Kalamizu : Jurnal Sains, Sosial, dan Studi Agama
Volume 2 Number 8, Agustus (2026), 178-191

Cyber Warfare in Middle Eastern Cross-Border Conflicts: IHL Compliance, 2024–2026

Muhammad Shadiq Ahyar Noer[1], Satya Rizkiano Adha Pratama[2], Daffa Alnida[3], Ida Susilowati[4]

[1,2,3,4]University of Darussalam Gontor, Indonesia
Email Correspondence : idasusilowati@unida.gontor.ac.id

Kata Kunci :

Perang Siber; Konflik Lintas Batas; Timur Tengah; Hukum Humaniter Internasional; Keamanan Internasional

Abstrak

Perkembangan teknologi digital telah mengubah karakter konflik bersenjata kontemporer dengan menjadikan ruang siber sebagai salah satu arena persaingan dan operasi strategis. Konflik lintas batas di Timur Tengah selama 2024–2026 memperlihatkan meningkatnya penggunaan operasi siber yang berlangsung bersamaan dengan aktivitas militer, operasi informasi, dan persaingan geopolitik. Penelitian ini menganalisis perkembangan perang siber dalam konflik lintas batas di Timur Tengah serta mengevaluasi kepatuhan aktor terhadap prinsip distinction, proportionality, military necessity, dan precautions in attack. Penelitian menggunakan pendekatan kualitatif, studi kasus, dan analisis deskriptif-analitis berdasarkan literatur akademik, dokumen hukum internasional, laporan organisasi internasional, laporan keamanan siber, dan media kredibel. Hasil penelitian menunjukkan bahwa perang siber telah menjadi bagian dari konflik multidomain, khususnya dalam konflik Israel–Iran dan Israel–Gaza. Namun, evaluasi kepatuhan terhadap HHI dibatasi oleh persoalan atribusi, status target, infrastruktur dual-use, dampak terhadap penduduk sipil, dan keterbatasan bukti mengenai tujuan serta tindakan pencegahan pelaku. Prinsip-prinsip HHI tetap relevan, tetapi penerapannya harus dilakukan secara kasus per kasus berdasarkan bukti yang dapat diverifikasi.

Keywords :

Cyber Warfare; Cross-Border Conflict; Middle East; International Humanitarian Law; International Security

Abstract

Digital technology has transformed contemporary armed conflict by making cyberspace an arena of strategic competition and operations. Cross-border conflicts in the Middle East during 2024–2026 show growing cyber activity alongside military operations, information campaigns, and geopolitical rivalry. This study analyzes cyber warfare in these conflicts and evaluates compliance with the principles of distinction, proportionality, military necessity, and precautions in

attack. Using a qualitative case-study and descriptive-analytical approach, it draws on academic literature, international legal documents, international-organization reports, cybersecurity reports, and credible media coverage. The findings show that cyber operations have become part of multidomain conflict, especially in the Israel–Iran and Israel–Gaza contexts. Assessment of compliance with International Humanitarian Law remains difficult because of attribution problems, uncertain target status, dual-use infrastructure, civilian effects, and limited evidence about operational purpose and precautionary measures. IHL principles remain applicable, but compliance must be assessed case by case on verifiable evidence rather than by assuming that all cyber activity during conflict constitutes a legal violation.

INTRODUCTION

The development of information and communication technologies has fundamentally changed the character of contemporary armed conflict. Conflict that was once conducted primarily through conventional military force now extends into multiple domains, including cyberspace. Cyberspace enables states and non-state actors to interfere with communications, government networks, energy infrastructure, health services, and other strategically important systems. Digital technology therefore functions not merely as a social and administrative support tool, but also as an instrument for pursuing political and military objectives. In armed-conflict settings, the use of cyber capabilities raises the question of how such conduct should be assessed under International Humanitarian Law (IHL) (Rid, 2012; Valeriano et al., 2018).

This question is particularly relevant to cross-border conflicts in the Middle East, a region characterized by persistent geopolitical tension involving states, armed groups, and external actors. Developments during 2024–2026 demonstrate that confrontation has not been limited to physical attacks. Cyber activities have been used to obtain information, disrupt communications, weaken an adversary's capabilities, and influence the course and perception of conflict. As a result, cyberspace has become increasingly difficult to separate from military operations and national security strategy.

