applied sciences

MDPI

Article

A Study on Cyber Target Importance Quantification and Ranking Algorithm

Kookjin Kim [1,2], Seunghwan Oh [3], Donghwan Lee [1], Jiwon Kang [1,3], Jungsik Lee [4] and Dongkyoo Shin [1,2,3,*]

[1] Department of Computer Engineering, Sejong University, Seoul 05006, Korea; gramist8529@gmail.com (K.K.); dhwlee@sju.ac.kr (D.L.); jwkang@sejong.ac.kr (J.K.)
[2] Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul 05006, Korea
[3] Cyber Warfare Institute, Sejong University, Seoul 05006, Korea; shoh@sejong.ac.kr
[4] Cyber/Network Technology Center 3 Team, Agency for Defense Development, Seoul 05661, Korea; godsider@add.re.kr
* Correspondence: shindk@sejong.ac.kr

Abstract: Most of the challenges and conflicts facing countries and groups today involve cyberspace. Therefore, military forces around the world are developing methods (doctrines) and weapon systems to conduct cyberspace operations in order to dominate cyberspace. To conduct cyberspace operations, cyber target information must be collected in cyberspace, and cyber targets must be selected to achieve effective operational objectives. In this study, we develop a target importance rank (TIR) algorithm based on the PageRank algorithm that quantitatively calculates the importance of each target in cyberspace for cyber target selection. The proposed algorithm was developed to quantify the degree of connectivity, criticality, and exposure of computer network hosts, and to create a list of target importance priorities based on the quantified values.

Keywords: cyberwarfare; cyberspace; cyberspace operation; cybersecurity; cyber target

Citation: Kim, K.; Oh, S.; Lee, D.; Kang, J.; Lee, J.; Shin, D. A Study on Cyber Target Importance Quantification and Ranking Algorithm. *Appl. Sci.* **2022**, *12*, 1833. https://doi.org/10.3390/app12041833

Academic Editor: Leandros Maglaras

Received: 8 January 2022
Accepted: 7 February 2022
Published: 10 February 2022

1. Introduction

The world is constantly developing information and communication technology and infrastructure, and cyberspace is recognized as the core basis for information administration services and the operation of major national infrastructure. With the recent surge in state-based cybercrime and terrorism, systematic cyberattacks are posing serious challenges to national security.

The Department of Defense (DoD) separates cyberspace from other spaces such as land, sea, air, and space, and has announced the DoD Strategy for Operating in Cyberspace, defining cyberspace as the fifth battlefield. Accordingly, the DoD is building a cyber warfare response system [1]. In addition, JP 3-12 classifies cyberspace operations (CO) as cyber network operations (CNO), defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO) [2].

As the world has recognized the cyberspace domain as an operational and mission domain in earnest, we have been faced with the current trends in which we need to secure the ability to conduct COs from a macroscopic perspective in order to secure "cyberspace dominance." The COs conducted by military forces require active and positive cyberspace actions, as well as cyberspace defense. To perform cyber intelligence, surveillance, and reconnaissance (ISR) in an enemy's cyberspace during peacetime and identify and manage targets, active COs are essentially required. The identified potential targets are recommended through the target development and prioritization process, which is the second stage of the targeting process. In this second stage, basic and intermediate target development is performed, and a list of verified and approved targets is created as a cyber target list. Finally, target priorities must be given.

In this study, a target importance rank (TIR) algorithm based on the PageRank algorithm was used to explain the items to be considered when assigning priorities to the cyber target list and calculating the cyber target importance (CTI) scores for the items to be considered. The TIR algorithm was derived based on the PageRank algorithm to calculate the CTI score. This score is used to suggest a way to assign priorities.

2. Related Works

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation, as well as the experimental conclusions that can be drawn.

2.1. Definition of Cyberspace Operations and Cyber Objects

COs are operations that use cyber-related capabilities to achieve military purposes in cyberspace. Cyber operations are largely divided into CNO, DCO, and OCO. JP 3-12 (2018) [2] describes cyberspace where COs are performed as three largely interrelated layers, and FM 3-12 (2021) [3] describes the cyberspace objects of each layer as follows:

The physical network layer consists of IT devices (PCs, servers, routers, etc.) in a physical domain that provide the storage, transmission, and processing of information within cyberspace, including connections between data stores and network components.

The logical network layer consists of logical programming (OS, apps, etc.) that runs network components and network elements related to each other in an abstract manner in a physical network.

A persona network layer is a cyberspace perspective created by using rules applied to the logical network layer to develop digital representations of an individual or an individual's identity in cyberspace and extract data from the logical network layer. These persona network layers may be directly related to individuals or organizations (e-mails, IP addresses, web pages, phone numbers, SNS accounts, etc.) by integrating some personal or organizational data (e-mails, IP addresses, social media accounts, etc.).

2.2. Definition of Cyber Target and Cyber-Targeting Process

2.2.1. Definition of Cyber Target

The target refers to a specific area or complex of the enemy, such as facilities, units, equipment, and personnel who are judged to engage in military action, and the target value is determined by the degree to which the commander contributes to achieving the operational objectives [4].

Target intelligence refers to a detailed and systematic analysis of nodes related to enemy personnel, units, locations, facility systems, missions, objectives, and capabilities as information, indicating vulnerability and importance by technology and identification of objects or groups [4].

The definition of a cyber target is similar to that of a target in military operations according to the contents of cyber objects in JP 3-60 [4] and 2.1. However, the targets of attacks include intangible as well as physical targets. That is, a cyber object existing in each layer of cyberspace may be a cyber target.

In this study [2], the dependence relationship of the cyberspace layer is interpreted as shown in Figure 1, defining the persona network layer as belonging to the logical network layer and the logical network layer as belonging to the physical network layer.

In addition, the cyber target is defined as a host (server, client) belonging to the physical network layer.

2.2.2. Definition of Cyber-Targeting Process

Targeting is used to systematically analyze and prioritize targets to achieve the commander's objectives in consideration of operational requirements, capabilities, and evaluation results, and to apply appropriate killing and non-killing measures to targets. Target development refers to the process of identifying, evaluating, and documenting potential

targets that contribute to the achievement of the commander's objectives as part of the second phase of the target-processing cycle [4].

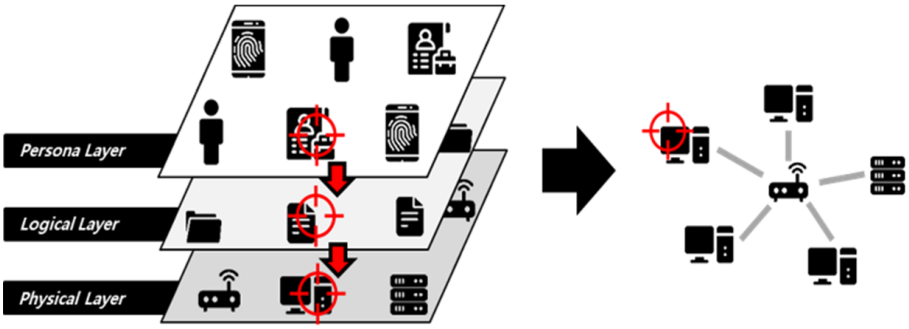

Figure 1. Three Cyberspace layers and Cyber Target.

