IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46SP/2025/4636625/
Vol. 2025 (37), Article ID 4636625

The Role of Cyberwar in Modern Warfare*

Nehaluddin AHMAD[1], Ahmad MASUM[2], Azeem KHAN[3] and Faizah RAHIM[4]

[1]MA, LLB, LLM (Lucknow University, India)
LLM (Strathclyde University, UK), LLD (Meerut University, India)
Senior Professor of Law, Universiti Islam Sultan Sharif Ali (UNISSA), Brunei Darussalam.
[2]LLB, MCL, PhD (International Islamic University Malaysia, Malaysia)
Associate Professor, Universiti Islam Sultan Sharif Ali (UNISSA), Brunei Darussalam.
[3]MCA (Kakatiya University, India), PhD (University of Malaya, Malaysia)
Assistant Professor, Universiti Islam Sultan Sharif Ali (UNISSA), Brunei Darussalam.
[4]LL.M (International Law), LL.B BSL (Hons), SHHB Faculty of Law,
Research Assistant & Tutor, Universiti Islam Sultan Sharif Ali (UNISSA), Brunei Darussalam.

Correspondence should be addressed to: Nehaluddin AHMAD, ahmadnehal@yahoo.com

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

Warfare in the twenty-first century has increasingly shifted from traditional battlefields to digital and informational spaces, with cyberwarfare becoming a central tool in both military strategy and diplomacy. Despite growing attention to cyber operations, there is limited research on how these tactics blur the line between peace and war and challenge established norms of sovereignty and international humanitarian law. The recent India-Pakistan confrontation illustrates how modern militaries now integrate cyber capabilities with conventional technologies, creating strategic, operational, legal, and ethical challenges that remain underexplored. This article examines news reports, open-source materials, official documents, and articles of contemporary cyber operations. Close reading of these sources reveals patterns that are not immediately visible, including a growing focus on controlling information rather than territory. The transformation complicates deterrence, raises normative and legal uncertainties, and presents difficult questions of accountability in cyberspace. It stresses that states need to build robust cyber policies, establish clear legal frameworks, and enhance interagency coordination to respond effectively to emerging threats. Drawing on these insights, the article identifies how cyber warfare is changing conflict behaviour, undermining the force of international law and reshaping security policy in today's digital and information-driven era. These findings highlight the importance for policymakers, legal and security professionals to not only consider changing levels of power or military systems imposed within military warfare, but furthermore to confront developments in this domain and battlefield environment of cyber-enabled warfare.

Keywords: Cyberwarfare, Modern Warfare, Digital Sovereignty, International Humanitarian Law, Information Security

Introduction

The tenor of 21st-century war has already changed substantially, moving well beyond battle to the digital and informational space. Conventional warfare – usually characterized as 'army and people moving', territory taken and kinetics used – is more frequently than not accompanied by – if not altogether replaced by – activities that engage networks, communication platforms and vital resources (Atrews, 2020). Cyberwarfare has become a must-have element of how statecraft proceeds, giving nation-states the kit to project power, weaken adversaries and advance strategies without having to cross borders. In that environment, access and control of information systems, data flows and digital infrastructure can matter just as much as traditional military hardware (Digmelashvili, 2023; Mercado, 2025).

Cite this Article as: Nehaluddin AHMAD, Ahmad MASUM, Azeem KHAN and Faizah RAHIM, Vol. 2025 (37) "The Role of Cyberwar in Modern Warfare" Communications of International Proceedings, Vol. 2025 (37), Article ID 4636625, https://doi.org/10.5171/2025.4636625

This transition presents deep challenges for conventional notions of sovereignty and territorial integrity. International law has historically defined force according to physicality, for example, Article 2(4) of the United Nations Charter prohibits the threat or attack of a state's territorial integrity or political independence. These boundaries can be muddied in cyber operations as well: such operations often occur from a distance, have no observable physical presence, and may be conducted in targeting (both civilian and military) infrastructure (Ahmad et al., 2024; Faisal Khan, 2025). Though such guidelines as the Tallinn Manual 2.0 recommend taking an international humanitarian law (IHL) approach to cyber operations, issues of attribution, proportionality, and defining digital attacks as acts of war remain unclear (Schmitt, 2017).

Contemporary conflicts illustrate how cyber operations supplement conventional military capabilities for today's battlefields (MacAk, 2017). Meanwhile, in the case of India-Pakistan alike, both countries possess high-end aerial and missile technologies, like JF-17 and Rafale fighter aircraft indicative of conventional kinetic forces (Haq, 2025; Patil, 2025). At the same time, state-linked cyber operations and electronic warfare have been incorporated into strategic planning. Such incidents as the defacements of government websites, intelligence intrusions, and targeted misinformation campaigns show how cyber capabilities can disrupt critical systems, influence public perception, and achieve strategic objectives without making land invasions. These phenomena illustrate a transition from a battlefield defined by geography to one defined by networks, data, and digital control (Rahimi & Jones, 2025).

There are other complicated legal, ethical, and strategic dimensions to cyber operations. Although digital threats can reduce immediate human casualties, they can also interrupt crucial civilian services, infringe on privacy, and incur long-term economic and social consequences. The dual use of digital infrastructure (civilian and military) makes adherence to the rules of distinction, proportionality and necessity under international humanitarian law difficult. Additionally, cyberwarfare alters traditional notions of deterrence: whereas conventional deterrence hinges on external threat indicators and retaliatory capabilities, cyber deterrence goes probabilistic in nature, based on evidenced capability, uncertainty of attribution, and threats of indirect disruption (Atrews, 2020; Barrett, 2017; Boothby, 2018; Digmelashvili, 2023; Healey, 2024; Rosenzweig, 2017).

