applied sciences

MDPI

Article

Design and Implementation of Multi-Cyber Range for Cyber Training and Testing

Moosung Park [1,2], Hyunjin Lee [3], Yonghyun Kim [2], Kookjin Kim [1,4] and Dongkyoo Shin [1,4,*]

[1] Department of Computer Engineering, Sejong University, Seoul 05006, Republic of Korea
[2] R.O.K Agency for Defense Development, Seoul 05771, Republic of Korea
[3] R.O.K Hanwha Systems, Seongnam 13524, Republic of Korea
[4] Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul 05006, Republic of Korea
[*] Correspondence: shindk@sejong.ac.kr

Abstract: It is essential to build a practical environment of the training/test site for cyber training and weapon system test evaluation. In a military environment, cyber training sites should be continuously developed according to the characteristics of the military. Weapons with cyber security capabilities should be deployed through cyber security certification. Recently, each military has been building its own cyber range that simulates its battlefield environment. However, since the actual battlefield is an integrated operation environment, the cyber range built does not reflect the integrated battlefield environment that is interconnected. This paper proposes a configuration plan and operation function to construct a multi-cyber range reflecting the characteristics of each military to overcome this situation. In order to test the multi-cyber range, which has scenario authoring and operation functions, and can faithfully reflect reality, the impact of DDoS attacks is tested. It is a key to real-world mission-based test evaluation to ensure interoperability between military systems. As a result of the experiment, it was concluded that if a DDoS attack occurs due to the infiltration of malicious code into the military network, it may have a serious impact on securing message interoperability between systems in the military network. Cyber range construction technology is being developed not only in the military, but also in school education and businesses. The proposed technology can also be applied to the construction of cyber ranges in industries where cyber-physical systems are emphasized. In addition, it is a field that is continuously developing with the development of technology, such as being applied as an experimental site for learning machine learning systems.

Keywords: cyber training; cybersecurity test and evaluation; scenario authoring; cyber range

check for updates

Citation: Park, M.; Lee, H.; Kim, Y.; Kim, K.; Shin, D. Design and Implementation of Multi-Cyber Range for Cyber Training and Testing. *Appl. Sci.* **2022**, *12*, 12546. https://doi.org/10.3390/app122412546

Academic Editors: Peter R.J. Trim and Yang-Im Lee

Received: 2 November 2022
Accepted: 6 December 2022
Published: 7 December 2022

1. Introduction

Cyberwar, even in the recent case of the Russia-Ukraine conflict, is represented in the form of a hybrid warfare scenario accompanied by regular warfare, and it is constantly carried out in peacetime. Accordingly, countries around the world are advancing cyber security technology to enhance their ability to carry out cyberwarfare and following development procedures that emphasize security in the development of weapons systems. The basis of cyber warfare performance will be the strengthening of the cyberspace. Therefore, the training of personnel capable of carrying out defense and attacks will be the basis of cyber power. Realistic defense training is more efficient when conducted in a real-world environment. It is common to conduct such training in a virtual simulation environment because the nature of cyberwarfare can cause irreversible damage to the actual system in the training process. However, a training environment that lacks realism makes it difficult to expect practical results.

In order to attain a robust cyber defense capability, cybersecurity capabilities should be equipped from the time the weapon system is built, and while it is tested and evaluated.

Jim Highsmith emphasized that technical debt incurred when things are not properly fixed exponentially increases over years [1].

A cyber range is a practice field that provides the ability to research, develop, test, or conduct cyber training on military capabilities in cyberspace [2]. In order to properly evaluate tests, it should be conducted in a realistic cyber range environment. In addition, cybersecurity capabilities and interoperability functions should be implemented prior to operational test and evaluation to ensure the success of system development [3]. In other words, in order to increase the effectiveness of cyber training, it is necessary to build a cyber range that resembles a realistic environment. Moreover, a cyber range that resembles a real system can also be used as a test evaluation site for weapon systems.

In a military system where accuracy and security are emphasized above all else, it is necessary to build a realistic cyber range and conduct a variety of training and test evaluations. Recently, each military has been building its own cyber range that simulates the battlefield environment of each military. However, since the actual battlefield is an integrated operation environment, the cyber range built does not reflect the integrated battlefield environment that is interconnected. In order to overcome this, the concept of a multi-cyber range proposed in this paper will be developed into a highly useful concept. This paper presents a tool to allow a single cyber range to realistically link multiple cyber training ranges and authoring scenarios that are connected between ranges based on integrated management measures between training ranges.

In this way, the construction of practical testbeds in various kinds of education and research is required, and it is a reality that is actively being researched and developed in schools and government institutions. Therefore, the main agenda of this paper, the design structure of connecting and expanding various ranges, will be indispensable for the development of cyber ranges.

The remainder of this paper is structured as follows. Section 2 describes related works. Section 3 proposes a practical cyber range structure that can also be used for cyber training and interoperability assessment, explains the scenario-building measures and related functional elements, and presents the results of the implementation. Section 4 conducts cyber warfare experiments in range-connected situations to verify that the built range can best represent a cyber threat/combat situation. Section 5 describes the contributions of this paper and the direction of future research.

2. Related Works

2.1. National Cyber Range (NCR)

DARPA in the U.S. has operated a cyber training range since 2009 and is moving it to the U.S. Test and Training Resource Management Center (TRMC) for further development to facilitate use in real-world training and test evaluations. For test spaces in the security area, L1 switches can be used to interface with the range to support training and test evaluations even in multi-level security environments [4]. In addition, during the weapon system acquisition lifecycle, all six stages of Cyber Test and Evaluation (T&E) were supported, and the range was developed to a level where test evaluation results were officially recognized.

The main capabilities of NCR are:

1. Multiple Independent Levels of Security (MILS) architecture enables simultaneous operation of multiple trials in different secret classes;
2. Quick emulation of complex operational environments;
3. Automation support for accurate repeated testing;
4. Support for different types and disciplines (test, training, research, etc.).

NCR serves as a cyber range that provides a mission-adaptive, hi-fidelity cyber environment for assessing independent and objective cyber testing and progressive cyberspace capabilities. It also integrates the test evaluation infrastructure of cyberspace through partnerships across the U.S. Department of Defense, the U.S. Department of Homeland Security, and industry and academia. The NCR facility is a special certified communication information facility that maintains a variety of hardware and software computing resources and provides a test environment that encompasses wired and wireless networks.

Vincent E. set out 11 limitations based on their experience using NCR and cited the need for further development [5]. Since NCR was developed, the use of case statistics in Table 1 shows that it has been applied to training and various tests. In other words, it shows that the role of the cyber range is not only for training and practice, but also for the development of weapon systems as a field for test evaluation.

Table 1. Number of NCR Uses by Sector.

	FY11	FY12	FY13	FY14	FY15	FY16
Cyberspace Capability DT&E	1	3	3	2	4	8
Cyberspace Capability OT&E		1	1		3	2
Cyberspace Capability M&S/R&D			5	7		
Training/Exercises		1	3	11	22	27
Mission Rehearsal		1	1		2	4
MDAP Cybersecurity DT&E				2	9	17

However, most of the limitations of NCR mentioned in [5] are management factors. It is an aspect caused by the need for many participants and it is difficult to systematically manage complex NCR resources. Problems that cannot be controlled when multiple ranges are connected and seem to require systematic automation of the management system.

2.2. *Capability of Cyber Training System*

A cyber training system is a system in which the training manager (White Team) prepares and controls the training environment, while the trainers, the cyber attacking group (Red Team) and the defenders (Blue Team), can train in the training environment. The cyber training system consists of a cyber battlefield environment construction function that simulates the actual battlefield environment as a cyber battlefield environment, a scenario authoring function that can produce various scenarios for training, and a training control function that can control, monitor, and evaluate training. The cyber training system is operated in the following order: training plan setting, training goal setting, writing of training scenario, training performance according to the scenario, training monitoring, evaluation and post-analysis of training results, and reporting of training results [6].

Usually, in the military, some units have established a cyber training range, which is used to train cyber warriors, and the ranges are mainly composed to mimic the Internet environment. As the aspects of cyber warfare become more complex, the level needed for training must also be advanced, especially in the area of defense, where tactical training of the concept of simulated combat needs to be carried out. The training scenario has the essential role of providing a user interface to design the training and mounting it into the training system. From this point of view, the training scenario should be able to include a number of factors that can increase the diversity and quality of the training. This is because the test evaluation should be carried out in the same environment as the environment in which the system will be operated, such that a complete mission-based test evaluation can be carried out. For example, a Distributed Denial of Service (DDoS) attack on an Army Corps server would cause problems with the transfer of data interlocked to the Joint Command, Control, Communication, Computer and Intelligence (C4I) system, which in turn would limit the Joint Chiefs of Staff's perception of the Army situation. Therefore, the mission of a Joint Operations War is bound to be affected.