In military operations, the targeting process is divided into a deliberate targeting process of reviewing and analyzing targets over a period that is sufficient to carry out a normal targeting process and a dynamic targeting process of quickly processing unexpected targets.

The deliberate targeting process is as follows. The target information maintains a close relationship with the operation and has continuity, as shown in Figure 2, for each cycle [4].

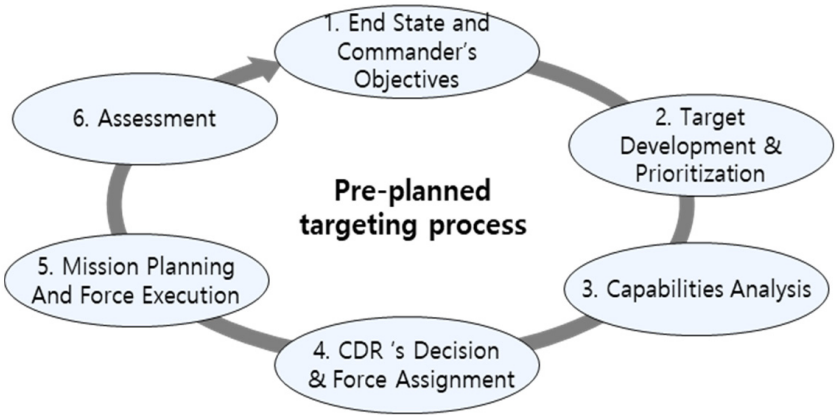

Figure 2. Deliberate Targeting Process.

In this study, various studies and manuals are referenced to define the cyber-targeting process based on the deliberate targeting process in Figure 2.

The US Chairman of the Joint Chiefs of Staff guidelines CJCSI 3370.01B (2016) [5] describes more detailed content in the field of target development in JP 3-60 (2020) [4]. In addition, it contains the procedures and contents of each stage of target development, the output, electronic target folders (ETF) used in the development stage, and the contents of the target DB. It also defines data on joint targets, information and intelligence relationships, target development roles and responsibilities, and targeting process cycles, as well as presenting data items and examples for basic, intermediate, and detailed target development in the target development stage. Franz [6], the current head of operations at the U.S. Cyber Command, said that the integration of cyberspace operational effectiveness is essential in the joint forces' operational planning and implementation in the cyber domain. It has also been suggested that the targeting process in a cyberspace operation be implemented in accordance with the targeting process of the joint unit commander. This also explains the application of the six-step procedure of the targeting process, major operational documents such as the United States CYber COMmand Joint Integrated Prioritized Target List (USCYCOM JIPTL) and Master Cyber Attack Plan (MCAP), and cooperation matters.

Combining these studies and manuals [4–6], the cyber-targeting process applies the same steps as in Figure 2. It is executed in conjunction with the targeting process of joint operations. In addition, the contents of each stage are adjusted and executed in accordance with CO. Accordingly, in this study, the CO targeting process and main activities are summarized as shown in Figure 3.

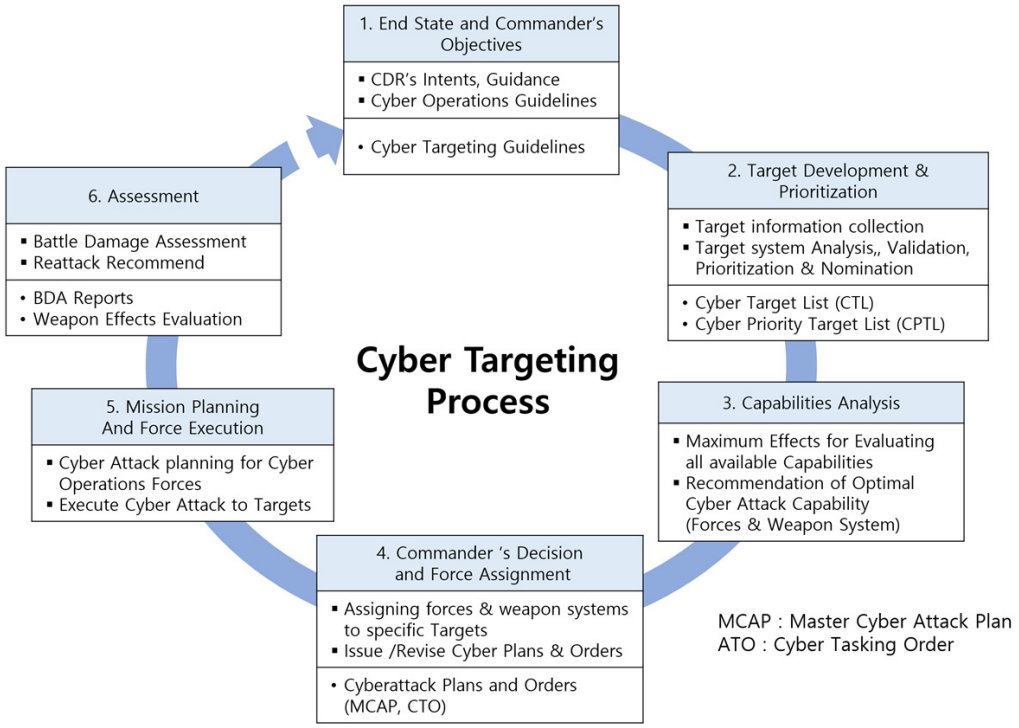

Figure 3. Cyber-Targeting Process.

2.3. Cyber Target Development and Cyber Target Prioritization Process

2.3.1. Cyber Target Development

In the second stage of the targeting process, "target development and prioritization," target information collection, target analysis, target development and validation, and prioritization are performed. The cyber target development stage is applied in the same way as military operations [2]. In target development, potential targets are analyzed first, followed by target development at the entity level. Target development at the entity level goes through the following process:

1. Basic Target Development;
2. Intermediate Target Development;
3. Detailed Target Development.

Each process is divided into the minimum essential data required according to the targeting process, such as the identification of basic information about the target, analysis of functional characteristics, and mission performance. The list of targets necessary for the execution of CO is also maintained and managed by applying the target list of military operations mutatis mutandis. In addition, the candidate target list (validation targets), CTL (target has been verified and there are no specific restrictions on engagement), cyber prioritization target list (CPTL) (prioritized based on CO commander's objectives), etc., should be created and managed in various forms.

2.3.2. Cyber Target Prioritization Process

The priorities of military targets are selected by integrating the target nomination list (TNL) recommended by the component forces according to the goals of the joint force

commander and reviewing them in relation to the commander's objectives and operational point of view. Prioritization of the CTL is also normally applied according to the "Cyber Force Operation Guidelines" according to the commander's objectives.

When examining the priority selection items for the component military target recommendations of the military operations, as shown in Table 1, the target recommendation priority criteria can be divided into three items.

Table 1. Component military recommendation target priority criteria.

Index	Target Recommendation Priority Criteria
1	Adequacy of the commander to achieve his objectives
2	Target importance
3	Target suitability

The US JP 3-60 [4] presents special considerations for prioritizing military operations targets. To summarize, it is organized into three types, as shown in Table 2. The following items are considered when calculating a target's priority:

1. Adequacy for the achievement of the commander's objectives (compliance with commander's objectives and operating guidelines: Criteria Item 1, Special Consideration Item 1);
2. The importance of targets (relative importance between targets in cyberspace: Criteria Item 2);
3. Target suitability (Special Consideration Items 2, 3).

