Defence Science Journal, Vol. 75, No. 1, January 2025, pp. 27-34, DOI : 10.14429/dsj.20149

Designing Simulation Logic of Cyber Operations on Physical Space Using C2 Effectiveness Measurement

Sangjun Lee and Dongsu Kang*

Department of Computer Science and Engineering, Korea National Defence Univ., Nonsan - 330 21, Republic of Korea
**E-mail: dasekang@korea.kr*

ABSTRACT

The existing cyber operations training is based on working units, which makes it difficult to expect timely orders from commanders conducting physical warfare-focused operations. This study applies the effectiveness measurement and damage assessment quantification methods of the targeting assessment process to design a simulation logic for cyber operations training in conjunction with physical warfare. Random information variables are substituted into the command and control (C2) effectiveness measurement methodology to assume the impact of modulation attacks on C2 capabilities. The value of enemy assets determined in physical space and information errors in cyberspace are used as variables to measure operational effectiveness, converted into parameters, and entered into the simulator to assess damage. By applying the proposed simulation logic to the air operations case, it can be demonstrated that the increase in information error and the value of enemy assets reduces the operational effectiveness and increases the damage. By visualising this in a training model of a constructive environment, cyber operations command and response procedures can be mastered simultaneously.

Keywords: Simulation logic; Cyber operation training; Cyberspace quantification; Cyber measure of effectiveness; Cyber battle damage assessment

NOMENCLATURE

σ_a^2 : Information errors after a cyberattack (Initial value is σ^2, no errors)
p : Probability value (Initial value is p_c)
C_1 : Arbitrary constant
α : Probability multiplier
K : Effectiveness multiplier

1. INTRODUCTION

In the face of escalating military tensions with North Korea, the United States and the Republic of Korea have recently developed joint guidelines specifying detailed standards for cybersecurity, and continue to expand their capabilities to conduct joint operations in all areas, including cyberspace, by mastering and sharing information and response procedures through cyber alliance training[1].

However, the current level of cyber operation training is a red-teaming type[2], which may be suitable for specific cyber defence organisations or individual professionals to enhance their tactical abilities. Because of the lack of coordination with physical warfare units, these cases can act as factors that do not significantly recognise the importance of cybersecurity. Therefore, it is necessary to shift to a complex and expanded training method that connects cyber operations and physical space by merging existing types and table top types[3]. To this end, this study aims to contribute to multidomain integrated operations by visualising the quantified impact of adversary cyberattacks on physical warfare in the Modelling and Simulation (M&S) in a constructive environment.

The rest of the paper is organised as follows. Section 2 presents limitations and alternatives to existing studies for quantifying cyberspace, and Section 3 designs a procedure for simulating cyber operations in the M&S model. Section 4 validates the designed simulation logic with an air operations effectiveness measurement and damage assessment case study, and Section 5 concludes with a summary of the research.

Received : 30 April 2024, Revised : 05 September 2024
Accepted : 06 September 2024, Online published : 10 January 2025

2. LITERATURE REVIEW

2.1 Quantification of Cyber Operations

In physical warfare, all targets must be evaluated organically to derive missions (or end states) at the war level[4]. The targeting assessment process is divided into two parts: assessment metrics to measure the task, effectiveness, and evaluation objectives (e.g., Measure of Effectiveness (MOE)), and the Combat Assessment (CA), such as the Battle Damage Assessment (BDA), which measures the results of the engagement conducted by the task force. The outputs of the CA feed back into the combat task at the tactical level, which is the first step in the targeting assessment process[5]. In contrast to physical space, operational activities in cyberspace, which is defined as a virtual environment, are classified as noncombatant forces comprising intangible elements. As these elements are diverse and complex, which limits instrumentation and measurement, research is being conducted to quantify them by relating to the aforementioned procedures[6].

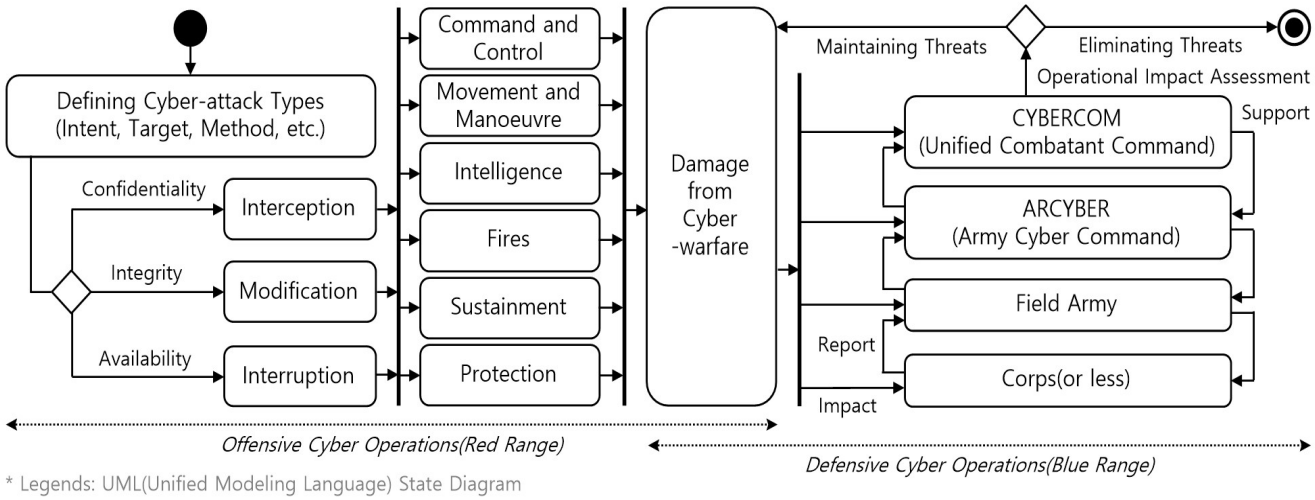


Figure 1. Cyber operations procedure.