Nikos Oikonomou proposed in [7] the need to connect and integrate services with the European cyber range due to the high cost of building and managing the cyber range, while Olivier Jacq proposed in [8] the need to build a Maritime cyber range through the Maritime's cyber risk assessment. In addition, Adamantini emphasized in [9] that it is difficult for a single organization to build and manage multi-domain ranges. Therefore, it is necessary to connect ranges from different organizations to achieve real-world fidelity, and, when connecting multiple ranges, use Virtual Private Network (VPN) technology to connect. In addition, outside of the military, ordinary schools and enterprises are also building cyber ranges, and are also evolving into services using cloud technology.

In addition, cyber ranges are also being used for security education, in various industries, and the construction of intelligent learning models. The cyber range was built to train procedures for analyzing/handling threats in real-world environments based on cyber threat scenarios in a more real-world cyber-physical environment rather than a theoretical approach to cybersecurity education [10]. The results of education at the university level proved how efficient it is to conduct it in a practical educational environment. The testbed was built for efficient learning of machine learning systems in the SCADA environment [11]. It is a well-known fact that the accuracy of a machine learning system is determined by the amount of training data that is required. To this end, cyber security researchers conducted an experiment to build a realistic cyber range to learn a machine learning system while carrying out a cyber-attack. By learning based on various cyber threat data that are difficult to obtain in real systems, the role of a cyber range in the development of intelligent models is being emphasized.

To develop a distributed intrusion detection system applied in an industrial control system environment, the test bed built a cyber range with a mix of physical equipment, simulation models, and emulated models [12]. This also drove the functional and performance accuracy of intrusion detection systems by building and testing in realistic environments.

SWaT is used to understand the impact of cyber and physical attacks on water treatment systems, to evaluate the effectiveness of attack detection algorithms, and to evaluate the effectiveness of defense mechanisms when a system is under attack [13]. Experience with testbeds has emphasized the importance of conducting research in an active and realistic environment.

Smyrlis, M. researched a model-based scenario authoring technology to improve user adaptability in cyber education. This study enabled the creation of customized training scenarios based on a comprehensive, model-based description of the organization and its security posture [14].

Ukwandu, E. examined and classified existing cyber ranges and testbeds. The latest trends detail the different dimensions of this classification and highlight the diminishing differentiation between application areas [15]. Chouliaras, N. et al. conducted a systematic survey of 10 cyber ranges developed over the past decade through structured interviews. The existing cyber range determined that there were many elements requiring improvement with new technological developments. They also mentioned that in the near future, digital twin technology will be applied to cyber range construction technology [16].

As such, it can be seen that cyber ranges are needed in many areas. In addition, cyber range technology incorporating artificial intelligence and IoT technology continues to be developed. The issue of emulating weapons systems in the military is also a very important issue and should be considered.

3. Multi-Cyber Range Structure for Training, Testing, and Evaluation

3.1. Structure of Range

It is necessary to establish an environment in which the battlefield management system environment is centered on supporting the Joint Chiefs of Staff and the tactical environment of each military branch can be comprehensively simulated to enable mission-based evaluation. As shown in Figure 1, each military branch shall establish a range of their own, and the Joint Chiefs of Staff shall design/build a light bulb range based on the joint command and control system to interconnect, train, and test functions.

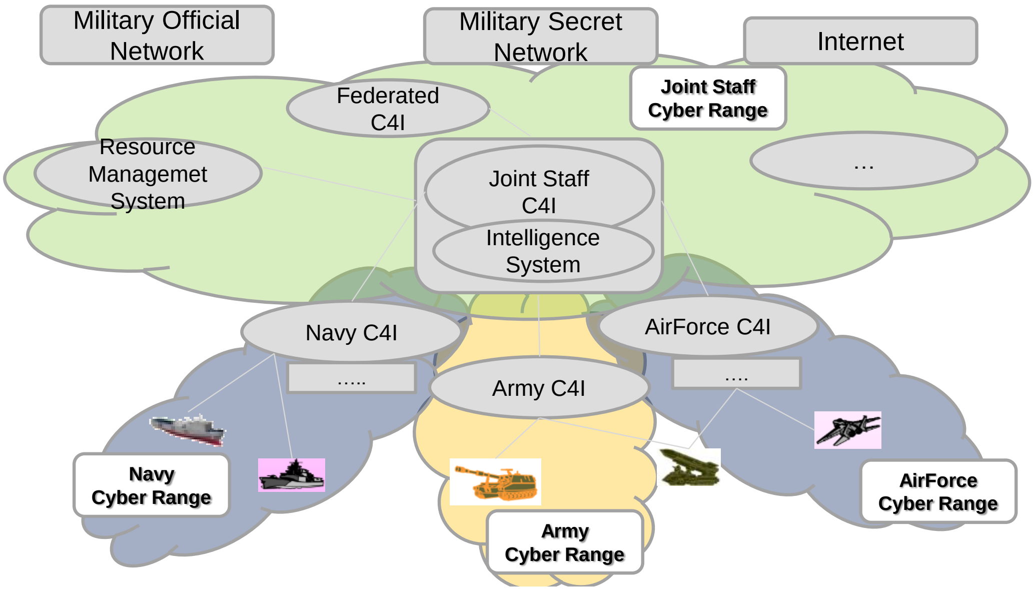


Figure 1. Operational architecture of theater level cyber range.

3.1.1. Networking for Federating Ranges

Centered on the Joint Chiefs of Staff Range, each army unit's cyber range must be configured around the battlefield management system where each subsystem is connected to the Live Virtual Constructive (LVC) concept in order to construct mission-based cyber training and a weapon system test evaluation environment. Therefore, each military cyber training range should develop a range environment around the battlefield management system, and it should be connected as in actual conditions.

Even in an actual environment, the C4I system of each group shares information situations based on Message Text Format (MTF) messages through an interoperating server, and the ability to interoperate information is an important element of the implementation of joint operation warfare. Therefore, in each cyber range, each battlefield management system should be simulated to support responses to interoperating messages. This can be simulated based on the Interface Control Document (ICD) between each system.

In addition, each battlefield management system synchronizes the battlefield situation through synchronization between centers with the concept of a distributed center, which is also an important function of the battlefield management system. Therefore, when simulating a battlefield management system, the synchronization between servers is also an important simulation object.

A Cross Domain Solution (CDS) is used to securely link areas with different secret ratings. The connection between ranges via CDS has the advantage of allowing trainers to train in a real-world environment by actually reflecting the operating environment of the battlefield management system, and to conduct interoperability assessments before an Operational Test (OT) that has not been carried out in the proposed range. However, a separate management channel is required for configuration management and scenario sharing between ranges, which can be used to establish a separate Range Management Channel, such as in Figure 2, using a VPN.

3.1.2. Architecture of Range Management Function

Focusing on the battlefield management system, the range configuration capability is similar to the actual operating system in sub-tactical systems, intranets, and the Internet and should be gradually expanded. Each cyber range has essential functions such as configuration management, scenario creation, and test data generation for independent operation.

However, for configuration and creation of scenarios over a range-to-range connection, a special channel is needed to control whether or not a separate range resource can be managed and supported. To this end, it is proposed to build a portal around the main range with the necessary functions to share and connect the status of resources to conduct training and test evaluation. The proposed management configuration is the same as in Figure 3.

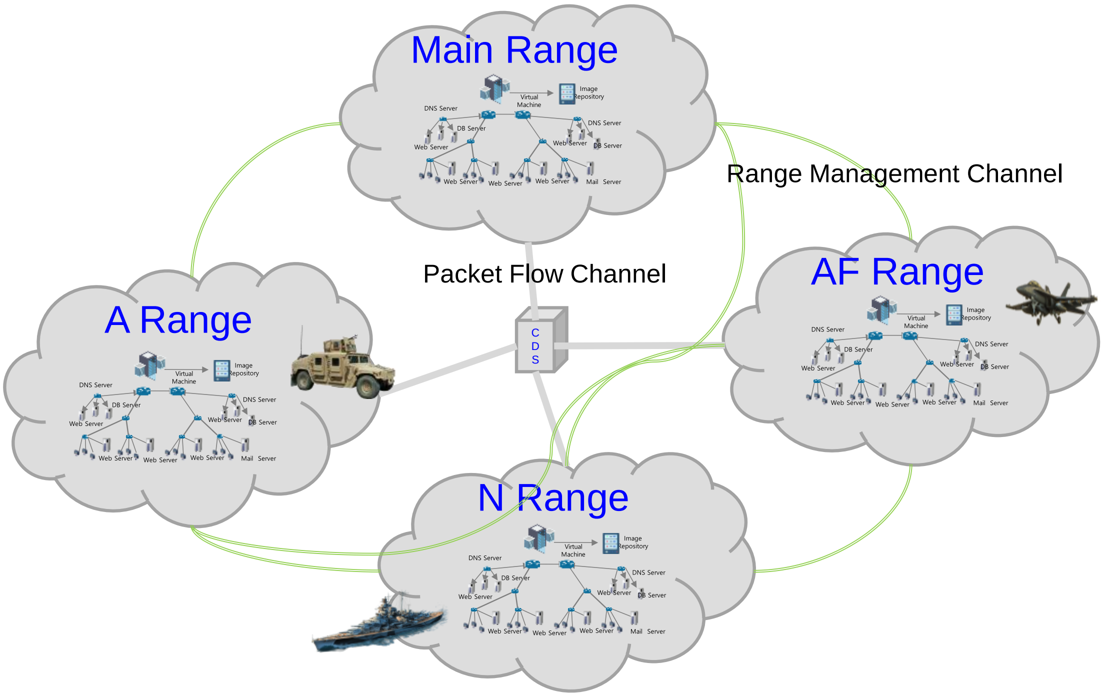


Figure 2. Networking architecture for connecting ranges.

