for a given situation without constructing equipment or other resources. On the other hand, operation-based cyber training focuses on effective activities and actions through improving, measuring, and training cyber capabilities in a realistic training environment by constructing a virtual or secure network [10]. Each cyber training does not have a hierarchical relationship, and two or more types of cyber training are sometimes integrated to achieve the training purpose.

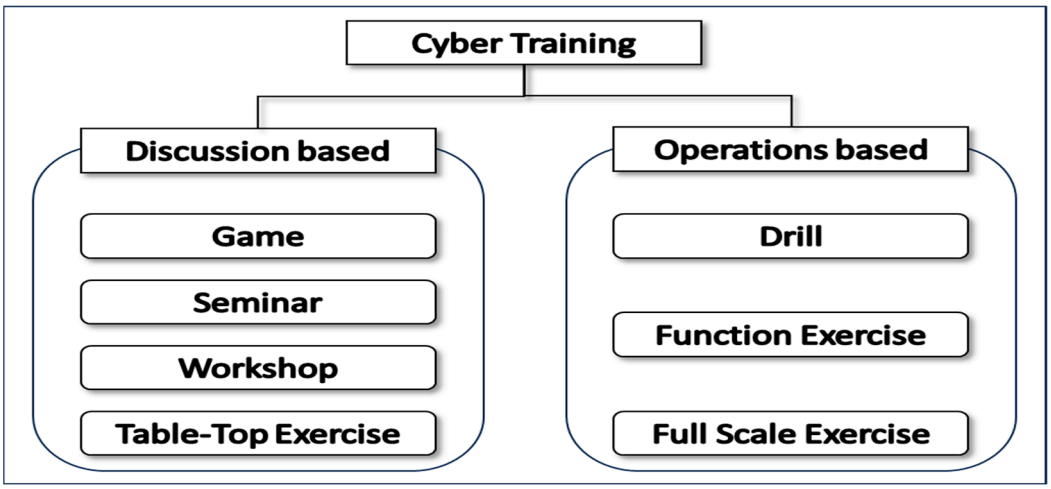

Figure 2. Types and Method of Cyber Training.

"Seminar" is an informal discussion that provides an overview of new or updated plans, policies, procedures, protocols, resources, authorities, concepts, and ideas. "Game" is played by two or more teams that make decisions and take actions in a hypothetical situation. The outcomes of player actions can be predetermined or dynamically determined. They are useful for validating procedures or assessing resource requirements. "Workshops" are similar to seminars but with increased interaction between participants and a focus on training outcomes. To be effective, they should always have clearly defined objectives, focus on specific issues, and involve relevant stakeholders. "Table-Top Exercise" is a discussion-based session where team members meet in an informal classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator guides participants through a discussion of one or more scenarios. "Drill" is most effective when regularly repeated because they are used to reinforce practice. The procedures being reinforced should already be validated and approved, and organizational-

level awareness should be established. They are typically used to learn new equipment, validate procedures, or practice skills. "Functional Exercise" is designed to validate and assess the coordination, command, and control capabilities of personnel. Exercise scenarios are typically conducted in a realistic, real-time environment that simulates the movement of personnel and equipment. Exercise control uses a situation list to ensure that activities remain within predefined bounds and objectives are met. Simulators inject scenario elements to simulate real-world events and are used to enhance current capabilities and achieve high adaptability. "Full-Scale Exercise" is the most complex type of exercise and is multi-agency, multi-jurisdictional, and multi-disciplinary exercises that aim to validate multiple aspects of preparedness. Activities in exercise scenarios are driven by operational-level, real-time event updates that attempt to reconstruct the stress environment of a real-world event. Personnel and resources are realistically mobilized, and the problems are realistic and require critical thinking and quick and effective responses. Situations and events that may occur between exercises may occur simultaneously.

2.4. Relationship of Cyber Training Purpose and Types/Method

The relationship between the purpose and type/method of cyber training can be shown in Figure 3. Among discussion-based cyber exercises, "Game" is mainly conducted for the purpose of "Identification", while "Seminar" and "Workshop" are conducted for "Identification" and "Testing". "Table-Top Exercise" is widely used for various purposes such as "Practice", "Communication/Collaboration", and "Policy Development". Among activity and behavior-based cyber exercises, "Drill" is primarily used for "Identification" and "Testing" purposes and may also be utilized in some exercises, while "Functional Exercise" is used for "Testing" purposes and, like "Drill", may also be utilized in exercises. "Full-Scale Exercise", which is the most widely practiced, is mostly conducted as comprehensive drills and exercises for training purposes. The relationship between training purpose and type/method is to recommend the type and method that is appropriate for the purpose. It is possible to apply the purpose and type differently from the figure below, and it is possible to design the type and method of training by mixing several purposes. Therefore, it is appropriate to utilize the types and methods of training that meet the objectives as a guide. "Drill" and "Functional Exercise" are not performed completely for the purpose of "Exercise mechanisms and/or procedures" but are performed partially to achieve that purpose, so they are marked as half.

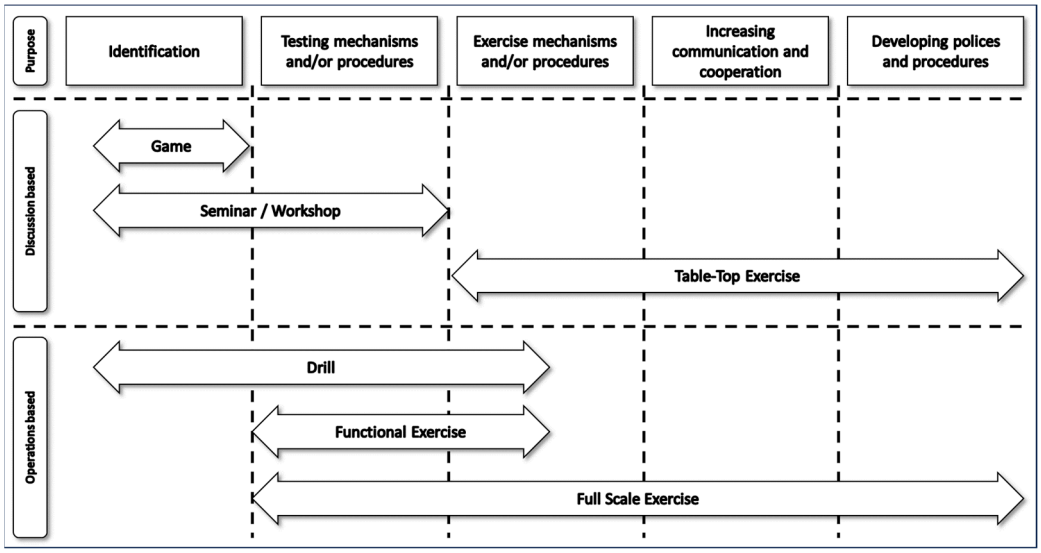

Figure 3. Relationship of Cyber training purpose and types/method.