However, the methods presented may lead to different assessment results depending on the subjective view of the expert or the environment in which the actual operation is conducted[7-14]. In particular, a CA calculated without considering assessment metrics cannot create a cycle of the targeting assessment process and may fail to provide the information required between operations. Therefore, the M&S requires the design of a formalised analysis tool to simulate the effects of cyber operations in conjunction with physical warfare, as well as a procedure to simultaneously measure and assess MOE and BDA throughout a single operation in a unified process.

2.2 Cyber Operation Algorithms

Cyberattacks are carried out to destroy the three goals of information security: Confidentiality, Integrity, and Availability, and MITRE Corp. has standardised the effects of cyberattacks into six categories: Degradation, Interruption, Modification, Fabrication, Unauthorised Use, and Interception[15]. The types of cyberattacks can be broadly categorised as interception, modification, and interruption based on the three objectives of the attacks on each information security target, and other similar categories can be further classified into different types of sub-attacks.

The U.S. Army's Field Manual for Operations (FM 3-0) identifies six warfighting functions as the core capabilities for achieving operational objectives: C2, Movement and Manoeuvre, Intelligence, Fires, Sustainment, and Protection[16]. In cyber operations, the warfighting functions are targeted by the adversary, and the cyber operations performance based on the type and objective of the proposed attack is shown in Fig. 1[17].

When a cyberattack of the defined type is executed against interception, modification, and interruption arise as damage caused by cyber warfare to the six major warfighting functions of friendly forces. In the military domain, the ultimate goal of an adversary cyberattack is to interrupt the C2. Therefore, the scope of this study is limited to the direct impact of modification attacks that compromise the integrity of the C2 and the indirect impact on fires function.

2.3 C2 Effectiveness Measurement Method

US DARPA (Defence Advanced Research Projects Agency) recognised the problem that C2 provides significant influence in winning or losing wars. To apply advanced C2 concepts to combat management, the Office of Naval Intelligence, which participated in the study, presented a methodology for quantifying the value of C2's information acquisition, processing, and exchange performance parameters in engagements between weapon systems.

By substituting the pre- and post-engagement relative combat power ratios, as measured by improvements such as information sharing and enhancement and force coordination, into a generalised form of Lanchester's Law, the method was able to derive the impact of enhanced or degraded C2 system performance on combat outcomes under certain conditions, confirming that C2 can be a significant force factor in combat outcomes.

Improvements are a key factor in determining the value of enemy and friendly assets, which are divided into two main categories: probability multipliers, consisting of non-combat factors (time, information, etc.), and ratio multipliers, consisting of combat factors (maximum range of a weapon, etc.), and are affected by the number and type of weapons, including troops[18].

To measure the impact of errors in information caused by a tampering attack, a type of cyberattack intended to threaten the integrity of data, on the C2 capabilities of the friendly forces targeted by the attack, a parametric function is needed to quantify it. To this end, we apply C2 effects measurement, which can efficiently measure the increase or decrease in C2, to measure and evaluate the impact of cyber operations on physical space. For this purpose, the degree of information error is set as a variable and data is calculated from the information engineering perspective, and the following four points are assumed.

- The change in the error variable of the information would have been caused by an adversary cyberattack
- To analyse only the operational impact of the information variable between effectiveness calculations, combat

power factors (ratio multipliers) such as the detailed specifications of the weapon system are not considered

- If there are no errors in the information, the combat effectiveness of the weapon system is not reduced and the operation has a 100 % chance of success
- At the command post, there is no change in the time required for C2 of the target detection to attack the decision phase of the emergency targeting process.

3. CYBER OPERATION PROCEDURE

3.1 Designing Simulation Procedure

In the military domain, to link cyber operations to physical warfare, an integrated simulation process can be designed to quantify impacts through a targeting assessment process and plot the results into an M&S in a constructive environment, as shown in Fig. 2.

First, the Red Operator conducts both physical and cyberattacks on friendly power assets operating under random battlefield conditions. The Blue Operator, who has the value of a specific asset, will be affected by the enemy's physical attack reflecting the battlefield change factors, and the time and combat power of the operation will be affected, as the value of the enemy's asset increases, the decline in combat power will also increase. In addition, cyberattacks can cause errors in the information provided by weapon systems that rely on the control system, causing indirect damage to the operator.

Indicative information errors are considered along with the increasing value of enemy assets to feed into the C2 effectiveness method and are used to analyse the MOE degraded by cyber operations. The operational impact of the BDA assessment from the previously measured MOE is then simulated and visualised in the M&S through the simulator.

The evaluated BDA supports the commander's command decision by feeding back into the tasking process, and after simulating the impact of the M&S, the cyber crisis judgement and information judgement are provided to the operators, enabling commanders and staff to master the command process of cyber operations and practitioners in cyber protection units to master the response process.