Cyber warfare creates a specific legal problem because the boundary between military and civilian objects is often difficult to identify in digital environments. Contemporary digital infrastructure frequently has a dual-use character: the same communication network, data center, energy system, transport network, or other digital service may support both civilian life and military activity. A cyber operation directed at such infrastructure may therefore affect civilians even when the operation is intended to achieve a military objective. Disruption of health care, communications, energy, financial services, or public administration can increase civilian vulnerability

in conflict zones (Dinniss, 2012; Schmitt, 2017).

These concerns are closely related to the core principles of IHL. The principle of distinction requires parties to distinguish between combatants and civilians and between military objectives and civilian objects. Proportionality requires an assessment of whether expected incidental civilian harm would be excessive in relation to the concrete and direct military advantage anticipated. Military necessity requires a legitimate military purpose within the limits imposed by IHL, while precautions in attack require feasible measures to avoid or minimize civilian harm. The principle of humanity further emphasizes that military action must not generate unnecessary suffering (Additional Protocol I, 1977; Dinstein, 2022).

Applying these principles to cyber operations is nevertheless difficult. Cyber operations may be launched remotely, routed through third-party infrastructure, and designed to conceal the identity of the actor. Attribution is therefore a major challenge. Moreover, not every cyber operation produces immediate physical destruction. Operations may deny access to data, manipulate systems, interrupt services, or alter information without visibly damaging hardware, while still producing serious consequences for civilian life. These features have generated debate over when cyber conduct becomes an 'attack' for IHL purposes and how harm should be measured (Hathaway et al., 2012; International Committee of the Red Cross [ICRC], 2019).

The legal challenge is intensified by the pace of technological change. Existing IHL principles provide a framework for limiting conduct during armed conflict, but their application to specific cyber techniques remains contested. Questions about the status of digital targets, thresholds of harm, dual-use infrastructure, attribution, and responsibility have become central to contemporary debate. The central issue is therefore not whether cyberspace is outside the law, but how established legal norms apply to technologically different forms of coercion and disruption (Mačák, 2017).

Previous scholarship on cyber conflict and international law has generally developed in three directions. One group of studies examines the normative application of international law to cyber operations, including the concepts of attack, attribution, and IHL obligations. A second group emphasizes security and strategy, treating cyberspace as a domain of interstate competition involving offensive and defensive capability, intelligence, and critical-infrastructure protection. A third group focuses on Middle Eastern conflict, including Israel–Palestine, Israel–Iran, armed groups, and external involvement. A gap remains in systematically connecting cyber operations in the Middle East during 2024–2026 with case-specific evaluation under the principles of distinction, proportionality, military necessity, and precautions in attack (Buchanan, 2020; Smeets, 2022).

This study addresses that gap by analyzing cyber warfare in Middle Eastern cross-border conflicts during 2024–2026 with IHL as the principal evaluative framework. It identifies actors, targets, purposes, methods, and impacts before assessing each case against the four core principles. The study does not assume in advance that every cyber operation constitutes an IHL violation. Instead, it

distinguishes between confirmed facts, actor claims, technical attribution, and political attribution, and it limits legal conclusions where public evidence is insufficient.

CONCEPTUAL FRAMEWORK

Cyber warfare is understood in this study as the use of cyber capabilities in the context of strategic competition or armed conflict to obtain information, disrupt systems, weaken an adversary, or support broader military and political objectives. The concept must be distinguished from related categories. Cyber espionage primarily concerns covert information acquisition; cyber attack refers more narrowly to conduct that disrupts, damages, or affects systems and data; and cyber operation is a broader term covering actions conducted through or against computer systems. These distinctions matter because not every cyber activity is automatically an act of war or an attack within the meaning of IHL (Kello, 2017).

Cross-border conflict refers to conflict in which actions, actors, or consequences extend beyond the territorial boundaries of a single state. Cyberspace expands this cross-border character because an operation may be conducted from one state, routed through servers in another, and directed at systems located elsewhere. Geography therefore becomes less decisive for identifying the operational location, while questions of jurisdiction, attribution, and legal responsibility become more complicated (Tsagourias, 2012; Maurer, 2018).

