

INFORMATION WARFARE - THE INTERNATIONAL LEGAL REGIME EVOLUTION, CHALLENGES, ARCHITECTURE, AND THE PATH FORWARD

*Prof. Dr. Shabana Fayyaz**

Abstract

The use of information warfare is now increasingly fusing cyber intrusions, infrastructure compromises, disinformation, and synthetic media using artificial intelligence in ways that are blurring the lines between peace and armed conflict. International law is not lacking, but the rules are scattered between sovereignty and non-intervention, state responsibility, jus ad bellum, international humanitarian law (IHL), human rights law and platform regulation. The current debate on both topics is largely conducted in isolation: problems of technical cyber operations and cognitive information operations overlap in the issues of attribution, threshold, civilian harm, and state control of information flows. The article explores the UN Charter, ARSIWA, IHL, the Tallinn Manuals, UN cyber-governance processes, and selected state practices through the lens of qualitative doctrinal legal research and comparative case analysis. It looks at the cyber threat of Stuxnet, Salt Typhoon, and the India-Pakistan conflict of May 2025 as different types of information warfare. The analysis concludes that IHL cannot stand alone to regulate continuous activity that does not reach the threshold of armed conflict and that the treaty has a vital role to play in the regulation of information operations in situations where they are linked to armed conflict. It also suggests that the clash of different visions on digital sovereignty is an obstacle to norm formation. A reform agenda, based on the interpretation of the lex specialis, is proposed with a focus on attribution, critical civilian digital infrastructure, AI-generated synthetic media and accountability in the platform mediated information environment.

Keywords: Information Warfare, Cyber Operations, IHL, Jus Ad Bellum, Tallinn Manual, Attribution, Deepfakes, AI Disinformation, India-Pakistan, Operation Sindoor, Lex Specialis.

*Prof. Dr. Shabana Fayyaz is serves as Associate Professor at the Department of Defence and Strategic Studies, Quaid-i-Azam University, Islamabad. The author can be reached at sfayyaz@qau.edu.pk.

Introduction

The 'fog of war is the uncertainty within which commanders must act', Clausewitz said. However, uncertainty is not just an inherent part of today's information warfare but is also actively created through cyber operations, disinformation, synthetic media and the manipulation of information systems. So, the legal issue isn't merely a function of novel technologies; it's a function of novel uses of ambiguity.

This transition poses a threshold and classification issue for international law. Questions of attribution, status, causation and territorial effects, and the existence or intensity of conflict, are of central importance to international humanitarian law (IHL), the law of state responsibility, *jus ad bellum*, and principles of sovereignty and non-intervention. Each of these can be confused in the case of information warfare, by proxy actors, distributed digital effects, ambiguous timing, and cognitive operations, which can have strategic consequences without actually destroying anything. It is thus not a question of whether international law is applicable in any way, but whether one legal regime or another is applicable and at what threshold, and by what evidentiary basis.

By 2026, information warfare has become the constant backdrop to great-power competition. By the beginning of 2026, Ukrainian law enforcement had thwarted more than 14,000 large-scale cyberattacks. AI-generated deepfakes were used at scale for the first time in the India-Pakistan confrontation of May 2025 and in June 2025 during the Iran conflict.¹ It was a compelling example of the combined power of domestic media and synthesized AI.

Research Gap and Methodological Framework

There are multiple parallel streams of legal literature in the field of cyber/information operations. Sovereignty, state responsibility, prohibition on the use of force and attribution are the most common ways to evaluate cyber intrusions, while non-intervention, human rights, media governance and platform regulation are the most frequent approaches to disinformation and influence operations and IHL comes to the fore once cyber operations are linked to an armed conflict. This creates a conflicted discussion where technical, cognitive and structural aspects of information operations can be viewed as distinct issues while in practice they may be utilized together.

This article attempts to find a way to tackle that fragmentation by reconceptualising information warfare as a spectrum of overlapping practices and not as a technology category, per se. It makes a threefold contribution. Firstly, it creates a multi-level legal analysis, to differentiate between the threshold of armed conflict and during armed conflict. Second, it contrasts the various modalities of information warfare to draw attention to common issues of attribution, legal thresholds, civilian harm and accountability. Third, it relates these doctrinal issues to a new conflict on digital sovereignty, platform governance and state control over information infrastructure.

The article is guided by two questions: (1) to what extent can existing international legal regimes regulate technical, cognitive, and structural information warfare across the continuum between peacetime competition and armed conflict; and (2) what do select cases and state practices reveal about the adequacy of existing rules on sovereignty, attribution, use of force, civilian protection, and control of information flows?

Qualitative doctrinal legal research method and comparative case analysis method are used in the study. The doctrinal part looks at the UN Charter, the International Law Commission's (ILC's) Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), pertinent rules of IHL, case law of the International Court of Justice (ICJ) and the International Criminal Tribunal for the former Yugoslavia (ICTY), as well as the Tallinn Manuals, UN cyber-governance processes, and official or publicly reported state positions already mentioned in the article. These materials are read together to find the points of similarity, differences and regulatory overlap.

Because of their different legal aspects on the same issue, three main cases are being compared. Stuxnet was technical information warfare that could have physical effects, Salt Typhoon was strategic intrusion, sovereignty and attribution in the legal grey zone below armed-attack level and India-Pakistan confrontation in May 2025 was cognitive information warfare, AI-generated content and attribution of escalatory effects in a mixed state-commercial-media-platform environment. The other examples in the article are illustrative only, and are not intended to provide separate case studies.