3.2 Occurring Weapon Control System Error

A modification of the integrity of the data will result in errors in the information the system presents to the user. Because the degree of information error may vary depending on the intent, method, and target of the attack and cannot be explicitly measured, the M&S requires a variable determination process through a simulated random sampling method for decision-making under general uncertainty conditions to determine the degree of information error. The representative simulated random sampling methods are Monte Carlo (MCS) and Latin Hypercube Sampling (LHS). MCS relies on randomness to draw two random samples from the entire uniformly distributed area, which has the disadvantage that the samples drawn may tend to be biased toward a particular space. The LHS relies on uniformity, or planned randomness, to divide the entire area into small similar intervals and sample each interval in

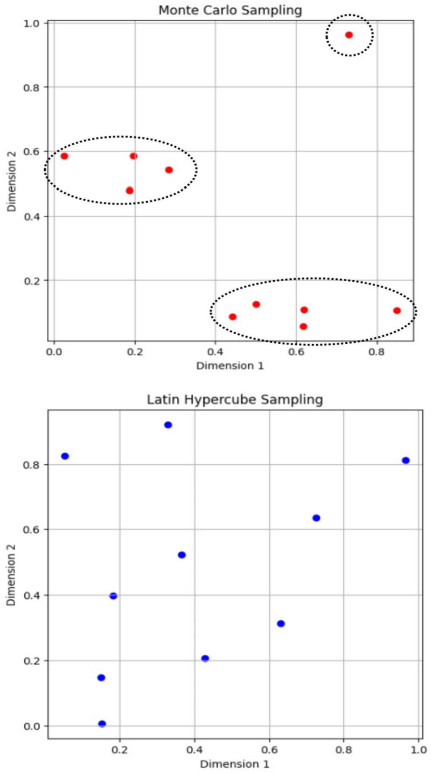


Figure 3. Sampling results using MCS, LHS.

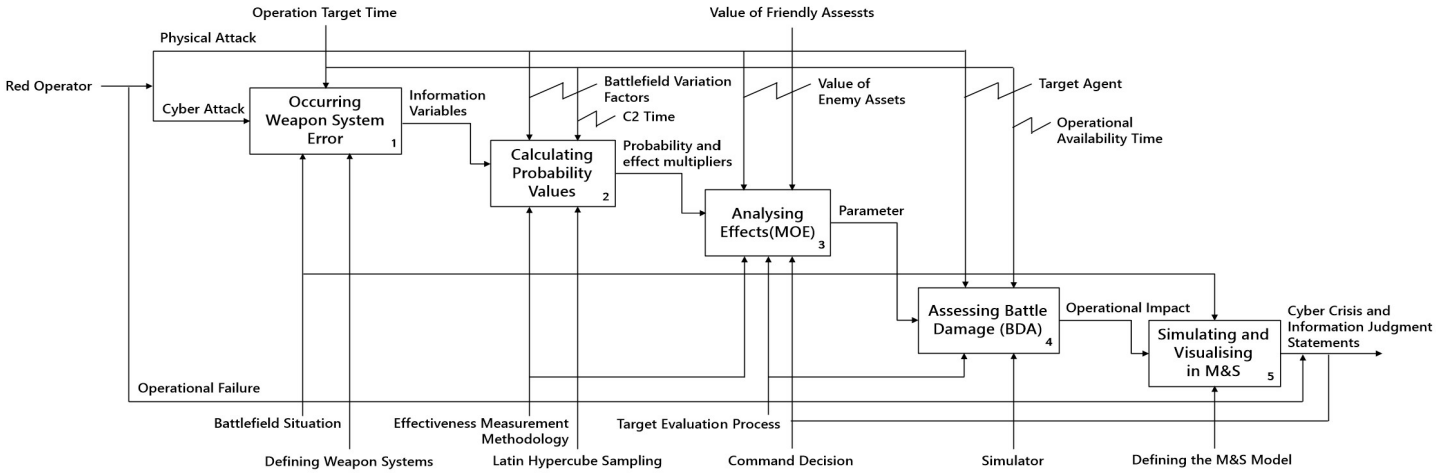


Figure 2. Procedure of cyber operation in conjunction with physical warfare.

rotation to avoid overlap as much as possible. Therefore, the samples are distributed over the area. Fig. 3 is an example of ten random numbers generated by the Python code to compare each sampling method. In this study, we use LHS, a relatively uniform sampling method in the M&S, to determine the degree of information error.

3.3 Calculating Probability Values

In the C2 effectiveness measurement, under the condition that hostile objects are randomly distributed in the area of interest A (ρ), the uncertainty of area (ΔA) is a function of the velocity of the platform (v_p), the accuracy of the initial information, and the C2 turnaround time (t_{cs}, control system). The probability value of detection and correct association within t_{cs} is defined as given in Eqn. (1).

$$p_c = \frac{1}{1+\rho\Delta A} = \frac{1}{1+C_1\rho v_p t_{cs}^2 \sigma^2} \tag{1}$$

In the probability value, the response preempted time of the operational force is the sum of the control system time and the available response time ($T_p = t_{cs} + t_a$). It must also satisfy $p = \alpha p_c$ ($\alpha > 1$) by α, which is a potential that represents the increment between p_c and p due to the improvement of C2 system performance. Therefore, α is derived from the difference in available time, which depends on the C2 system performance, and the preset degree of information error, as shown in Eqn. (2).

$$\alpha = \frac{1-\sigma_a^2}{p(1-\sigma_a^2)+(1-p)(1-\sigma^2)} \tag{2}$$

3.4 Analysing Operations Effects

To calculate the MOE, both the probability multiplier and the rate multiplier must be considered simultaneously. In the M&S, the ratio multiplier is a factor that can be automatically determined by the physical battlefield configured in the constructive environment, the MOE calculation only considers α constructed around the information variables. Substituting the value of enemy and and friendly assets (N', M') in a linear state into Lanchester's Square Law, the MOE calculation that reflects the changed value of enemy and friendly assets ($<N'^2>_j$, $<M'^2>_j$) after a single engagement j is shown in Eqn. (3). Accordingly, the MOE changed by the adversary's cyberattack can be presented as Eqn. (4), taking into account the α.