In contemporary warfare, cyber operations serve a wide range of warfare phases. They are used to gather intelligence before open hostilities, to erode adversary readiness, and to create a strategic environment. Cyberattacks during battle can affect communications, logistics and weapons systems, affecting both operational effectiveness and perceived strategy. Even in peacetime, cyber operations can cement benefits or facilitate favorable settings for future combat (Noel & Reith, 2021). Thus, the India-Pakistan escalations stand as a striking illustration of how this relationship has been manifested, whereby cyber capabilities have been deployed in conjunction with traditional military operations to achieve strategic aims and minimize overt territorial conflict (Haq, 2025; Patil, 2025).

Understanding how cyber operations intertwine with conventional military approaches and what they mean for strategic decision making helps to better navigate complex legal and ethical issues – foundational in understanding current warfare. This article analyses these changing dimensions using selected case studies of the India-Pakistan conflict, Russia-Ukraine war and U.S.-Israeli cyber campaigns against Iran. These case studies demonstrate how digital warfare is redefining hostilities and the principles of deterrence from the standpoint of international humanitarian law and how such a framework has been used within the contemporary security sphere.

The Role of Cyberwar in Modern Warfare

The new phase of 21st century warfare, however, requires an adaptation of traditional military operations and is characterized by a reliance on cyberwarfare capabilities. Cyberwarfare also allows states to coerce, degrade key systems, and realize strategic goals without physically entering hostile territory (Noel & Reith, 2021). Unlike classical kinetic war, where most of the times victory is determined by territory, with the destruction of opposition, in modern warfare it now depends to a greater degree upon a strategic monopoly on information systems, networks, as well as digital infrastructure. Control of such systems can be pivotal in determining the success of operational effectiveness, public perception, and strategic decisions (Biggio, 2025; Khalifeh, 2025).

To grasp the strategic and operational implications of cyberwarfare, scholars have devised models that classify offensive cyber operations as having specific onset and intention. Jason Healey, for example, specifies three fundamental phases: pre-hostilities, rear-echelon or pre-battle, and battlefield. Within these phases, cyber operations might be organized around things like intelligence exploitation, network or system disruption, trust erosion, or attacks on critical infrastructure and weapons systems. This conceptual model suggests that cyber abilities are not auxiliary tools but part of military planning, which create strategic, operational, and psychological effects on military operations without a direct face-to-face confrontation (Healey, 2024).

Cyber Operations Prior to Hostilities

Cyber operations before open conflict gather intelligence, evaluate adversary capabilities, and shape the strategic environment. These could include, e.g., reconnaissance of military networks, theft of sensitive technological information, and targeted disruptions tailored to undermine confidence in operational systems (Faisal Khan, 2025). Real-world examples include Russian reconnaissance of Ukrainian networks prior to 2022, and the U.S.-Israeli Stuxnet operation against Iran's nuclear program. These operations show that cyber activities can have effects analogous to kinetic military operations since the need for direct combat is reduced and thus strategic leverage (Biggio, 2025; Freilich, 2024; Katikar, 2024; Khalifeh, 2025; Lindsay, 2013; Weber, 2023).

From an international humanitarian law standpoint, pre-hostilities operations are generally not considered armed attacks, but states should take the indirect effects on civilian systems into account. For instance, intelligence collection on networks used for military and civilian purposes can inadvertently disrupt civilian communications or vital services, requiring distinction and precautions. Even in the absence of immediate harm, the planning and execution of these operations should account for civilian exposure to disruption (Healey, 2024; Healey & Jervis, 2020).

Cyber Operations in Rear-Echelon or Pre-Battle Phases

Once hostilities start or direct engagement is planned, cyber operations typically complement tactical objectives. These involve disruptions to communications, interferences with logistics, and attempts to demoralize. One example is that Russian cyber targeting of Ukrainian rail lines and battle-management systems during the ongoing conflict show that digital operations can hamper operational mobility and degrade command effectiveness. Cyberattacks during this phase will, however, not directly damage civilians, but may indirectly harm the provision of vital services, making it difficult to comply with the IHL principles of proportionality and precaution (Healey, 2024; Kivi, 2025; Ormrod et al., 2023; Rahimi & Jones, 2025; Regencia, 2025; Stinissen, 2015). The tactical amalgamation of cyber and traditional tactics during this phase demonstrates the blurring of digital and kinetic realms. Cyberattacks may achieve tactical goals with little physical damage, but indirect impacts on civilian populations and infrastructure must be taken into consideration. Operational planning needs to take into account the military advantage expected and whether the civilian casualties that may be associated with cyber operations do not, paradoxically, exceed international humanitarian norms (Ahmad et al., 2024; Barrett, 2017; Bia et al., 2022; Digmelashvili, 2023; Healey, 2024; Kostyuk & Gartzke, 2024; Lonergan & Lonergan, 2022; Noel & Reith, 2021; Pedersen & Jacobsen, 2024).

Cyber Operations on the Battlefield

In the battlefield, cyber operations can effectively assist conventional forces by giving them live intelligence, tampering with their operational data and disrupting weapons systems or battle-management system (Ahmad et al., 2024; Healey, 2024; Khalifeh, 2025). Ukraine's mid-flight drone hacks demonstrate how cyber capabilities can shape the outcome of fights without kinetic strikes. Cyber operations can, under different conditions, bring psychological and operational pressure to bear on the adversary by reducing their situational awareness or building mistrust in weapon systems, and in many cases can be as powerful an attack as a conventional one (Biggio, 2025; Ormrod et al., 2023).

