SCIENTIFIC OASIS

Journal of Operational Intelligence

Journal homepage: www.jopi-journal.org
eISSN: 3009-4267

Analysis of the Stages of Military Cyber Operations using the COBRAC Method and p, q Quasirung Orthopair Fuzzy Decision Making Framework

Hakan Ayhan Dağıstanlı[1, *]

[1] Department of Industrial Engineering, Turkish Military Academy, National Defense University, Ankara, Turkiye

ARTICLE INFO

Article history:
Received 18 February 2025
Received in revised form 7 May 2025
Accepted 26 May 2025
Available online 1 June 2025

Keywords:
Military Operations; Cyber Operations; Cyber Attacks; Cyber Space; Cyber Security; MCDM; COBRAC; p, q Quasirung Orthopair Fuzzy Numbers.

ABSTRACT

This study aims to analyze the phased structure of military cyber operations and reveal the relative importance of each stage based on expert evaluations. The analysis, which covers seven fundamental phases—reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives—was conducted using the Comparisons between Ranked Criteria (COBRAC) method. The results demonstrate that operational success in military cyber activities is not solely determined by the direct impact on the target, but also by the preparatory processes that lead to such effects. The findings indicate that reconnaissance and weaponization are particularly critical in terms of strategic planning and technical capability development. The delivery and installation phases are also prominent, as they ensure the sustainability of the operation and persistence within the target system. In contrast, exploitation and C2 stages, while functionally important, appear to play a more flexible and instrumental role. The lowest score was assigned to the actions on objectives phase, suggesting that in military cyber operations, long-term access, intelligence gathering, and maintaining digital superiority are often prioritized over immediate destructive outcomes. To verify the reliability of the ranking results, a sensitivity analysis was performed using the p, q Quasirung Orthopair Fuzzy Decision-Making Framework, and the consistency of the outcomes was confirmed. Overall, the study offers a comprehensive perspective on the nature of military cyber operations and recommends that future research focus on modeling dynamic decision-making processes, conducting interdisciplinary analyses, and developing advanced decision support systems.

1. Introduction

Cyber operations can be defined as a set of digital actions that either target or are conducted through information technology infrastructures [1]. These operations are carried out not only by

* *Corresponding author.*
E-mail address: rdagistanli@kho.msu.edu.tr

https://doi.org/10.31181/jopi31202550

state actors but also by non-state entities and may serve various purposes such as data exfiltration, disabling systems, or sabotaging communication networks [2]. The growing strategic importance of cyberspace on a global scale has transformed these operations from merely technical activities into multidimensional tools with political, economic, and military implications [3–5]. Within this framework, cyber operations have become fundamental components of modern security paradigms.

Military cyber operations, as a specific subset of general cyber operations, are designed and executed to directly serve national security objectives [6]. These operations may aim to neutralize enemy command and control systems, disrupt military communications, interfere with satellite links, or disseminate false information for psychological effect [7]. Functioning in integration with other elements of military campaigns, such cyber activities can be carried out simultaneously with kinetic attacks, or independently as preventive or deterrent actions [8]. In this context, cyberspace is considered the fifth domain of warfare—alongside land, sea, air, and space—and is positioned as an indispensable dimension of military strategies.

The nature of military cyber operations demands a high level of technical expertise, rapid decision-making mechanisms, and the ability to adapt to an ever-changing threat environment. These operations are often conducted under principles such as stealth, non-attribution, and indirect impact, thereby transcending conventional norms of warfare and taking on the characteristics of hybrid threats [9]. Moreover, the ambiguity of boundaries between offense and defense in cyberspace raises ethical and legal concerns surrounding such operations [10]. Military cyber operations not only require technological capacity but also a strategic vision, as they constitute next-generation instruments of power projection by which states seek to gain superiority without direct conflict.