$$\text{when} \quad <MOE>_j = \frac{<N'^2>_j - <M'^2>_j}{N^2} \tag{3}$$

N', M': the value of friendly and enemy asset

$$\text{where} \quad <\hat{MOE}>_j = \frac{\alpha <N'^2>_j - <M'^2>_j}{N^2} \tag{4}$$

N', M': the value of cyber friendly and enemy assets

The rate of increase in MOE without accounting for the combat power factor, K, can be expressed as Eqn. (5), and based on the calculated probability value, multiplier data, and the C2 effectiveness measurement, because the change in C2 system performance can be measured ($\hat{MOE} = K \times MOE$).

$$K = \frac{<\hat{MOE}>_j}{<MOE>_j} = \frac{\alpha <N'^2>_j - <M'^2>_j}{<N'^2>_j - <M'^2>_j} \tag{5}$$

N', M': the value of cyber friendly and enemy assets

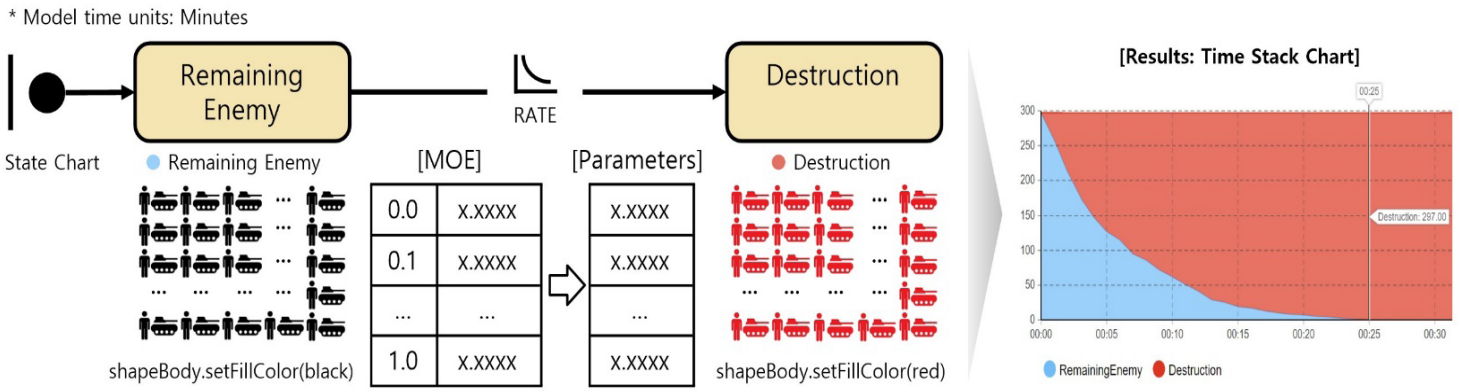
3.5 Assessing Battle Damage and Simulation

To apply the C2 theory to cyber operations, it is critical to quantify noncombat power, and the method defines noncombat power as a function of information error and time available. If operational effectiveness was measured based on information errors caused by adversary cyberattacks, the BDA can be evaluated with time available as a variable based on the calculated MOE to assess the full range of non-combat power factors defined by the method.

In the military M&S, a weapon score approach is applied to evaluate BDA, which takes into account the performance of multifunctional weapon systems[19]. However, since these approaches contain sensitive information and it is difficult to obtain public data, the study utilised the AnyLogic simulator, an object-oriented software that supports multi-modeling. The evaluation was performed using an agent-based technique, and the simulation identified two factors: the number of units that can be destroyed within the initial assigned operational time and the time required to destroy all assigned units, as shown in Fig. 4.

4. CASE STUDY: CLOSE COMBAT ATTACK

We analyse and assess the operational impact of an adversary cyberattack on a close combat attack (CCA). CCA is an operation in which attack helicopters are deployed in groups of two to four to conduct real-time attacks on temporary targets