It is worth noting again that the IHL principles are quite pertinent in this stage. Cyber operations should maintain distinction, proportionality, and military necessity. Objectives of targeting systems can serve military and civilian functions at the same time, and thus such targets must be meticulously assessed to reduce incidental harm (Ahmad et al., 2024). Such a strategy could lead to disaster or damage, for example, as disabling a military communication network may end up affecting emergency services or hospital communications when they are sharing infrastructure with civilian telecommunication services, presenting an identifiable legal and ethical risk. Cyber operations need to be evaluated for proportionality, so that the estimated military benefit outweighs any incidental indirect effect on civilians (Larsson, 2025; Melzer, 2011; Rodenhäuser, 2025).

Defensive Measures and Ethical Considerations

Defense plays a key role in the strategic utility of cyber operations. States need to continue to be resilient in case of attacks on networks, in communications, or in critical infrastructure. Defense efforts include measures such as system segmentation, redundancy, rapid recovery mechanisms, and partnership with private-sector technology vendors. Ukraine's containment of Russian power-grid attacks with the help of companies like Microsoft and Google demonstrates an integrated defense architecture as a key to maintaining operational effectiveness and protecting civilians (Couzigou, 2018; Healey, 2024; Khalifeh, 2025; Kivi, 2025; Kvartsiana, 2023; Rahimi & Jones, 2025; Stinissen, 2015).

Cyberwarfare is an ethical quandary in its own right. So far, it can produce short-term fewer human casualties than with conventional kinetic strikes but with respect to its indirect impact on civilian populations, vital services, and economic stability, it cannot be ignored. For cyber operational planning to deliver such operational benefits, technical and legal assessments must be incorporated into the overall process to ensure alignment with international norms and that no disproportionate harm results from these operations (Couzigou, 2018; Healey, 2024; Khalifeh, 2025a; Kivi, 2025; Kvartsiana, 2023; Rahimi & Jones, 2025; Stinissen, 2015).

Strategic Implications

Cyberwarfare fundamentally reshapes the nature of deterrence. Conventional deterrence depends on observable capabilities – troop figures, or weapons – to deter aggression. It is probabilistic and based on threat or capability display which is hard to attribute accurately. This opens new vectors for miscalculation, escalation, and unintended civilian impact. The cyber operations strategic, operational, and legal issues are critical to national security planning and international stability (Davis, 2015; Faisal Khan, 2025; Fischer, 2019; Fischerkeller & Harknett, 2017; Healey, 2024; Healey & Jervis, 2020; Sharma, 2010).

In conclusion, cyberwarfare has fundamentally changed the nature of modern conflict by integrating offensive and defensive cyber operations into all aspects of the war. Healey's framework shows how cyber operations can be implemented systematically in pre-hostilities, pre-battle, and battlefield phases, having unique aims and effects. When viewed together with the principles from IHL, this analysis reiterates the importance of strategic operational planning, strong defensive measures, and international norms to assist organizations in how to conduct cyber operations (Healey, 2024; Healey & Jervis, 2020; Larsson, 2025; Noel & Reith, 2021; Pedersen & Jacobsen, 2024). The next section analyzes case studies of how cyber capabilities complement traditional military activity and how they have shaped 21st century conflict.

Comparative Case Analyses of Contemporary Cyber Conflicts

The Four-Days 2025 India-Pakistan Conflict

India and Pakistan's confrontation from May 7 to May 10, 2025, is a glaring demonstration of the way in which cyberwarfare is now a cornerstone of contemporary military strategy. Both share large conventional military strength and their JF-17 and Rafale jets. But now, this event shows us that controlling information and cyberspace can be as important as war on land. Some of their cyber tactics were to collect intelligence, disrupt communication networks, tamper with data relating to military operations, and launch strategic campaigns to shape public opinion and decisions during this four-day fight. These digital undertakings show the merging of traditional conflict with cyber-enabled tactics, mirroring the more general evolution of conflict in the 21st century (Aryan, 2025; Atrews, 2020; Basu, 2022; Digmelashvili, 2023; Haq, 2025; Liao, 2025; Patil, 2025; Shafiq Ur Rahman et al., 2024).

Cyber reconnaissance had a significant role prior to direct operation to shape the strategic environment. Both India and Pakistan reportedly carefully monitored an adversary's military networks, airbase deployments, and command-and-control infrastructure (Aryan, 2025; Haq, 2025; Liao, 2025; Patil, 2025). These pre-hostilities operations adhere to Healey's framework that describes cyber activities as activities performed for the purpose of intelligence gathering, adversary readiness mitigation, and the creation of strategic leverage without physical engagement. Overall, these operations are non-kinetic but not without IHL considerations (Healey, 2024). A well-thought-out and robust assessment of dual-use systems allows military actors to operate independently of nonmilitary civilian functions; while ensuring they satisfy principles of distinction and precaution. Even indirect disruption of civilian communications or essential services could lead to issues of proportionality and necessitation of operational planning aimed at minimizing inadvertent harm (Ahmad et al., 2024; Biggio, 2025; Shafiq Ur Rahman et al., 2024).

As hostilities escalated, cyber operations were deployed in the rear-echelon or before the onset of hostilities to affect logistical coordination, communication networks, and battle-management software. These operations hampered operational efficiency and uncertainty of decision-making at both a tactical and operational level, showcasing that cyberwarfare could complement conventional force readiness. From an IHL viewpoint, the targeting of dual-use systems should be assessed closely to determine who is more affected in the targeting and by what means of civilian population. At this phase, cyber-operations also reflect both operational influence and psychological influence in which adversaries' perceptions and decisions are shaped while not resorting to physical violence (Ahmad et al., 2024; Biggio, 2025; Davis, 2015; Digmelashvili, 2023; Melzer, 2011; Mercado, 2025; Noel & Reith, 2021; Pedersen & Jacobsen, 2024; Rahimi & Jones, 2025; Rodenhäuser, 2025; Shafiq Ur Rahman et al., 2024).