3. An Examination of Cyber Training in the United States

Globally, the United States has the most advanced and organized cyber capabilities. In addition, the United States publicly discloses information about its cyber training. This study will examine the most advanced and publicly disclosed U.S. cyber training and provide implications. The United States conducts cyber training at both the national and defense levels. The Department of Defense's cyber missions and functions are divided into cyber operations and cybersecurity. The Cyber Mission Force (CMF) is responsible for cyberspace operations and is comprised of National Mission Teams/National Support Teams, Combat Mission Teams/Combat Support Teams, and Cyber Protection Teams. National Mission Teams/National Support Teams protect national security and interests, monitor adversary activities, and interdict and defeat cyberattacks. Combat Mission Teams/Combat Support Teams support the Unified Combatant Commands and conduct military cyber operations. Cyber Protection Teams protect and defend military networks and critical missions, respond to active threats, and conduct preventive and active defense missions [11,12].

3.1. Examples of Cyber Training at the United States National Level

The U.S. Cybersecurity and Infrastructure Security Agency's (CISA) "Cyber Storm" is a government-sponsored, biennial cyber training that has been running since 2006 and provides a framework for broader cybersecurity training. It brings together the public and private sectors to simulate the discovery and response to a major cyber incident affecting national critical infrastructure. In March 2022, the eighth Cyber Storm exercise brought together more than 2000 participants from the U.S. government (federal, state, and local), the private sector, and main international partners to investigate the discovery and response to a large-scale, critical cyber incident affecting critical infrastructure sectors [11–14].

"Cyber Shield" is a defense-focused cyber training designed to develop, train, and exercise National Guard cyber capable units, cyber network defense teams, threat analysis teams, reporting mechanisms, and leaders. The purpose of the training is to provide a collective training event to assess Cyber Network Defense Teams (CND-Ts) and set the conditions for team validation [13–16].

The Cyber Defense Exercise (formerly NSA Cyber Exercise) is an annual competition organized by NSA information assurance experts that is conducted in a competitive manner. It tests the skills to build, secure, and defend networks against hostile attacks. It has been held since 2001 and is sponsored by the Information Assurance Directorate and conducted in partnership with several organizations within the NSA [13–16].

3.2. Examples of Cyber Training at the United States Defense Level

"Cyber Flag" is a multinational cyber military exercise organized by the U.S. Cyber Command (CYBERCOM), which has been held annually since 2011 to strengthen coalition cyber readiness and partnerships with allies and friendly nations. It consisted of tactical-level cyber defense exercises and symposium-style seminars centered at the U.S. Military Cyber Training Center. The tactical exercises were conducted to share risk information and identify effective countermeasures to verify the effectiveness of defensive operations and to master the procedures of defensive cyber operations, including identifying, analyzing/sharing, eliminating, and denying cyber threats. The symposium included a briefing by U.S. Cyber Command and panel discussions by participating nations, as well as academic discussions to promote cooperation among allies in cyberspace and identify ways forward [13–16].

"Cyber Guard" is a training program organized by CYBERCOM to practice a nationwide response to a major incident affecting U.S. critical infrastructure. Conducted annually since 2012 by CYBERCOM in conjunction with the mission of the U.S. National Guard, it is a tactical-level cyber exercise involving military, public, and civilian cyber operations organizations such as CMF teams. However, its main focus is to practice and improve information sharing, cooperation with government and civilian response systems, and

military support plans and processes in the event of a serious cyber breach of national or civilian critical facilities. Cyber Guard is constantly evolving and expanding to meet the needs of the Ministry of Defense and the nation [13–16].

"Cyber Night" provides a joint cyber training certification and validation event to conduct force assessment and validation of CMF and cyber operations. It is a regularly scheduled training event provided by CYBERCOM for CMF teams to train on a variety of missions. "Cyber Lightening" is a cyber domain exercise/training event hosted by CYBERCOM as part of Global Lightning, a global integrated exercise coordinated and led by U.S. Strategic Command (USSTRATCOM). The 2020 Global Lightning exercise elements include Cyber Lightning (CYBERCOM), Vigilant Shield (North American Aerospace Defense Command/NORTHCOM), and Turbo Challenge (U.S. Transportation Command). "Cyber Hunt Even" is the Air Force's 567th Cyber Operations Wing's bimonthly cyber training that began in early 2018, with the primary objective of strengthening participants' defensive tactical, technical, and procedural (TTP) skills [13–16].

3.3. Implications of U.S. Cyber Training

In Figure 4, the purpose, type/method, and level of cyber training conducted at the national and defense levels in the United States are shown. As a leader in cyber training, the types and methods of cyber training have been diversified in the United States depending on the purpose of the training at both the national and defense levels, and training is being conducted at the technical, operational, and strategic levels.

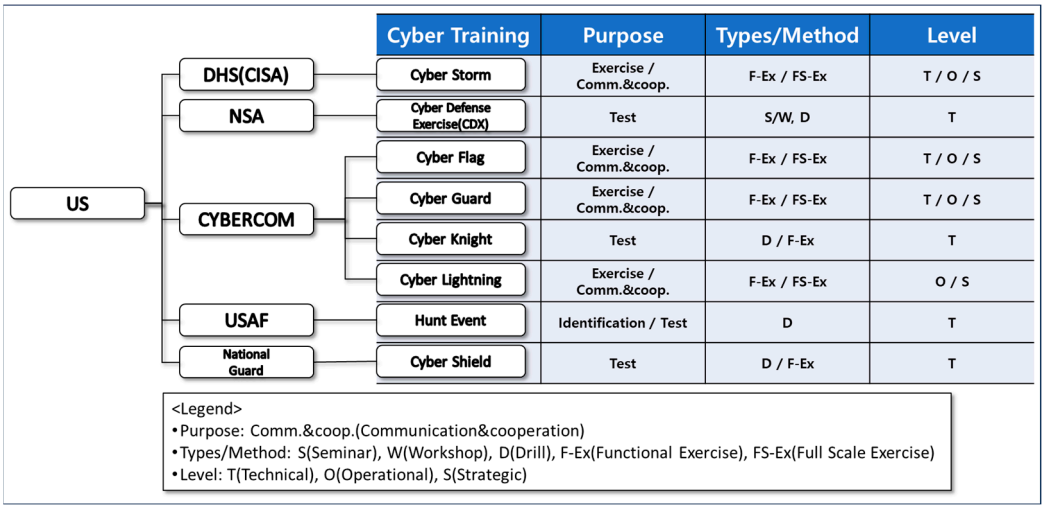

Figure 4. Summary of major cyber training cases in the U.S.