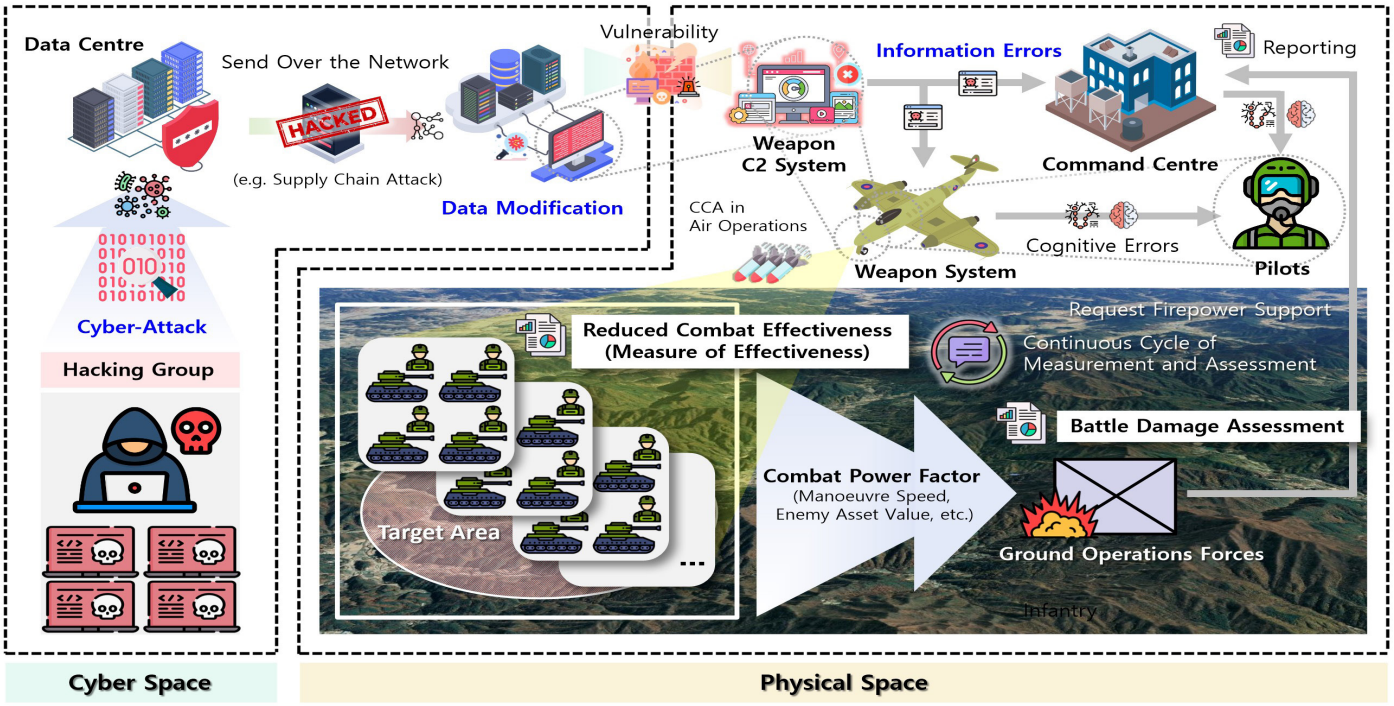


Figure 5. Engagement scenario for CCA operations.

within 1–2 km of ground forces[20]. The goal is a preemptive strike within 30 min using the kill chain concept dynamic targeting assessment process[21]. The target information is primarily directed at enemy mechanised infantry, which is highly mobile. In particular, the North Korean mechanised infantry is a brigade-centric enemy mobile force[22] whose mobility is typically estimated at 5 to 15 km/h.

The following are engagement scenarios. A manoeuvre battalion of a North Korean mechanized infantry brigade is approaching the front of a friendly ground operation force at 15 km/h, the maximum manoeuvring speed (v_p) for mechanised units, and the ground operation force has requested a CCA from its superior unit for target "1" ($\rho = 0.6666\ldots$) in a 1.5 km^2 (1.5 km wide × 1 km long) area of interest. It was determined that 5 min (0.0833 hr) would be required for C2 (t_{cs}) out of the operational target time (T_p) of 30 min, resulting in a total of 25 min of tactical availability (t_a). At this time, since cyberattacks, such as supply chain attacks, are carried out by malicious actors in cyberspace, much (or all) of the information provided by the attack helicopter's C2 system becomes erroneous (σ_a^2) due to the manipulation of data stored by the weapon system. Errors in the information directly affect command posts and weapon systems located in physical space and indirectly lead to cognitive errors in the pilots receiving the information from these systems.

The resulting effects are manifested as reduced effectiveness of weapon systems and increased damage to friendly forces in parallel with other elements of combat power, such as the value of enemy assets, in the physical space of the battlefield.

The calculated MOE and BDA are reported to the command post to iterate on C2 procedures and procedures for responding to an attack. The battlefield situation constructed based on these settings is shown in Fig. 5.

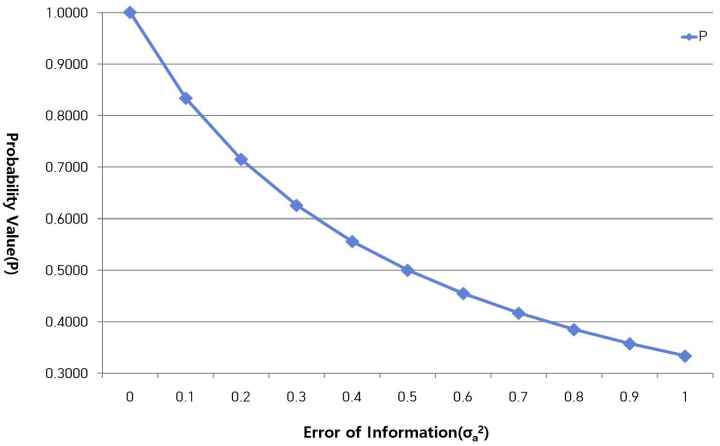


Figure 6. Changing probability values.

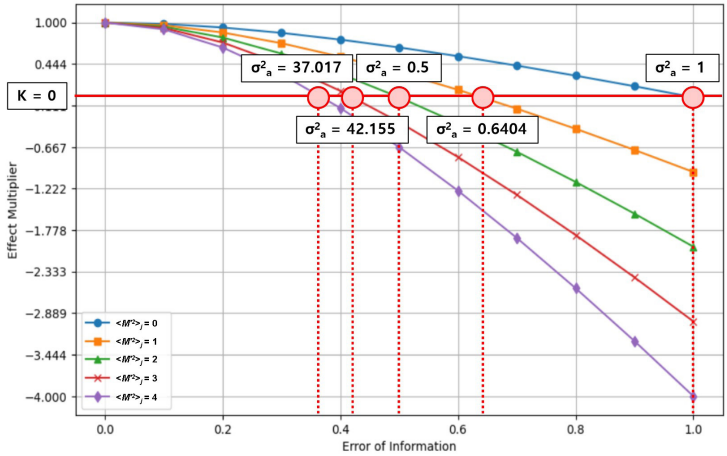


Figure 7. Changes in effectiveness multiplier.