Table 2. Special considerations for prioritizing military operations.

Index	Special Considerations
1	Achieving goals in the Joint Forces Commander's objectives
2	Sensitive targets for political or collateral damage: special measures required
3	HVT (High-Value Target), HPT (High-Payoff Target), TST (Time-Sensitive Target), component-group important target

Based on the above, the cyber target prioritization process was designed as shown in Figure 4. The priority analysis items are selected based on the commander's objectives, importance of the target, and suitability of the target, and can be added or excluded, if necessary, by the commander. A cyber target prioritization item is applied in consideration of the characteristics of the CO, and by quantifying and aggregating them, cyber targets can be prioritized. The cyber priority target list becomes a CPTL, which is utilized in the third stage of targeting (capability analysis) and operational planning.

To give priority to the CTL, this study proposes a method for calculating and prioritizing the importance score for each target to quantify its importance among the cyber target priority analysis items.

2.3.3. Definition of Cyber Target Importance

The importance of targets in military operations can be summarized as seen in Table 3 by referring to [2,6]. In summary, important targets (regions, facilities, bases, etc.) of enemy defense operations can be selected as sub targets. It is possible to calculate the importance of each target and give it a relative priority. Considering Table 3 and the manual [3,4], the definition of target importance in CO CTI is the relative importance between cyber targets in cyberspace. This is a value representing how much damage can be inflicted on the enemy if a specific target is attacked while CO are being carried out. Therefore, it is necessary to select a cyber target from among the enemy cyber assets and evaluate the importance of the target by first considering the host as defined in 2.2.1 in terms of the value of the target.

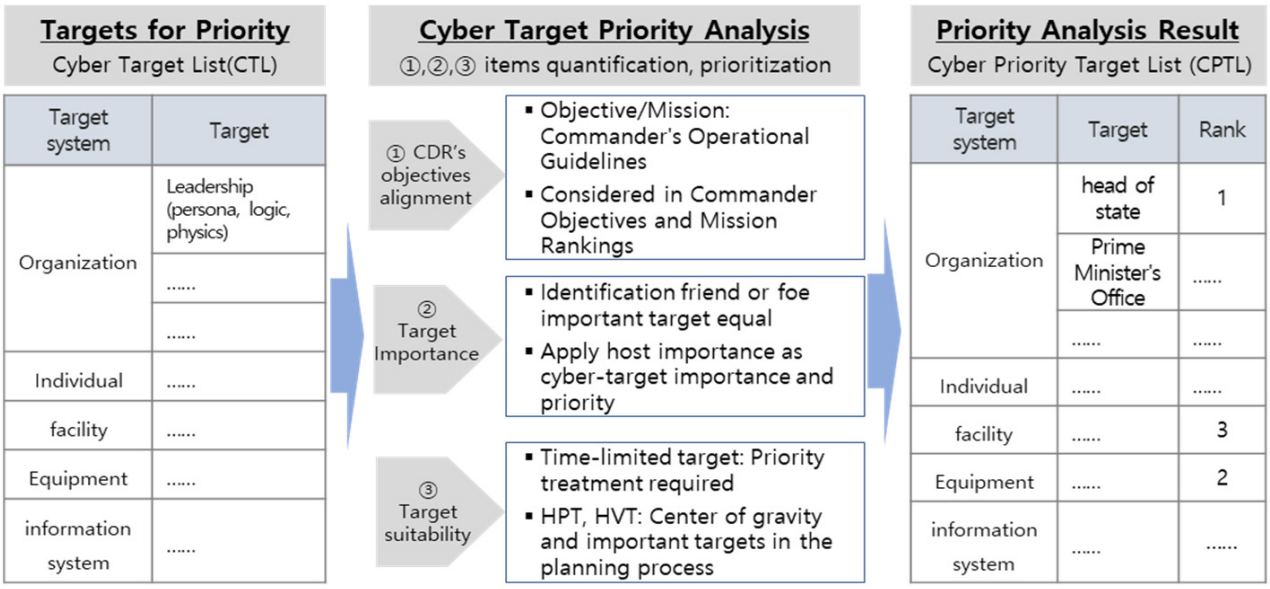

Figure 4. Cyber Target Prioritization process.

Table 3. Importance of targets in military operations.

Target Importance	Special Considerations
Intermediate target development stage (Significance)	Consider the value of the target from the enemy's point of view and the analysis of the target system
Importance of target system analysis (Criticality)	Value, Depth, Recuperation, Capacity

2.4. Case Study on Quantifying Importance of Cyber Assets

In 2.2.1, a cyber target is defined as a host (server, client) belonging to the physical network layer, and research cases deducing the importance of the host among cyber assets were investigated.

2.4.1. PageRank Algorithm

Page and Brin et al., [7,8] proposed the PageRank algorithm. The PageRank algorithm assigns a numerical weight to each element of a hyperlinked document set such as the World Wide Web (WWW) and performs power iteration to quantitatively calculate the relative importance within the set.

The PageRank algorithm outputs a probability distribution that is used to represent the likelihood that a person who randomly clicks on a link will arrive at a particular page. It is assumed that the distribution of all the pages it can collect when the computer process starts is evenly divided. That probability is expressed as a numeric value between 0 and 1. For example, a probability of 0.3 is usually expressed as a "30% probability" that something will happen. In other words, a page with a PageRank of 0.3 means that there is a 30% chance that a person who clicks on any link will be directed to the corresponding document.

The PageRank calculation formula is shown in Equation (1), and the definitions of the parameters used in the formula are listed in Table 4. Analyzing Equation (1), all the pages and hyperlinks in the WWW can be expressed as vertices and arcs. As a calculation example of the PageRank algorithm, we want to derive the value of page p_1 out of 6 pages. At this time, when the value of d is 1 and the link and PageRank values of each page are

as shown in Figure 5, the PageRank value of p_1 is 1/6 (total number of pages) + {(0.1/5) + (0.3/2) + (0.05/1) + (0.2/10) + (0.3/3)} = 0.51.

$$PR(p_i) = \frac{1-d}{|M(p_i)|+1} + d \sum_{p_i \in M(p_j)} \frac{PR(p_j)}{|L(p_j)|} \quad (1)$$

Table 4. PageRank algorithm parameter definitions.