IHL is used as the normative framework for evaluating cyber conduct that is sufficiently connected to armed conflict. The framework focuses on whether the target is a lawful military objective, whether expected civilian harm is excessive, whether the operation serves a legitimate military purpose, and whether feasible precautions have been taken. This framework is especially important for digital infrastructure that combines civilian and military functions (Geneva Convention IV, 1949; ICRC, 2019).

METHODS

This research uses a qualitative case-study approach. It is designed to understand cyber warfare in Middle Eastern cross-border conflict and to evaluate documented conduct against IHL norms rather than to perform statistical measurement. Each case is examined in its conflict context by identifying the actor, target, purpose, method, and consequences of the operation and then comparing those characteristics with the principles of distinction, proportionality, military necessity, and precautions in attack.

The study is descriptive-analytical. The descriptive component maps the development and characteristics of cyber warfare during 2024–2026, including the actors involved, forms of operation, targets, strategic purposes, and documented impacts. The analytical component evaluates those facts under IHL. An operation is not classified as an IHL violation merely because it has been reported or attributed in media coverage; where the actor, purpose, or effects cannot be confirmed, the analysis records the evidentiary limitation and avoids categorical legal conclusions.

The object of research is cyber warfare or cyber operations connected with cross-border conflict in the Middle East during 2024–2026, especially operations linked to the Israel–Iran and Israel–Gaza contexts. Cases are selected when they have a plausible connection with armed conflict or cross-border tension and have an actual or potential effect on military interests, civilian infrastructure, or civilian populations.

The study relies on secondary data gathered through literature review and documentation. Sources include academic studies of cyber warfare, IHL, armed conflict, cybersecurity, and Middle Eastern geopolitics; the 1949 Geneva Conventions and relevant Additional Protocols; United Nations and International Committee of the Red Cross materials; cybersecurity and research-institute reports; and credible national and international media. Media reports are used mainly to identify chronology and incidents and are cross-checked where they concern attribution, casualty or loss estimates, operational purpose, or alleged legal violations.

Data analysis proceeds through identification, classification, and normative evaluation. First, relevant cyber incidents are identified and documented by time, affected area, alleged actor, target, type of operation, purpose, impact, and source. Second, targets are classified as military objectives, civilian objects, dual-use infrastructure, government systems, critical infrastructure, or other relevant categories, with attention to civilian consequences. Third, each case is evaluated under the four IHL indicators. Findings are categorized as indicating compliance, insufficient evidence to determine compliance or violation, or indicating possible non-compliance. This three-part outcome is intended to prevent overstatement where cyber attribution and operational evidence remain uncertain.

Source triangulation is used to strengthen validity. Information about an incident is compared across government documents, international organizations, cybersecurity reports, academic publications, and credible media where possible. The study distinguishes verified facts from claims by conflict parties and from unconfirmed attribution. Its principal limitations are dependence on publicly available information, the secrecy of many cyber operations, uncertainty about technical and legal attribution, and the fact that the analysis does not seek to establish definitive criminal or state responsibility.

RESULT AND DISCUSSION

Dynamics of Cyber Warfare in Middle Eastern Conflicts, 2024–2026

Developments during 2024–2026 show that cyberspace has become increasingly integrated into geopolitical confrontation and military operations in the Middle East. Cyber activity has not been limited to destructive attacks on infrastructure. It has also included data theft, disruption of digital services, influence operations, disinformation, website defacement, distributed denial-of-service (DDoS)

activity, and efforts to obtain strategic advantage. The pattern is therefore better understood as part of hybrid or multidomain conflict in which diplomatic, military, intelligence, informational, and cyber instruments operate simultaneously (Nye, 2017; Valeriano et al., 2018).

The Israel–Iran confrontation illustrates this integration. Microsoft Threat Analysis Center reporting cited in the source manuscript observed that after the October 2023 Hamas attack on Israel, actors affiliated with the Iranian government increased cyber and influence activity intended to support Hamas-related objectives and weaken Israel and its supporters. The same reporting also noted that some early claims of attacks could not be verified or lacked a clear operational connection to the conflict. This distinction is important because the existence of cyber claims during a conflict does not establish their technical authenticity, strategic effect, or legal attribution (Microsoft Threat Analysis Center, 2024).