The United States conducted cyber training at the national and defense levels. At the national level, it emphasized cooperation between related organizations and other countries. At the defense level, training was systematically conducted at various levels (strategic, operational, tactical) and on scales that matched the training objectives. To achieve these training objectives, it developed various training scenarios and tried to build a flexible cyber range. Accordingly, it actively applied cutting-edge ICT technologies, including virtualization technology, to build a cyber training site that matched the training objectives.

After examining the trends of cyber exercises in the United States, the following implications were drawn for the development of the cyber training system. First, it is necessary to establish a systematic procedure for conducting cyber training. The procedure should secure a training system consisting of planning, preparation, execution, and evaluation. In particular, it is necessary to provide practical feedback to improve participants' cyber response capabilities and reflect them in the planning and design of future exercises during the evaluation phase. Second, various training scenarios should be organized according to the purpose of the training. Developing scenarios specific to the purpose and context of

each exercise will maximize the effectiveness of the training. It is increasingly necessary to prepare for realistic exercises by including the latest cyberattack techniques and cybersecurity incidents that are rapidly evolving. Third, it is necessary to build a simulation environment based on virtualization technology. It requires implementing an environment similar to the real system by utilizing virtualization technology and conducting cyber training using varying attack techniques and the number of participants within the simulation environment. In addition, it is necessary to build and operate specialized training grounds separately and integrate them in consideration of mission and regional characteristics. Fourth, it is necessary to conduct effective training by applying the latest information and communication technologies. In particular, a more effective and efficient training system will be possible if a cloud environment is used to build a training range and if a real-time automatic evaluation system and RED team operation using AI are established.

4. Key Components of Cyber Training

Cyber training requires a cyber range to support them. A cyber range simulates a network environment and injects scenarios for cyberattack or defense into the target network environment (cyberspace or simulated environment) to provide the necessary environment for participants to conduct cyber training. The components of cyber training can be categorized into two phases: preparation and execution. The preparation phase consists of Environment and Scenario, and the execution phase refers to Operation, which is the actual cyber training [17]. The details of each component are described in the following sections.

4.1. Cyber Training Environment

Cyber range is an interactive and simulated platform that replicates networks, systems, tools, and applications. They provide a safe and legal environment for acquiring hands-on cyber skills and offer a secure setting for product development and security posture testing. A cyber training environment refers to the area of hardware required to build a cyber range [18].

A cyber training environment is a cyber range. Specifically, it refers to the networks and systems subject to training in the cyber range. The networks and systems in the cyber range simulate various environments such as institutional networks, SCADA (Supervisory Control And Data Acquisition), IoT (Internet of Things), mobile, etc. Due to these characteristics, the network environment must be well simulated, and the technology factor is of utmost importance [19]. The cyber range environment refers to the cyberspace that is the target of training. Therefore, a cyber range is often applied to cyber threat scenarios by expanding from network test beds. Closed networks used for special purposes, such as SCADA, are also simulated for training purposes.

In recent years, due to space and cost issues, virtualization technology has been used more and more than physical systems. In other words, with the development of virtualization technology, training environments are being built using virtual machines, and the training target environment is being expanded by building them together with physical systems. In particular, the Cyber-Physical System (CPS) requires a physical system that connects to cyberspace, so physical systems are operated in parallel [20].

The cyber range can be divided into Management Area, White Area, Offense Area, and Defense Area [17]. The Management Area is responsible for managing the systems for operating the training range, participating trainees, accessing the Web interface (portal), training scenarios, etc. Various systems are required for this purpose. The management system manages the overall cyber range. The DB system stores and manages all data generated during the training. The real-time response monitoring system observes the status of systems in the defense area during real-time response training. The preventive security and reactive monitoring system observes the status of systems accessed by trainees during preventive security and reactive training. The training score system collects and processes the scores of trainees in the process of solving preventive security, real-time

response, and reactive training scenarios. The capability assessment system evaluates the trainees' cybersecurity capabilities based on their training scores and the training missions they have performed.

The white area simulates websites and users in the training network, i.e., it generates normal traffic to the defense area to provide an analysis environment for real cyber incidents. This requires a normal website simulation system, which is a set of websites to simulate the training network environment accessed by users in the defense area. The normal user simulation system generates web server access traffic to simulate users accessing web servers in the defense area [21].

During real-time response training in the attack area, web servers and devices in the defense are attacked. The level of attack varies depending on the stage of the cyber crisis alert. In the attack area, the web server attack system performs attacks that exploit the vulnerabilities of web servers in the defense area simultaneously or one after another, depending on the training scenario. The terminal attack system performs attacks by receiving commands from the C&C (Command and Control) through malicious code secretly installed in the terminal. The defense area is the area the trainees must protect from cyberattacks, and the system configuration can vary depending on the training scenario.

4.2. Cyber Training Scenario

A training scenario is training content that allows you to perform a cyberattack or defense in the environment of a cyber range. Scenarios are tasks that trainees participating in training must perform. Through scenarios, cyber training participants can experience cyber attacks or defenses as if they were real. Scenarios can be built on the cyber range environment through vulnerable systems. Therefore, the more similar the cyber training ground environment is to the training target network, the better the scenario reflects reality. Depending on the scenario content, it can comprise various fields such as attack, defense, incident investigation, and prevention. An attack scenario is a cyberattack on a specific target, while a defense scenario is a defense against a cyberattack [22]. An incident investigation analyzes the cause of the incident and the damage to the system that was attacked, and a prevention scenario is about eliminating vulnerabilities in the system that could lead to a cyberattack. In addition, a scenario is a set of tasks that trainees in cyber training must perform, either in a problem-solving format or as a series of practical training. The more similar the scenario is to the network being trained, the more realistic the scenario will be. Therefore, the scenario must be able to define and represent the cyber threat situation [23,24].

There are two main types of exercise scenarios: Capture the Flag (CTF) and Live-Fire. The CTF method is a method of approaching vulnerabilities in already installed systems and solving problems. There are two types of CTF: the Jeopardy-style method, which solves security-related problems in various fields, and the Attack-Defense method, which finds and fixes security problems in virtual machines with vulnerable services. The Live-Fire method performs cyberattacks or defenses in real time. Cyberattacks or defenses are performed in real time, so cyber training can be conducted in realistic situations [8].

4.3. Cyber Training Operation

Operating a training range for cyber training requires adequate physical space, technical equipment, software, a secure environment, operations and maintenance personnel, education and training programs, and evaluation systems. The operation involves the actual execution of training after the training scenario is injected into the cyber training environment. Training participants are classified into the Red Team, Blue Team, Green Team, and White Team according to the role they perform. In addition, depending on the role of the training participant, it can be conducted as training based on cyber threat scenarios, hacking response training, Blue Team/Red Team bilateral training, and vulnerability assessment training.