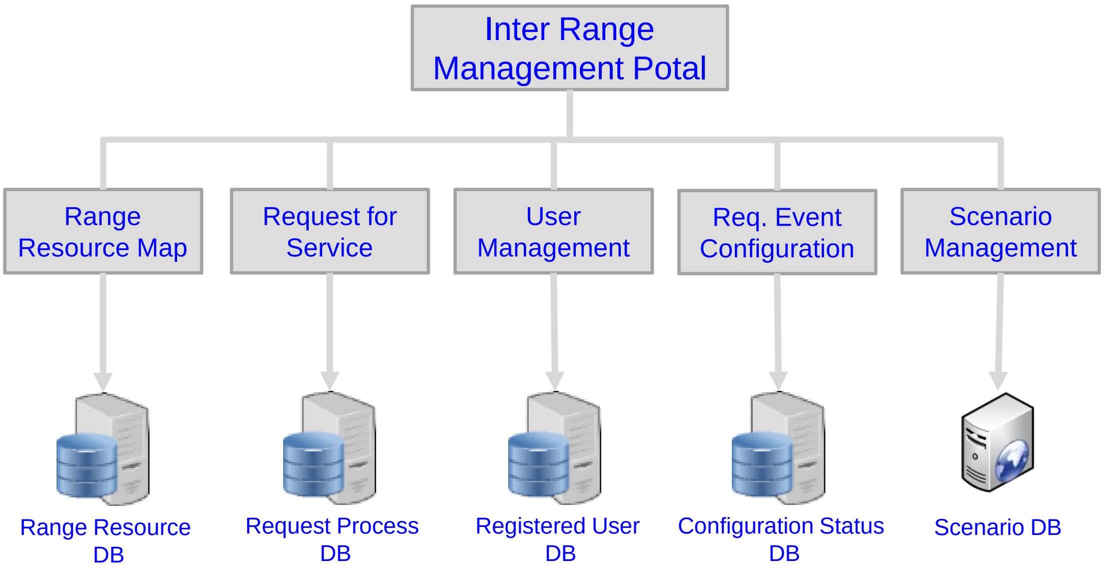


Figure 3. Multi-Cyber Range Management Function.

Each range shares the DB through a multi-cyber range management portal operated by the main range and cooperates with the range configuration. Each range lists the assets it has and presents the default configuration as a service template. Users who will utilize the assets of other ranges to conduct training and testing will apply for services using the service request management function, and refer to the default configuration templates provided by each range. In addition to the hardware and delivery functions that make up the range, a request form is written, including the traffic generation requirements and the coordination team (Red, Blue, White).

The Range Configuration Management module maps the available resources provided by each range based on the contents of the service request to configure the optimal range. The user management module is managed and executed by the user participating in the training and testing, and the requested support personnel at each event. Traffic Flow controls normal traffic between ranges by range, depending on the scenario in which it is written.

3.2. Multiple Cyber Range Scenario Authoring and Traffic Flow Control

3.2.1. Scenario Management

Scenario authoring at a single range is the basic procedure of starting with training/test information, constructing a configurable network topology at the range, and creating a normal/abnormal traffic distribution plan that meets the training/test intention. The training/test authoring tool facilitates recycling or extending existing utilization scenarios based on procedures performed at a single range.

In a multi-range environment, the network, traffic generation, and training/test participants and agents must be able to configure the training/test environment based on the resources allowed at each range. Hence, as shown in Figure 4, even in a single range scenario configuration procedure, it is necessary to have a multi-range configuration consultation procedure for each step. Figure 5 represents the scenario procedure in an existing single range. Figure 6 illustrates the procedure for configuring a scenario in a multi-range environment. For example, constructing a training/testing scenario in an environment where the Joint C4I System and the Army C4I System are interoperated, and an environment in which all ranges participate will be a theater-level test environment. Scenario authoring proceeds is done modularly in a single range without a negotiation process of the range. In the Figures 5 and 6, the purple line is linked to the detailed configuration function to help constructing the overall scenario by specifying the range to which the resource to be configured in the training or test belongs.

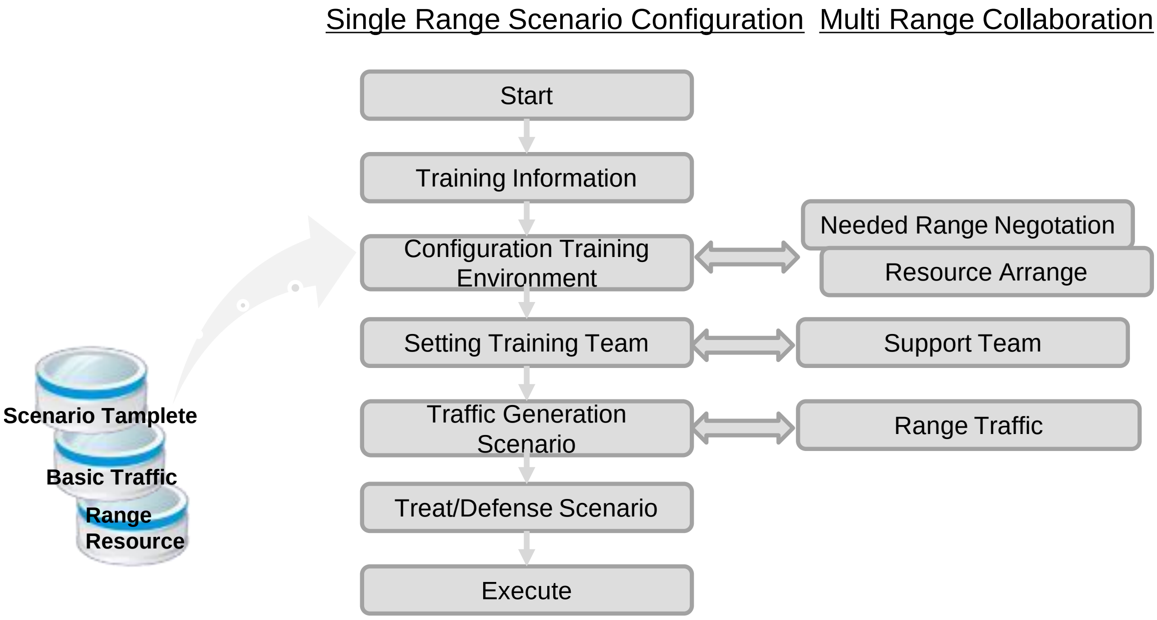


Figure 4. Procedure for Scenario Authoring.

Procedurally constructed scenarios are stored in the DB and recycled in the future, or selected as the default template so that the scenario can evolve. Based on the basic template scenario and the historical scenario, additional resource configuration should be able to configure the licensed resources in a drag and drop manner, as shown in Figure 7, and all resources are managed by tagging their range affiliations.

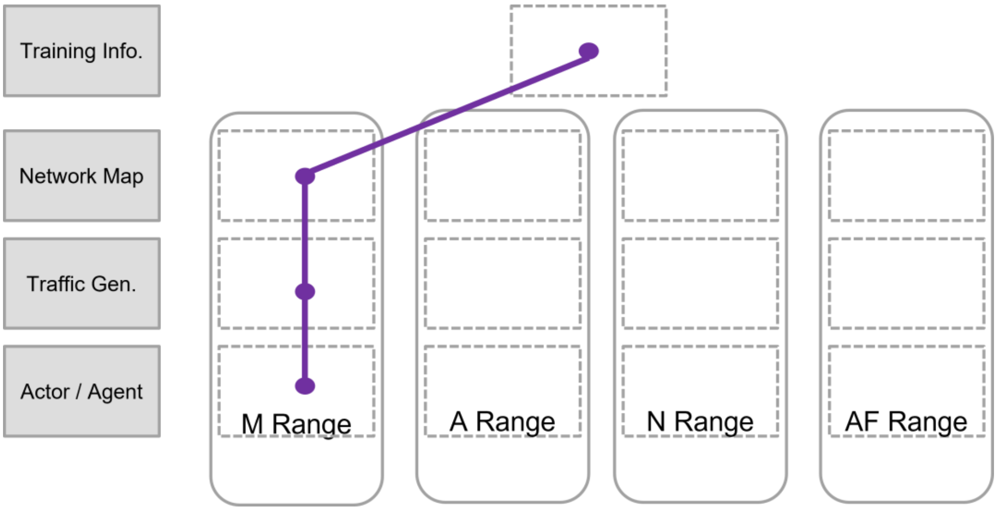


Figure 5. Scenario Authoring at Single Range.