On the battlefield, cyber capabilities increasingly conformed to traditional operations. The use of real-time intelligence exploitation, distortion of operational data, and disruption of weapons or battle-management systems gave forces tactical advantage. Drone hacks in mid-air, reportedly, even derailed surveillance and targeting operations, showing how digital interventions can affect combat results without inflicting physical damage. These operations provide insight into the strategic and psychological aspects of cyberwarfare, demonstrating its ability to change battle-space dynamics, undermine confidence in weapons systems, and impact adversary choices (Ahmad et al., 2024).

Defensive measures, too, were a key consideration in the India-Pakistan context. Each country apparently instituted network segmentation, threat detection, emergency recovery protocols, and partnerships with private cybersecurity companies to secure vital infrastructure and keep operations running smoothly (Aryan, 2025; Basu, 2022; Haq, 2025; Patil, 2025). These measures show that cyberwar is not simply an offensive weapon; cybersecurity must also possess powerful defenses to protect military effectiveness and civilian infrastructure, supporting IHL norms. Defense is essential to safeguarding a strategic advantage with minimal and appropriate civilian casualties and enhancing resilience to threats (Ahmad et al., 2024; Biggio, 2025; Digmelashvili, 2023; Melzer, 2011; Shafiq Ur Rahman et al., 2024).

For centuries, wars in both India and Pakistan have been about who we kill and kill, but the larger ramifications for modern warfare lie in the broader context of this. First, it shows that offensive and defensive cyber capability has the potential to achieve strategic, operational and psychological goals, while avoiding large scale kinetic encounters. Second, and perhaps most notably, it captures the eroding distinction between peace and war in the current era of cyberspace, between the projection of power in virtual spaces, no less, than they do on physical ground. Thirdly, it highlights the need to integrate IHL concepts into cyber engagements. Although cyber-attacks can lower casualties in the short term in a proportionate way compared to traditional targets, the indirect effects on civilians and dual-use infrastructure must be managed in clear terms of legality, proportionality and ethics. Lastly, this case study illustrates some fundamental elements of how deterrence dynamics in cyberwarfare have evolved, with the demonstration of capability, resilience, and uncertainty of attribution being significant drivers of adversary behavior in cases of non-threatening direct physical confrontation (Aryan, 2025; Basu, 2022; Haq, 2025; Patil, 2025).

The India-Pakistan 2025 conflict illustrates that there is no contemporary battle without the marriage of force on the part of both adversaries online and in-land. Understanding them, considering contemporary warfare theory and IHL principles reveals that cyberwarfare is recasting strategic, operational, and ethical dimensions of 21st-century conflicts.

Russia-Ukraine War

The Russia-Ukraine war is a perfect example of the depth, severity and complexity of cyberwarfare in modern-day high-intensity conflict. Due to rapid but only limited confrontations, the Russia-Ukraine war provides constant cyber campaigns running alongside conventional military exercises with its impacts being on the national infrastructure and civilian population (Regencia, 2025; Rosenzweig, 2017).

From the beginning of hostilities, cyber operations, both offensive and defensive, have been an integral part of operational strategy. Russia is alleged to have employed wiper malware, disseminated denial-of-service cyberattacks and digital disinformation campaigns against Ukrainian military command networks, energy grids and communication infrastructure. Ukraine's response was to give state, as well as the private sector, tools to sustain businesses online and protect civilian infrastructure and withstand attacks. Its mix of offensive and defensive cyber scenarios reveals dimensions in cyberwar that are strategic, operational and psychological that were not visible on the India–Pakistan case (Kvartsiana, 2023).

Cyber operations in Ukraine were well-coordinated covering different stages of multiple phases of war. In the pre-hostilities stage, reconnaissance and infiltration of the Ukrainian military was carried out via reconnaissance technology and network intrusion for readiness and attack vulnerability testing and critical infrastructure threat analysis. After hostilities began, cyber activity was focused on the rear-echelon activities of logistics, communications, and supply chain obstruction to disrupt operational movement. On the battlefield, cyber capabilities were utilized to disrupt command-and-control platforms, manipulate intelligence systems and disrupt key weapons operations. This multiple stage strategy shows that offensive cyber approaches can systematically advance tactical and strategic priorities at multiple moments in contemporary conflict (Kivi, 2025). IHL matters are especially relevant in the context of Russia-Ukraine. The impact of attacks on dual-use infrastructure – power grids and water systems, for instance – will mostly be felt by civilian populations. Proportionality, distinction and precautionary actions must be strictly adhered to, but the sheer complexity and scale of cyber operations make it a complex exercise in anticipating collateral damage. Ukraine has defensive strategies like system segmentation,

collaboration with technology companies, and accelerated restoration processes that allow for civilian mitigation of damage without compromising military capability (Kivi, 2025; Kvartsiana, 2023; Ormrod et al., 2023; Al Jazeera, 2025; Regencia, 2025; Stinissen, 2015).

Strategically, the Russia-Ukraine case highlights the transformative role that cyberwarfare plays in contemporary conflict. Digital campaigns can shape the battlefront, impact morale, and produce psychological costs that extend far beyond the field of battle. The development of cyber capabilities is reconfiguring deterrence, too, demanding that states now think about deterrence in terms of robustness not only of kinetic retaliation, but also the potential for retaliation in the digital realm. Both the strategy and humanitarian dilemmas of modern warfare necessitate robust international norms and legal frameworks to address these issues in cyber operations (Davis, 2015; Khalifeh, 2025; Rahimi & Jones, 2025).

Essentially, the Russia-Ukraine incident illustrates how cyberwarfare works on a scale and intensity level, shaping war on its own, touching the civilian population, and challenging the traditional frameworks of law and conduct.