A physical space of appropriate size and stability is required to operate the cyber range, and technical equipment such as servers, switches, routers, and networks are required to operate the cyber range. In addition, software (learning modules, simulations, testing tools, etc.) for operating the cyber range, as well as network configuration, server, and application security with enhanced security as various hacking and cyberattack scenarios are simulated, are necessary [4]. For ongoing maintenance and operation, operations and maintenance personnel and specialized trainers (white hackers) who can provide the latest skills and knowledge are required. A training system should be established to organize the education/training curriculum by situation and level, provide various training programs, and run scenarios that allow trainees to gain experience similar to real-life situations by performing simulated attack scenarios in cyber training [25]. A system for tracking and evaluating the progress of trainees should be in place to measure their performance and generate reports.

Training operations are concerned with the actual execution of the training after the training scenario has been injected into the cyber range environment [17]. Training participants are categorized into the Red Team, Blue Team, Green Team, and White Team according to the roles they play. Red Team (RT) is the role of conducting cyberattacks, and if the scenario is a cyberattack, the trainee can perform the role of the Red Team, while if it is a cyber defense, the task can be performed by the White Team that runs the training. Blue Team (BT) is a role that performs a defense against a cyberattack by the Red Team and can enhance the trainees' ability to respond to cyber threats by performing cyber defense. The Green Team (GT) is responsible for building the cyber range environment and does not directly participate in the training; instead, it builds a training environment where scenarios are injected. It also builds the environment of the cyber range and monitors the status of the built system. The White Team (WT) is responsible for injecting training scenarios and operating the training, conducting training through scenario execution, and managing and calculating the trainees' scores. The scores obtained are utilized as important information to identify the degree of training performance of the trainees [26].

5. Hybrid Cyber Training System and Integrated Cyber Range

A hybrid cyber training system and an integrated cyber range are proposed in this section. To this end, the cyber training trends in the United States identified in Section 3 are analyzed based on the concepts of exercise and training defined in Section 2, and the construction of a virtualization-based simulation environment and the application of the latest information communication technology are examined. Additionally, the development direction is derived from the perspectives of the cyber training components classified in Section 3—namely, Operation, Scenario, and Environment.

This study investigated trends in cyber training being conducted in the United States and analyzed the implications to derive effective cyber training implementation methods and cyber range composition plans. In addition, it distinguished the components of cyber training and suggested directions for improvement from the operational and environmental perspectives.

The cyber training methodology and cyber range configuration proposed in this paper are based on the opinions of participants and operators who actually conduct cyber training. In addition, we visited related organizations that conduct cyber activities and support cyber training and derived our findings based on their opinions on improvements for effective cyber activities.

5.1. Hybid Cyber Training System

Cyber training is generally categorized into three types. The first is a discussion-based cyber training system. It aims to improve the ability to perform cyber activities and maintain defense posture. It is conducted in the following order: situation occurrence, initial response, situation action, and follow-up action. The second type is a cyber training system targeting real systems. It aims to identify the vulnerabilities of real systems and cultivate

the ability to perform effective cyber activities. By utilizing training scenarios based on training objectives and tasks, cyberattacks are conducted against real systems, and defense measures are taken in response. To maintain the service and data level of the real system, the cyberattack is conducted up to the penetration stage for training. The third type is a simulation-based cyber training system. It is conducted in a simulated environment to improve the ability to take countermeasures against various cyberattacks and situations. It is a training that secures response capabilities through various cyberattacks in a virtual cyber environment and conducts unlimited cyberattacks without considering the service and data levels of the virtual information system. In terms of the purpose of cyber training, discussion-based drills are suitable for training for identification and communication/cooperation, cyber training conducted against real systems focuses on the purpose of identification, and simulation-based drills focus on the purpose of policy development.

Discussion-based cyber training is training on countermeasures against cyber situations based on discussions and reports. It does not require a small budget for training preparation and the deployment of equipment, so measures against cyber situations are carried out through discussion and situation reports. The training period can be freely set, so short-term and long-term training programs can be designed. In addition, it is possible to check and improve the measures and response procedures in the event of a cyber situation with minimal resource investment. Disadvantages include limited technical response capabilities to actual cyberattacks and the acquisition of know-how based on experience. It is limited in improving technical response measures and utilization of tools/solutions. In addition, it is difficult to expect creative measures due to mechanical responses and situation reports according to the planned situation due to the lack of tension and actual experience in the urgency of cyber incidents. There are limited factors in securing and improving technical capabilities for cyber activities.

Cyber training against real systems can improve attention to the information system to be defended and protected through cyberattacks and defenses against them. Vulnerabilities of real systems can be identified and corrected after training, and separate spaces and facilities for cyber training are not required. However, cyberattacks and defense activities that may interfere with the service availability of the actual information system are limited, and only activities that meet the purpose of the training are possible. Operators of real systems may feel burdened and reluctant to conduct training, which may limit their ability to organize various cyberattack forms and training scenarios. In addition, to protect the services and data of the real system, it is only possible to proceed to the penetration stage, which limits the ability to check the impact of cyberattacks.

Simulation-based cyber training enables various cyberattacks and defense activities without limitation in a simulated environment that is identical to the real environment. Training can be conducted regardless of information system damage or service failure. Various attack attempts after the infiltration stage of a cyberattack are possible, allowing for ripple effects and various training scenarios. However, there may be cases where it is not possible to simulate a real system. It is technically impossible to perfectly simulate real-world systems, and the implementation of non-public software into virtualization solutions is limited. In addition, the technical shortcomings and limitations of virtualization and emulators can affect the results and effectiveness of training. This means that technical limitations can affect the simulation environment and training outcomes. Space, facilities, and equipment are required to set up a simulation environment (utilizing virtualization technology).

To conduct effective cyber training, it is necessary to establish a hybrid training system that integrates both forms of training. Real-world-based training and training in simulated environments have opposite advantages and disadvantages. Therefore, rather than selecting one type of training, it is necessary to conduct both types of training simultaneously and integrate them so they complement each other.

There are two ways to time a hybrid training regime: temporal integration and spatial integration, as shown in Figure 5. Temporal integration involves real-world training in the

first half of the year and simulation in the second half of the year. In the first and second half of the year, training is conducted alternately in real-world training and simulation environments. Alternatively, real-world-based training can be conducted in the first and second halves of the program, with additional training in a simulated environment in the interim period. Spatial integration is the combination of real-world and simulation environments to form a training environment. Real-world equipment and simulated equipment can be organized in the same space. If there is a physical distance between the real system and the simulation equipment, they can be logically connected through a network to form the same training environment. In this way, simulated attacks can be carried out on the real system within a range that does not compromise services and data, and cyberattacks can be carried out in the connected simulation environment without any restrictions, providing the best of both worlds. By first penetrating the simulation equipment to secure a bridgehead and then attacking the real system serviced by the internal network, a realistic training environment can be organized.