Parameter	Definition
PR	PageRank: The probability that a random clicker of a link will reach a specific page (range: 0 to 1)
p_i	Page p_i
$M(p_i)$	Set of pages pointing to page p_i
p_j	Pages pointing to page p_i (may be represented by an edge)
$L\left(p_j\right)$	Set of hyperlinks on page p_j pointing to page p_i
d	Damping factor: The probability that a web surfer will click on a link to another page without being satisfied with that page (range: 0 to 1)

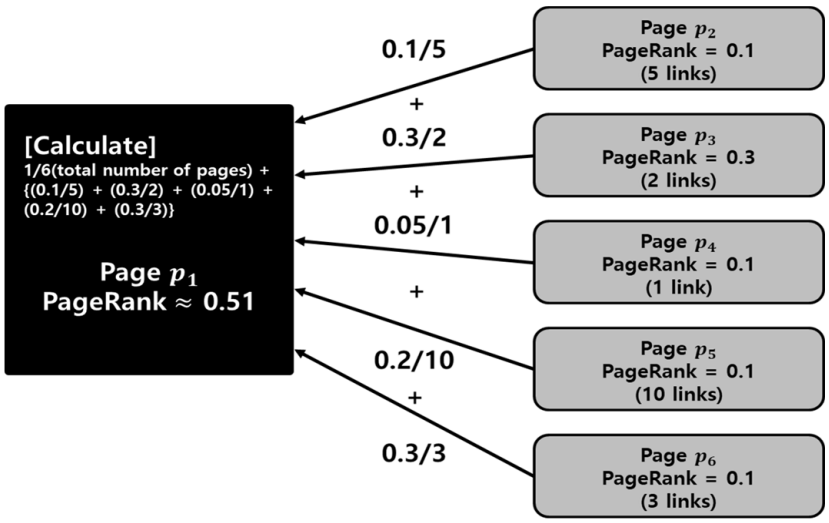

Figure 5. PageRank calculation example.

2.4.2. Event Prioritization Framework

Kim et al. (2014) [9] proposed an event prioritization framework (EPF) that determines priorities according to the influence of events on the host. This framework quantitatively calculates the network's host exposure, asset criticality, and events to hosts (sum of comprehensive event effectiveness, event clustering, etc.). Then, using the calculated value, the priority is determined according to the effect of the event on the host.

Host exposure (HE) is a potential attack risk value that synthesizes various vulnerabilities of a host. The calculation formula is as shown in Equation (2), and the definitions of the parameters used in the Equation are listed in Table 5. Asset criticality (AC) is quantified by considering app, network, data, command, and operation system (OS) importance values using the TOPSIS [10] algorithm proposed by Yoon et al. (1995).

$$\begin{aligned} HE_{C,I,A}(h_i) = IC_{C,I,A}(h_i) * (10-y) * MI_{C,I,A}(h_i)^{W_{MI}} * MV(h_i)^{W_{MV}} \\ * ACA(h_i)^{W_{ACA}} + ATT_{C,I,A}(h_i, x, y) \end{aligned} \quad (2)$$

Table 5. EPF parameter definitions.

Parameter	Definition
IC	Initial compromise level: Potential damage level of host h discovered by vulnerability scanner
MI	Max impact : Potential maximum impact of a vulnerability present in host h for each of the CIA elements
MV	Max vulnerability : The sin gle largest vulnerability in the set of known vulnerabilities for host h
ACA	Access vector: Minimum access required for an attacker to compromise your system Complexity: Average level of complexity required for an attack Authentication: Minimum number of authentications required by a hacker when attacking a system using one or more vulnerabilities
ATT	Attack surface with two parameters x and y: Potential damage to the vulnerability
W_k	Weight for k

2.4.3. Host Severity Assessment Cases

As part of the cyber command and control real-time decision support technology project conducted by the Korea Defense Science Research Institute, the impact on mission performance was evaluated when the network infrastructure was subjected to a cyber-attack. To evaluate the impact, we mapped and managed the dependency on assets and missions, and used the indicators listed in Table 6 to evaluate the criticality of the host asset based on confidentiality, integrity, and availability (CIA).

Table 6. Host Criticality Metrics.

Evaluation	Evaluation Factor	Weight	Points
C	- Degree of risk to mission when asset information is leaked (severe, partial risk, minor, etc.) - Amount of confidential information contained in each asset (more than 100, 20–99, less than 20)	0.5	3
I	- The degree of possibility of failure to perform duties and services due to falsification of asset information (severe, partial risk, minor, etc.) - The degree to which the original information can be recovered in the event of falsification of asset information (impossible to recover, recoverable after a certain period, easy to recover within 1 h)	0.5	3
A	- When the use of the relevant asset is impossible, the degree to which it is impossible to perform a task or service because there is no replacement (backup) asset (more than 24 h, 1–24 h, less than 1 h) - The importance of the mission related to the asset (high, medium, low) - Number of daily sessions for the asset (greater than 500, between 100 and 500, less than 100) - Amount of communication data using assets (more than 10 GB, 1–10 GB, less than 1 GB)	0.25	4

3. Design of Target Importance Rank Algorithm

In this section, the cyber target development and cyber target importance of 2.3 are synthesized to derive target importance criteria for CO. In addition, the TIR algorithm is designed to quantify the score of each criterion by synthesizing the 2.4 cyber asset importance quantification research cases. Finally, scenarios (network topology, experimental data) to verify this algorithm are designed based on the STUXNET case.

3.1. Identification of Cyber Target Materiality Criteria and Utilization Parameters

The cyber target importance quantification method defined in Section 2.3.3 was derived by synthesizing the research cases in 2.4.

Equation (1) calculates the connectivity of each page through parameters such as $M(p_i)$ and outputs the probability distribution using parameter d. Therefore, we change the definition of the connectivity between pages to the connectivity between hosts. We then compute d as the "asset criticality" value and assign a cyber target importance using the PageRank algorithm.

As the cyber target is defined as the host in Section 2.2.1, the host exposure in Equation (2) can be assumed to be the target exposure, and the exposure degree, which is the vulnerability of the target, can be quantitatively calculated using EPF.

Finally, using the indicators in Table 6, the target criticality, which is the degree of influence when attacking the host, can be quantitatively calculated.

Based on these research results, three criteria for the importance of cyber targets were defined as listed in Table 7. When deriving the scores for each standard item quantitatively, factors that can be utilized were identified with Table 8.

Table 7. Cyber Target Importance Criteria.

Criteria	Definition
Target Connectivity	The degree of dependence of the target on other hosts
Target Criticality	Influence when attacking a target
Target Exposure	The extent to which the target is exposed to the vulnerability

Table 8. Identification of parameters for quantifying Target Importance Criteria.

Criteria	2.4.1 Equation (1)	2.4.2 Equation (2)	2.4.3 Table 6
Target Connectivity	<Table 4 $M(p_i)$>	-	-
Analysis: Connectivity between pages can be quantified as a set of hosts adjacent to the target host.			
Target Criticality	<Table 4 d>	-	<Table 6>
Analysis: Using Table 6, the criticality of the target can be quantified, and by substituting this into in Table 4, it can be defined as 'the probability of moving to another network if the network is not important from the attacker's point of view.			
Target Exposure	-	<Equation (2)>	-
Analysis: The exposure of the host—that is, the exposure of the target—can be quantified using vulnerability-related parameters.			

Analyzing Table 8, Equation (1) has two target importance criteria. It is a suitable algorithm for synthesizing the elements of the research cases of this paper. In addition, if Equation (2), which can quantify the target exposure, is properly fused with Equation (1), the importance of the target can be calculated quantitatively.

In the next section, Equations (1) and (2), and Table 6, are used to design the TIR algorithm to be used to achieve the purpose of this study.

3.2. TIR Algorithm Design and Prioritization Method

In this section, we propose a method for calculating the score for each surrender using the identified parameters and criteria listed in Tables 7 and 8. By synthesizing the calculated scores, the cyber target score is then calculated, and a plan is proposed that can be used to select priorities.