From a functional perspective, military cyber operations are broadly categorized into three main types: defensive cyber operations, cyber espionage activities, and offensive cyber operations [11]. Defensive cyber operations involve efforts to protect, monitor, analyze, detect, and respond effectively to unauthorized access attempts targeting a state's information systems and computer networks. These operations play a vital role in ensuring the continuity of military infrastructure and in safeguarding digital assets critical to national security. Cyber espionage operations refer to the use of computer networks for intelligence purposes to covertly gather confidential or strategic data from target or adversary systems—typically long-term and low-visibility in nature. Lastly, offensive cyber operations are designed to disrupt, deny, degrade, or destroy enemy systems or the information within them, and can potentially yield direct or indirect physical effects. These three types of operations collectively define the defensive and offensive dimensions of military cyber strategies, forming the core elements that shape state-level warfare capabilities in the digital age.

In this study, the phases of military cyber operations are examined in order of importance using a multi-criteria decision-making method known as Comparisons between Ranked Criteria (COBRAC). The phases were derived from existing literature and evaluated by subject-matter experts. The rest of the paper is organized as follows: Section 2 presents an extensive review of the literature. Section 3 introduces the COBRAC method and its application. Finally, Section 4 discusses the results and provides concluding remarks.

2. Related Literature

The evaluation of the effectiveness of cyber operations requires a multidimensional and dynamic decision-making environment; therefore, Multi-Criteria Decision-Making (MCDM) techniques are increasingly employed in this field. The literature demonstrates that various methods have been applied to help decision-makers assess operational alternatives in the face of

the complexity and uncertainty of cyber threats. Moreover, studies emphasize the preference for MCDM approaches integrated with fuzzy logic, particularly in situations characterized by high levels of uncertainty. In this context, MCDM techniques emerge not only as tools for technical analysis in the planning and execution of cyber operations, but also as decision-support mechanisms that enable the objective assessment of strategic priorities. A summary of selected studies from the literature is presented in Table 1.

Table 1
Literature Summary for Cyber Security using MCDM

Year	References	Solution
2020	[12]	Hesitant fuzzy sets MCDM
2021	[13]	PROMETHEE II
2023	[14]	Neutrosophic MCDM
2023	[15]	TOPSIS and Fuzzy MCDM
2023	[16]	AHP
2023	[17]	α-Discounting MCDM
2025	[18]	Fuzzy OffLogic and MCDM Approach

In addition to Table 1, Bholl [19] conducted a comprehensive study analyzing research in the field of cybersecurity that employed MCDM methods between 2010 and 2023. The findings of the study indicate that hybrid methods were the most frequently utilized approaches.

Beyond studies in the cybersecurity domain, the literature related to the COBRAC method has also been examined. Pamucar *et al.,* [20] introduced the method in their study for selecting the optimal Big Data platform. Biswas *et al.,* [21] further developed the method within a novel p,q-Quasirung Orthopair Fuzzy Set-based group decision-making framework in their research on technology adoption in the sugarcane supply chain.

3. Methodology and Application

3.1 COBRAC

The COBRAC (Comparisons Between Ranked Criteria) method is a technique used in MCDM to determine the weights of criteria based on their rank order of importance. The method consists of the following steps, the details of which have been explained in the study conducted by Pamucar *et al.,* [20].

Step 1: Determine and Rank the Criteria.

Decision-makers identify the relevant criteria for the problem and rank them in order of importance.

Step 2: Determine the Pairwise Rank Differences.

According to the ranking, the decision-maker assigns a score representing the difference in importance between each pair of adjacent criteria.

Step 3: Calculate the Total Differences.

Sum all the pairwise rank differences

Step 4: Calculate the Weights.

Weights are calculated starting from the least important criterion, which is assigned a base weight of 1. Each preceding criterion adds the corresponding rank difference.

Step 5: Normalize the Weights.

The weights are normalized so that their sum equals 1.

The COBRAC method is based on the decision-maker's qualitative judgment of the relative importance differences among criteria. It is intuitive, easy to implement, and useful in many MCDM applications.

3.2 Application

In the application phase of this study, the stages presented in Table 2 of the study by Brantly and Smeets [11] were utilized. These stages were evaluated by subject-matter experts.

Table 2
Stages of a cyber operation

No	Stage	Description
1	Reconnaissance	Research, identification, and selection of targets
2	Weaponization	Pairing remote access malware with exploit into a deliverable payload
3	Delivery	Transmission of weapon to target
4	Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
5	Installation	The weapon installs a backdoor on a target's system allowing persistent access
6	Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network
7	Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target.