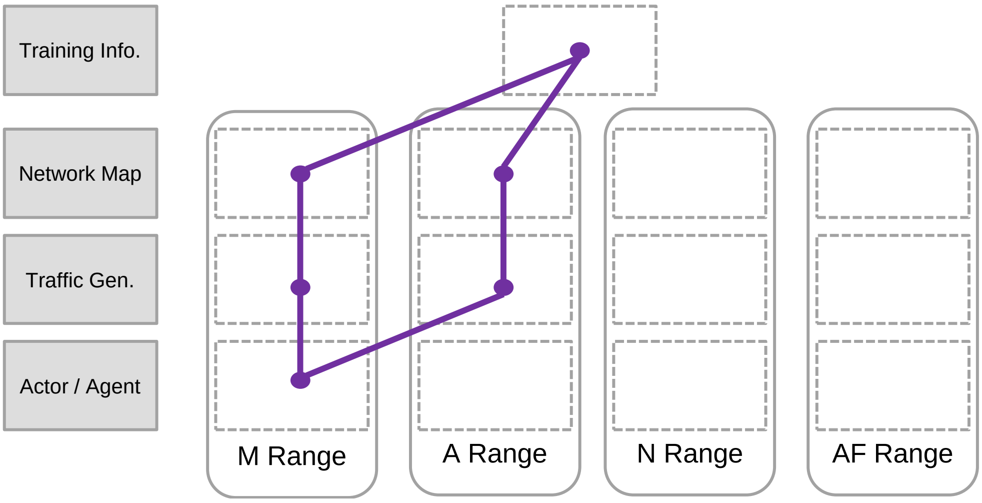
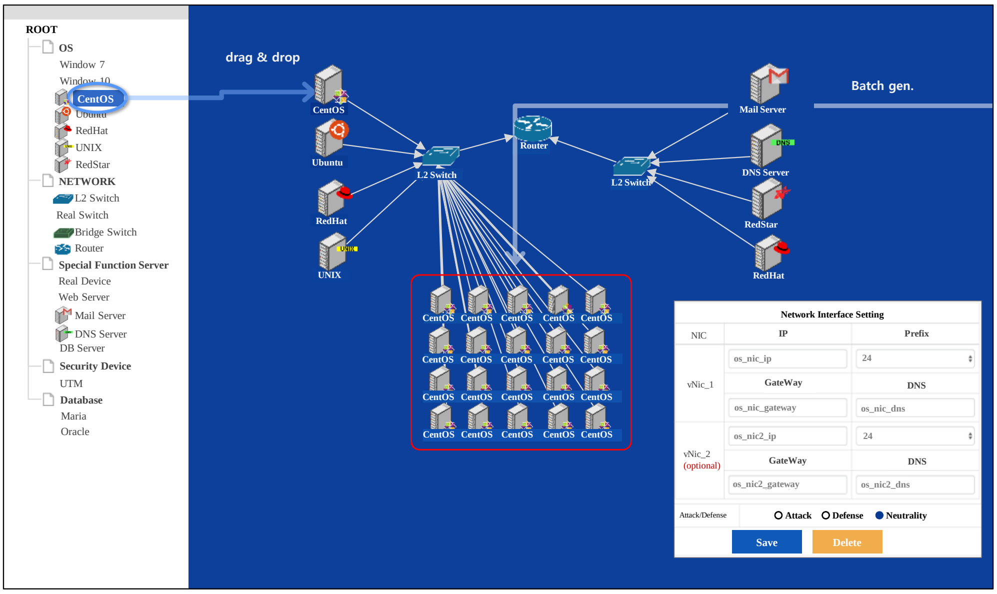


Figure 6. Scenario Authoring through Multi-Range.



Network Interface Setting

NIC	IP	Prefix
vNic_1	os_nic_ip	24
	GateWay	DNS
	os_nic_gateway	os_nic_dns
vNic_2 (optional)	os_nic2_ip	24
	GateWay	DNS
	os_nic2_gateway	os_nic2_dns

Attack/Defense ○ Attack ○ Defense ● Neutrality

Save Delete

Figure 7. Network Map Configuration Function.

3.2.2. Normal Traffic Generation

Normal traffic generation and reproduction is a very important factor in the reproduction of the actual environment, and at the same time as the establishment of a practical training and test evaluation environment. In a related study [17], network traffic was generated in three ways: probabilistic generation, replication of actual network traffic, and the use of instruction lists for applications in the test network. Bieniasz, J. et al. proposed a new approach to generating datasets for cyber threat research on multi-node systems [18]. This has been made useful in fields where information concealment technology is applied. Traffic in military systems is likely to generate traffic with regular statistics depending on wartime/peacetime situations. Therefore, the method of replicating and generating actual network traffic according to the situation is considered the most efficient. The traffic used by a cyber range requires the process of building a dataset, as shown in Figure 8 [19].

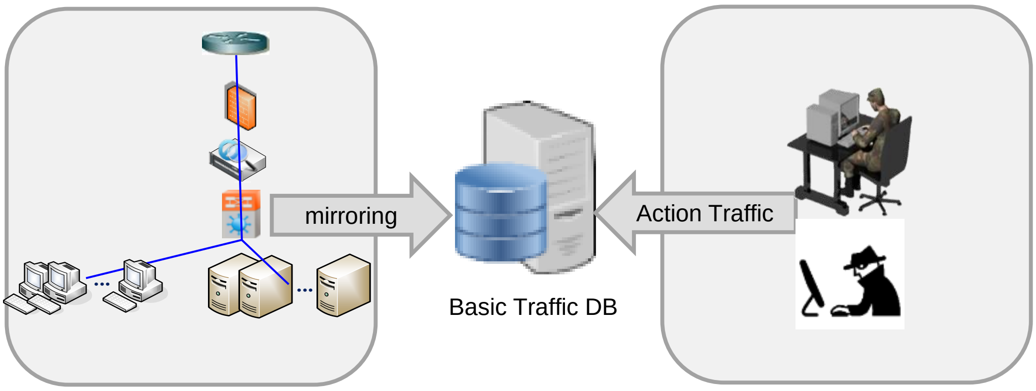


Figure 8. Collect real operation traffic.

In order to develop a plan for traffic generation, a traffic generating node must first be set up in the network topology. The traffic generating node should be specified on the basis of what actually occurs at the server node, but, according to the scenario, a special node can be set up to generate the collected traffic, and the traffic generated by the terminal node may be generated by mixing the use of the terminal traffic template by designation. The terminal traffic template selects the terminal traffic template to be used in the basic dataset DB, and grasps the traffic distribution terminal through the traffic distribution terminal information in the header. In addition, the traffic distribution process can be reproduced through the number of messages and traffic type information.

In the battlefield management system, direct traffic between the terminals is limited, so assuming the traffic between the terminal and the server, it is possible to reproduce simple traffic. Normal traffic is managed in a Packet Capture (PCAP) file and used as basic data by managing the data set collected during peacetime/training, and the server included in the configuration of the network map is essentially designated as traffic generation equipment and operated. Traffic generated at the other terminal should be separately specified to generate traffic. In addition, since the characteristics of training and test evaluation are set at the time to be reproduced, and not the current time, traffic generation should also be designed so that a multiplier generation or hold function can be given a timer function.

In order to establish a practical environment, traffic flow reflecting the characteristics of the military battlefield management system needs to be efficient to perform with the concept of replay based on the information collected. Attack traffic generation is often replayed by building existing case data into a basic data set, but it is difficult to judge it as actual traffic due to differences in training and testing environments. Therefore, if possible, traffic is naturally generated by attack agents or Red Team actions that are applied to training and testing, so a separate attack traffic generation is not necessary for real-world environment configuration.

Traffic generating nodes according to the scenario are specified as shown in Figure 9 to configure a normal training environment. TA1 and TA2 nodes can be considered as acting as interoperating servers that make up each system, and the TS1 node can be assumed to be a node that generates information as they move. However, when configured in a scenario that requires a separate small amount of traffic generation for training purposes, traffic generation agents such as mail behavior and Internet usage behavior are utilized without using large basic traffic.