Activity intensified again during the direct Israel–Iran escalation in 2024. The source manuscript cites S2W analysis from April 2024 describing increased activity by threat actors mentioning or targeting Israel and Iran, with government sectors among the prominent targets. In the Israeli context, reports included attempted sale of access to government servers and documents allegedly originating from the Ministry of Defense, while Iranian government institutions were also targeted. Such observations must remain separate from claims of state responsibility, because technical activity against a government system does not by itself prove that another state ordered, directed, or legally controlled the operation.

The cyber dimension became more visible during the open Israel–Iran conflict in June 2025. The source manuscript refers to Middle East Institute and Atlantic Council analyses that characterized cyber activity during the twelve-day conflict as involving information-space manipulation, domestic narrative management, external influence, attacks on financial institutions, hacktivism, and data-related operations. Yet these analyses also suggested that the operational effects of most cyber activity were limited compared with the consequences of kinetic strikes. This finding does not make cyber operations strategically irrelevant; rather, it indicates that cyber effectiveness may lie in disruption, intelligence, narrative control, or pressure rather than large-scale physical destruction.

Non-state actors and hacktivists further complicate the landscape. Research discussed in the source manuscript on the Israel–Gaza conflict found an increase in web defacement and DDoS attacks after the outbreak of war, followed by a decline in intensity. Much of this activity was politically motivated and conducted by actors supporting one side rather than by identifiable state military forces. The resulting environment blurs the boundaries among state cyber operations, state-affiliated groups, hacktivism, criminal conduct, and influence activity and thereby complicates IHL classification and attribution.

Case Studies

Israel–Iran Cyber Activity in 2024

The 2024 Israel–Iran escalation demonstrates how geopolitical confrontation can generate cyber activity in parallel with military tension. Government systems and state-linked institutions reportedly became targets. From an IHL perspective, however, a government-owned digital system is not automatically a military objective. Its legal status depends on its nature, location, purpose, or use and on whether it makes an effective contribution to military action such that its neutralization would offer a definite military advantage under the applicable legal standard (Schmitt, 2017).

The case also highlights attribution problems. A group's claim of responsibility does not automatically establish that the group conducted the operation, and proof that a group acted does not automatically establish state responsibility. Attackers may route operations through third-party infrastructure, use compromised systems, or make false claims. The source manuscript therefore treats 2024 as evidence of increasing strategic use of cyberspace and of the difficulty of reaching reliable conclusions about responsibility from public reporting alone (Tsagourias, 2012).

Israel–Iran Cyber Warfare in June 2025

The June 2025 Israel–Iran conflict provides a clearer context for examining cyber operations alongside active hostilities. Reports cited in the manuscript describe activity against financial institutions, attempted data theft, hacktivism, and information operations. They also show a gap between claimed attacks and independently verified impact. Reuters reporting referenced in the manuscript noted claims by groups linked to Iran regarding compromised systems and stolen data, while some claims lacked sufficient supporting evidence. Other reports described cyber activity affecting Iranian financial systems.

For analytical purposes, the case requires a separation of three questions: what was claimed, what technical evidence demonstrates, and what political or legal attribution can be sustained. These are not equivalent categories. The case also illustrates how cyber operations may support kinetic conflict without producing the same form of physical damage, thereby reinforcing the multidomain character of contemporary hostilities.

Cyber Activity in the Israel–Gaza Conflict

The Israel–Gaza conflict likewise produced increased cyber activity by a range of actors, including web defacement and DDoS attacks. The source manuscript notes that much of this activity was associated with non-state actors and hacktivists and that the increase was comparatively short-lived. Such operations vary in effect: a temporary website disruption may have very different humanitarian and legal implications from an operation that disables a service essential to civilian survival.