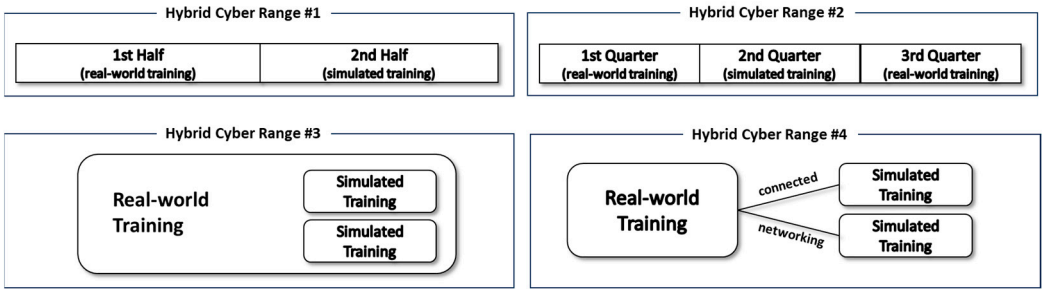

Figure 5. Types of hybrid cyber range.

To explain, specifically, temporal integration is designed to alternate between actual training and virtual space training according to the training schedule of twice a year and three times a year based on the number of training sessions. In the spatial integration method, a model is presented that builds a virtual space where training is possible within the actual system, and it trains and builds a training environment by connecting the actual system and the virtual training space through a network.

5.2. Operating Integrated Cyber Ranges

The operational concept of an integrated cyber range is to build and operate individual cyber ranges considering the cyber environment of the training headquarters and subordinate organizations (branches). An integrated cyber range means connecting distributed training centers through a network and utilizing them as a single training center. Through this, specialized services and resources of each cyber range can be shared, and there is a spatial advantage of participating in training from a distance. The methods and purposes of cyberspace utilization by the training headquarters and each subordinate organization are different. In general, the training headquarters conducts high-level cyber activities. Each subordinate organization utilizes various data in cyberspace to carry out detailed purposes and missions. To conduct effective cyber activities, it is necessary to build cyber ranges individually to reflect the characteristics of each organization's cyberspace, as shown in Figure 6, and the training headquarters should conduct integrated cyber training by interconnecting subordinate organizations to achieve high-level goals.

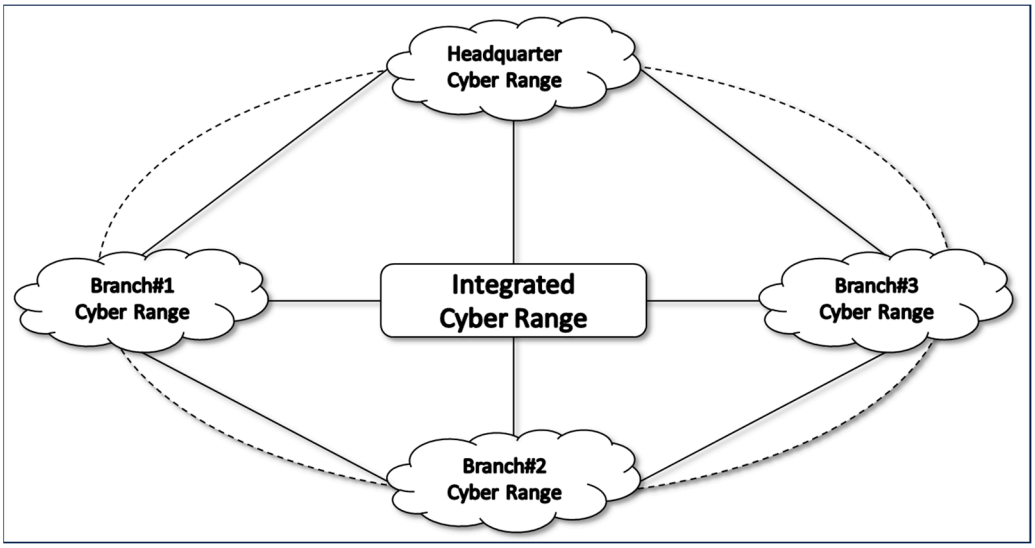

Figure 6. Concept of integrated cyber range.

Through the operation of an integrated cyber range, it is possible to conduct training to improve the ability to perform cyber activities within the specialized cyberspace of subordinate organizations. It is possible to check the performance of cyber activities in the specialized environment of the subordinate organization and derive directions for improvement. It can provide a test bed to test and evaluate the detailed functions of the subordinate organization in terms of cybersecurity. Cyber training can be conducted on various scales depending on the sub-organizations participating in the training center. It is also possible to share the capabilities and resources of each cyber range. The training center can support specialized counter-organizations in the cyber training of subordinate organizations and distribute and simulate traffic and normal user activities between exercises to effectively utilize resources.

To operate such an integrated cyber range, first, management capabilities are required for efficient linkage and integration of cyber ranges. The ability to plan, conduct, control, and evaluate cyber training centrally at the training headquarters must be secured, and the ability to develop scenarios that meet the training objectives according to the size and level of training participants is required. It is also necessary to design and configure infrastructure, such as cloud environments, for effective sharing of various capabilities and resources. Second, management and support capabilities are required to network the cyber ranges of the training headquarters and subordinate organizations. Technical network environment planning and protocols such as IP and bandwidth are required to connect cyber ranges.

To operate an effective integrated cyber range, a training environment that can support the integrated training center must be established in advance. It is necessary to design a training range for practical training in cyberspace that reflects the characteristics of subordinate organizations. A hybrid training system (real system + simulation) should be established by reflecting the detailed functions and networks operated by subordinate organizations in the simulation. An implementation plan for embedded SW (embedded software) included in the detailed functions should be secured. Specialized scenarios should be developed, and specialized counterattack organizations should be operated. In addition, a budget and effective management plan for distributed cyber ranges are needed. It is necessary to establish a plan for effective training operations by efficiently distributing resources rather than duplicating investments.

To establish an effective cyber range, various considerations should be examined [27]. Effectiveness is a review of whether it is possible to perform missions and tasks, and it should consider whether the ability to perform missions and tasks that can contribute to the achievement of cyber training goals is secured. The organization's ability to perform

missions is improved. Scalability is a review of whether it is possible to interlock and expand with other cyber training systems and should consider whether it is possible to comply with interoperability for interlocking and integrating military, civilian, and overseas cyber ranges and to hold cyber competitions (hacking defense, attack/defense, vulnerability identification, etc.) using the training range infrastructure. In terms of affordability, the efficiency of budget and space should be considered to prevent duplication of investment and maximize space utilization. In terms of utilization, it should be able to identify vulnerabilities in the actual system providing the service, provide a testbed for cyber capabilities, and conduct a trial evaluation of cybersecurity. It should also be able to certify the ability of individuals and units (teams) to perform cyber activities. Finally, modernization should consider the application and utilization of cutting-edge information and communication technologies such as Al, Cloud, 5G, etc., and the ability to quickly reflect the latest cyberattack techniques into scenarios.