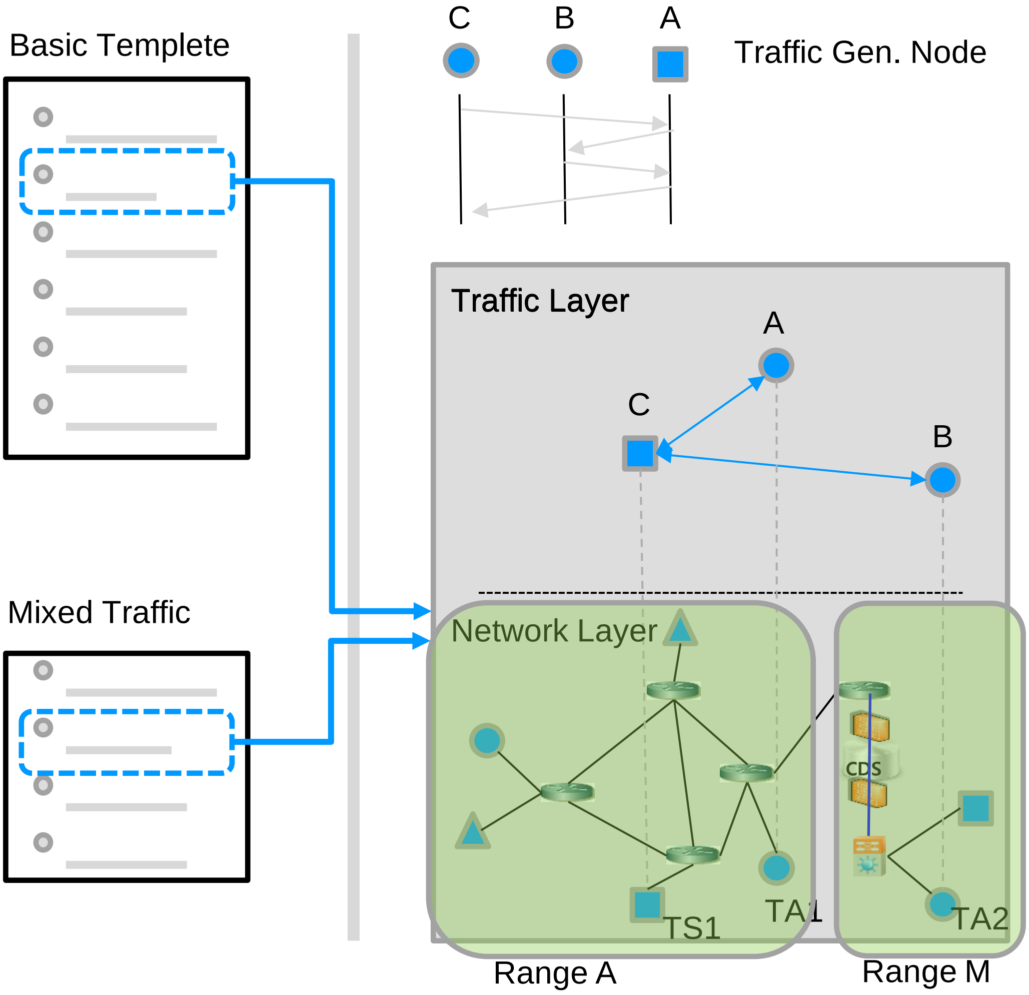
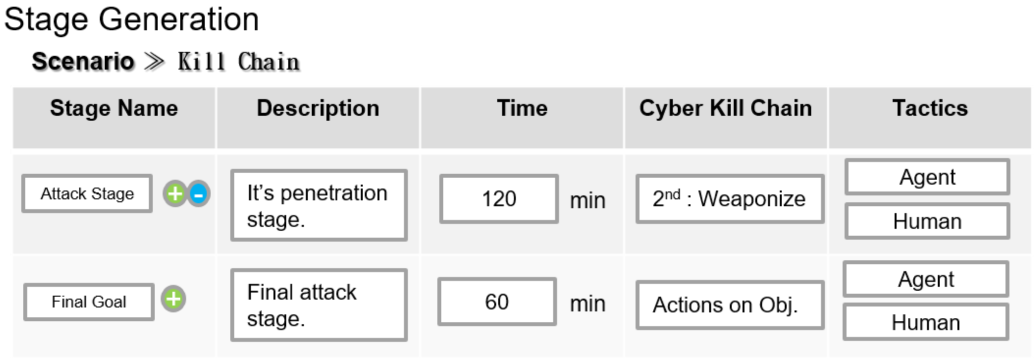


Figure 9. Mapping traffic generation node.

3.2.3. Automatic Scoring

The training is basically based on MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and consists of the Red Team's combat action in the seventh phase of the Cyber Kill Chain. We proposed a way to set the desired time by phase/combat action and set the desired time, as it is continuously supplemented during training. When integrating the desired time for each phase/combat action into the score for each phase designated by the manager into the score for each phase of the battle, it shall be possible to evaluate whether the task given at the time of the desired time is actually achieved by reflecting compliance with the desired time.

The phase generation function should record relevant information around the phase name and time, such as in Figure 10, and if the desired time is specified for each combat action, the training score can be automatically calculated according to Equation (1). However, the combat performance score reflects the manual score by the training instructor.



Stage Generation

Scenario ≫ Kill Chain

Stage Name	Description	Time	Cyber Kill Chain	Tactics
Attack Stage	It's penetration stage.	120 min	2nd : Weaponize	Agent Human
Final Goal	Final attack stage.	60 min	Actions on Obj.	Agent Human

Figure 10. Phase generation function.

$$\text{Phase Score} = \sum(\text{Combat Action Score } \times (\text{Desired Time}/\text{ExecuteTime})) \quad (1)$$

As a result of the training, the scores for each trainer/team are automatically calculated based on whether the combat action performed was achieved, and the timeliness of the mission is evaluated to reflect the desired time. The Combat Action Score is calculated by monitoring CPU usage and file system/process/network changes. However, it is necessary to control the training time by stipulating that the performance time for each combat action shall not exceed 1.5 times the desired time. Monitoring user behavior for automatic evaluation is limited because it is calculated based on some system change information. Therefore, this automatic calculation feature is suitable for defensive training against known attacks and is not suitable for free attack/defense training of Red and Blue teams.

As a result of the training, the scores for each trainer/team are automatically calculated based on whether the combat action performed was achieved, and the timeliness of the mission is evaluated to reflect the desired time. However, it is necessary to control the training time by stipulating that the performance time for each combat action shall not exceed 1.5 times the desired time. The situation that occurs between trainings is controlled/analyzed through a visualization tool that shows the range configuration topology, a detailed event list, and the results of the attack/defense behavior analysis, such as in Figure 11.

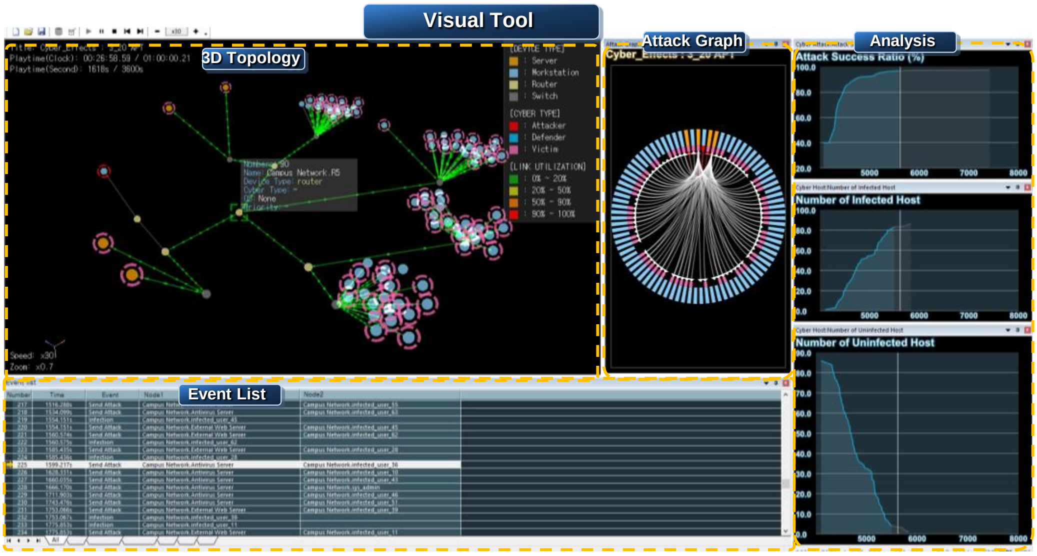


Figure 11. Training situation visualization.

4. Cyber Warfare Experiment with Range Connection

The importance of information sharing in modern warfare is, needless to say, a key element of battlefield operations. Training and evaluation of cybersecurity is emphasized as being mission-oriented [20], and mission-oriented assessments require that all environments in which the system operates are reproduced in order for a proper mission-oriented assessment to be achieved. Therefore, since the battlefield management system of each army is operated in conjunction with the tactical system operated by each military, and at the level of the Joint Chiefs of Staff, it has a hierarchical structure in which the battlefield situation is synthesized in conjunction with the command and control system of each army. Thus, the joint chiefs of staff and the cyber range of each army must be linked to the training and test evaluation to achieve practical training and test evaluation.