U.S.-Israel Cyber Operations Against Iran

The U.S.-Israeli organized cyber operations against Iran's Natanz nuclear center are a quintessential example of offensive cyberwarfare against key infrastructure. By using exclusively digital methods to accomplish strategic military objectives, these operations showed how cyberwarfare can have practical effects in the absence of direct kinetic acts. The best-known example is Stuxnet, intended to disrupt Iran's nuclear enrichment facilities. Stuxnet delayed Iran's nuclear program while minimizing direct human casualties through manipulation of industrial control systems, avoiding physical strikes (Aanonsen, 2025; BBC, 2012).

It also illustrates the relevance and application of cyberwarfare in Healey's framework. Pre-hostilities and operational cyber operations were carefully planned and interlinked with other actions, combining intelligence gathering information collection and the use of systems at their target locations, with intentional disruption on critical infrastructure. The intent was very particular: to disable military-related nuclear capabilities and limit the damage done to military-related nuclear capabilities without having a wider civilian consequence. This one operation is a classic case of cyberwarfare as an execution with a focus on tactics as both part of the reality and a strategy and showcases the complexity of cyberwarfare, which is how advanced such a notion considers a "strategic" capability to achieve political and military objectives without occupying other nations or fighting wars in traditional forms, where borders can be both political and military with no traditional borders (Healey, 2024).

From an IHL standpoint, there were fundamental principles on distinction, proportionality and precaution which the operations of this operation are relevant. The cyberattack was aimed at a facility of armed-military program, minimizing the civilian casualties that could lead to the need for security measures – a military imperative. But any cyber-attack that touches upon dual-use infrastructure – even indirectly – should be monitored closely to avoid the unequal harm to civilian groups. While Stuxnet's limited collateral impact suggests that cyberwarfare may indeed conform to IHL on a theoretical level, it also reveals the challenges of ensuring compliance once an attack is deployed with respect to a set of interconnected technological systems whose effects have unpredictable dominoes (Aanonsen, 2025; Arshad, 2025; BBC, 2012; Singer, 2015; Umar, 2025).

This case essentially highlights strategic implications for contemporary warfare as well. First, it shows that cyberwarfare can be a tool of covert strategic influence, advancing an objective with plausible deniability. Second, it illustrates the long-term operational and psychological ramifications of digital disruption, as adversaries must now expect vulnerabilities in cyberspace alongside conventional military threats. Finally, it demonstrates the way in which cyber operations change the calculus of deterrence: rivals are now confronted with exposure to precise, remotely-conducted attacks on critical facilities, in the absence of direct kinetic attacks (Aanonsen, 2025; Arshad, 2025; BBC, 2012; Singer, 2015; Umar, 2025).

In general, this case demonstrates the nature of cyberwar as a strategic weapon is changing and will be able to evolve. Stuxnet is a good example of an entirely cyber offensive, designed to satisfy strategic military goals with minimal human suffering on the ground. This demonstrates the varied manifestations of cyberwarfare in modern conflicts, the ethical and legal implications of such combat, the necessity of incorporating cyber operations within a large domain as well as a longer range of defensive and strategic missions (Aanonsen, 2025).

Implications of Cyberwarfare

Generally, the previous case studies serve to reveal the status of cyberwarfare incorporation in modern military strategy, reflecting not only its strategic implications for warfare but also its philosophical importance. Four common threads arise from these examples: operational effectiveness, applicable legal frameworks, ethical concerns, and strategic dilemmas. Undercutting these themes is the variety of dimensions of operation, strategy,

and ethics that define contemporary warfare with cyberwarfare. Cyber capabilities have been critical to collaborative planning and execution of military actions amidst the increasingly digital and informational domains that define the battlefield today within these scenarios (Digmelashvili, 2023; Katikar, 2024; Kostyuk & Gartzke, 2024; Melzer, 2011). In India-Pakistan, cyber operations were integrated with traditional air power to interrupt communications networks, intelligence systems, and logistics, while simultaneously impacting morale and decision-making (Aryan, 2025; Basu, 2022; Liao, 2025). The scale that such operations can impose, and its complexity, are exemplified by the ongoing Russia-Ukraine war where cyber operations have centered around military command networks, energy grids, and civilian-critical systems, establishing a feedback loop of operational and psychological effects (Kivi, 2025; Kvartsiana, 2023; Ormrod et al., 2023; Regencia, 2025; Al Jazeera, 2025; Stinissen, 2015). The US-Israel campaign against Iran, best illustrated by the Stuxnet campaign, shows us that cyberwarfare can be an effective and precise tool in the manufacturing of interests with political will itself (Aanonsen, 2025; Arshad, 2025; BBC, 2012; Singer, 2015; Umar, 2025). These cases collectively suggest that cyberwar is something more than merely an added step, but part and parcel of the actualization of operational, psychological, and political outcomes within a process that is re-shaping conventional understandings of war and deterrence.

Legally and ethically, IHL remains the standard for evaluating cyber operations. The principles of distinction, proportionality, and precaution apply when operational activities involve dual-use infrastructure such as power grids, communication systems, and industrial facilities (Ahmad et al., 2024). In the 2025 India-Pakistan conflict, comprehensive operational planning enabled pre-hostilities and rear-echelon cyber activity to impact adversary readiness without inflicting disproportionate impact on civilian populations. The scope of Russia-Ukraine's cyber operations is also an impediment to IHL compliance, based largely on a high level of intensity and duration, especially since both indirect effects on civilian life and essential services are more damaging. In contrast, the U.S.-Israel cyber campaign against Iran demonstrates that if cyber operations are purposefully designed to meet IHL requirements, with appropriate controls, minimal civilian casualties can occur while the government maximizes strategic aims. These examples emphasize, in parallel, that, even with these capabilities, cyber operations alone can help mitigate direct physical human loss of life, yet ethical and legal concerns persist, especially in the context of dual-use systems and the potential for cascading or unintended effects (Ahmad et al., 2024; Melzer, 2011; Rodenhäuser, 2025; Schmitt, 2013, 2014; Shafiq Ur Rahman et al., 2024).