The Gaza case also demonstrates the vulnerability of civilian digital infrastructure. The source manuscript cites 2024 OCHA reporting that damage to

infrastructure, fuel and spare-parts shortages, and conflict conditions contributed to network disruptions and impeded repair of mobile and internet services. Importantly, these communication failures cannot automatically be attributed to cyber attack, because physical destruction, energy shortages, and operational constraints may produce similar effects. The case is therefore used as evidence of civilian dependency on communications infrastructure rather than as proof of a specific cyber attack.

Evaluation of Compliance with International Humanitarian Law

Distinction

Distinction is a central difficulty in cyber warfare because digital systems associated with a state may still be civilian objects. Government networks, communications systems, data centers, and financial infrastructure may serve civilian, administrative, and military functions at the same time. The Israel–Iran cases show reported activity against government and financial sectors, but ownership by a government or strategic importance alone does not automatically make a system a lawful military objective (Additional Protocol I, 1977; Schmitt, 2017).

The decisive question is whether the object effectively contributes to military action and whether its destruction, capture, or neutralization offers a definite military advantage in the circumstances ruling at the time. Where an infrastructure is dual-use, the attacker must assess the relevant military function without ignoring the system's civilian role. Publicly available reporting in the cases examined often does not disclose enough information about the actual function of the target to determine compliance conclusively.

Proportionality

Proportionality remains relevant even where a cyber operation causes little or no immediate physical destruction. Networked systems can generate cascading effects: disruption of one digital service may affect health care, electricity, communications, banking, public administration, or humanitarian coordination. The legal assessment therefore cannot be reduced to visible hardware damage; it must consider reasonably foreseeable consequences for civilians and civilian objects (Dinniss, 2012; ICRC, 2019).

The source manuscript notes that cyber effects during the 2025 Israel–Iran conflict were generally more limited than kinetic effects. This does not eliminate proportionality concerns. A temporary financial or communications outage may still impose substantial social costs depending on its scale, duration, and civilian dependency. Because available evidence rarely reveals the anticipated military advantage or the attacker's pre-operation assessment, proportionality conclusions must remain case-specific and often provisional.

Military Necessity

Military necessity requires a legitimate military purpose and does not permit

every technically possible cyber action. The Israel–Iran cases show cyber activity serving different purposes, including intelligence collection, system disruption, narrative management, and political influence. These purposes are not legally interchangeable. An operation intended to achieve a concrete military effect must be distinguished from propaganda, espionage, political signaling, or hacktivism that may occur during conflict without constituting the same type of IHL-governed attack.

The closer the relationship between the targeted system and an identifiable military objective, the stronger the basis for analyzing the operation through military necessity. Conversely, where the target's military relevance is unclear, the mere availability of technical access is not enough to justify treating the system as a lawful target.

Precautions in Attack

Cyber operations require particular attention to precautions because digital systems are highly interconnected. Feasible precautions may include accurate target identification, assessment of dependencies, limiting the code or access path to the intended system, testing for unintended propagation, selecting techniques that reduce civilian disruption, and suspending an operation if the expected civilian effects become excessive or the target cannot be verified.

The Gaza communication case illustrates why such precautions matter even though the documented communication failures cannot automatically be characterized as cyber attacks. Civilian and humanitarian actors depend on communication infrastructure for information, coordination, emergency response, and aid delivery. Any cyber operation capable of impairing such services must therefore account for these civilian functions and the risk of cascading consequences.

Table 1. Compliance Evaluation Matrix

Case	Distinction	Proportionality	Military Necessity	Precautions	Overall Evaluation
Israel–Iran cyber activity, 2024	Status of several targets remains insufficiently verified	Documented effects vary	Connection to armed conflict is not always certain	Public information is limited	Compliance cannot be determined comprehensively

Case	Distinction	Proportionality	Military Necessity	Precautions	Overall Evaluation
Israel–Iran war, 2025	Some targets were strategic institutions, but attribution and function require verification	Cyber effects were relatively limited compared with kinetic strikes	Some activity had strategic purposes, but not all can be classified as military action	Public evidence is limited	Insufficient basis to classify all activity as a violation
Israel–Gaza cyber activity	Many activities involved non-state actors and hacktivists; target status varied	DDoS and defacement produced different levels of impact	Relationship to military objectives was often unclear	Information on precautions is very limited	Compliance is difficult to determine without fuller attribution and context

Challenges in Enforcing IHL in Cyber Warfare

Attribution is one of the most significant barriers to IHL enforcement in cyberspace. In conventional hostilities, the identity of the attacking force can often be inferred from troops, weapons, territory, and observable operations. Cyber operations may instead be routed through third-party networks, compromised devices, proxy infrastructure, or deliberately deceptive technical indicators. Consequently, the technical operator, the group claiming responsibility, and the state that might bear legal responsibility may be different entities (Hathaway et al., 2012; Tsagourias, 2012).