3.2.1 Reconnaissance Phase

The reconnaissance phase, which is the first and most critical stage of military cyber operations, encompasses target identification and information-gathering activities that directly influence the success of the operation [22]. During this phase, the operator aims to collect detailed data on potential target systems, network infrastructures, defense mechanisms, and vulnerabilities within the cyber environment. Reconnaissance activities can be conducted through either passive or active methods. Passive reconnaissance is typically carried out using open-source intelligence (OSINT) to avoid leaving traces; this method involves analyzing social media, websites, IP records, and DNS information. In contrast, active reconnaissance engages directly with the target system through techniques such as port scanning, service enumeration, and network mapping to obtain deeper insights [23]. In a military context, reconnaissance extends beyond the collection of technical data to include the evaluation of operational factors such as the strategic significance of the target, the integrity level of the system, and the potential consequences of an attack. This information forms the foundation for determining which targets should be prioritized and what tactics should be employed in subsequent phases. Therefore, the reconnaissance phase not only lays the groundwork for operational planning but also enhances the precision of target engagement.

3.2.2 Weaponization Phase

The weaponization phase represents the preparatory stage for the implementation of military cyber operations, and it is a critical period where operators design operational tools and malware based on the information gathered during the reconnaissance phase [24]. In this phase, cyber weapons specifically tailored or configured to exploit the vulnerabilities of the target system are developed. These cyber weapons may consist of software components such as viruses, trojans, worms, rootkits, backdoors, or zero-day exploits. Additionally, a key objective of this phase is to customize these tools in a way that provides tactical advantages, such as ensuring confidentiality, stealth, persistence, and minimizing detection by the target system for as long as possible.

The weaponization process is not merely a technical software development activity; it also involves planning the effects that will serve the strategic purpose of the operation—such as system disruption, data corruption, or psychological deterrence—and enabling the functionality of the tools accordingly [23]. As emphasized in NATO doctrines, the weaponization phase is the stage in which the military cyber operation's "effect-generation" capacity is designed, and in this respect, it resembles the ammunition preparation processes of conventional weapon systems. Therefore, the activities conducted during this phase require multidimensional expertise, including not only technical proficiency but also the accurate interpretation of intelligence and the precise identification of tactical objectives.

3.2.3 Delivery Phase

The delivery phase symbolizes the transition to the implementation stage of military cyber operations and marks the critical moment when the operational process officially begins. In this phase, the malware or exploit developed during the weaponization phase is deployed to reach the target system [25]. The delivery methods are determined based on the target's security architecture, system vulnerabilities, and user behaviors. These methods may include phishing emails, fake software updates, physical media such as USB drives, malicious links, web exploitation (drive-by download), or more complex attacks such as "supply chain" attacks.

The delivery process is not only a technical transfer action but also a tactical transition step that ensures the operation is initiated securely and without detection. In the military operational context, the choice of delivery method typically varies depending on the nature of the operation, the strategic importance of the target, and the desired level of impact. For instance, an operation targeting high-value military assets may require a sophisticated delivery scenario involving social engineering elements, while operations against lower-tier targets may adopt a strategy that spreads via automated systems. Furthermore, the success of the delivery directly impacts the persistence and control capacity in subsequent phases of the operation; thus, timing, environmental conditions of the target system, and the principle of low detectability are critical factors. Consequently, the delivery phase is not merely a transmission step but is considered a pivotal point that shapes the overall success of the operation.

3.2.4 Exploitation Phase

The exploitation phase is a critical stage where the malware or exploit delivered to the target system during the delivery process triggers a vulnerability, enabling the execution of malicious code [26]. This phase marks the point at which the operation becomes technically effective and control over the target system is first established. In the context of military cyber operations, exploitation is not merely a technical exploit but also a threshold that lays the groundwork for the initiation of strategic impacts. At this stage, the operator uses vulnerabilities in the target system (such as software flaws, misconfigurations, or human errors) to bypass security mechanisms and trigger the core components of the attack.

Exploitation activities are typically carried out through "zero-day" vulnerabilities or known but unpatched flaws. Once this phase is successfully completed, the operator may gain privileged access to the system and seek ways to remain within the system without disrupting its normal operation. Furthermore, the exploitation phase may vary depending on the type of target; for instance, in an attack on a command-and-control (C2) system, the goal may be to seize instant access and communication, while in an operation against critical infrastructure, long-term sabotage strategies may be implemented [27].