3.2.1. Cyber Target Connectivity Score Calculation Method

According to Section 2.2.1 which defines cyber targets as hosts, the definition of 'd' in Table 4 is changed to 'the probability of moving to another network if the network is not

important from an attacker's point of view', and the page(p) in Equation (1) is changed to host(h) as shown in Equation (3).

$$PR(h_i) = \frac{1-d}{|M(h_i)|+1} + d \sum_{h_i \in M(h_j)} \frac{PR(h_j)}{|L(h_j)|} \quad (3)$$

3.2.2. Cyber Target Criticality Score Calculation Method

An arbitrary value between 0 and 1 is substituted for d (damping factor) in Table 4. This is calculated by dividing the value derived using the indicators in Tables 6–10 so that it conforms to the target importance calculation method. In Section 2.4.1, because the value of d is applied globally, the average of the d values of hosts belonging to one network cluster is calculated, and the score of d in Table 9 is calculated, as shown in Figure 6.

Table 9. PageRank-based Target Connectivity scoring parameters.

Parameter	Definition
h_i	Host h_i
$M(h_i)$	Set of hosts associated with host h_i
h_j	Hosts associated with Host h_i [Neighbor Hosts] (Can be represented by an edge, connected in both directions to each other.)
$L\left(h_j\right)$	A set of close hosts of host h_j connected to host h_i.
d	Probability of moving to another network if the network is not important from the attacker's point of view

Table 10. TIR parameters.

Parameter	Definition
TIR	Host h_i's Target Importance Rank
$HE_{C,I,A}(h_i)$	Host Exposure of Host (Target) h_i
d	Probability of attacker finding another target when target criticality is low

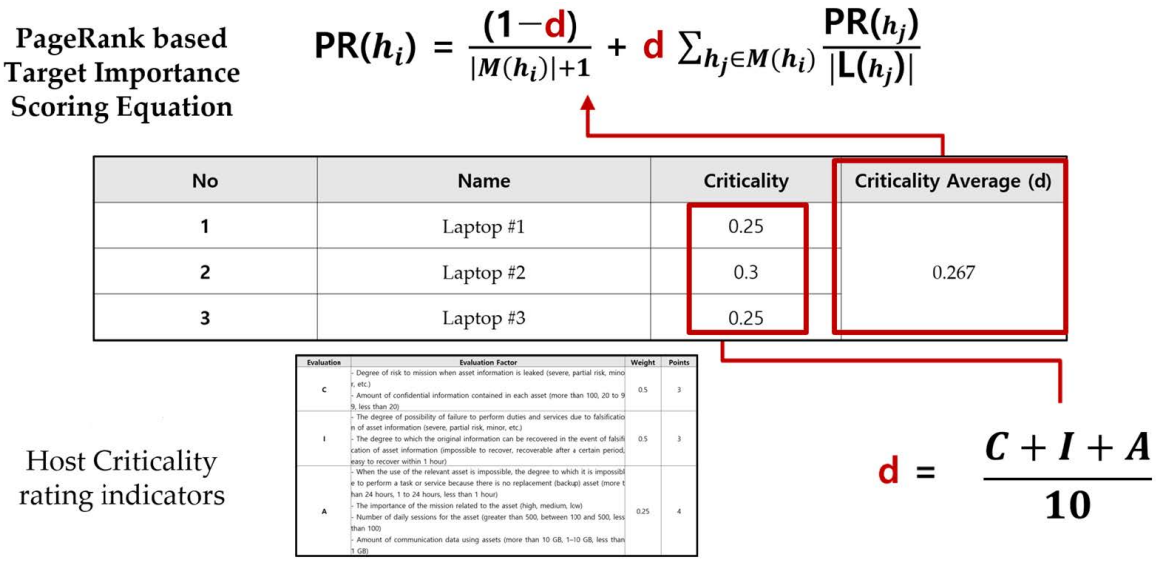

Figure 6. Cyber Target Criticality score calculation method.

3.2.3. Cyber Target Exposure Score Calculation Method

Previously, the target connectivity and target criticality were derived among the target importance criteria, and finally the target exposure was derived from Equation (2) for the HE value in Section 2.4.2. First, the definition of HE is changed to the "potential attack risk value that synthesizes various vulnerabilities on the target." The derived HE value is integrated into the PageRank-based target importance assignment formula derived as shown in Equation (3) and defined as TIR. Accordingly, PR is changed to TIR, as shown in Figure 7.

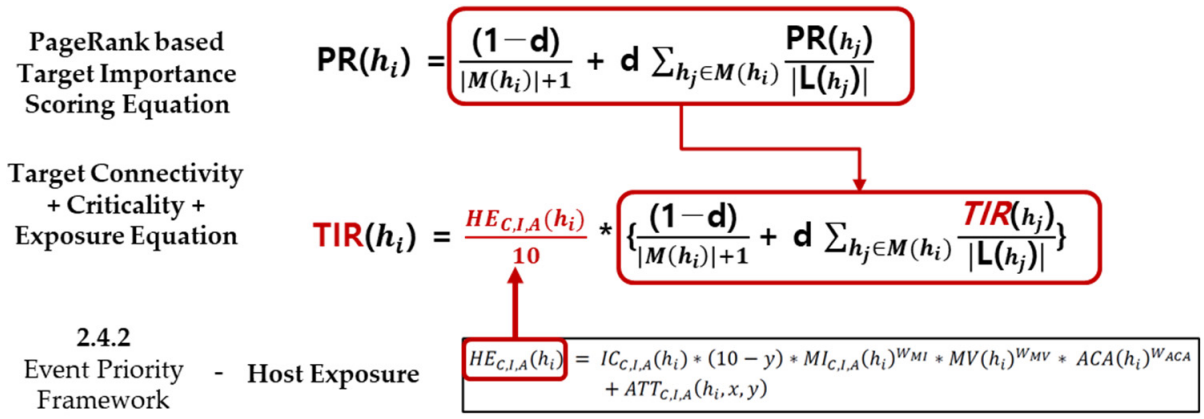

Figure 7. Cyber Target Exposure score calculation method.

3.2.4. TIR Scoring and Prioritization

The score elements for each cyber target importance criterion from Sections 3.2.1–3.2.3 are summarized, as shown in Figure 8. Accordingly, Equation (4) for synthesizing the target importance score is derived. Equation (4) is an algorithm for deriving the target importance score using the PageRank algorithm proposed in this study. The parameters to be used comply with the contents of Table 9, but the added parameters and changed definitions are provided in Table 10.