The samples are not statistically representative but are selected purposefully. There are also evidentiary limitations in cyber attribution, such as

classified intelligence, disputed public attribution and non-bindingness of instruments like the Tallinn Manuals which influence the analysis. The goal is thus not to create a generic causal model, but to shed light on common legal issues and determine if the current architecture offers consistency in the law as it applies to the various modalities of information warfare.

Analytical Framework: A Layered Approach to International Law

The Layered Legal Framework

There is no one legal regime which can be used to evaluate information warfare. Extra armed conflict operations can involve sovereignty, non-intervention, State responsibility, HR obligations, domestic cyber regulation, and if effects meet threshold, jus ad bellum. However, when an armed conflict has already been declared, IHL imposes a supplemental series of rules on the conduct of armed conflict and the protection of civilians.² The legal framework applicable in this case is thus multi-layered: its scope of application varies according to the nature of the operation, its attribution, its impact and the legal environment in which it is carried out.

Why IHL Matters - and Why It Is Not Sufficient Alone

The information operations were an appropriate part of the analysis, as they could impact on military decision-making, civilian communications, hospital systems, water systems, surrender, warning systems and other functions directly related to the conduct and humanitarian effects of armed conflict. Under such circumstances, there are legal benchmarks, such as distinction, proportionality, precautions, protection of civilian objects and the rules of perfidy. The article thus tests the applicability of current rules to the digitally mediated and cognitively shaped effects which were not specifically considered when the rules were framed, with the help of IHL.³

Meanwhile, IHL does not apply to all types of information warfare. Cyber intrusion, influence activity and manipulation of information access can be ongoing in peacetime or below the threshold for the application of the law of armed conflict. It would thus be a mistake to treat IHL as the only framework, as this would only replicate the divide the article attempts to explain. The boundaries of IHL have analytical significance: they illustrate the need to look at IHL in conjunction with

the law of armed conflict, sovereignty, non-intervention, state responsibility, jus ad bellum, human rights law, domestic regulation, and platform governance.⁴

Norm Formation as a Secondary Explanatory Lens

Process-based norm formation is also adopted as a second explanatory lens. The existing rules are identified by doctrinal analysis while process theory explains how official attribution statements, state responses, UN processes, soft-law instruments and regulatory experiments can help to build up expectations regarding responsible conduct over time. This separation of relevant law and the formation of new norms is observed throughout the analysis in order not to give the impression that the policy proposals are already binding legal rules.⁵

Evolution of The International Legal Regime

The Classical Framework

The ban on the use of force in Article 2(4) of the UN Charter (1945) in conjunction with the right of self-defense in Article 51 created a two-part legal framework: a state could not resort to force except in the exercise of the right of self-defense, or on the basis of a Security Council authorization.⁶ This was an architecture of kinetic, visible, state-executed, and widely held violence. The old understanding of sovereignty based on the Westphalian system of 1648 should now be read in an era where 'territory' is an abstraction that is challenged and 'force' can take the form of malicious code or fabricated video productions.⁷

In the Nicaragua Case (1986), the International Court of Justice developed the 'effective control' test on the attribution of the conduct of non-state actors to States.⁸ Although it is an old document, its conceptual structure, including the distinction between 'armed attack' that would invoke Article 51 and lesser 'uses of force', is the structure that must be used to classify cyber and information operations to this day.⁹

The Stuxnet Inflection Point

Iran's Natanz uranium enrichment facility was attacked in the Stuxnet operation (2009-2010) believed to have been launched by the U.S. and Israel, which compromised approximately 1,000 centrifuges and made it seem as though everything was functioning as usual.¹⁰ It showed that cyber tools could have effects like those of kinetic tools, and set up a model of plausible deniability; Iran could

not argue self-defense under international law because attribution was based primarily on journalistic investigation.

The Tallinn Manuals

Tallinn Manual (2013) and Tallinn Manual 2.0 (2017) have been developed under the auspices of NATO's CCDCOE and are the most systematic attempt to map existing law to cyber and information operations.¹¹ Both documents are non-binding. The Rule 4 of Tallinn Manual 2.0 clearly states that "States shall not use cyber means that are inconsistent with the sovereignty of other states," which is directly at odds with the United Kingdom's interpretation that "sovereignty is not a free-standing rule which would apply to cyber operations," as is the case with SolarWinds (2020) and Salt Typhoon (2024).¹² In the Manual's treatment of influence operations, the group agreed that purposefully dishonest information fed to the population of one state by another state might be considered an infringement of the right to sovereignty, or an infringement of the prohibition on intervention, but the issue of thresholds was far from unanimous, and it was difficult to apply the traditional coercion-based law to cognitive manipulation.¹³

The UN Cyber Governance and Emerging International Criminal

Accountability for Cyber Operations

Since 2004, there has been a UN Group of Governmental Experts (GGE) which has concluded important reports stating that international law does apply to cyberspace (UNGGE, 2013) and has formulated eleven voluntary norms of responsible state behavior (UNGGE, 2015).¹⁴ The 2017 GGE failure – a disagreement over the applicability of IHL to state cyber operations – highlighted the existing geopolitical split, with Russia and China being opposed to IHL application and fearing it would validate state offensive cyber operations. In January 2026, the Lieber Institute noted: "states remain reluctant to re-engage with basic questions about the applicability of IHL to cyber operations" and that they have been "reaffirming without elaborating."