In this context, the exploitation phase is not only a technical transition but also a strategic phase where the "internal defenses" of the target system are breached, and the operation evolves into a controllable structure. This phase is also critical from an ethical and legal perspective, as it directly interferes with the integrity of the enemy system and may produce results approaching thresholds for "use of force" under international law.

3.2.5 Installation Phase

The installation phase occurs after the successful execution of malicious code during the exploitation phase, where the operator embeds malicious components into the target system's infrastructure to ensure persistence [28]. The primary objective of this phase is to establish long-term control over the target system, secure future access, and create a platform for further advanced operations if necessary [29]. Common techniques used during the installation process include the deployment of rootkits, backdoors, scheduled tasks, or malicious components disguised as system services.

In the context of military cyber operations, the installation phase is a strategic step that ensures the sustainability of the operation. It functions as a "launching pad" for long-term intelligence gathering, continuous system manipulation, or actions that may later create physical effects. During this phase, maintaining persistence while avoiding detection is crucial; therefore, attackers use advanced concealment techniques, such as bypassing antivirus software, deleting event logs, and mimicking system behavior.

The installation phase is also the "operational basing" stage of a cyber operation; in other words, it establishes the necessary digital infrastructure to remain undetected and unimpeded within the enemy system. As such, the installation phase plays a decisive role in the effectiveness and depth of military cyber operations, making it not only a technical but also a strategic and logistical step.

3.2.6 Command and Control - C2 Phase

The Command and Control (C2) phase is where the attacker establishes sustainable access to the target system and dynamically manages the operation [30]. During this phase, the deployed malware communicates with the attacker's infrastructure in the external world, enabling the attacker to issue commands, extract data from the system, or send additional payloads [31]. The C2 infrastructure allows for the remote management of cyber operations, facilitating flexible and continuous control over the target system.

While traditional C2 structures are based on the "client-server" model, communicating with a central server, more advanced methods have been used in recent years to make detection more difficult. These methods include "peer-to-peer" networks, DNS tunneling, HTTPS obfuscation, social media-based C2, and the abuse of cloud services. In the context of military cyber operations, the C2 phase provides not only a technical command mechanism but also the tactical flexibility needed to achieve operational objectives and the ability to update the operation continuously.

This phase also represents the dynamic management layer of a cyber operation; the attacker not only gains access but also makes decisions based on developments within the target system, such as adjusting data collection routines or deploying new attack vectors. Therefore, the security, confidentiality, and continuity of the C2 infrastructure are critical to the success of the operation. In military operations, such infrastructures are typically designed to be multi-layered, geographically dispersed, and difficult to detect. As a result, the C2 phase lies at the intersection of both technical architecture and strategic planning.

3.2.7 Actions on Objectives Phase

The Impact on the Target phase is the final stage of military cyber operations, where the most direct and significant effects are executed [27]. In this phase, the attacker applies specific actions to the system to achieve the strategic or tactical objectives identified at the beginning of the operation [28]. These actions may include stealing data (cyber espionage), disrupting system functionality (denial of service), corrupting or deleting data (sabotage), altering system behavior (deception and redirection), or creating physical effects on critical infrastructure components (such as attacks targeting SCADA systems).

In the military context, this phase aims not only at technical outcomes but also at generating political, economic, and psychological effects. For example, the disabling of a command-and-control center with cyber tools may not only damage the information infrastructure but also directly impair combat capabilities. Similarly, disrupting military communication systems could weaken decision-making processes or lead to misdirection. Therefore, this phase represents a critical period where the physical world consequences of an operation initiated in cyberspace become apparent and may potentially lead to "kinetic effects."

The activities carried out in this phase typically also involve elements such as avoiding traceability, making detection difficult, and eliminating traces after the operation. Additionally, after the operation is completed, monitoring the target system, analyzing the acquired data, and learning for future similar operations are also considered part of this phase. In short, the Impact on the Target phase represents the critical point that solidifies the strategic success of a military cyber operation and reveals its final effects.