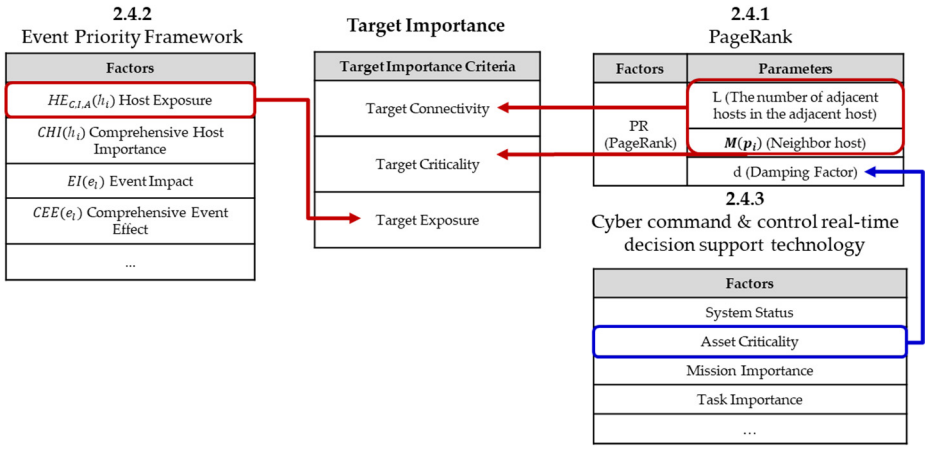

Figure 8. Linking factors of research cases by Target Importance Criteria.

The network topology is transformed into a logical structure, as shown in Figure 9, to derive the target importance priority. Then, using the TIR algorithm, the results listed in

Table 11 are obtained. Finally, if the TIR scores are sorted in descending order, the important targets are listed from the top.

$$TIR(h_i) = HE_{C,I,A}(h_i) * \left\{ \frac{1-d}{|M(h_i)|+1} + d \sum_{h_j \in M(h_i)} \frac{TIR(h_j)}{|L(h_j)|} \right\} \quad (4)$$

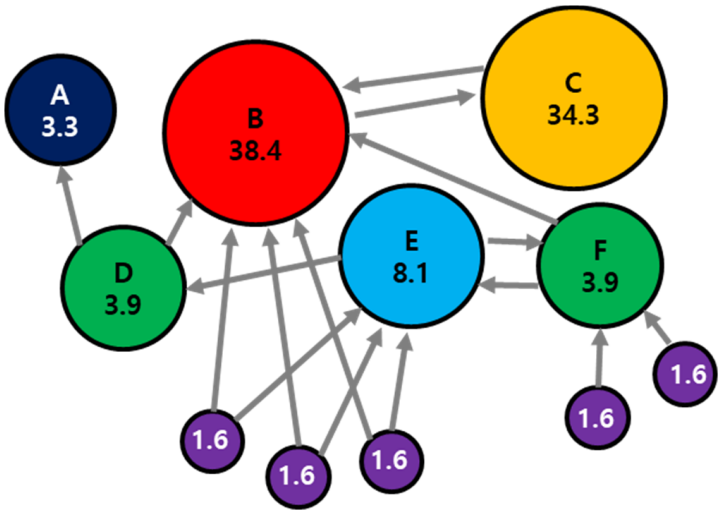

Figure 9. Examples of logical network topologies for deriving Target Importance priorities.

Table 11. PageRank-based Target Connectivity scoring parameters.

Rank	Target (Host)	Target Exposure	Target Criticality	Target Connectivity	TIR
1	B	0.9	0.88	6	38.4
2	C	0.6	0.44	5	34.3
3	E	0.4	0.33	4	8.1
4	D	0.2	0.11	2	3.9
4	F	0.2	0.11	2	3.9

4. Design of Experimental Scenario and Experiment Results

4.1. Design of Experimental Scenario

4.1.1. Analysis of STUXNET Case

The STUXNET attack, which destroyed and incapacitated the SCADA system of an Iranian nuclear power plant, was an incident in which a centrifuge in the Iranian Natanz nuclear facility was damaged as a result of a series of cyberattacks between 2007 and 2012 [11]. The Iran nuclear facility target system consists of the Natanz nuclear facility and Arack; the centrifuge, power supply system, and SCADA system can be viewed as target components. The identified cyber targets were the PLC H/W, PLC logic control S/W, etc., considering the three layers of cyberspace [11]. The SCADA system is a major piece of equipment that collects and controls data in real time. It is mainly installed in computer-controlled core infrastructure such as power plants, oil and gas pipelines, refineries, and water supply facilities, and programmable logic controllers (PLCs) H/W. The PLCs at the Natanz nuclear facility that STUXNET attacked were Simatic Step 7 controllers from Siemens, Germany. STUXNET infected this system to tamper with the PLC code blocks, hide the tampered code, and execute the hidden tampered code block when Step 7 was called. The final targets of STUXNET's attack were two central processing units, S7-315 and S7-417. In this case, certificates from trusted companies were used to prevent exposure by automatic detection systems. In order to break into the computers in the facility (Air-Gap),

we used vulnerabilities that existed between computers or between computers and USB. An analysis of the above text shows that the Natanz nuclear facility is a production and enrichment facility among Iranian nuclear facilities, and can be classified as a component of a target system. As a target, it can be classified as a centrifuge, a power supply system, and a SCADA system. For the selection of the target, the experiment was performed by selecting the SCADA system and PLCs as dual components and selecting the access path to connect the internal worker PC via USB.

4.1.2. STUXNET Case-Based Network Topology and Scenario Data Configuration

A scenario was constructed using the attack graph designed based on the STUXNET case, as shown in Figure 10, out of the cases [11,12] introduced in Section 4.1.1. The goal of the operation and the commander's goal were to neutralize the target industrial process at the bottom of Figure 10, and it was assumed that the operation was performed in cyberspace. After that, it was assumed that the targets analyzed according to the cyber target processing procedure in Figure 3 were composed of the network topology structure shown in Figure 11.

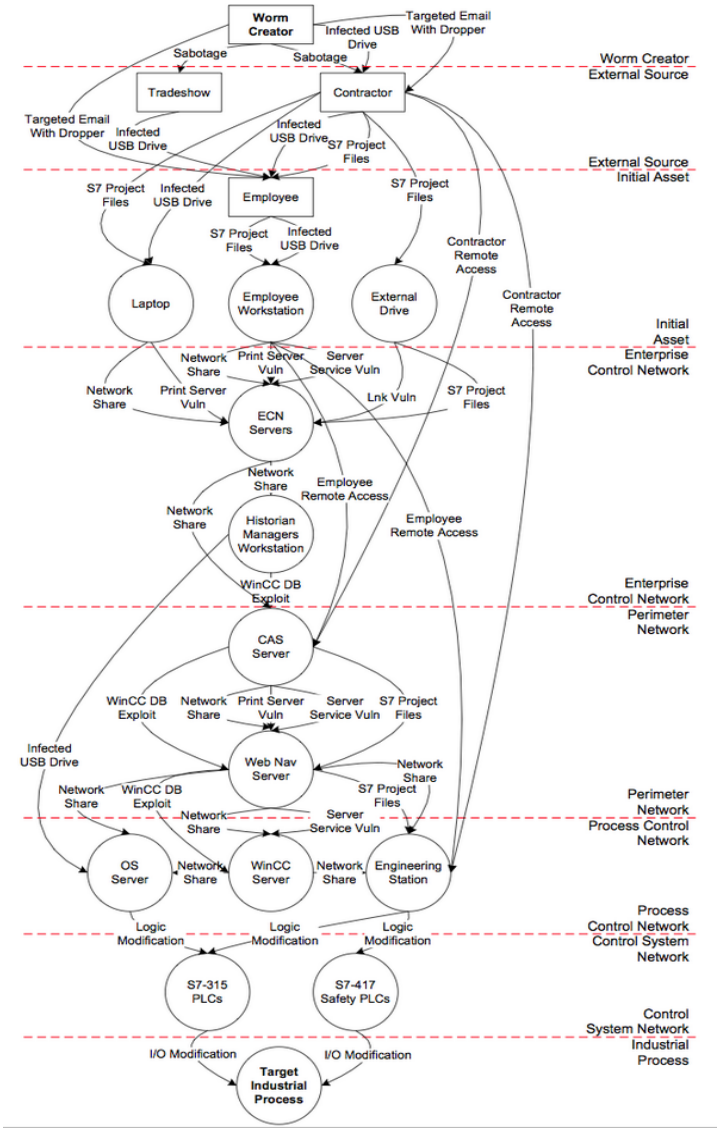

Figure 10. Attack Graph designed based on STUXNET case.