The ICC Office of the Prosecutor's 2025 Policy on Cyber-Enabled Crimes is also significant as it recognizes that cyberattacks against civilian infrastructure could be war crimes.¹⁵ The war in Ukraine, especially the attack on the Kyiv star

telecom provider that caused communications disruption and emergency warnings for millions of people in December 2023, is viewed as a potential prosecution case.¹⁶

Unpacking Information Warfare: Typology and Legal Classification

Information warfare can be broken down into three modalities for analytical purposes. Technical information warfare includes operations against digital infrastructure, including cyberattacks, intrusion operations, electronic warfare, and supply-chain compromises that are in compliance with the law. Second, cognitive information warfare, which attacks convictions and decision-making with "disinformation, psychological operations and the effects through AI-generated synthetic media is diffused, delayed and in real time not legally traceable. Thirdly, structural information warfare works systemically, by affecting governance, algorithm and laws, thereby changing norms.¹⁷

Russian strategic doctrine considers "information confrontation" a permanent state of competition between technical, psychological and narrative operations and does not differentiate between the times of peace and war, and plays with legal uncertainty as a strategic instrument.¹⁸ In Taiwan Strait contingencies, the PLA doctrine promotes "cognitive domain operations" for "cognitive superiority" by influencing enemy perceptions.¹⁹

Case Study: Salt Typhoon and the Legal Grey Zone (2024–2025)

The Salt Typhoon intrusion - attributed to Chinese state-sponsored actors - penetrated the core telecommunications infrastructure of at least nine major US carriers, providing access to the communications of senior US government officials. US and allied governments-imposed sanctions in January 2025. From an international-law perspective, Salt Typhoon illustrates the grey-zone problem: under the Tallinn Manual's approach, intrusion into core telecommunications networks may implicate sovereignty and inherently governmental functions, yet the operation remained below the 'armed attack' threshold triggering Article 51. The available responses - countermeasures, diplomatic protest, and sanctions - may therefore appear limited when compared with the strategic significance of the intrusion.

There is a recent case study in cognitive information warfare arising from the India-Pakistan confrontation in May 2025. This clash was a major South Asian

crisis where AI-created and fabricated content had a major role in influencing public opinion. From a legal perspective, the case illustrates a structural challenge: The case law on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) explains how to define conduct attributable to a state, but it is more difficult to apply the ARSIWA when disinformation is provided or amplified by commercially operated domestic media and platform users who are not state organs under the ARSIWA (Article 4) or who do not demonstrate state control under the ARSIWA (Article 8).²⁰ The issue is thus not the lack of attribution rules, but the evidentiary and institutional challenge of using a state-centric approach to attribution in a mixed information ecosystem.²¹

Case Study: Indian Media Fabrications — May 7–10, 2025

Documented false claims broadcast by major Indian television channels during Operation Sindoor: (1) Times Now Navbharat: Indian forces have entered Pakistan. (2) Zee News: Indian Army has captured Islamabad; Pakistan has surrendered. (3) Aaj Tak: Terrorists have commenced suicide attacks on Indian Army units. (4) Multiple channels aired the 2020 Beirut port explosion as footage of Indian strikes on Pakistani targets. (5) Israeli Iron Dome interception footage from 2021 was broadcast as live Indian air defence footage. (6) AI-generated deepfake videos depicted Pakistan's PM Shehbaz Sharif conceding defeat — fabricated using AI voice cloning and lip-sync technology. (7) Misinformation alleged India had struck Pakistan's Kirana Hills nuclear site, causing radioactive leakage. Sources: Al Jazeera Media Institute; Reuters Institute (Oxford); IFJ; South Asian Voices.

Pakistan is a case in point of how middle powers can be simultaneously targeted by cognitive operations from abroad and be internally fractured by information environments. In May 2025, during the crisis between India and Pakistan, there were fabricated claims that spread on social media. Deepfakes claimed to depict Pakistan's Prime Minister Shehbaz Sharif conceding defeat and there were fake claims that India had attacked the Kirana Hills nuclear facility in Pakistan. Various scenes were wrongly identified and were re-released, causing public panic and strategic confusion. The Bulletin of the Atomic Scientists and the International Federation of Journalists conducted investigations on how disinformation, and believing it by prominent leaders, can drive decision makers to escalation and miscalculation.²²

The lack of unity in the domestic information environment in Pakistan exacerbates these vulnerabilities. An analysis by the Center for International Media Assistance (CIMA) in 2019 indicated that approximately 65 per cent of Pakistanis aged 16–34 are getting their news online, where they are vulnerable to orchestrated disinformation campaigns. During the 2018 elections, fabricated stories about then-Prime Minister Nawaz Sharif and false claims about Cambridge Analytica's involvement persisted despite debunking. The government responded with a "Fake News Buster" Twitter account, which counters claims of lies.²³ The initiative was met with mixed responses, however, and also revealed that there is a lack of collaboration between government agencies, civil society and media outlets.

Institutional fragmentation in the cyber-governance architecture in Pakistan. The Prevention of Electronic Crimes Act (PECA 2016) and the National Cyber Security Policy 2021 are the underlying laws, and enforcement is spread thin between the Federal Investigation Agency's National Response Centre for Cyber Crime (NR3C), Pakistan Telecommunication Authority, Ministry of IT and Telecommunications, and provincial police forces. The Stimson Center's 2025 review highlights that PECA has no specific provisions for critical infrastructure protection and that NR3C suffers from resource limitations and has limited technical and judicial expertise. Furthermore, Pakistan is not a party to the Budapest Convention on Cybercrime and keeps stressing on sovereignty at international forums for cyber governance.²⁴

Pakistan has been working towards enhancing cyber resilience since 2023. It has participated in the Global Forum on Cyber Expertise (GFCE) in May 2023, which expresses its engagement in international cooperation in the field of Cyber capacity building. The Committee for Computer Emergency Response (CERT) Rules 2023 provided a legislative framework to establish a National Computer Emergency Response Team (NCERT) and it was announced that NCERT will be operational by mid-2025.²⁵ The rules are designed to establish a three-tiered (national, sectoral and organizational) cybersecurity framework in line with the principles of the United Nations and to streamline and facilitate the reporting of incidents and the analysis of threats and early-warning. The challenge in implementing these reforms will be the governing of coordination among agencies and involvement of the private sector in Pakistan.