Among the latest information and communication technologies, the priority of technologies required to build an effective cyber range was identified through a survey. Among the representative information and communication technologies, the technologies that are related to the construction of cyber range and can be applied to maximize the purpose of training are categorized by users involved in training and summarized as shown in Figure 7. From the results, the importance of AI, Bigdata, and Cloud technologies was greatly recognized. Across all user groups, these three technologies accounted for 70 to 80 percent of the training. Training participants and operators expect AI capabilities to improve automated attacks and user responses, and operators expect cloud technologies to increase the scalability and versatility of training grounds. In the future, it is expected that more sophisticated and complex forms of cyber training will be possible through the development of AI technology, and the infrastructure for this will need to be developed based on cloud technology. In particular, cloud technology is expected to play a role as a core technology in the integrated training center proposed in this paper, and VM technology and high-speed network technology will be combined to maximize the integration capability.

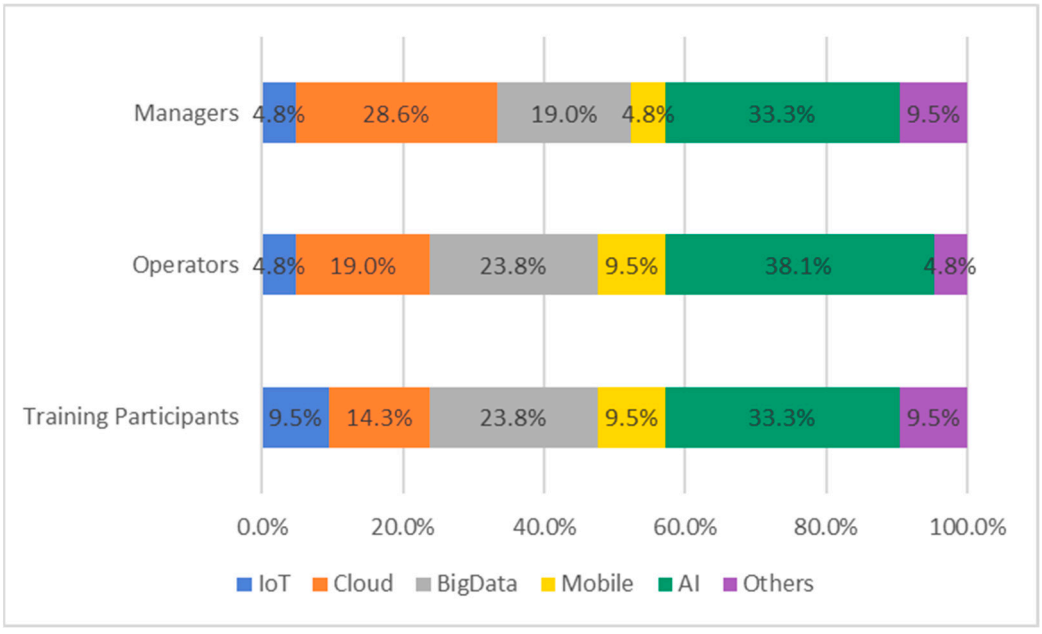

Figure 7. Information and communication technology related to cyber range.

In this section, we propose a new cyber training method and a cyber training site construction plan to effectively respond to threats and attacks in a situation where cyber threats are increasing, and cyber attacks are becoming more sophisticated. By conducting training simultaneously in an actual system that provides actual services and virtual training space, we can expect a training effect similar to real situations. In addition, we

propose an integrated cyber range construction plan that can support effective cyber training by connecting each cyber range to a network to meet various training purposes and requirements.

6. Survey Analysis to Determine the Type of Training by Each User

To design effective cyber training, a survey was conducted to determine the frequency and type of training by each user. The survey conducted in this study was conducted to derive effective cyber training implementation methods and flexible cyber range composition methods. The survey was conducted on participants who actually participated in cyber training and operators who operate and manage cyber ranges. (However, since the participants in the survey belonged to the Ministry of National Defense of South Korea, their security policy restricts the disclosure of their detailed affiliations and survey results.) In the survey, users were divided into three groups: the "Training Participants", who participate in training and perform cyberattack and defense missions; the "Operator", who builds, organizes, and operates the cyber range; and the "Manager" who designs and manages cyber training policies and provides feedback on training results. According to the survey results, the preferred frequency of cyber training for each user is shown in Figure 8. In terms of the number of cyber training sessions, users felt burdened by exceeding four training sessions per year and preferred to conduct training at regular intervals. In addition, it was recognized that the training effect would be low if it were performed once a year, and the burden of preparing for training would increase if it were performed 12 times.

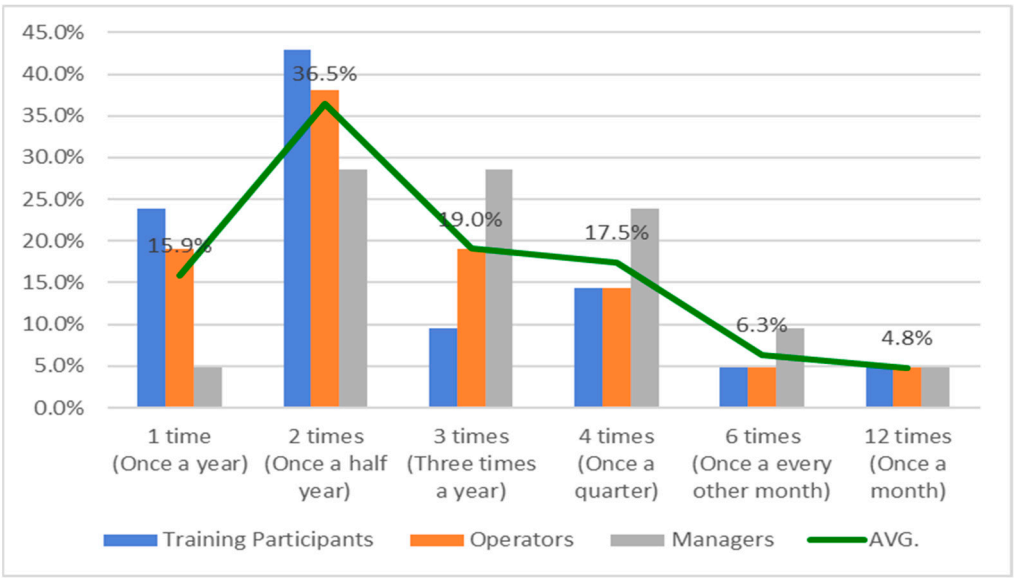

Figure 8. Preference for the number of cyber trainings by user.

As another survey result, the preferred training type of each user is shown in Figure 9. In terms of training type, the participants preferred a mix of cyber training in real and simulated environments, but the operator who prepares and builds the training preferred a simulation that is relatively easy to build rather than a hybrid training with a complex structure. The managers chose the hybrid form of training based on its effectiveness.