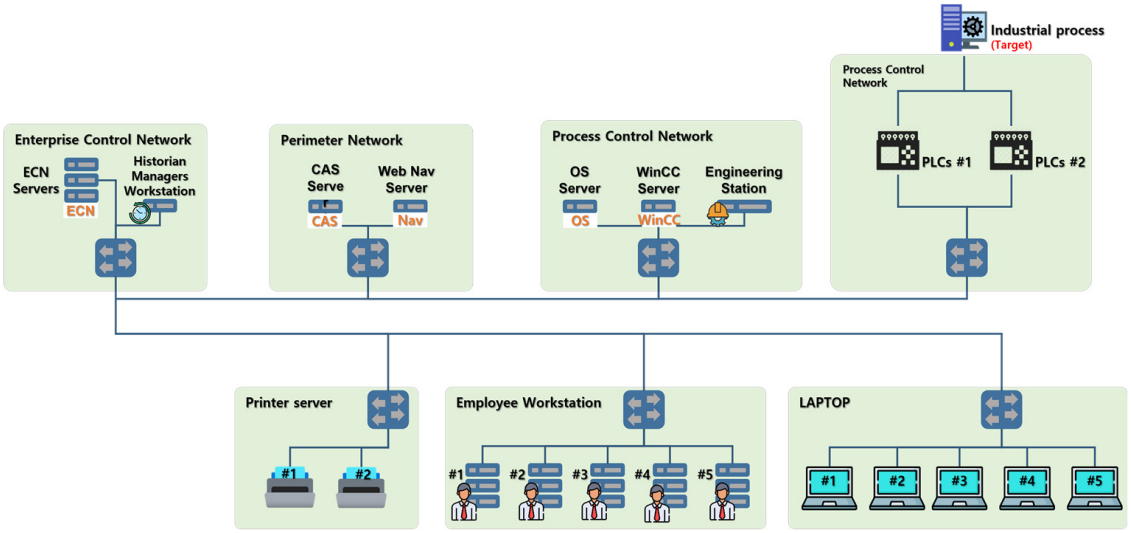

Figure 11. STUXNET case-based network topology (Physical).

Each vertex in Figure 10 is defined as one node in Figure 11, which shows the network structure. In addition, assuming that there can be multiple nodes such as a printer server, employee workstation, and laptop, 2–5 nodes were placed. The cluster consisted of each tier in Figure 10, except for the initial asset layer and the print server. Each cluster was also assumed to be connected to one switch, and the switches were assumed to be connected to each other in one direction.

To perform the TIR proposed in this study, it needed to be converted into a logical network topology as shown in Figure 9. It could be converted as shown in Figure 12 through the following process:

1. It is assumed that nodes clustered based on the switch (clotted with a green background) may communicate internally with each other because of the switch;
2. Connect the nodes in one cluster to each other.

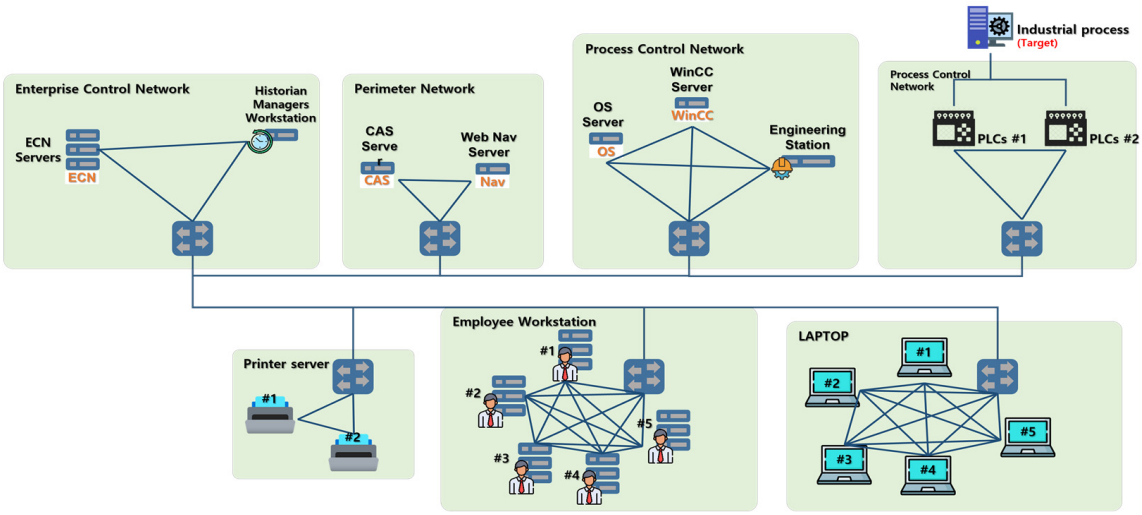

Figure 12. STUXNET case-based network topology (Logical).

Among the nodes in Figure 12, the common vulnerabilities and exposures (CVE) of the hosts were selected by combining the contents of case [11] and Figure 10. In the case of an engineering station, as shown in Figure 10, there was only network share in the call related to the vulnerability. After that, the Windows shell LNK (CVE-2010-2568)—a network share

vulnerability introduced in the cases in [11]—was selected as a vulnerability, and common vulnerability scoring system (CVSS) v2 [13] parameter scores were inserted. There were a total of two neighboring hosts (other hosts in the same cluster), and this operation was repeated to generate data to be used in the experiment, as listed in Table 12.

Table 12. Part of scenario data.

Name	CVE	CVSS v2						Target Exposure
		AV	AC	Au	C	I	A	
Engineering Station	CVE-2010-3944	0.395	0.71	0.45	0.7	0.7	0.66	7
	CVE-2020-7586	0.395	0.71	0.45	0.3	0.3	0.28	
	CVE-2009-3676	1	0.61	0.45	0	0	0.66	

4.2. Experiment Result

By substituting the scenario data listed in Table 12 into the TIR algorithm (Equation (4)) written in 3.2 and the priority selection method, the target priority was derived as listed in Table 13.

Table 13. Part of TIR algorithm experiment result data.