Table 1. Calculation of multiplier based on '*p*'

Information error (σ_a^2)	Probability values (p)	Probability multiplier (α)	Effectiveness multiplier (K)				
			$<M'^2>_j = 0$	$<M'^2>_j = 1$	$<M'^2>_j = 2$	$<M'^2>_j = 3$	$<M'^2>_j = 4$
0.0	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
0.1	0.8333	0.9818	0.9818	0.9636	0.9455	0.9273	0.9091
0.2	0.7143	0.9333	0.9333	0.8667	0.8000	0.7334	0.6667
0.3	0.6250	0.8615	0.8615	0.7231	0.5846	0.4462	0.3077
0.4	0.5556	0.7714	0.7714	0.5429	0.3143	0.0858	- 0.1428
0.5	0.5000	0.6667	0.6667	0.3334	0.0000	- 0.3333	- 0.6666
0.6	0.4546	0.5500	0.5500	0.1000	- 0.3500	- 0.8000	- 1.2499
0.7	0.4167	0.4235	0.4235	- 0.1529	- 0.7294	- 1.3058	- 1.8823
0.8	0.3846	0.2889	0.2889	- 0.4222	- 1.1333	- 1.8444	- 2.5555
0.9	0.3572	0.1474	0.1474	- 0.7053	- 1.5579	- 2.4105	- 3.2631
1.0	0.3333	0.0000	0.0000	- 1.0000	- 2.0000	- 3.0000	- 4.0000

Table 2. Information errors and the impact of asset value on MOEs

MOE	σ_a^2	$<M'^2>_j = 0$			$<M'^2>_j = 1$			$<M'^2>_j = 2$		
		MÔE	Difference	Decline (%)	*MÔE*	Difference	Decline (%)	*MÔE*	Difference	Decline (%)
	0.0	1.0000	0.0000	0.00	1.0000	0.0000	0.00	1.0000	0.0000	0.00
	0.1	0.9818	0.0182	1.82	0.9636	0.0364	3.64	0.9455	0.0545	5.45
	0.2	0.9333	0.0667	6.67	0.8667	0.1333	13.33	0.8000	0.2000	20.00
	0.3	0.8615	0.1385	13.85	0.7231	0.2769	27.69	0.5846	0.4154	41.54
	0.4	0.7714	0.2286	22.86	0.5429	0.4571	45.71	0.3143	0.6857	68.57
1.0000	0.5	0.6667	0.3333	33.33	0.3334	0.6666	66.66	0.0000	1.0000	100.00
	0.6	0.5500	0.4500	45.00	0.1000	0.9000	90.00	- 0.3500	1.3500	135.00
	0.7	0.4235	0.5765	57.65	- 0.1529	1.1529	115.29	- 0.7294	1.7294	172.94
	0.8	0.2889	0.7111	71.11	- 0.4222	1.4222	142.22	- 1.1333	2.1333	213.33
	0.9	0.1474	0.8526	85.26	- 0.7053	1.7053	170.53	- 1.5579	2.5579	255.79
	1.0	0.0000	1.0000	100.00	- 1.0000	2.0000	200.00	- 2.0000	3.0000	300.00

Set a randomly sampled σ_a^2 as the information variable to calculate the p. The constant (C_1) applied to it was assigned a value of 28.8259 so that with an information error of 0.5, the probability value also becomes 0.5. The probability value is calculated by Eqn. (1). The probability value decreases proportionally to the information error, and the graph in Fig. 6 shows an exponential function.

According to the third assumption, in Eqn. (5), K must also be 1 when α is 1. Therefore, the value of the friendly asset required to calculate K is automatically determined by the number that the difference from the value of the enemy asset can be 1 ($<N'^2>_j - <M'^2>_j = 1$). As a result, this can represent a state in which the value of the friendly asset remains intact in the absence of the enemy's physical threat, and does not take into account situations in which the number of friendly forces or combat power in the existing possession increases or decreases beyond a certain level compared to the value of the enemy asset.

Then, the α based on p, and K based on the change in friendly and the enemy asset value can be calculated, as shown in Table 1. Since p decreases as σ_a^2 increases, α also decreases proportionally to the p. It can be seen that K, which is affected by α, has the same value as α when there is no impact from the value of the enemy asset ($<M'^2>_j = 0$). However as the value of $<M'^2>_j$ increases, K decreases to a greater extent. The point

Table 3. Simulation results for physical space impact of cyber operations

MÔE	Parameter	Destroy units within available time (25min)	Time to complete the operation
1.0000	0.1650	297	25 min
0.9818	0.1620	297 (± 0)	25 min (± 0)
0.9333	0.1540	295 (- 2)	27 min (+ 2min)
0.8615	0.1421	293 (- 4)	29 min (+ 4min)
0.7714	0.1273	290 (- 7)	32 min (+ 7min)
0.6667	0.1100	284 (- 10)	37 min (+ 12min)
0.5500	0.0908	272 (- 25)	45 min (+ 20min)
0.4235	0.0699	242 (- 55)	58 min (+ 33min)
0.2889	0.0477	206 (- 91)	85 min (+ 60min)
0.1474	0.0243	147 (- 150)	166 min (+ 141min)
0.0000	0.0000	0	-

at which K becomes zero due to increasing information error as shown in Fig. 7.