Pakistan's relationship with international legal regimes is a delicate mix of sovereignty and cooperation. In a note verbatim to the UN Office for Disarmament

Affairs, Pakistan has reiterated that the principles of sovereign equality, non-intervention and peaceful settlement of disputes are fully applicable to Cyberspace in March 2023. It voiced its support for the development of a legally binding international instrument on responsible state behaviour, noted that international humanitarian law is applicable to cyber operations and urged to outlaw cyber-attacks which indiscriminately target critical civil infrastructure or use digital technologies to spread fear and chaos through disinformation.²⁶ The three positions correspond to Pakistan's traditional views about UN-led processes and its reservations about regional instruments such as the Budapest Convention.

In April 2026, Pakistan has raised the alarm at the United Nations Committee on Information about the impact of technological advancements on the spread of disinformation, misinformation and hate speech, which has eroded public trust and social cohesion.²⁷ The delegation noted its special concern regarding the use of digital platforms in context of foreign occupation and conflict and the use of artificial intelligence, deepfakes and synthetic media to spread falsehoods. Pakistan requested the application of the Secretary-General's Global Principles for Information Integrity in an inclusive manner, the promotion of media and digital literacy and increased cooperation with technology companies. It vowed to collaborate with the UN system for a truthful and inclusive information environment.

But there are significant structural problems. Reporters Without Borders has reported the cases of journalists and critics being prosecuted under PECA, thereby showing how fake news laws can be used to stifle political dissent.²⁸ Despite efforts to combat disinformation in Pakistan, capacity limitations, poor inter-agency coordination and insufficient public media literacy continue to impede the country's capacity to fight disinformation. Historical animosities and echo chambers contribute to making it hard to be resilient to the cross-border disinformation campaigns. This will not only need to be complemented by enhanced technical protective measures but also inclusive governance, independent media fact checking, Track 1.5 diplomacy in times of crisis and regional cooperation to develop common standards for countering disinformation.

Pakistan's international legal stance is sovereignty oriented yet is mindful of the cooperative approach. It will support UN-led frameworks like the Open-Ended Working Group and the Group of Governmental Experts and is against unilateral norms and favours regional cooperation.²⁹ There have been suggestions

by analysts to create a “cybersecurity credits” model and a South Asian Cyber Security Network as a means to encourage cooperation by rewarding responsible behavior. Through national CERT, cooperation through GFCE, and legal reforms that will balance rights with security, Pakistan will be better equipped to navigate the complex terrain of information warfare.

Comparative Case Analysis: Three Modalities, Three Legal Gaps

The three main cases show that reading comparatively, information warfare does not create a single legal problem. Rather, modality, effects, and the nature of the relationship between the operator and the state determine which rules and evidentiary challenges are applicable. The comparison below demonstrates the analytical role of the cases as opposed to being a collection of illustrations.

Dimension	Stuxnet (2009-2010) ³⁰	Salt Typhoon (2024-2025) ³¹	India-Pakistan (May 2025) ³²
Primary Modality	Technical / cyber-physical	Technical / infrastructure intrusion	Cognitive / AI-disinformation
Principal Target/Effect	Nuclear enrichment infrastructure; physical damage	Core telecommunications and sensitive communications	Public perception, crisis narratives, and strategic signalling
Central Legal Issue	Use-of-force threshold and attribution	Sovereignty, attribution, and below-threshold strategic harm	State responsibility for mixed state/private information ecosystems
IHL Relevance	Potentially significant where linked to armed conflict or attack effects	Generally limited absent armed-conflict nexus	Context-dependent; strongest where content affects conduct of hostilities or civilian protection
Regulatory Gap Exposed	Classification of cyber effects and lawful response	Mismatch between strategic harm and available legal response	Difficulty translating cognitive and platform-mediated harm into state-centric legal categories

There is a common pattern in the comparison. Stuxnet is particularly pressing on the cyber – use of force – armed attack nexus due to its physical impact. Salt Typhoon puts more emphasis on sovereignty and attribution – given that strategic harm can be significant even if the operation fails to meet the Article 51 criteria. The Indian-Pakistan situation illustrates another issue: cognitive effects, even without a straightforward application of the traditional state-attribution norms, can lead to panic, misperception, and escalation in activity of commercially run media and in the use of diffused platform users. Thus, the cases confirm the central argument of the article that the problem is not that there is no law at all, but legal fragmentation.

The Attribution Problem

According to the articles of the International Law Commission (ILC) on the Responsibility of States for Internationally Wrongful Acts (ARSIWA, 2001), States are internationally responsible for internationally wrongful acts committed on their behalf. In the ICJ Nicaragua case (1986), very strict “effective control” rule was established, implying that the State must directly order or control the specific operation.³³ The overall control test, adopted in the case of Tadić (1999), is an “overall control” test in which general direction or support may suffice. States can then be strongly involved in cyber operations without being held legally liable, as it is often hard to establish direct and specific control over the cyber operation.³⁴

Technical attribution – improved through malware signatures, infrastructure analysis, language patterns and operational timing. However, it is more difficult to fulfill the ARSIWA legal attribution. It is often classified, false-flag operations, such as Olympic Destroyer malware, was deliberately designed to implicate North Korea, China and other actors at the same time, mislead attribution, and the ICJ effective control test demands proof of direct state direction, which can't always be publicly provided.³⁵

Most significantly, attribution uncertainty is strategically used to prevent victim states from mounting a lawful response. States use proxy groups, including hacker groups, patriotic volunteers, and cyber mercenaries, to provide deniability.³⁶ Russia's GRU-Fancy Bear (APT28) and FSB-Cozy Bear (APT29) connections are examples of such efforts to evade ARSIWA Article 8 attribution criteria.