Name	CVE	CVSS v2						Host Exposure					Target Connectivity	Target Criticality	Target Exposure	TIR (Result)
		AV	AC	Au	C	I	A	IC	MI	MV	ACA	ATT				
S7-315 PLCs	CVE-2012-3015	0.395	0.61	0.45	0.7	0.7	0.66	1	0.66	1.14	1.27	4	2	9.5	9.37	9
	CVE-2010-2772	0.395	0.61	0.45	0.7	0.7	0.66									
	CVE-2016-9159	1	0.61	0.45	0.3	0	0									
	CVE-2016-9158	1	0.71	0.45	0	0	0.66									
S7-417 Safety PLCs	CVE-2012-3015	0.395	0.61	0.45	0.7	0.7	0.66	1	0.66	1.14	1.2	4	2	9	9.31	8.95
	CVE-2016-9159	1	0.61	0.45	0.3	0	0									
	CVE-2010-2772	0.395	0.61	0.45	0.7	0.7	0.66									
WinCC Server	CVE-2010-2772	0.395	0.61	0.45	0.7	0.7	0.66	1	0.66	1.14	1.29	4	3	8	9.47	8.45
	CVE-2007-3039	1	0.71	0.56	0.7	0.7	0.66									
	CVE-2009-1536	1	0.35	0.45	0	0	0.28									
	CVE-2008-4250	1	0.71	0.45	0.7	0.7	0.66									
	CVE-2009-3676	1	0.61	0.45	0	0	0.66									

For target connectivity, according to the Section 2.2.1 cyber target definition, the number of edges between hosts (excluding switches among the parts grouped in the green box in Figure 12) was used. The target criticality was quantified according to Table 6 and replaced with qualitative items, and weights were selected as MI: 1, MV: 0.5, and ACA: 1 when calculating the target exposure. When calculating up to the process in Figure 6, the target connectivity and target criticality scores were synthesized by selecting the initial PR value as 0.1 and performing power iteration four times to make the vector values similar. Finally, the TIR score was calculated by multiplying the target exposure value and sorted in descending order to finally derive the results listed in Table 13. As a result, the S7-315 PLCs were selected as the most important targets. This will allow commanders to easily understand target priorities and issue correct operational guidelines.

5. Conclusions

In this study, a method for assigning cyber target importance to calculate cyber target priorities was developed. To conduct the research, the importance of the target was defined by first examining domestic and foreign manuals. To calculate the importance score of the defined target, PageRank, an event prioritization framework, and host criticality evaluation cases were investigated.

The TIR algorithm was designed by deriving target importance criteria based on the investigated cases and synthesizing the formulas and indicators of the research cases. To prove this, the STUXNET case was analyzed, experimental data were created, and an experiment was conducted.

As a result, the S7-315 PLCs, which were physically and logically the closest to the objectives of the operation, were selected as the most important targets.

When designing cyber operations, the TIR algorithm can be used to determine which of the cyber targets located on the network are the most important. In addition, it could be a good reference for flexibly designing the operation by checking the connectivity, criticality, and exposure scores of the target, respectively.

In the private sector, if the TIR algorithm is used when designing operations belonging to the red team during cyber defense training, the operation success rate can be further increased. Cybersecurity teams can use the TIR algorithm to identify the riskiest network nodes and establish security measures for them.

Overall, our experiments with the TIR algorithm derive the importance of assets in cyberspace. This suggests that it is very useful in terms of cybersecurity.

In future research, after collecting BGP-Archive-Data and processing it into geographic information, the network status map will be visualized on the battlefield map. From this visualized network information, we will collect information (PC, Server, IP, SNS ID/PW, E-Mail, etc.) on friendly network areas, hostile network areas and private network areas and identify target groups. Thereafter, there are plans to further develop procedures and techniques for cyberattacks, such as prioritizing each target within the identified target group and selecting a policy to attack the target.

Author Contributions: Conceptualization, K.K., S.O. and D.S.; funding acquisition, D.S.; methodology, K.K., D.L. and J.L.; design of TIR algorithm, K.K., S.O. and D.L.; supervision, D.S.; validation, J.K.; writing—original draft, K.K. and S.O.; Writing—review & editing, D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Defense Acquisition Program Administration and Agency for Defense Development under the contract UD210004ED.

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:

TIR	Target Importance Rank
DoD	Department of Defense
CO	Cyberspace Operations
CNO	Cyber Network Operations
DCO	Defensive Cyberspace Operations
OCO	Offensive Cyberspace Operations
CTI	Cyber Target Importance
ETF	Electronic Target Folders
USCYCOM JIPTL	United States CYber COMmand Joint Integrated Prioritized Target List
MCAP	Master Cyber Attack Plan
CPTL	Cyber Prioritization Target List
TNL	Target Nomination List
WWW	World Wide Web
OS	Operating System
SNS	Social Networking Service
EPF	Event Prioritization Framework
HE	Host Exposure
AC	Asset Criticality
CIA	Confidentiality, Integrity, and Availability
PLCs	Programmable Logic Controllers
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
AV	Access Vector

AC	Access Complexity
Au	Authentication
IC	Initial Compromise Level
MI	Max Impact
MV	Max Vulnerability
ACA	Access Vector/Complexity/Authentication
ATT	ATTack surface

References

1. Gates, R.M. *Quadrennial Defense Review Report*; Department of Defense: Washington, DC, USA, 2010.
2. Scott, K.D. *Joint Publication (JP) 3-12 Cyberspace Operation*; The Joint Staff: Washington, DC, USA, 2018.
3. Hersey, N.S. *FM 3-12 Cyberspace and Electromagnetic Warfare*; Department of the Army: Washington, DC, USA, 2021.
4. Scaparrotti, C.M. *Joint Publication 3-60 Joint Targeting*; Joint Chiefs of Staff: Washington, DC, USA, 2013.
5. Joint Chiefs of Staff. *CJCSI 3370.01B, Target Development Standards*; Joint Chiefs of Staff: Washington, DC, USA, 2016.
6. Franz, G. *Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter*; Meade, F.G.G., Ed.; United States Cyber Command: Maryland, MD, USA, 2012; Volume 14, pp. 14–16.
7. Brin, S.; Page, L. The Anatomy of a Large-Scale Hypertextual Web Search Engine. *Comput. Netw. ISDN Syst.* **1998**, *30*, 107–117. [CrossRef]
8. Page, L.; Brin, S.; Motwani, R.; Winograd, T. The pagerank citation ranking: Bringing order to the web. *Tech. Rep. Stanf. Digit. Libr. Technol. Proj.* **1998**.
9. Kim, A.; Kang, M.H.; Luo, J.Z.; Velasquez, A. A Framework for Event Prioritization in Cyber Network Defense. *Tech. Rep. Nav. Res. Lab* **2014**.
10. Yoon, K.; Hwang, C. *Multiple Attribute Decision Making: An Introduction*; Sage: Newbury Park, CA, USA, 1995.
11. Falliere, N.; Murchu, L.O.; Chien, E. W32. stuxnet dossier. *White Pap. Symantec Corp. Secur. Response* **2011**, *5*, 29.
12. Nguyen, H.H.; Palani, K.; Nicol, D.M. An approach to incorporating uncertainty in network security analysis. In Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp (HoTSoS), ACM, New York, NY, USA, 4 April 2017.
13. Scarfone, K.; Mell, P. An analysis of CVSS version 2 vulnerability scoring. In Proceedings of the 3rd International Symposium on Empirical Software Engineering and Measurement, Lake Buena Vista, FL, USA, 15 October 2009.