A second challenge is the legal status of the operation itself. DDoS, data theft, espionage, system manipulation, destructive malware, and influence operations generate different consequences and cannot automatically be placed within a single legal category. Some activities may fall below the threshold of an IHL 'attack' even when they are strategically significant. The legal analysis must therefore begin with the characteristics and effects of the specific operation rather than with the label 'cyber warfare.'

Dual-use infrastructure is a third challenge. Communications networks, data centers, energy systems, and digital platforms commonly serve civilian and military users simultaneously. This makes the principles of distinction and proportionality especially difficult to apply. A target may contribute to military action but also support hospitals, emergency services, banking, public administration, and ordinary civilian communication. Accurate functional assessment is therefore essential.

The digital environment also complicates proof and documentation. Operational evidence may be deleted, encrypted, hidden, altered, classified, or held by private companies. Public reporting may depend on claims by conflict parties or commercial cybersecurity firms with different levels of access. These evidentiary limitations reduce the ability of researchers and legal institutions to verify intent, target selection, expected effects, and precautionary measures.

Fragmentation of actors further complicates responsibility. State agencies, armed groups, patriotic hackers, criminal organizations, contractors, and loosely organized hacktivist communities may participate in the same conflict ecosystem. Establishing the legal status of the actor, the degree of state direction or control, and the connection between an operation and ongoing hostilities can therefore be difficult.

Finally, cyber operations are inherently transnational. Infrastructure in several jurisdictions may be involved in a single operation, while relevant evidence may be controlled by foreign states or private entities. The enforcement problem is thus not simply a lack of legal norms; it also concerns interpretation, evidence, attribution, jurisdiction, cooperation, and the practical ability to apply existing law to technically complex operations.

Implications for International Relations

Cyber warfare expands the concept of international security from physical territory into digital infrastructure and information systems. The Israel–Iran cases demonstrate that cyber operations can accompany conventional force and strategic signaling. States may use cyber capabilities to impose costs, collect intelligence, disrupt systems, and influence perceptions without necessarily crossing the same visible thresholds associated with kinetic attack. This creates additional uncertainty in crisis management and deterrence (Lindsay, 2013; Nye, 2017).

Cyber capability is also becoming part of national power. States with advanced technical capacity can project influence despite disparities in conventional military strength, while less capable states may rely on proxies, affiliated groups, or asymmetric techniques. In the Middle East, this can alter calculations of vulnerability and resilience and can encourage investment in offensive and defensive cyber capacity (Buchanan, 2020; Smeets, 2022).

The growing integration of cyber, military, intelligence, and information activities produces increasingly multidomain conflict. One incident may combine physical strikes, information operations, network intrusion, propaganda, economic pressure, and diplomatic messaging. This convergence makes it harder to determine when a discrete cyber operation should be analyzed as part of hostilities and when it remains within espionage, criminality, or political influence.

For civilian protection, the key implication is that digital infrastructure has become part of human security. Communications, health services, energy, banking, public administration, and humanitarian coordination increasingly depend on digital systems. Civilian harm may therefore arise not only from destroyed buildings but also

from loss of access to services. This expands the practical importance of protecting civilian digital infrastructure under IHL (Geneva Convention IV, 1949; ICRC, 2019).

Cyber attribution has also become a diplomatic issue. Governments may publicly attribute operations to signal resolve, justify sanctions, build coalitions, or shape international narratives. Yet incorrect or premature attribution can itself increase escalation risk. The evidentiary uncertainty identified in the cases studied therefore has consequences not only for legal responsibility but also for interstate stability and crisis communication.