Strategically, these case studies suggest that cyberwarfare has redefined deterrence and coercion. States now place emphasis on an assessment of cyber capability and on securing critical systems to sway an adversary's decision-making process. Cyberspace being probabilistic and often anonymous complicates traditional military calculations and this results in a universe where the mere act of digital disruption can shape behavior just as much or more than any conventional use of kinetic force. Simultaneously, integration of offensive and defensive cyber capabilities is imperative; resilience, via systems redundancy, threat monitoring, rapid response, and collaboration with public-private actors, is the basis of continued operations while incurring minimal damage to civilians and infrastructure. These conflicts also show the need for coherent international norms in addition to governance structures. It is the lack of common protocols for cyber-related action that amplifies the likelihood of escalation, miscalculation, and accidental civilian casualties. A strong legal and ethical background for cyber operations is crucial for stabilizing contemporary conflict, holding states accountable, and integrating cyberwarfare into military strategy in a responsible manner (Barrett, 2017; Basu, 2022; Bia et al., 2022; Biggio, 2025; Couzigou, 2018; Davis, 2015; Faisal Khan, 2025; Lonergan & Lonergan, 2022; MacAk, 2017; Melzer, 2011; Rodenhäuser, 2025; ŠARF, 2017; Schmitt, 2017; Shafiq Ur Rahman et al., 2024).

Ultimately, the aggregate analysis of these case studies demonstrates the transformation of the landscape of contemporary conflict by cyberwarfare. By migrating the front line to the cyber space, influencing strategic and psychological elements, and challenging classical dynamics of deterrence and intervention, cyber operations require the attention of critical jurisprudential, moral, and operational considerations. All the case studies mentioned above demonstrate that the application and use of cyberwarfare are varied, from limited regional conflicts to strategic targets and a scale of large-scale operations, while also stressing the critical importance of incorporating such capabilities, defense, and the use of international instruments of deterrence, including international law, into the 21st century military strategies (Barrett, 2017; Basu, 2022; Bia et al., 2022; Biggio, 2025; Couzigou, 2018; Davis, 2015; Faisal Khan, 2025; Lonergan & Lonergan, 2022; MacAk, 2017; Melzer, 2011; Rodenhäuser, 2025; ŠARF, 2017; Schmitt, 2017; Shafiq Ur Rahman et al., 2024).

Conclusion

Contemporary warfare is more reliant on cyber capabilities which once emerged as adjunct instruments of the state. The cases of India-Pakistan, Russia-Ukraine, and U.S.-Israel against Iran discussed previously illustrate how operational, strategic, and psychological objectives may be pursued through cyberspace, and how this may no longer be achieved through kinetic force. Cyberwarfare is changing the way states project power and affect

adversaries through network disruption, manipulation of information and assault on critical infrastructure. These conflicts show that combining cyber operations blurs the line between war and peace: They extend hostilities into a digital realm, as well as informational and psychological domains. As those mentioned cases above indicate, cyber operations also help with the maintenance of deterrence and efficiency in operations; precision campaigns such as Stuxnet showcase the possibility of pursuing objectives with almost no physical destruction (Aanonsen, 2025; Arshad, 2025; Katikar, 2024; Khalifeh, 2025; Larsson, 2025; Melzer, 2011; Noel & Reith, 2021; Pedersen & Jacobsen, 2024; Pernice, 2018; Umar, 2025; Ur Rahman et al., 2024).

IHL still provides a basic architecture for the determination of distinction, proportionality and precaution, but the indirect and cascading effects of cyberwarfare make these principles even more complex when dual-use or civilian systems are taken for advantage of as a result. While these operations might lower direct casualties, they raise new humanitarian and accountability issues. This illustrates how much we need international norms and cooperative frameworks in place to govern state behavior in cyberspace. As digital power continues to define strategic advantage, the future of warfare is bound to rely not only on technological prowess but also on the observance of legal and ethical obligations that uphold stability, keep civilians safe, and prevent escalation (Atrews, 2020; Barrett, 2017; Boothby, 2018; Digmelashvili, 2023; Healey, 2024; Rosenzweig, 2017).