The linguistic evaluations made by five different experts regarding these phases are shared in Table 3, with corresponding scores and totals provided in Table 4. Figure 1 displays the final evaluations, while Figure 2 shows the sensitivity analysis results for changes at the p level when q=2.

Table 3
Linguistic Assessments

No	Stage	DM1	DM2	DM3	DM4	DM5
1	Reconnaissance	EH	VH	EH	EH	EH
2	Weaponization	EH	EH	EH	H	EH
3	Delivery	EH	VH	EH	H	VH
4	Exploitation	VH	VH	VH	VH	H
5	Installation	EH	H	EH	MH	VH
6	Command & Control	MH	H	VH	MH	H
7	Actions on Objective	M	H	VH	M	MH

Table 4
Score Matrix

No	Stage	DM1	DM2	DM3	DM4	DM5	Sum
1	Reconnaissance	9	7	9	9	9	8.6
2	Weaponization	9	9	9	8	9	8.8
3	Delivery	9	7	9	8	7	8
4	Exploitation	7	7	7	7	8	7.2
5	Installation	9	8	9	6	7	7.8
6	Command & Control	6	8	7	6	8	7
7	Actions on Objective	5	8	7	5	6	6.2

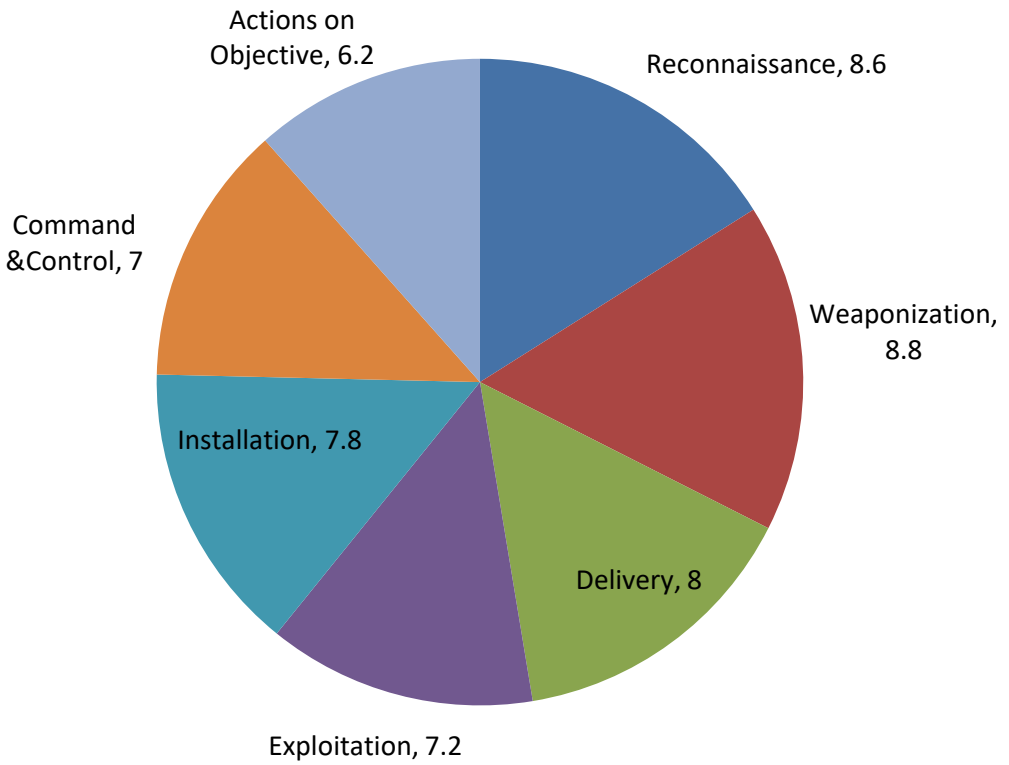

Fig. 1. Evaluation of military cyber operations stage

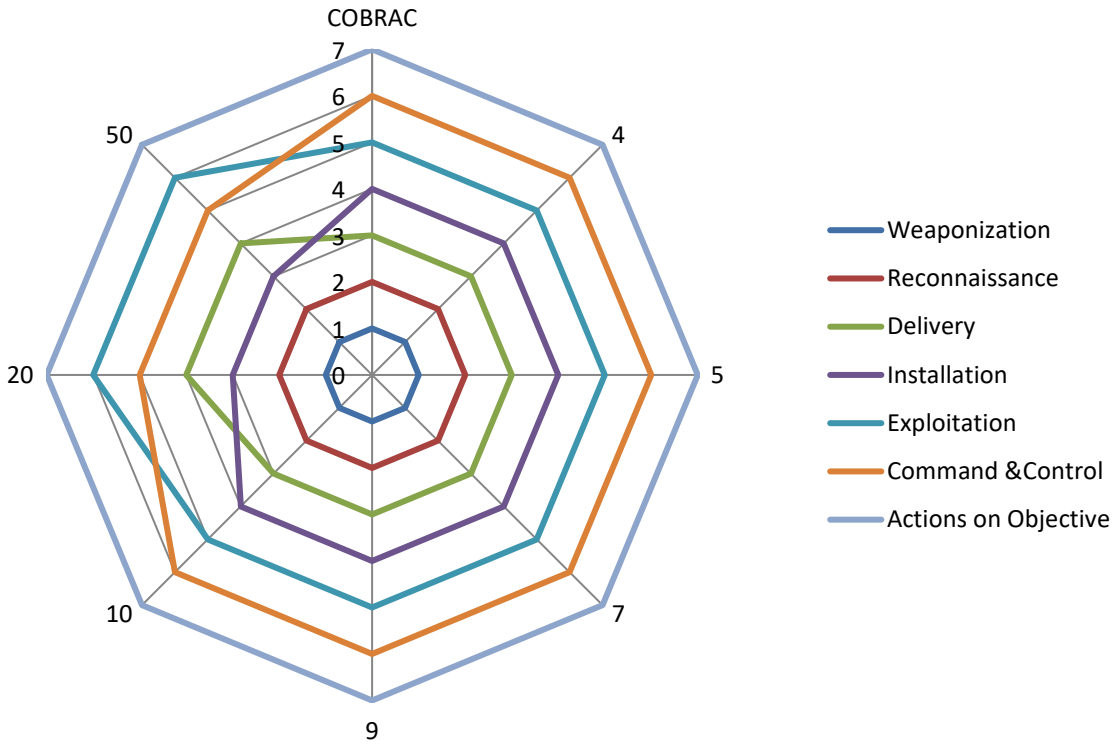

Fig. 2. Outcome of the sensitivity analysis

4. Conclusions

The evaluation presented demonstrates the relative importance of different stages of military cyber operations through numerical scores, and the analysis conducted based on these scores highlights that the nature of cyber operations relies not only on producing effects on the target but also on the comprehensive preparatory processes necessary to achieve these effects. The highest-rated phases, weaponization and reconnaissance, clearly indicate that the most critical aspects of the operation are based on strategic planning, target identification, and the development of technical tools. The fact that these two phases collectively account for roughly a quarter of the operation emphasizes that the success of the operation is often determined in its initial steps, where success or failure is decided. In particular, the type of malware used in the weaponization process, advanced persistence techniques, and the level of stealth directly impact the security and success of subsequent steps, while the reconnaissance process lays the intelligence foundation for the entire operation by collecting operational information, ranging from target selection to the analysis of architectural vulnerabilities.

The high ratings for the delivery and installation phases further highlight the criticality of the points at which the operation first makes contact with the system and establishes persistence. The tunneling techniques used during these processes, the camouflage of the payloads, and the installation techniques ensuring persistence on the target system all contribute to making the operation technically sustainable. In contrast, the exploitation and command-and-control (C2) phases received more moderate ratings. This suggests that while these phases are necessary for the operation, they play a more instrumental role in terms of strategic significance. In particular, the fact that command-and-control mechanisms can be designed in various ways indicates that this step is assessed as more flexible in terms of operational priorities. However, as the detection of command-and-control infrastructures could jeopardize the entire operation, it is clear that this phase must also be carefully managed from a technical standpoint.