Strategic Effects and Legal Risks

Realistically, information warfare is a means of power projection other than armed force. North Korea's Lazarus Group has had a significant cyber capability below kinetic conflict thresholds, including the Sony Pictures attack in 2014, the Bangladesh Bank heist (\$81 million) in 2016, and the WannaCry ransomware in 2017, which caused \$4 billion worth of damages.³⁷

With the advent of synthetic media in AI comes a qualitatively new level of cognitive information warfare. The WEF March 2026 analysis noted that deepfakes have reached a critical juncture in 2026 – they are realistic, ubiquitous, and part of the normal landscape of electoral and military competition. A deepfake video of the winner withdrawing, using fake footage from a broadcaster, was used in Ireland's presidential elections in 2025.³⁸

The June 2025 Iran conflict was the first time deepfakes were used as a tactical military tool, as hundreds of videos were produced in two weeks to create false impressions of Iranian and Israeli military victories and to boost morale.³⁹ This gives rise to legal questions on Additional Protocol I: do they constitute perfidy as provided in Article 37 or prohibited acts of psychological terror against civilians as provided in Article 51(2)? According to a study published in *Laws* (MDPI, November 2025), while deepfakes mimicking surrender are in violation of IHL, the majority of the cognitive warfare content falls into a legal grey zone where it is not clearly defined by current treaty law.

The epistemic nature of international law relies on facts for judicial reasoning and state attribution, and information warfare undermines the facts on which it is based. Where disinformation and synthetic evidence through AI is pervasive, it simply does not get in the way of individual cases, but it undermines the legal reasoning itself. A Bloomsbury Intelligence and Security Institute study released in January 2026 found that 'epistemic infrastructure degradation' is the biggest long-term strategic threat posed by AI-powered information warfare.

The Collapse of the Offensive-Defensive Binary

The *jus ad bellum* aspects of the UN Charter assumes a distinct order: armed attack and legitimate defence. Information warfare disrupts this logic: Operations are extended, cumulative, and below the legal threshold until a kinetic conflict is realized.⁴⁰ Under existing frameworks, the Volt Typhoon intrusion – that allowed pre-positioning access to U.S. critical infrastructure for possible activation

in a Taiwan conflict scenario – is strategically akin to mining a harbor or pre-deploying forces to an enemy's border, but is legally hard to classify.

The US Cyber Command doctrine of "persistent engagement" is based on continuous operations within adversary networks, rather than reactive operations in response to crises, a departure from the Article 51 paradigm of discrete armed attack and self-defense. Strategically defensive, operationally offensive and continuous.⁴¹ This raises legal questions about whether the activity constitutes a violation of sovereignty under Tallinn Manual Rule 4, but the U.S. does not wish to endorse any interpretation to maintain the flexibility of operations.

The EU's Digital Services Act (2022/2065), effective from 2024, will require large online platforms, including social media, to observe due diligence in relation to disinformation, which has been described by Chinese and Russian diplomatic statements as ideologically-driven interference in sovereign information governance.⁴² Under the legal notion of non-intervention, there is no operational threshold to identify when non-intervention turns into unlawful intervention.

Digital Sovereignty and Competing Models of Information Governance

The issue of digital sovereignty shows that there is no universal notion of sovereignty in the cyber world or of the sovereignty over cross-border information flows. Sovereignty is not just related to a rule of territorial intrusion, but it is also about control over digital infrastructure, platform regulation, data and algorithms, and the capacity of states to safeguard their political and social information environment. Cognitive and structural information warfare are examples of this meaning where the 'target' might not be physically damaged but access, visibility or public trust is.

In practice, there are competing models in the States. The United Kingdom's stance, as mentioned in the context of the Tallinn Manual, is against the belief that sovereignty ought to be a standalone rule for any cyber intrusion, and the US persistent-engagement doctrine focuses on the notion of ongoing operational access to an adversary network. In the Russian and Chinese views, more emphasis is placed on the state control of information space and on information or cognitive competition that never stops.⁴³ The new EU approach is regulatory – the Digital Services Act and the AI regulation aim to assert control via obligations for platforms to perform due diligence, transparency and labelling. Pakistan's stance is

sovereignty-driven and pragmatic, emphasizing respect for sovereign equality and non-interference, while also engaging in UN-led cyber activities and advocating for enhanced international norms.⁴⁴

These distinctions have legal significance since they can influence the definition of an unlawful intrusion, a legitimate regulation, or a permissible counter-information activity. They also make the establishment of customary rules difficult: the same regulatory action can be understood by one state as a protection of the information environment and by another as an interference on the information governance of the sovereign state. Comparative state practice thus further underscores the importance of separating territorial sovereignty, political non-intervention, control of critical digital infrastructure, and regulation of private platforms that are operated from a country, from a single consolidated doctrine of 'digital sovereignty'.

In terms of information warfare, this means that the element of sovereignty has to be viewed in conjunction with platform power. Meta, Google, X, TikTok and other private entities affect access, amplification and moderation internationally, but their powers do not easily map onto the state-to-state logic of international law. The new regime is therefore plural – state sovereignty, international legal rules, domestic regulation, private platform governance are all overlapping. This is not only an institutional issue but also is part of the substantive law loophole that any future information-warfare regime will have to plug.