The source manuscript consequently emphasizes the importance of international cooperation. Information sharing, confidence-building measures, incident documentation, technical investigation, and mechanisms for reducing misperception can improve both accountability and stability. The future of cyber governance will depend not only on creating new rules but also on clarifying how existing principles apply and developing the institutional capacity to verify and enforce them (United Nations General Assembly [UNGA], 2015; UNGA, 2021).

CONCLUSION

This study shows that cyber warfare became an important dimension of Middle Eastern cross-border conflict during 2024–2026. The Israel–Iran and Israel–Gaza contexts demonstrate that cyberspace is no longer merely a supporting environment but part of a broader conflict strategy involving intelligence collection, system disruption, influence operations, hacktivism, and activity against digital infrastructure. This development strengthens the connection among technology, military power, national security, and international politics.

The study finds that the core principles of IHL remain relevant to cyber operations, especially distinction, proportionality, military necessity, and precautions in attack. Their application, however, is more complex than in many conventional situations because digital infrastructure may be dual-use, target status may be uncertain, effects may cascade across interconnected systems, and public evidence may not reveal the attacker's purpose or precautionary process. Compliance must therefore be assessed case by case.

Attribution is a central obstacle to legal enforcement. Claims about state or group involvement are not always independently verifiable, and the technical operator, the group claiming responsibility, and the state that could bear legal responsibility may not be the same entity. Accordingly, political attribution should not automatically be treated as proof of legal responsibility.

The analysis also demonstrates that not all cyber activity occurring during conflict is automatically an IHL violation. Espionage, hacktivism, influence operations, data theft, DDoS, and destructive attacks differ in character and consequence. Legal evaluation must first determine the operation's connection to armed conflict, the status of its target, its purpose, its expected and actual effects on civilians, and the precautions taken. On the public evidence described in the source manuscript, there is

no adequate basis for concluding that all cyber operations in Middle Eastern conflicts during 2024–2026 violated IHL.

Nevertheless, the humanitarian risk is significant when cyber operations affect civilian digital infrastructure. Disruption of communications, health care, energy, finance, and public services may produce serious civilian consequences even without visible physical destruction. Protection of civilians in modern conflict must therefore account for dependency on digital systems as well as physical objects.

The study recommends stronger technical attribution and digital-investigation capacity, improved protection of civilian digital infrastructure, greater international clarity concerning the application of IHL to cyber operations, and stronger cooperation through information sharing, confidence-building measures, and mechanisms for preventing escalation. The principal challenge is not simply the absence of law, but the difficulty of applying existing norms to a transnational, technically complex, and evidentially opaque domain.

REFERENCES

Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.

Dinniss, H. H. (2012). Cyber warfare and the laws of war. Cambridge University Press.

Dinstein, Y. (2022). The conduct of hostilities under the law of international armed conflict (4th ed.). Cambridge University Press.

Geneva Convention relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), August 12, 1949, 75 U.N.T.S. 287.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. California Law Review, 100(4), 817–885.

International Committee of the Red Cross. (2019). International humanitarian law and cyber operations during armed conflicts: ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. ICRC.

Kello, L. (2017). The virtual weapon and international order. Yale University Press.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Mačák, K. (2017). From cyber norms to cyber rules: Re-engaging states as law-makers. Leiden Journal of International Law, 30(4), 877–899. https://doi.org/10.1017/S0922156517000358

Maurer, T. (2018). Cyber mercenaries: The state, hackers, and power. Cambridge University Press.

Microsoft Threat Analysis Center. (2024, February 6). Iran surges cyber-enabled influence operations in support of Hamas. Microsoft.

Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. International Security,

41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3.

Rid, T. (2012). Cyber war will not take place. Journal of Strategic Studies, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press. https://doi.org/10.1017/9781316822524

Smeets, M. (2022). No shortcuts: Why states struggle to develop a military cyber-force. Oxford University Press.

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. Journal of Conflict & Security Law, 17(2), 229–244.

United Nations General Assembly. (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General (A/70/174). United Nations.

United Nations General Assembly. (2021). Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final substantive report (A/75/816). United Nations.

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). Cyber strategy: The evolving character of power and coercion. Oxford University Press.