The characteristics of the battlefield management system are built and operated in a distributed environment, and the guarantee of traffic for synchronization between distributed servers is an important factor in matching the battlefield situation. In cyber defense, training, security testing, and evaluation between battlefield management systems, the match of the battlefield situation is achieved through the exchange of messages between each system. Other major generated traffic is situational information input and inquiry by the user. Therefore, ensuring the flow of Enterprise Application Integration (EAI) traffic between server sites and message traffic between interoperating servers is an important evaluation indicator for accomplishing the task. Therefore, based on the Information Exchange Requirements (IER) between the battlefield management systems, the success of training and test and evaluation can be analyzed around the flow of interoperating data.

For the experiment, when two ranges were configured, as shown in Figure 12, and a DDoS attack in the form of User Datagram Protocol (UDP) flooding occurred on the Corps server according to the malicious behavior of an insider in the A Range network, as shown in Figure 13. The effect of the IER between the joint C4I system interoperating servers in conjunction with the Corps server was experimented with and the limitation of sharing the battlefield situation by cyberattack was investigated.

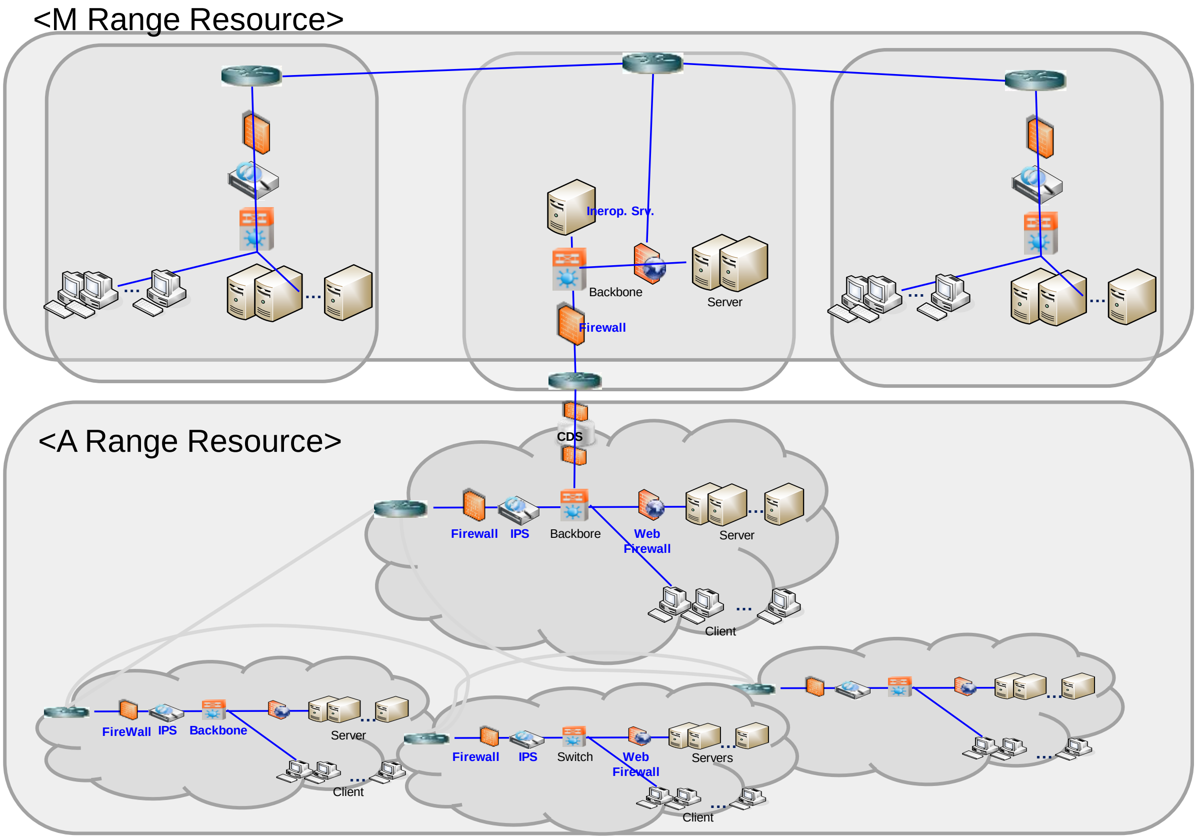


Figure 12. Multi-range configuration example (Joint Staff C4I 3, Army C4I 4 SITE).

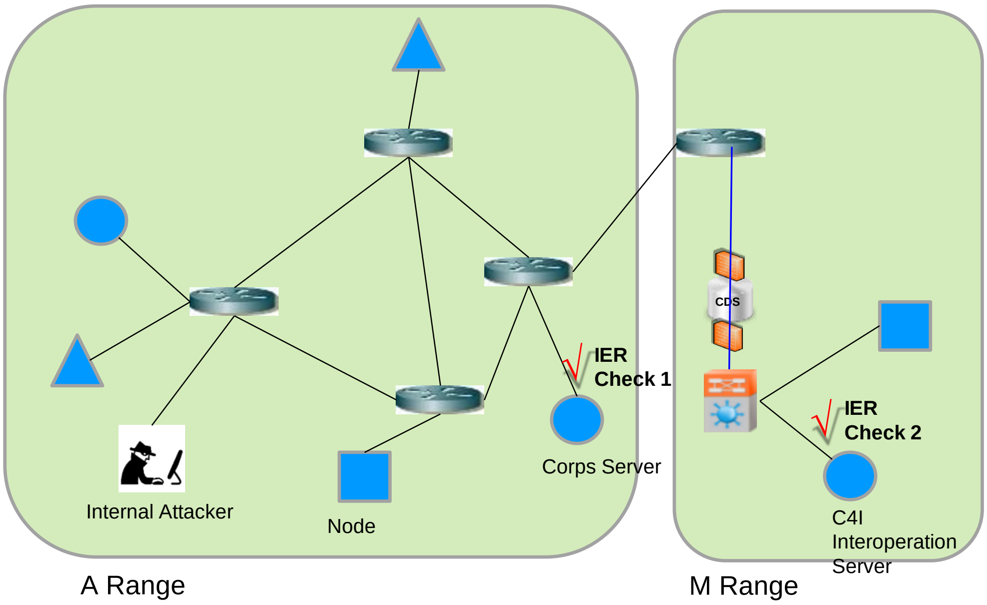


Figure 13. Test environment for IER process.

There are attacker terminals and a number of C4I terminals inside the Army network, and an IER occurs between the Corps server and the Joint Chiefs of Staff C4I interoperating server. The attacker terminal hijacks the antivirus server inside the Army network to configure the Command and Control (C&C) server, and the terminal is infected through the antivirus patch. The infected terminal generates a DDoS attack on the legion server, affecting the transmission quality of the IER.

The experimental environment is shown in Table 2. The experiment was performed in a total of eight scenarios, and the DDoS attack traffic characteristics by scenario are shown in Table 3. Specific items measured by the scenario are shown in the table.

Table 2. Experiment Characteristics.

Item	Value	Information
	IER Information	
IER delay limit	3 s	
IER traffic size	1500 bytes	Exponential distribution
IER interval	0.1 s	Exponential distribution
	DDoS Attack Information	
# of DDoS participating terminals	Max. 82	Increased cyberattack progress
Attack start time	300 s	
Attack duration	1000 s	
Attack interval	0.1 s	
Attack traffic size	1~15 Kbits	Various per scenarios

Table 3. DDoS Attack Load for Each Scenario.

Scenario #	1	2	3	4	5	6	7	8
DDoS traffic size (kbits)	15	14	13	12	9	6	3	1
Attack interval (s)	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Average DDoS Attack Traffic (Mbps)	11.7	10.9	10.1	9.4	7.0	4.7	2.4	0.8

1. IER delay limit: The delay limit that IER should be received by in order to not to affect a military operation. It is a concept similar to service level agreement (SLA).
2. IER size and inter-arrival time: These factors are used to define traffic characteristics of IER. Average traffic volume of IER can be calculated by IER size/IER interval.
3. DDoS Attack Information: These parameters describe the characteristics of a DDoS attack by an attacker; # of DDoS participating terminals means the number of terminals that generate the DDoS attack traffic. DDoS attack maintains during the attack duration after the attack start time. Attack interval and DDoS traffic size mean the attack traffic generation interval and the traffic size per a DDoS attack, respectively. Thus, we can calculate the traffic volume of the DDoS attack by DDoS traffic size/attack inter-arrival time.
4. End-to-end IER transmission delay: Automation support for accurate repetitive testing of the time it takes from the generation of an IER on the Corps C4I server until the Joint Chiefs of Staff interlocking server receives the IER.
5. IER received ratio: The percentage of IERs sent that are successfully received.
6. IER success ratio: The percentage of IERs received that arrive within the IER delay limit (the percentage of IERs that satisfy timeliness).
7. IER failure ratio: The ratio of received IERs to those who arrive after three times the IER latency limit time.
8. IER perished ratio: The percentage of IERs received that exceed the IER delay limit time but arrive within three times the IER delay limit time.

Figure 14 shows the number of cyberattack infected terminals over time. Terminals participating in DDoS attacks are variable depending on the time of the vaccine patch. The patch time is variable depending on the scenario, but the attack start time dramatically increases, and the infection occurs even during the course of a DDoS attack.