Norm Formation and the Way Forward

Process Theory and Norm-Formation

McDougal and Lasswell were process-oriented; they saw international law developing in state claims and responses, and scholars such as Harold Koh and Duncan Hollis extended the process-oriented view of international law to cyberspace. Collective attribution statements by States such as the United States (US), the United Kingdom (UK), the European Union (EU) and allied governments are legal claims, political assertions, and contributions that help define the contours of emerging customary international law.⁴⁵

The Lex Specialis Imperative

The fragmentation highlighted in this article opens up the question of the presence of a *lex specialis* oriented regime: treaty and customary rules particularly adapted to the nature of information warfare. The goal would not be to replace the UN Charter, state responsibility or IHL, but to explain how they interact and fill in the gaps that are constantly repeated. There are four concrete measures which are worth considering.⁴⁶

First, a binding treaty that bars information operations against elections and democratic infrastructure, as Russia's Internet Research Agency did in 2016, in European elections (2024–2025), and in Ireland's presidential election (2025) using AI.

Second, an International Cyber Attribution Mechanism, similar to the OPCW Investigation and Identification Team, should be established to give UN-backed technical attribution that correlates with various levels of proof that will be relevant in diplomatic, sanctions, and ICC settings.

Thirdly, there should be an interpretation and, if required, supplementation of Additional Protocol I, Article 54 to also cover digital systems on which such objects are essential to civilian survival. The most obvious examples are hospital management and water-treatment control systems, where the loss of their digital functions would have the same humanitarian consequences as an actual attack on the system. Where disruption foreseeably impacts essential civilian services, there should be separate and carefully-defined protections for broader critical systems, such as financial clearing infrastructure.

Fourth, there is a need for more clarity and guidance regarding the use of synthetic media generated by AI in armed conflict, which further includes Additional Protocol I, Article 37–38 on perfidy and misuse of protected signs. Special attention should be paid to deepfake videos aimed at feigning surrender, fabricating war crimes or interfering with lifesaving civilian communications. The EU AI Act's labelling requirements are set to come into effect in 2026, offering a regulatory framework for reference, although these will be limited to a specific jurisdiction and do not address the rules that apply to the state's military use.

Global Administrative Law and Platform Governance

Any framework worth its name should take into account the central role of private entities like Meta, Google, X and TikTok etc., which exercise de facto control over the global information environment, and are not subject to complete international legal oversight. There is reason to believe that the Global Administrative Law (GAL) framework will provide a basis for transparency in algorithms, disclosure of state-sponsored content and audit-access mechanisms increasingly that resemble converging legal requirements and not just policy preferences. EU Digital Services Act based on due diligence for large platforms with more than 45 million users in the EU offers a regulatory model to lower the systemic vulnerability to Information Warfare, if internationalized.⁴⁷

Incremental Normativity

According to constructivist norm life-cycle model of Martha Finnemore and Kathryn Sikkink, norms are more effectively built up through a gradual process of emergence, cascade, and internalization. There is increasing consensus against hospital ransomware as evidenced by the evolving Counter Ransomware Initiative (CRI), which has 68 states by 2024.⁴⁸ These types of incremental norms may be more achievable than broad and all-encompassing treaties, providing a calculus of compliance and basis for future legally binding norms.

A State of Intermediacy and Normative Pluralism

In the last years, ICRC scholarship started to think of cyberspace as a ‘state of intermediacy’ where the demarcation of war and peace becomes increasingly blurred. Low-intensity cyber and information operations take place on an ongoing basis and rarely meet the threshold of armed conflict that would normally invoke the law of armed conflict.⁴⁹ Consequently, the field of information operations is one in which the international humanitarian law, human rights law and domestic regulatory regimes overlap but none is exhaustive. The war/peace dichotomy is undermined by ongoing competition for the informational advantage, and the result is normative pluralism: traditional international law sits side-by-side with soft law instruments, platform terms of service and domestic laws to regulate conduct.

Information operations fall into many instances into what legal scholars describe as a “grey zone” for two reasons that are related. Firstly, many cyber and influence operations take place outside of an armed conflict where IHL is not the regime in place. Second, whether a cyber (or cognitive) operation constitutes an

“attack” under conduct-of-hostilities rules can depend on its intended effects and is still disputed with regard to non-physical effects. The Lotus principle sometimes is cited to say that as long as a given action is not expressly forbidden by a rule, it is still permitted. Operating without the destruction of physical property, operations for the manipulation of perception, attitudes, and behavior consequently reveal areas where current rules of the treaties give only limited guidance.⁵⁰ Propagandistic broadcasts and civilian lies on social media are legitimate, as long as they do not rise to the level of an attack, according to the commentary to the Tallinn Manual. However, they can be a source of confusion in times of crisis and hamper civilian protection. Scholars advocate a policy against information operations against civilians that pose a threat to their life or are disproportionate to the expected benefits.

Thus, the information warfare creates a state of what can be called “normative pluralism” where no one legal system is any longer in regulatory control. Cyber and information operations operate in multiple regimes, and States instead find themselves in overlapping regimes of IHL, human rights law, cyber regulation, data governance and private platform authority. Quasi-public obligations for private companies exist, such as the EU Digital Services Act and Artificial Intelligence Act, which impose due-diligence obligations on large platforms to moderate disinformation and label media produced with AI.⁵¹ A holistic approach to information warfare will thus need to combine these regimes and acknowledge that a host of actors such as States, international organisations, technology firms and civil society have a role to play in creating stability in the information environment.