The phase with the lowest score, actions on objectives, typically represents the visible result of cyber operations, but the rating suggests that its strategic importance may be more limited. This implies that, particularly in the military context, objectives such as intelligence gathering, establishing permanent access to systems, and building infrastructure for future operations are considered more prioritized than direct destructive effects. Therefore, the goal of cyber operations is not only to harm enemy systems but also to secure long-term access and control, and even to gain a continuous advantage in the digital domain. This holistic assessment academically underscores that military cyber operations are multilayered structures based not only on outcomes but also on processes, continuity, and high levels of technical precision.

This study has demonstrated that the success of military cyber operations is not solely dependent on the final effects on the target, but rather on the preparatory processes that make those effects possible. The prominence of the reconnaissance and weaponization phases underscores the fact that operational success largely depends on strategic planning and the development of technical tools. Future research should focus on the detailed modeling of these critical phases, the integration of dynamic decision-making processes into operational stages, and the evaluation of factors influencing the success of cyber operations through broader expert input. Moreover, considering not only the technical but also the political, ethical, and legal dimensions of cyber operations through interdisciplinary analyses will enhance academic depth and offer more comprehensive strategic insights for military decision-makers. In this context, the development of decision-support systems aimed at increasing the flexibility and effectiveness of military cyber operations in the face of an evolving threat landscape should be regarded as a key area of future research.

Funding
This research received no external funding.

Conflicts of Interest
The authors declare no conflicts of interest.

Data Availability Statement
The datasets generated during and/or analyzed during the current study is available from the corresponding author on reasonable request.

Acknowledgement
This research was not funded by any grant.

References
[1] O'Leary, M., O'Leary, M., & McDermott, C. (2019). Cyber operations. Apress. https://doi.org/10.1007/978-1-4842-4294-0
[2] Baştan, Y., & Oran, F. Ç. (2024). Rus Dış Politikasında Siber Müdahale Yöntemi Olarak Dezenformasyon Operasyonları. Yönetim Bilimleri Dergisi, 22(53), 1205–1230. https://doi.org/10.35408/comuybd.1457165
[3] Jensen, B., Valeriano, B., & Maness, R. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. Journal of Strategic Studies, 42(5), 58–80. https://doi.org/10.1080/01402390.2018.1559152
[4] Willett, M. (2022). The Cyber Dimension of the Russia-Ukraine War. Survival, 64(5), 7–26. https://doi.org/10.1080/00396338.2022.2126193
[5] Zhao, B., et al. (2023). Manufacturing Conflict or Advocating Peace? A Study of Social Bots Agenda Building in the Twitter Discussion of the Russia-Ukraine War. Journal of Information Technology & Politics, 21(2), 176–194. https://doi.org/10.1080/19331681.2023.2189201
[6] Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implication. International Conference on Information Warfare and Security, XII. Reading: Academic Conferences International Limited.
[7] Schulze, M. (2020, May). Cyber in war: Assessing the strategic, tactical, and operational utility of military cyber operations. In 2020 12th International Conference on Cyber Conflict (CyCon) (Vol. 1300, pp. 183–197). IEEE. https://doi.org/10.23919/CyCon49761.2020.9131733
[8] Lin, H. (2022). Russian cyber operations in the invasion of Ukraine. The Cyber Defense Review, 7(4), 31–46.
[9] Wither, J. K. (2016). Making Sense of Hybrid Warfare. Connections, 15(2), 73–87. https://doi.org/10.11610/Connections.15.2.06
[10] Mačák, K. (2021). Unblurring the lines: Military cyber operations and international law. Journal of Cyber Policy, 6(3), 411–428. https://doi.org/10.1080/23738871.2021.2014919
[11] Brantly, A., & Smeets, M. (2020). Military operations in cyberspace. Handbook of military sciences, 1–16. https://doi.org/10.1007/978-3-030-02866-4_19-1
[12] Erdoğan, M., Karaşan, A., Kaya, İ., Budak, A., & Colak, M. (2020). A fuzzy based MCDM methodology for risk evaluation of cyber security technologies. In *Intelligent and Fuzzy Techniques in Big Data Analytics and Decision Making: Proceedings of the INFUS 2019 Conference, Istanbul, Turkey, July 23-25, 2019* (pp. 1042–1049). Springer International Publishing. https://doi.org/10.1007/978-3-030-23756-1_123
[13] Torbacki, W. (2021). A hybrid MCDM model combining DANP and PROMETHEE II methods for the assessment of cybersecurity in industry 4.0. Sustainability, 13(16), 8833. https://doi.org/10.3390/su13168833
[14] AbdelMouty, A. M., & Abdel-Monem, A. (2023). Neutrosophic MCDM methodology for assessment risks of cyber security in power management. Neutrosophic Systems with Applications, 3, 53–61. https://doi.org/10.61356/j.nswa.2023.18
[15] Alhakami, W. (2023). Computational study of security risk evaluation in energy management and control systems based on a fuzzy MCDM method. Processes, 11(5), 1366. https://doi.org/10.3390/pr11051366
[16] Bouramdane, A. A. (2023). Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. Journal of Cybersecurity and Privacy, 3(4), 662–705. https://doi.org/10.3390/jcp3040031
[17] Mohamed, R., & Ismail, M. M. (2023). Evaluation of Cyber Insecurities of the Cyber Physical System Supply Chains Using α-Discounting MCDM. Infinite Study. https://doi.org/10.61356/j.nswa.2023.98