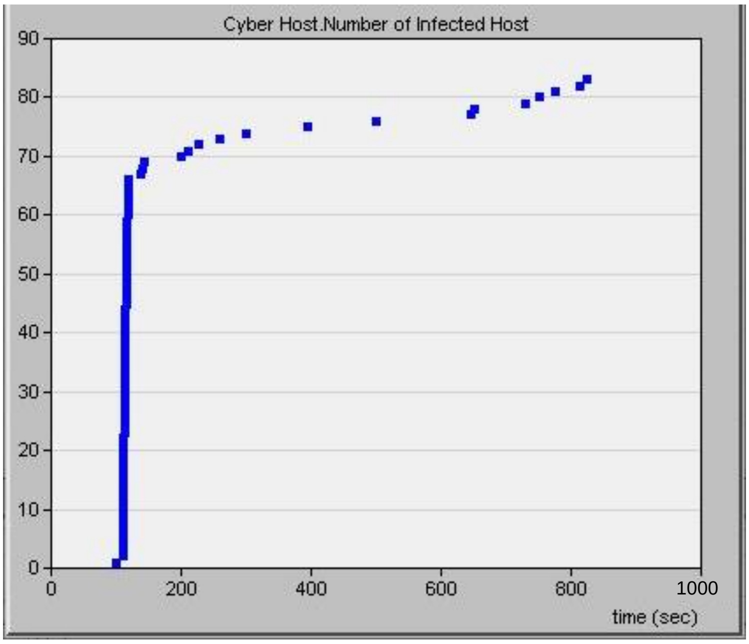


Figure 14. Number of devices participating in a cyberattack according to simulation time.

Figure 15 shows the end-to-end IER transmission delay according to the simulation time by scenario. The figure shows that the delay in end-to-end IER transmission increases during the time of the DDoS attack. In particular, scenarios 1 and 2 show that DDoS traffic exceeds the link load (the link on the legion server is 10 Mbps, creating a bottleneck for experimentation), resulting in a dramatic increase in transmission delays. Not only can DDoS attack traffic be affected by end-to-end transmission delays even when the traffic is less than the link load, but it takes a certain amount of time to process the IERs that have been queued up even after the end of the attack.

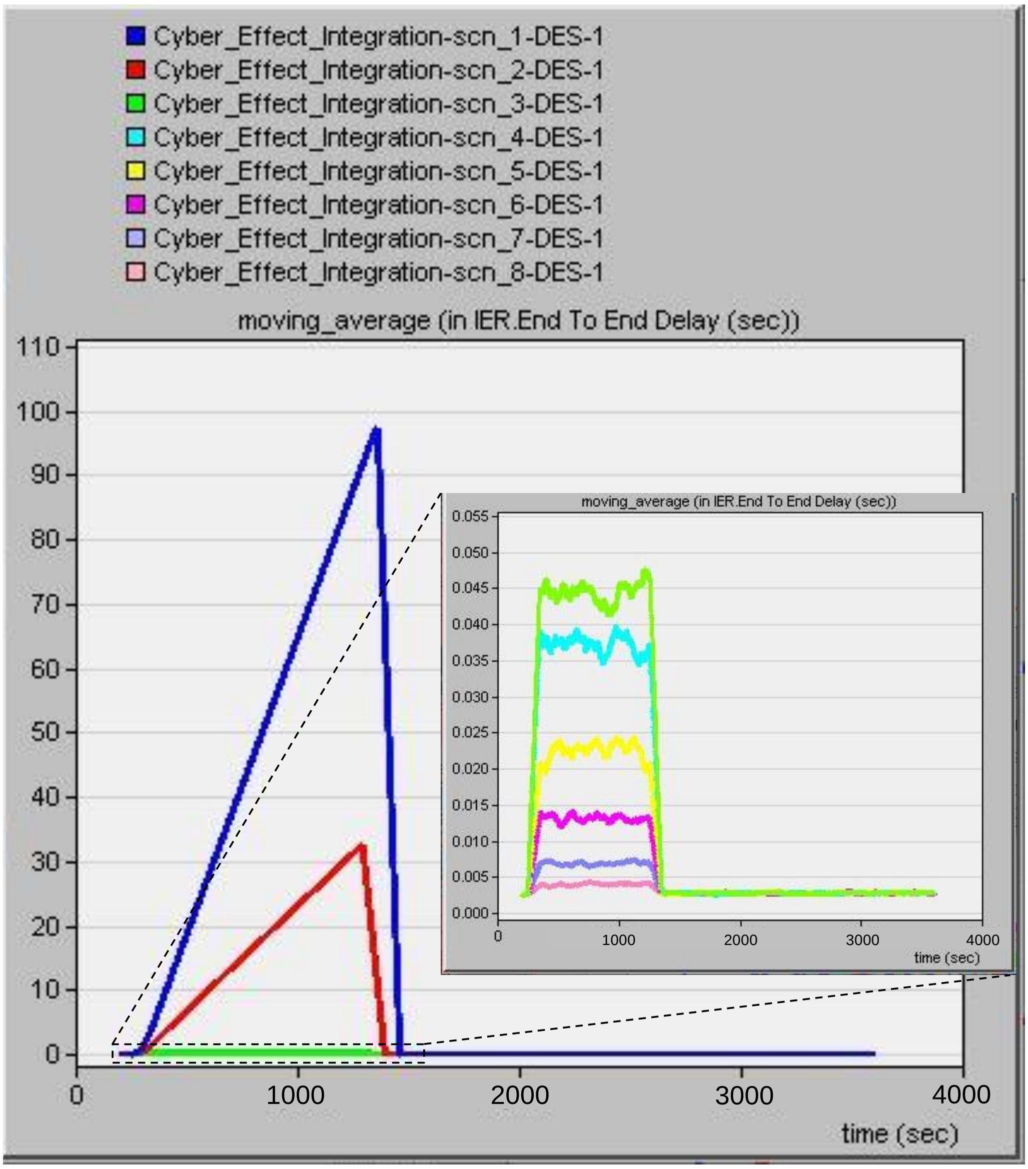
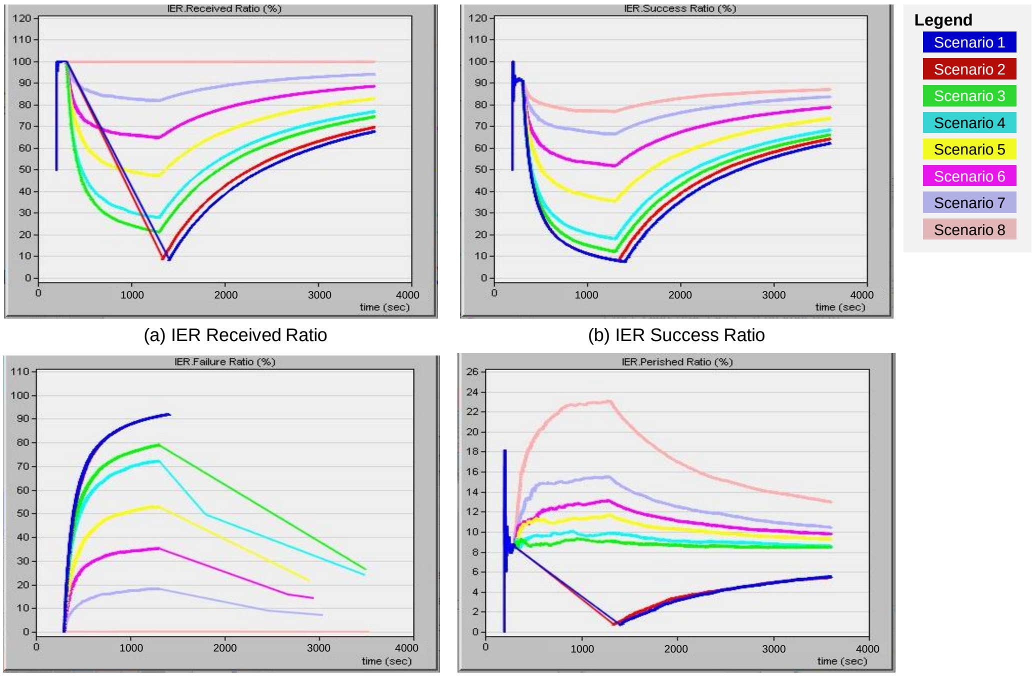


Figure 15. End-to-end IER transmission delay according to the DDoS attack volume.

Figure 16 is an illustration of the transmission characteristics of the IER according to the scenario: (a) is the reception rate of the IER, (b) is the success rate of the IER transmission, (c) is the IER transmission failure rate, and (d) is the IER delay reception rate. (a) shows that in all scenarios, except scenario 8, the IER reception rate decreases during the DDoS attack and then increases again when the DDoS attack ends. However, (b), (c), and (d) show that the IER did not satisfy the timeliness required and exceeded it by 20%, even in situations where the DDoS attack was low relative to the link load (scenarios 7 and 8). Therefore, a cyberattack by an internal attacker can have a serious impact on the battlefield management system.