Reconceptualizing Information Warfare and Societal Access

Moreover, the notion of ‘information warfare’ is not even stable in terms of its conceptual architecture. Richard W. West notes that the United States has no consistent definition: Laws and military doctrine distinguish disinformation and psychological operations, and cyber-operations, and other regulatory frameworks are focused on harmful speech. According to West, today's information warfare is not just about speech; it's about access to information. Disinformation operations use algorithmic curation, metadata profiling and micro-targeting to influence informational exposure — not just spread misinformation.⁵²

The international law consequences are significant. Regulating content alone cannot address algorithmic amplification and data-driven profiling. This

means the information environment is increasingly in need of regulation, not just of content, but of algorithmic amplification, data extraction and recommendation infrastructures. According to West, the law should cover not just what is being said, but also the ‘infrastructure that delivers and amplifies’ communication.⁵³ The EU Digital Services Act and AI Act are early moves to impose such obligations, and global norms are still in their infancy.

Social trust and epistemic infrastructure are information operations' targets. These operations lead to the destruction of the epistemic infrastructure, contribute to polarization, provide fuel to hate speech and hinder democratic deliberation. There is, therefore, a clear need to combine media literacy, public education and cross-border cooperation with normative regulation in effective legal responses. Resilience thus requires taking account of information warfare not just as a military tool, but also as an attack on the cognitive sovereignty of societies.⁵⁴

Conclusion

This article has suggested that information warfare is now more than a side-line to conventional warfare. The interplay between technical, cognitive and structural aspects of operations blurs the line between peacetime competition and armed conflict, and the current legal rules are dispersed between a range of fields including sovereignty, non-intervention, state responsibility, *jus ad bellum*, IHL, human rights law, domestic law and platform governance. The fundamental issue is not thus a total lack of potential law, but rather fragmentation, with each of the regimes setting different thresholds; different understandings of “harm”; different evidentiary requirements; and different assumptions about who is involved.

The comparative cases confirm that. Stuxnet was a good example of the challenges in defining a cyber operation that had physical consequences, while Salt Typhoon was a good example of the grey area between strategic cyber intrusions and the armed-attack threshold and the May 2025 India-Pakistan Confrontation is an example of how cognitive and AI-driven information effects can be a driver for escalation and not so easy to classify within state-centric rules. IHL is useful when information operations are linked to armed conflict and have an impact on civilians or the conduct of hostilities, but it cannot govern the entirety of the activities below threshold. Different conceptions of digital sovereignty also complicate the common rules' development. This means that a path forward must be a mix of incremental norm building and a reform agenda oriented toward a *lex specialis*: more robust attribution, more explicit protection of critical civilian digital systems, rules on

synthetic media in armed conflict, and more accountability for platform mediated information operations. The main thesis of the article is that the future legal framework should not artificially distinguish between the technical and cognitive aspects of information warfare.

References

- ¹ Qasim Rajoka, “Disinformation and Deepfakes: Improving Crisis Communications in India and Pakistan,” *Bulletin of the Atomic Scientists*, January 29, 2026, <https://thebulletin.org/2026/01/disinformation-and-deepfakes-improving-crisis-communications-in-india-and-pakistan/>.
- ² Tilman Rodenhäuser and Kubo Mačák, “Even ‘Cyber Wars’ Have Limits. But What If They Didn’t?,” *Humanitarian Law & Policy Blog*, International Committee of the Red Cross, March 9, 2021, <https://blogs.icrc.org/law-and-policy/2021/03/09/even-cyber-wars-have-limits/>
- ³ Henning Lahmann, “Protecting the Global Information Space in Times of Armed Conflict,” *International Review of the Red Cross* 102, no. 915 (2020): 1227–1248, <https://international-review.icrc.org/articles/protecting-the-global-information-space-in-times-of-armed-conflict-915>
- ⁴ International Committee of the Red Cross, “International Humanitarian Law and Cyber Operations during Armed Conflicts,” November 28, 2019, <https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts>
- ⁵ Martha Finnemore and Duncan B. Hollis, “Constructing Norms for Global Cybersecurity,” *American Journal of International Law* 110, no. 3 (2016): 425–479, <https://doi.org/10.1017/S0002930000016894>
- ⁶ United Nations, *Repertory of Practice of United Nations Organs, Supplement No. 7, Volume I, Article 2(4)* (New York: United Nations), https://legal.un.org/repertory/art2/english/rep_supp7_vol1_art2_4.pdf
- ⁷ Camille Mulcaire, “How ‘Westphalian’ Is the Westphalian Model?,” *E-International Relations*, February 3, 2014, <https://www.e-ir.info/2014/02/03/how-westphalian-is-the-westphalian-model/>
- ⁸ International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, I.C.J. Reports 1986, p. 14, June 27, 1986, <https://www.icj-cij.org/case/70>
- ⁹ Duncan Hollis, “Is a Use of Force the Same as an Armed Attack in Cyberspace?,” *Opinio Juris*, April 28, 2012, <https://opiniojuris.org/2012/04/28/is-a-use-of-force-the-same-as-an-armed-attack-in-cyberspace/>
- ¹⁰ Michael N. Schmitt et al., eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), <https://doi.org/10.1017/9781316822524>.
- ¹¹ Schmitt et al., *Tallinn Manual 2.0*
- ¹² Michael J. Glennon, “The Blank-Prose Crime of Aggression,” *European Journal of International Law* 35, no. 1 (2024), <https://www.ejil.org/article.php?article=3298&issue=162>
- ¹³ Dan Efrony and Yuval Shany, “A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice,” *American Journal of International Law* 112, no. 4 (2018): 583–657, <https://doi.org/10.1017/ajil.2018.86>.
- ¹⁴ United Nations Group of Governmental Experts, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174 (2015), <https://digitallibrary.un.org/record/799853?ln=en>.
- ¹⁵ International Criminal Court. (2025). *Questions and answers: The ICC Office of the Prosecutor’s policy on cyber-enabled crimes under the Rome Statute*. Retrieved from <https://www.icc-cpi.int/about/otp/questions-and-answers-the-icc-office-of-the-prosecutors-policy-on-cyber-enabled-crimes-under-the-rome-statute>
- ¹⁶ “KyivStar Cyber Attack: A Deep Dive into Cyber Warfare in Ukraine,” *AFCEA International*, July 1, 2025, <https://www.afcea.org/signal-media/cyber-edge/kyivstar-cyber-attack-deep-dive-cyber-warfare-ukraine/>.