[18] Yang, Z. (2025). Evaluation of Intrusion Detection Systems in Cyber Security using Fuzzy OffLogic and MCDM Approach. Neutrosophic Sets and Systems, 85, 343–360.
[19] Bhol, S. G. (2025). Applications of Multi Criteria Decision Making Methods in Cyber Security. Cyber-Physical Systems Security, 233–258. https://doi.org/10.1007/978-981-97-5734-3_11
[20] Pamucar, D., Simic, V., Görçün, Ö. F., & Küçükönder, H. (2024). Selection of the best Big Data platform using COBRAC-ARTASI methodology with adaptive standardized intervals. Expert Systems with Applications, 239, 122312. https://doi.org/10.1016/j.eswa.2023.122312
[21] Biswas, S., Pamucar, D., & Simic, V. (2024). Technology adaptation in sugarcane supply chain based on a novel p, q Quasirung Orthopair Fuzzy decision making framework. Scientific Reports, 14(1), 26486. https://doi.org/10.1038/s41598-024-75528-5
[22] Roy, S., Sharmin, N., Acosta, J. C., Kiekintveld, C., & Laszka, A. (2022). Survey and taxonomy of adversarial reconnaissance techniques. ACM Computing Surveys, 55(6), 1–38. https://doi.org/10.1145/3538704
[23] Yadav, T., & Rao, A. M. (2015, August). Technical aspects of cyber kill chain. In International Symposium on Security in Computing and Communication (pp. 438–452). Springer International Publishing. https://doi.org/10.1007/978-3-319-22915-7_40
[24] Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. Journal of Computer Virology and Hacking Techniques, 15, 277–305. https://doi.org/10.1007/s11416-019-00338-7
[25] Zhao, L. (2024). Navigating the Cyber Kill Chain: A modern approach to pentesting. Applied and Computational Engineering, 38, 170–175. https://doi.org/10.54254/2755-2721/38/20230549
[26] Allodi, L. (2017, October). Economic factors of vulnerability trade and exploitation. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1483–1499). https://doi.org/10.1145/3133956.3133960
[27] Kazimierczak, M., Habib, N., Chan, J. H., & Thanapattheerakul, T. (2024). Impact of AI on the Cyber Kill Chain: A Systematic Review. Heliyon. https://doi.org/10.1016/j.heliyon.2024.e40699
[28] Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K. K. R., & Javadi, H. H. (2019). Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures. Journal of Information Processing Systems, 15(4), 865–889.
[29] Matto, G. (2024). The Cyber Kill Chain Model and Its Applicability on The Protection of Students Academic Information Systems (SAIS) in Tanzanian HEIs. https://doi.org/10.51519/journalisi.v6i1.676
[30] Gardiner, J., Cova, M., & Nagaraja, S. (2014). Command & Control: Understanding, Denying and Detecting—A review of malware C2 techniques, detection and defences. arXiv preprint arXiv:1408.1136.
[31] Muller, L. P. (2024). Cybersecurity in practice: The vigilant logic of kill chains and threat construction. European Journal of International Security, 1–21. https://doi.org/10.1017/eis.2024.27