Bibliography

- Aanonsen, C. E. (2025). 'Stuxnet, revisited (again): producing the strategic relevance of cyber operations'. Journal of Cyber Policy, 10(1), 68–84. https://doi.org/10.1080/23738871.2025.2492570
- Ahmad, N., Faizah, R., & Hafizah, H. (2024). 'Enhancing Targeted Operations Through Drone Technology: Maximising Efficacy and Minimising Risk'. Communications of International Proceedings, Vol. 2024 (1), Article ID 4314624, https://doi.org/10.5171/2024.4314624.
- Ahmad, N., Rahim, F., & Aziz, N. (2024). 'Can International Humanitarian Law Regulate Recent Drone Strikes?: A Case Study'. Journal of East Asia and International Law, 17(1), 159–180. https://doi.org/10.14330/jeail.2024.17.1.09
- Arshad, M. H. (2025). 'View of US-Iran Cyber war and its impact on Israel.' Wah Academia Journal of Social Sciences, 4(1), 1134–1158.
- Aryan, K. (2025). 'Role of Electronic Warfare in India-Pakistan Conflict 2025' Global Defense News – GSDN [Online], [Retrieved October 28, 2025], https://gsdn.live/role-of-electronic-warfare-in-india-pakistan-conflict-2025/.
- Atrews, R. A. (2020). 'Threats, Security, Attacks, and Impact' [Online]. Journal of Information Warfare, 19(4), 17–28. https://www.jinfowar.com/journal/volume-19-issue-4/cyberwarfare-threats-security-attacks-impact.
- Barrett, E. (2017). 'On the relationship between the ethics and the law of war: Cyber operations and sublethal harm'. Ethics and International Affairs, 31(4), 467–477. https://doi.org/10.1017/S0892679417000454.
- Basu, A. (2022). 'India's International Cyber Operations: Tracing National Doctrine and Capabilities'. [Online], [Retrieved 23 October 2025] https://unidir.org/publication/indias-international-cyber-operations-tracing-national-doctrine-and-capabilities/.
- BBC. (2012). 'Iran "fends off new Stuxnet cyber attack"'. BBC News [Online], [Retrieved October 28, 2025], https://www.bbc.com/news/world-middle-east-20842113.
- Bia, L., Putra, S., & Sutanto, R. (2022). 'Formation of Cyber Forces for Encounter Modern Warfare and Cyber Warfare'. International Journal of Research and Innovation in Social Science, VI(VIII), 2454–6186.
- Biggio, G. (2025). 'Regulating non-kinetic effects of cyber operations: the 'Loss of Functionality' approach and the military necessity-humanity balance under International Humanitarian Law'. Journal of Conflict and Security Law, 30(2), 241–263. https://doi.org/10.1093/JCSL/KRAF008.
- Boothby, W. H. (2018). 'Regulating New Weapon Technologies'. New Technologies and the Law in War and Peace, 16–42. https://doi.org/10.1017/9781108609388.003.
- Couzigou, I. (2018). 'Securing cyber space: the obligation of States to prevent harmful international cyber operations'. International Review of Law, Computers and Technology, 32(1), 37–57. https://doi.org/10.1080/13600869.2018.1417763.
- Davis, P. K. (2015). 'Deterrence, Influence, Cyber Attack and Cyberwar'. International Law and Politics, 47(327), 327–355.
- Digmelashvili, T. (2023). 'The Impact of Cyberwarfare on the National Security'. Future Human Image (Vol. 19), 12-19. https://doi.org/10/29202/fhi/19/2.
- Faisal Khan, Z. (2025). 'Warfare and International Security: A New Geopolitical Frontier'. The Critical Review of Social Sciences Studies, 3(2), 513-527. https://doi.org/10.59075/k9cbhz04.

- Fischer, M. (2019). ‘The Concept of Deterrence and Its Applicability in the Cyber Domain’. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes 18(1), 69–92. https://doi.org/10.2307/26948850.
- Fischerkeller, M. P., & Harknett, R. J. (2017). ‘Deterrence is Not a Credible Strategy for Cyberspace.’ Orbis, 61(3), 381–393. https://doi.org/10.1016/j.orbis.2017.05.003
- Freilich, C. (2024). ‘The Iranian Cyber Threat.’ [Online] The Institute for National Security Studies, 5-98, https://www.inss.org.il/wp-content/uploads/2024/02/Memo230_IranianCyberThreat_ENG_digital.pdf.
- Haq, R. (2025). ‘Pakistan Downs India’s French Rafale Fighter Jets in History’s Largest Aerial Battle’ [Online], [Retrieved October 23, 2025] https://www.southasiainvestor.com/2025/05/pakistan-downs-indias-french-rafale.html.
- Healey, J. (2024). ‘Cyber Effects in Warfare: Categorizing the Where, What, and Why’ [Online], [Retrieved October 19, 2025] https://doi.org/10.26153/TSW/56029.
- Healey, J., & Jervis, R. (2020). ‘The Escalation Inversion and Other Oddities of Situational Cyber Stability’. Texas National Security Review, 3(4). https://doi.org/10.26153/TSW/10962.
- Healy, J. (2022) ‘Preventing Cyber Escalation in Ukraine and After’, War on the Rocks [Online], [Retrieved October 28, 2025] https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/.
- Katikar, H. (2024). ‘Stuxnet-Analysis and Implications of the World’s First Cyber-Weapon Stuxnet-Analysis and Implications of the World’s First Cyber-Weapon’. [Online], [Retrieved October 19, 2025], https://doi.org/10.13140/RG.2.2.10847.27043.
- Khalifeh, S. (2025). ‘The evolution of warfare from conventional to a digital battlefield: an analysis of cyber technology and artificial intelligence in the Lebanese-Israel conflicts’. Defense and Security Studies, 6(1), 91–102. https://doi.org/10.37868/dss.v6.id285
- Kivi, A. (2025). ‘Cyber resilience in Ukraine after beginning of Russia’s full-scale invasion’, [Master’s Thesis], Tallinn University of Technology, School of Information Technologies. https://digikogu.taltech.ee/en/Download/c6c814f0-f582-4509-8d29-dcbf87a5c434.
- Kostyuk, N., & Gartzke, E. (2024). ‘Fighting in Cyberspace: Internet Access and the Substitutability of Cyber and Military Operations’. Journal of Conflict Resolution, 68(1), 80–107. https://doi.org/10.1177/00220027231160993.
- Kvartsiana, K. (2023) ‘Ukraine’s Cyber Defense: Lessons in Resilience’. ReThink.CEE Fellowship [Online], [Retrieved October 20, 2025] Available at: https://www.gmfus.org/sites/default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf.
- Larsson, E. (2025). ‘Collateral Damage from Offensive Cyber Operations—A Systematic Literature Review’. Journal of Cybersecurity and Privacy 2025, Vol. 5, Page 35, 5(2), 35. https://doi.org/10.3390/JCP5020035.
- Liao, H. (2025). ‘Prospects & Perspectives Lessons from the Indo-Pakistani Air Battle’. In Prospects & Perspectives (Issue 33), [Online], [Retrieved October 23, 2025]. Available at: https://www.pf.org.tw/en/pfen/33-11364.html.
- Lindsay, J. (2013). ‘Stuxnet and the Limits of Cyber Warfare’. Security Studies, 22, 365–404. https://doi.org/10.1080/09636412.2013.816122
- Lonergan, E. D., & Lonergan, S. W. (2022). ‘Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises’. Security Studies, 31(1), 32–64. https://doi.org/10.1080/09636412.2022.2040584.
- MacAk, K. (2017). ‘From the vanishing point back to the core: The impact of the development of the cyber law of war on general international law’. 9th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2017, pp. 1-14, doi: 10.23919/CYCON.2017.8240333.
- Melzer, N. (2011). ‘Cyberwarfare and International Law’. [Online], UNIDIR Resources, 1–37. Available at: https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf.
- Mercado, V.A. (2025) ‘Cyber Warfare and the Future of Conflict’. [Online], Master’s thesis, Missouri State University. Available at: https://bearworks.missouristate.edu/theses/4078.
- Noel, G. E., & Reith, M. G. (2021). ‘Cyber Warfare Evolution and Role in Modern Conflict’. Journal of Information Warfare, 20(4), 30–44.
- Ormrod, A., Ormrod, D., & Slay, J. (2023). ‘Observations from the Russo-Ukrainian Conflict’. Journal of Information Warfare, 22(1), 76–87.
- Patil, S. (2025) ‘Operation Sindoor and India-Pakistan’s Escalated Rivalry in Cyberspace’. RUSI Commentary, [Online], [Retrieved October 19 October 2025], Available at: https://www.rusi.org/explore-our-research/publications/commentary/operation-sindoor-and-india-pakistans-escalated-rivalry-cyberspace.
- Pedersen, F. A. H., & Jacobsen, J. T. (2024). ‘Narrow windows of opportunity: the limited utility of cyber operations in war’. Journal of Cybersecurity, 2024, 14. https://doi.org/10.1093/cybsec/tyae014
- Pernice, I. (2017) ‘Cybersecurity Governance: Making Cyberspace a Safer Place’ [Online] HIIG Discussion Paper Series, Discussion Paper No. 2017-05, August 2017, pp. 1–27. https://doi.org/10.2139/SSRN.3012136.