The MOE changes proportionally to the number of friendly troops (N) according to Eqns. (3-4), so we used $N = 1$. The changes in the MOE as a function of the information error and the value of enemy assets are shown in Table 2. From the point at which K becomes zero, which is the data calculated earlier, the desired operational effectiveness by friendly forces can no longer be achieved through combat (red square area). As a result, when the battlefield in physical space is significantly affected by the enemy, it becomes difficult to achieve the desired operational effectiveness even with information errors caused by relatively small data modulations as shown in Fig. 8.

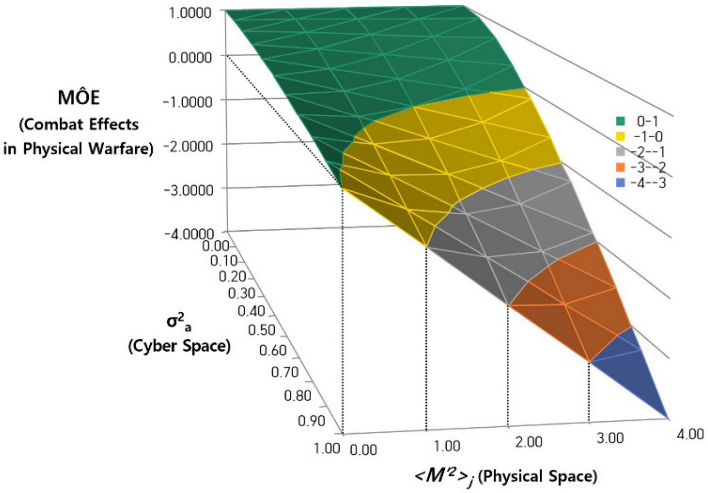


Figure 8. MOE effect reduction.

The values assigned to the simulator are shown in Table 3. The first unit is based on a common, unspecified size of a mechanised infantry battalion, giving a total of 297 units with 270 men (1 squad of 10 men × 3 squads × 3 platoons × 3 companies) and 27 armoured vehicles (1 squad of 1 vehicle × 27 squads). Differences in combat power between agents, determined by weapon scores in the M&S, were not accounted for between experiments. The initial parameter of 0.1650 was applied, a value that could destroy all 297 units initially assigned at 25 min (t_a), the launch attack, which is the final phase of dynamic targeting. The parameters for the BDA assessment were adjusted in proportion to the rate at which the MOE decreases with increasing information error.

The simulation results show that as MOE, decreases, the number of units that can be destroyed within the operational time available (t_a) decreases, and the time required to complete the operation to destroy all target units increases, as shown in Fig. 9.

This situation causes a shift from a traditional mission to defeat the enemy at a complete level to an incomplete mission of deterrence, repulsion, and delay where the enemy is still present. In other words, if the commander focuses on defeating the target unit, the time to complete the mission will increase and the survivability of the weapon system cannot be guaranteed. Conversely, if the focus is on maintaining operational availability, the threshold for the target unit is lowered, causing a loss of power due to fighting more enemy forces at a defence point where friendly forces are concentrated. This means that it can create favourable conditions for the enemy, upsetting the balance between mission completion and the commander's requirements.

5. CONCLUSION

Since military operations are centred on physical warfare, it is essential to introduce a tabletop cyber operations training method that complements the current red teaming type. This study proposes a simulation procedure for cyber operations in

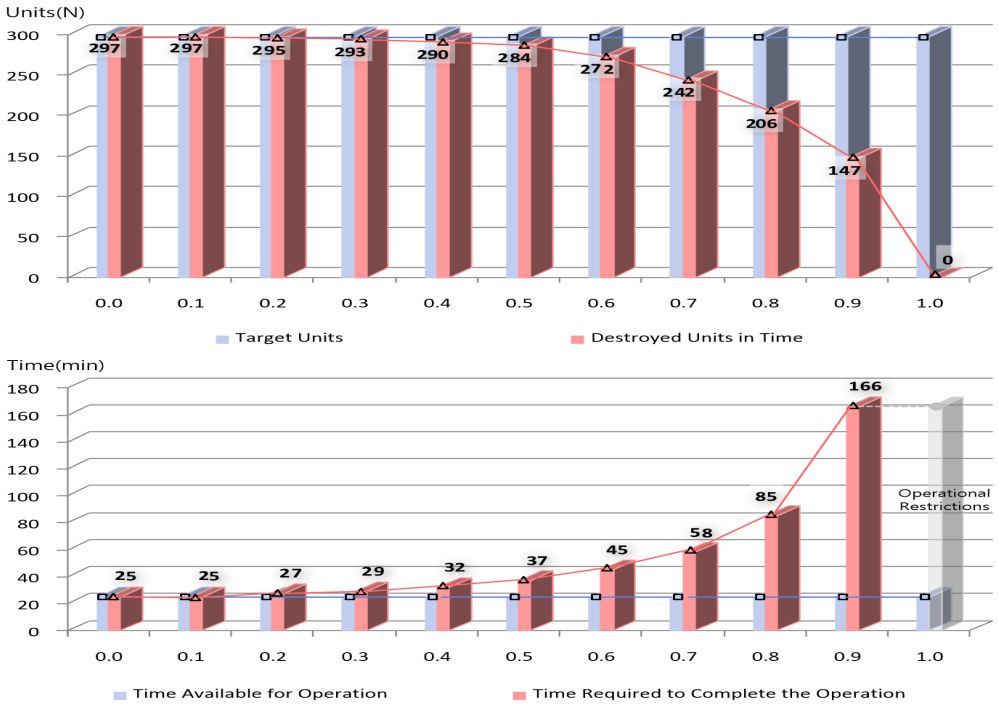


Figure 9. BDA evaluation results by simulator.

conjunction with physical warfare in the M&S, and a method for measuring effectiveness and assessing damage through it. In addition, to specify the logic of cyber operations simulation, detailed elements were determined and simulation feasibility was verified using a CCA engagement scenario. It is expected to raise awareness of the importance of cyber operations through the portrayal of situations between large-scale exercises that can simultaneously master the command procedures and the response procedures of units conducting cyber operations.