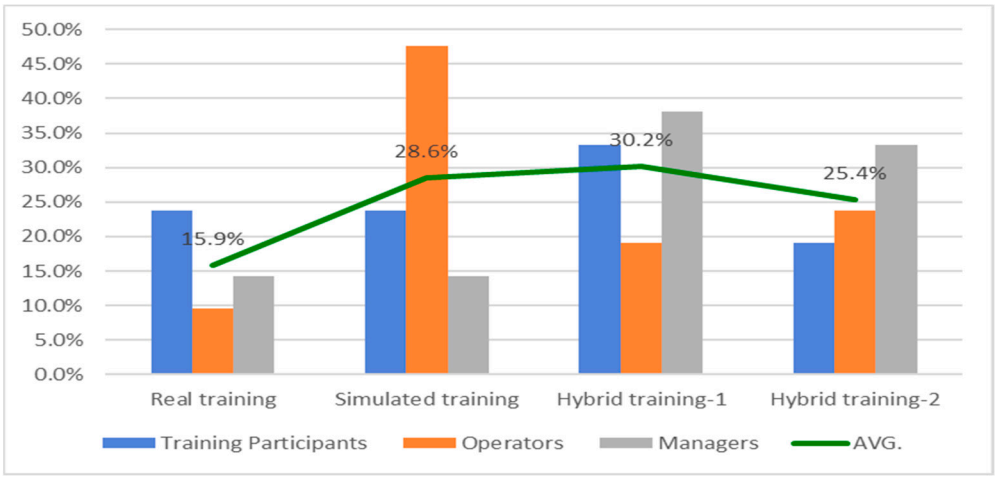

Figure 9. Preference for cyber training format by user.

As shown in the survey results, there is no ideal number and type of cyber training. The number and type of cyber training should be freely selected according to the purpose of cyber training and training conditions. In other words, it may be more effective to perform a variety of training methods than to continuously perform one type of training. Therefore, it is necessary to establish and carry out an annual training plan to meet the training objectives from a mid- to long-term perspective rather than a short-term perspective. Through the survey results conducted in this study, the optimal number of training sessions was selected, and the training implementation method was designed. In addition, the necessity of an integrated cyber range was confirmed by reflecting the needs of the operators, and a plan for constructing a flexible cyber range connected by a network was proposed. Based on the results of this survey, the optimal hybrid form of cyber training was derived. In addition, the necessity of the latest ICT technologies was surveyed for efficient operation of cyber training sites, and an integrated cyber training site connected to a remote network that meets the needs of participants and operators was proposed.

The results of this study were evaluated by identifying strengths and weaknesses through brainstorming with a group of experts involved in cyber training. The expert group is largely divided into four groups. The first is the people who create cyber policies, the second is the people who perform actual cyber activities such as cyber operations, the third is the operators who organize and manage cyber ranges, and the last is the researchers who conduct research related to cyber operations and cyber training. The results of this study were explained to these expert groups, their opinions were received, and the strengths and weaknesses were identified through brainstorming. Regarding the hybrid cyber training method, since it can conduct training on actual systems, it has the advantage of periodically identifying and supplementing vulnerabilities in actual systems, but it is expected to take a lot of time to prepare and design the training, so it should be managed by professional personnel. In addition, regarding the integrated cyber range operation method, it was mentioned that it can effectively utilize the unique characteristics of each cyber range and that remote training participants can participate in training through a network. However, it was pointed out that a high-quality network must be supported to organize a stable integrated cyber range and that the configuration is complex. In this study, it was determined that shortcomings pointed out could be resolved from the management and operational aspects, and based on the opinions of a group of experts, it was found that to conduct cyber training based on the results of this study, an organization and personnel that can fully support cyber training are necessary.

7. Conclusions

In this paper, given the implications of the U.S. cyber training trend and the perspective of the components of cyber training, a direction of cyber training development was derived.

This study proposes an effective method of conducting cyber training and an operation method for cyber range to appropriately respond to increasingly sophisticated cyber threats. A hybrid cyber training system was proposed as a temporal and spatial integration plan to simultaneously integrate simulation-based training with real-world target training. In addition, an integrated cyber range that can be interconnected by building individual cyber ranges that take into account the cyber environment of the training headquarters and subordinate organizations was presented. Through this integrated training center operation plan, it is possible to train the ability to perform cyber activities within the specialized cyberspace of subordinate organizations, and it is possible to plan training of various forms and participation scales and share the capabilities and resources of each cyber range. Since it is difficult to predict the rapidly evolving forms of cyber threats and cyber attacks, securing cyber response capabilities based on threats is limited. Therefore, this study provided a framework for effective and practical cyber training by deriving implications from the cyber training trends of the United States, which has the best cyber response capabilities, and collecting opinions from participants and managers of cyber training.

The hybrid cyber training and integrated cyber range operations proposed in this paper are presented at the conceptual level. It requires empirical verification. However, it is not easy to apply the hybrid cyber training system to real cyber training at once. In the future, it may be appropriate to design partial or phased cyber training exercises in a hybrid format to scale up after validating their effectiveness. In addition, Since the initial budget for building an integrated cyber range can be high, it is necessary to analyze the cost of facility investment versus sharing resources of each cyber range to ensure that it is operated in accordance with the training purpose.

Based on the results of this study, we propose policy recommendations to secure integrated cyber capabilities by conducting effective cyber training. First, for effective training, it is necessary to update the list of training tasks that match the training objectives. Through this list of training tasks, we can confirm what elements are necessary to meet the training objectives. In addition, when evaluating the training results, the list of training tasks can be used to present the level to be achieved, enabling effective evaluation and feedback. Second, efforts are needed to secure the ability to develop and operate scenarios that meet the training objectives. As the nature of cyber threats and cyber attacks is becoming more advanced due to the development of advanced ICT technologies, it is urgent to develop scenarios for effective cyber training that reflect and respond to them. The latest cyber threats and rapidly evolving cyber attack techniques and tactics must be reflected in the scenarios in a timely manner, and a budget, staffing, and related professional organizations are needed to support this. This is an area that requires a lot of time and effort, so it must be achieved through sufficient investment of time and resources. Lastly, the latest ICT must be applied to cyber training to enhance its effectiveness. Cyber training must be planned, prepared, conducted, and evaluated using AI, cloud, and virtualization technologies to effectively improve cyber capabilities. In particular, through the application of AI technology, it will be possible to efficiently perform AI attack techniques that have learned the latest attack techniques and the user's response capabilities through a feedback system learned by AI. Cloud and virtualization technologies will enable more flexible operation of cyber range and will be utilized as core technologies for building the integrated cyber range proposed in this study.