(a) IER Received Ratio

(b) IER Success Ratio

(c) IER Failure Ratio

(d) IER Perished Ratio

Figure 16. IER transmission characteristics under DDoS attack load.

The scenario applied in this paper is presented as a way to simulate or analyze the impact of a cyberattack on military operations in the event of a cyberattack on a military network. To respond to such an attack, the response team can mitigate a DDoS attack by restricting the total traffic or the amount of traffic circulating on individual nodes by checking IPS's anomaly detection policy in the path of the attacked node in the short term, and adjust the ACL of the real firewall or constructive model environment firewall to block access to the nodes participating in the DDoS attack. It can also analyze the command delivery information of the nodes involved in a DDoS attack to perform a response, such as blocking the connection of the C&C server that delivered the attack command, and can master these tips of action through the cyber range.

5. Conclusions

A military cyber range configuration should not only be configured as a training ground for cybersecurity education, but also as a training ground where the cyberspace guarded by the military can be realistically configured to carry out effective defensive operations. It should also serve as a testing ground for cyber ranges to conduct inorganic system development net weather security tests and interoperability tests.

To this end, the range of each Army, which was previously established in the form of a cyber defense training field, was developed around the battlefield management system of each Army, and the function of forming a scenario was developed by proposing a method of forming a range jointly by connecting each Army range together with the Joint Chiefs of Staff. Through this, we made it possible to conduct practical cyber defense training and proposed a test site for interoperability test evaluation during Development Tests (DT) in the development of weapons systems. As in the case of NCR in the U.S., we also need to make continuous progress through in-depth simulation of the actual battlefield management system based on the multi-range configuration presented in this paper. This research will ensure that, in the future, various tactical weapon systems can be combined with the battlefield management system, and the interoperability evaluation and security test of the new weapon system can be carried out.

We designed and built a method of combining the basic configuration results of the cyber range for training with several ranges. For actual interoperability test evaluation, it is necessary to develop a method for virtualizing and operating each application system. Additionally, the method of operation in conjunction with the tactical system over a wireless link needs to be addressed.

The advantages of the multi-cyber range proposed in this paper are as follows. First, a single range can be extended to form a training environment. Second, by creating an integrated test environment that looks like reality, mission-based impact assessment is possible. However, the disadvantage of this proposed technology is that it can further complicate the management element. As we have seen in the case of NCR, the operation of a cyber range has issues that require a great deal of management and engagement in terms of personnel. To overcome this, agent technology with various AI technologies is needed. In the future, automatic preferences, automatic traffic generation, and automatic attack agents should be developed to meet user needs.

Technically, we believe that this operating concept can be developed into a training and T&E system with greater realism and visibility by combining digital twin and metaverse technologies.

Author Contributions: Conceptualization, M.P.; Funding acquisition, D.S.; Methodology, K.K. and H.L.; Design of Scenario, Y.K.; Supervision, D.S.; Validation, H.L.; Writing-original draft, M.P.; 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 Korea 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:

NCR	National Cyber Range
TRMC	Test and Training Resource Management Center
T&E	Test and Evaluation
MILS	Multiple Independent Levels of Security
DDoS	Distributed Denial of Service
C4I	Command, Control, Communication, Computer and Intelligence
VPN	Virtual Private Network
LVC	Live Virtual Constructive
MTF ICD	Message Text Format Interface Control Document
CDS	Cross Domain Solution
OT	Operational Test
OS	Operating System
DNS	Domain Name System
GUI	Graphic User Interface
PMS	Patch Management System
IER	Information Exchange Requirements
CPE	Common Platform Emulation
CVE	Common Vulnerability Enumeration
ACL	Access Control List
PCAP ATT&CK	Packet Capture Adversarial Tactics, Technique & Common Knowledge
EAI UDP	Enterprise Application Integration User Datagram Protocol
C&C DT	Command and Control Development Test

References

1. Bloom, J. *The Financial Implication of Technical Debt*; CAST Software Ltd.: New York, NY, USA, 22 February 2011.
2. Damodaran, S.K.; Smith, K. *CRIS Cyber Range Lexicon*; Version 1.0 (Report 59-0001); MIT Lincoln Laboratory: Lexington, KY, USA, 2015.
3. Hutchison, S.J. *Shift Left! Test Earlier in the Life Cycle*; Defense Acquisition University: Fort Belvoir, VA, USA, 2013.
4. Oikonomou, N.; Mengidis, N.; Spanopoulos-Karalexidis, M.; Voulgaridis, A.; Merialdo, M.; Raisr, L.; Hanson, K.; Vallee, P.L.; Tsikrika, T.; Vrochidis, S.; et al. ECHO Federated Cyber Range: Towards Next-Generation Scalable Cyber Ranges. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021.
5. Urias, V.E.; Stout, W.M.S.; Van Leeuwen, B.; Lin, H. Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper. In Proceedings of the 2018 International Carnahan Conference on Security Technology (ICCST), Montreal, QC, Canada, 22–25 December 2018.
6. Pridmore, L.; Lardieri, P.; Hollister, R. National Cyber Range (NCR) Automated Test Tools: Implications and Application to Network-Centric Support Tools. In Proceedings of the 2010 IEEE AUTOTESTCON, IEEE, Orlando, FL, USA, 13–16 September 2010.
7. Ferguson, B.; Tall, A.; Olsen, D. National Cyber Range Overview. In Proceedings of the 2014 IEEE Military Communications Conference, Baltimore, MD, USA, 6–8 October 2014.
8. Jacq, O.; Salazar, G.P.; Parasuraman, K.; Kuusijarvi, J.; Gkaniatsou, A.; Latsak, E.; Amditis, A. The Cyber-MAR Project: First Results and Perspectives on the Use of Hybrid Cyber Ranges for Port Cyber Risk Assessment. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021.
9. Peratikou, A.; Louca, C.; Shiaeles, S.; Stavrou, S. On Federated Cyber Range Network Interconnection. In *Lecture Notes in Networks and Systems, Proceedings of the 12th International Networking Conference. INC 2020. Plymouth, UK, 5 January, 2020*; Springer: Berlin/Heidelberg, Germany, 2021.
10. Cruz, T.; Simões, P. Down the Rabbit Hole: Fostering Active Learning through Guided Exploration of a SCADA Cyber Range. *Appl. Sci.* **2021**, *11*, 9509. [CrossRef]
11. Teixeira, M.A.; Salman, T.; Zolanvari, M.; Jain, R.; Meskin, N.; Samaka, M. SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach. *Future Internet* **2018**, *10*, 76. [CrossRef]
12. Cruz, T.; Rosa, L.; Proença, J.; Maglaras, L.; Aubigny, M.; Lev, L.; Jiang, J.; Simoes, P. A cybersecurity detection framework for supervisory control and data acquisition systems. *IEEE Trans. Ind. Inform.* **2016**, *12*, 2236–2246. [CrossRef]
13. Mathur, A.; Tippenhauer, N. SWaT: Secure Water Treatment Testbed for Research and Training in the Design of Industrial Control Systems. In Proceedings of the IEEE Computer Society International Conference on Computers, Software & Applications, Vienna, Austria, 11 April 2016.
14. Smyrlis, M.; Somarakis, I.; Spanoudakis, G.; Hatzivasilis, G.; Ioannidis, S. CYRA: A Model-Driven CYber Range Assurance Platform. *Appl. Sci.* **2021**, *11*, 5165. [CrossRef]
15. Ukwandu, E.; Farah, M.A.B.; Hindy, H.; Brosset, D.; Kavallieros, D.; Atkinson, R.; Tachtatzis, C.; Bures, M.; Andonovic, I.; Bellekens, X. A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. *Sensors* **2020**, *20*, 7148. [CrossRef] [PubMed]
16. Chouliaras, N.; Kittes, G.; Kantzavelou, I.; Maglaras, L.; Pantziou, G.; Ferrag, M.A. Cyber Ranges and TestBeds for Education, Training, and Research. *Appl. Sci.* **2021**, *11*, 1809. [CrossRef]
17. Vishwanath, K.V.; Vahdat, A. Swing: Realistic and Responsive Network Traffic Generation, *IEEE/ACM. Trans. Netw.* **2009**, *17*, 712–725.
18. Bieniasz, J.; Szczypiorski, K. Dataset Generation for Development of Multi-Node Cyber Threat Detection Systems. *Electronics* **2021**, *10*, 2711. [CrossRef]
19. Botta, A.; Dainotti, A.; Pescapé, A. A tool for the generation of realistic network workload for emerging networking scenarios. *Comput. Netw.* **2012**, *56*, 3531–3547. [CrossRef]
20. Heinbockel, W.; Noel, S.; Curbo, J. Mission Dependency Modeling for Cyber Situational Awareness. In *NATO IST-148 Symposium on Cyber Defence Situation Awareness*; NATO: Sofia, Bulgaria, 3 October 2016.