REFERENCES

1. Lee, S. & Kang, D. Designing simulation logic of UAV cyber operation using cyber security framework. *IEEE Access*, 2024, **12**, 3488-3498. doi:10.1109/access.2023.3349131.
2. Kang, D. & Lee, M. A study of cyber warfare war games in modern warfare. Research Institute for National Security Affairs, Research Report. 2020. (Korean).
3. U.S. Joint chiefs of staff. Joint publication 5-0 joint planning. pp. IV 27-28, December 2020.
4. U.S. Joint chiefs of staff. Joint publication 3-60 joint targeting. pp. Appendix D 1-10, January 2013.
5. U.S. Joint chiefs of staff. CJCSI 3162.02 Methodology for combat assessment. Instruction, pp. Enclosure B 1-10, March 2019.
6. Choi, S.; Kwon, O.; Oh, H. & Shin, D. Method for effectiveness assessment of electronic warfare systems in cyberspace. *MDPI Symmetry*, 2020, **12**(12). doi:10.3390/sym12122107.
7. Bodeau, D.J.; Graubart, R.D.; McQuaid, R.M. & Woodill, J. Cyber resiliency metrics, measures of effectiveness, and scoring: Enabling systems engineers and program managers to select the most useful assessment methods. MITRE Corp., Tech. Rep. No. 18-2579. September 2018. https://www.mitre.org/news-insights/publication/cyber-resiliency-metrics-measures-effectiveness-and-scoring
8. Kim, Duhoe; Kim, Doyeon; Shin, Dongil; Shin Dongkyoo & Kim, Y. Cyber battle damage assessment framework and detection of unauthorized wireless access point using machine learning. *In* Proceedings of the 6th Int. Conf. on Frontier Computing, Kuala Lumpur, Malaysia, July 3-6, 2018. doi:10.1007/978-981-13-3648-5_59.
9. Nesbit, R. & Thaer, L.V. Study on cyber defence management. Defence Science Board, September 2016.
10. Thiem, L.S. A study to determine damage assessment methods or models on air force networks. Air Force Institute of Technology, Wright Patterson AFB., OH, USA, 2005. (M.S. Thesis)
11. Fortson, L.W. Jr. Towards the development of a defensive cyber damage and mission impact methodology. Air Force Institute of Technology, Wright Patterson AFB.,OH, USA, 2005.(M.S. Thesis)
12. Ostler, R.T. Defensive cyber battle damage assessment through attack methodology modeling. Biblioscholar Publisher, 2012.
13. Kim, S.; Jang, J.; Kwon, O.; Kim, J. & Shin, D. Study on cyberattack damage assessment framework. *IEEE Acces*s, 2022, **10**, 59270-59276. doi:10.1109/access.2022.3179977
14. Neace, D.L. Measuring cyber operations effectiveness. Air Univ. Research Rep., November 2014.
15. Musman, S.; Temin, A.; Tanner, M.; Fox, D. & Pridemore, B. Evaluating the impact of cyberattacks on missions. MITRE Corp., Tech. Rep., 2010.
16. U.S. Army. Field manual 3-0 operations. pp. Ch. 2 1-3, October 2022.
17. Kang, D. Lee, S. & Yoon, J. A study of GPS jamming and cyber operation simulation logic for the army synthetic battlefield training system. Korea Nat. Defence Univ., Technical Report 2023MNS03-3. October 2023. (Korean).
18. Schutzer, D.M. Selected analytical concepts in command and control; C2 theory and measure of effectiveness, vol. 2. Gordon and Breach Science Publishers, NY, USA, 1982, pp. 119-144.
19. Alle, P. Situational force scoring: Accounting for combined arms effects in aggregate combat models. RAND Inst., Tech. Rep. No. N-3423-NA. 1992.
20. Park, N.A Study on an option to replace air force CAS by army attack helicopters. Kook-min Univ., Seoul, ROK, 2023. (M.S. Thesis). (Korean).
21. Kim, K. A study on integrating multidimensional information for effective preemptive surgical strike. Korea Univ., Seoul, ROK, 2019. (PhD Thesis). (Korean).
22. Noh, Y.; Shin, J. & Lee, J. A study on the organization of basic tactical forces in the future ground forces. Korea Institution of National Defence Development, Research Rep. No. KIND-2012-12. September 2012. (Korean).

CONTRIBUTORS

Mr Sangjun Lee is currently pursuing an MS degree in computer engineering with Korea National Defence Univ., Nonsan, Republic of Korea. He is a Cyber Specialised Officer in the Ministry of Defence. His current research interests include: Defence M&S, cyber warfare, and cyber security.
In the current study, he conceived the idea for applying the method to cyber operations and wrote the original draft manuscript.

Prof Dongsu Kang is currently Professor of Computer Science and Engineering and the Director of the Department of Defence Science, Korea National Defence University. His main area of expertise is software security testing, penetration testing and AI-based systems testing.
In the current study, he was responsible for validating the results of the analysis, editing and improving the manuscript.