Author Contributions: Conceptualization, Y.S. and H.K.; Funding acquisition, D.S.; Methodology, Y.S. and H.K.; Design of Scenario, J.J.; Supervision, D.S.; Validation, J.J.; Writing—original draft, Y.S. and H.K.; Writing—review and editing, 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).

Data Availability Statement: Data are contained within the article.

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

References

1. Kihoon, K.; Jungho, E. A Study on the Model of Training Performance Measurement Specialized to Cyber Security Trainee for Cyber Security Professionals Acquisition. *J. Korea Soc. Digit. Ind. Inf. Manag.* **2016**, *12*, 56–69. [CrossRef]
2. Sangwoon, L.; Yongsuk, P. Research and Direction of Cyber Operation Education System for Fostering Common Situation Awareness about Cyber Operation -Focusing on non-Cyber Operations Unit Officer Education. *J. Converg. Secur.* **2019**, *19*, 13–22. [CrossRef]
3. Myungkil, A.; Yonghyun, K. Research on System Architecture and Simulation Environment for Cyber Warrior Training. *J. Korea Inst. Inf. Secur. Cryptol. (JKIISC)* **2016**, *26*, 533–540. [CrossRef]
4. Maki, N.; Nakata, R.; Toyoda, S.; Kasai, Y.; Shin, S.; Seto, Y. An effective cybersecurity exercises platform CyExec and its training contents. *Int. J. Inf. Educ. Technol.* **2020**, *10*, 215–221. [CrossRef]
5. Daesik, K.; Yonghyun, K. A Study of Administration of Cyber Range. *J. Internet Comput. Serv.* **2017**, *18*, 9–15. [CrossRef]
6. Brilingaitė, A.; Bukauskas, L.; Juozapavičius, A. A framework for competence development and assessment in hybrid cybersecurity exercises. *Comput. Secur.* **2020**, *88*, 101607. [CrossRef]
7. Leitner, M.; Frank, M.; Hotwagner, W.; Langner, G.; Maurhart, O.; Pahi, T.; Reuter, L.; Skopik, F.; Smith, P.; Warum, M. AIT cyber range: Flexible cyber security environment for exercises, training and research. In Proceedings of the 2020 European Interdisciplinary Cybersecurity Conference, Rennes, France, 18 November 2020; pp. 1–6. [CrossRef]
8. Dewar, R.S. *Cybersecurity and Cyberdefense Exercises*; ETH Zurich: Zurich, Switzerland, 2018. [CrossRef]
9. Aoyama, T.; Nakano, T.; Koshijima, I.; Hashimoto, Y.; Watanabe, K. On the complexity of cybersecurity exercises proportional to preparedness. *J. Disaster Res.* **2017**, *12*, 1081–1090. [CrossRef]
10. Maennel, K. Learning analytics perspective: Evidencing learning from digital datasets in cybersecurity exercises. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 7–11 September 2020; pp. 27–36. [CrossRef]
11. *DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*; US Government Accountability Office: Washington, DC, USA, 2019.
12. Joint Chiefs of Staff. *Cyberspace Operations*; U.S. Joint Publication: Washington, DC, USA, 2018.
13. Daesung, L. The Trends of Domestic and Overseas Cyber Security Training. *J. Korea Inst. Inf. Commun. Eng.* **2021**, *25*, 857–860. [CrossRef]
14. Daesung, L. The Review and Trends of Domestic and Overseas Cyber Security Training. *Proc. Korea Inst. Inf. Commun. Eng. Gen. Conf.* **2020**, *24*, 348–350.
15. Jaehak, Y.; Kijong, K.; Ikkyun, K.; Daesung, M. Trends in Cyber Range Technology in the Field of Information Security. *Proc. Korea Inf. Process. Soc. Conf.* **2022**, *2022*, 208–211. [CrossRef]
16. Jaehak, Y.; Kijong, K.; Ikkyun, K.; Daesung, M. Technological Trends in Intelligent Cyber Range. *Electron. Telecommun. Trends* **2022**, *37*, 36–45. [CrossRef]
17. Younghan, C.; Insook, J.; Inteck, W.; Taeghyoon, K.; Soonjwa, H.; Insung, P.; Jinsoek, Y.; Yeongjae, K.; Jungmin, K. Design and Implementation of Cyber Range for Cyber Defense Exercise Based on Cyber Crisis Alert. *J. Korea Inst. Inf. Secur. Cryptol.* **2020**, *30*, 805–821. [CrossRef]
18. ECSO. *Understanding Cyber Ranges: From Hype to Reality*; ESCO Publications: Dubai, United Arab Emirates, 2020.
19. Donghyeok, L.; Namje, P. Hacking Training Plan for Cyber Security in Industry 4.0. *J. Korean Inst. Inf. Technol. (JKIIT)* **2017**, *15*, 47–56. [CrossRef]
20. Suyoun, H.; Kwangsoo, K.; Taekyu, K. The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training. *J. Korea Inst. Mil. Sci. Technol.* **2019**, *22*, 797–805. [CrossRef]
21. Myungkil, A.; JungRyun, L. Research on Traffic Generation System for Cyber Training. In Proceedings of the Korean Institute of Communications and Information Sciences 2020 Autumn General Conference. 2020, Volume 73, pp. 241–242. Available online: https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10501181 (accessed on 30 July 2024).
22. Uihyeon, S.; Donghwa, K.; Myungkil, A. Layered Authoring of Cyber Warfare Training Scenario. *J. Internet Comput. Serv.* **2020**, *21*, 191–199. [CrossRef]
23. Donhwa, K.; Yonghyun, K.; Myungkil, A.; Heejo, L. Automated Cyber Threat Emulation Based on ATT&CK for Cyber Security Training. *J. Korea Soc. Comput. Inf.* **2020**, *25*, 71–80. [CrossRef]
24. Suyoun, H.; Haneul, R.; Donghwa, K. Design of Automated Cyber Threat Generating Architecture for Cyber-security Training System. In Proceedings of the Korean Institute of Communications and Information Sciences 2020 Summer Conference Proceedings. 2020, Volume 70, pp. 787–788. Available online: https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10498769 (accessed on 30 July 2024).
25. Haneul, R.; Suyoun, H.; Donghwa, K.; Seongyun, S. Structure Design of Automatic Download Threat and Defense Tools for Cyber Training Environment. In Proceedings of the Korean Institute of Communications and Information Sciences 2020 Summer Conference Proceedings. 2020, Volume 70, pp. 765–766. Available online: https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10498758 (accessed on 30 July 2024).

26. Munsoo, J. (A) Recommendation Algorithm for Red Team Strategy in Massive Cyber Defense Exercise. Ph.D. Thesis, Korea Advanced Institute of Science and Technology, Daejeon, Republic of Korea, 2021.
27. Joonsoo, K.; Kyeongho, K.; Moonsu, J. Cyber-physical battlefield platform for large-scale cybersecurity exercises. In Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 28–31 May 2019; pp. 1–19. [CrossRef]