- Rahimi, N., & Jones, H. (2025). ‘Cyber Warfare: Strategies, Impacts, and Future Directions in the Digital Battlefield’. Journal of Information Security, 16(02), 252–269. https://doi.org/10.4236/jis.2025.162013
- Regencia, T. (2025). ‘Russia-Ukraine war: List of key events, day 1,340’. Al Jazeera News [Online], [Retrieved October 19, 2025] https://www.aljazeera.com/news/2025/10/26/russia-ukraine-war-list-of-key-events-day-1340.
- Rodenhäuser, T. (2025). ‘International humanitarian law and connectivity disruptions during armed conflict’. Humanitarian Law & Policy [Online], [Retrieved October 19, 2025], https://blogs.icrc.org/law-and-policy/2025/07/03/international-humanitarian-law-and-connectivity-disruptions-during-armed-conflict/
- Rosenzweig, P. (2017). ‘The Reality of Cyber Conflict: Warfare in the Modern Age’, pp. 31–39. The Heritage Foundation [Online], [Retrieved 22 November 2025] https://www.heritage.org/sites/default/files/2019-10/2017_IndexOfUSMilitaryStrength_The%20Reality%20of%20Cyber%20Conflict_Warfare%20in%20the%20Modern%20Age.pdf
- Šarf, P. (2017). ‘Legality of Low-Intensity Cyber Operations under International Law’, Contemporary Military Challenges, (19/3), pp. 81–93 [Online], [Retrieved October 19, 2025] https://doi.org/10.33179/BSV.99.SVI.11.CMC.19.3.5.
- Schmitt, M. N. (2014). ‘Rewired warfare: rethinking the law of cyber-attack’. International Review of the Red Cross, 893, 189–206. https://doi.org/10.1017/S1816383114000381
- Schmitt, M. N. (2017). ‘Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.’ Cambridge University Press [Online], [Retrieved 15 October 2025] https://www.cambridge.org/core/books/tallinn-manual-on-international-law-applicable-to-cyber-warfare/7F2A3D94C9A1B2A78BFD3F9C3F8E1E48.
- Sharma, A. (2010) ‘Cyber Wars: A Paradigm Shift from Means to Ends’, Strategic Analysis, 34(1), pp. 62–73. doi: 10.1080/09700160903354450.
- Singer, P. W. (2015). ‘Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons’, Case Western Reserve Journal of International Law, 47, pp. 79-86. https://scholarlycommons.law.case.edu/jil/vol47/iss1/10.
- Stinissen, J. (2015). ‘A Legal Framework for Cyber Operations in Ukraine’, in Geers, K. (ed.) Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: NATO CCD COE Publications, pp. 123–134 [Online], [Retrieved October 20, 2025] https://ccdcoe.org/uploads/2018/10/Ch14_CyberWarinPerspective_Stinissen.pdf.
- Umar, M. (2025). ‘Iran and Israel Cyber Warfare and Interference of US’. Social Science Review Archives, 3(2), 2040–2048. https://doi.org/10.70670/SRA.V3I2.824
- Ur Rahman, S., Shaikh, M. A., Tahir, M., Naseem, I., Sriyanto, S., Bandar, N. F. A., & Zaman, K. (2024). ‘Navigating Modern Warfare Challenges: A Review Of The Evolution Of International Humanitarian Law In Cyberwarfare’. Journal of Southwest Jiaotong University, 59(1). https://doi.org/10.35741/issn.0258-2724.59.1.21
- Weber, V. (2023). ‘Why Great Powers Launch Destructive Cyber Operations and What to Do About It’ German Council on Foreign Relations (Policy Brief) [Online], [Retrieved October 23, 2025], https://dgap.org/en/research/publications/why-great-powers-launch-destructive-cyber-operations-and-what-do-about-it.