- ¹⁷ Jason Healey, "Cyber Effects in Warfare: Categorizing the Where, What, and Why," *Texas National Security Review*, April 16, 2025, <https://tnsr.org/2024/08/cyber-effects-in-warfare-categorizing-the-where-what-and-why/>.
- ¹⁸ International Institute for Strategic Studies, *Russia's Information Confrontation Doctrine in Practice* (London: International Institute for Strategic Studies, 2025), <https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/06/russias-information--confrontation-doctrine--in-practice-/09-pub25-077-russia-information-confrontation-v5.pdf>.
- ¹⁹ "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," *Jamestown Foundation*, July 22, 2025, <https://jamestown.org/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/>.
- ²⁰ International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, *Yearbook of the International Law Commission*, vol. 2, part 2 (2001).
- ²¹ "SAV Q&A with TCA Raghavan: One Year After the May 2025 Crisis," *South Asian Voices*, May 7, 2026, <https://southasianvoices.org/sav-qa-tca-raghavan-05-07-2026/>.
- ²² Anirban Nag, "Old Video Surfaces as India's Attack on Kirana Hills with Radiation Risk; Fact Check," *DigitEye India*, May 24, 2025, <https://digiteye.in/old-video-surfaces-as-indias-attack-on-kirana-hills-with-radiation-risk-fact-check/>.
- ²³ Daniel O'Maley, "Mapping Digital Disinformation around Elections: A Case Study of Pakistan's 2018 General Elections," *Center for International Media Assistance*, November 5, 2019, <https://www.cima.ned.org/publication/mapping-online-disinformation-around-pakistans-2018-general-elections/>.
- ²⁴ Rabia Malik, "Strategic and Structural Challenges of Cyber Warfare in Pakistan," *CISSAJK*, May 5, 2026, <https://cissajk.org.pk/strategic-and-structural-challenges-of-cyber-warfare-in-pakistan/>.
- ²⁵ Muhammad Asif, "Cyber Security Governance Challenges in Pakistan," *Khyber Journal of Public Policy* 3, no. 1 (2024), <https://nipapeshawar.gov.pk/KJPPM/PDF/CIP/P37.pdf>.
- ²⁶ Gulraiz Iqbal, "How Does International Law Byte into Pakistan's Cyber Governance?," *Stimson Center*, June 24, 2025, <https://www.stimson.org/2025/how-does-international-law-byte-into-pakistans-cyber-governance/>.
- ²⁷ Permanent Mission of Pakistan to the United Nations, "Statement by Pakistan at the 48th Session of the UN Committee on Information," *United Nations eStatements*, April 27, 2026, https://estatements.un.org/estatements/12.0080/20260427150000000/vLbjyKAt/XybfeoMkFMK_nyc_en.pdf.
- ²⁸ Reporters Without Borders, "Pakistan: Multiple Journalists and a Dozen YouTube Channels Targeted under PECA in Less than a Year," *RSF*, October 3, 2025, <https://rsf.org/en/pakistan-multiple-journalists-and-dozen-youtube-channels-targeted-under-peca-less-year>.
- ²⁹ United Nations Office for Disarmament Affairs, *Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025: Final Substantive Report* (New York: United Nations, 2025), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/UNODA.pdf.
- ³⁰ Joshua Alvarez, "Stuxnet: The World's First Cyber Weapon," *Center for International Security and Cooperation (CISAC)*, *Stanford University*, February 3, 2015, <https://cisac.fsi.stanford.edu/news/stuxnet>.
- ³¹ Meghal Donde, *Salt Typhoon Across the Internet: What AIDE Honeypots Reveal About a Persistent State-Linked Campaign* (Global Cyber Alliance, December 2025), <https://globalcyberalliance.org/wp-content/uploads/2025/12/PUBLIC-REPORT-Salt-Typhoon-Across-the-Internet.pdf>.
- ³² Gull-e-Areeba and Ahmed Waqas Waheed, "Weaponizing Information: A Study of Disinformation and Information Warfare between India and Pakistan," *Margalla Papers* 30, no. 1 (2026): 57-71, <https://margallapapers.ndu.edu.pk/index.php/site/article/view/373>.

-
- ³³ International Committee of the Red Cross, “ICJ, Nicaragua v. United States,” *How Does Law Protect in War? Online Casebook*, accessed May 10, 2026, <https://casebook.icrc.org/case-study/icj-nicaragua-v-united-states>
- ³⁴ International Criminal Tribunal for the Former Yugoslavia, “Prosecutor v. Duško Tadić,” *How Does Law Protect in War? Online Casebook*, International Committee of the Red Cross, accessed May 10, 2026, <https://casebook.icrc.org/case-study/icty-prosecutor-v-tadic>
- ³⁵ Andy Greenberg, “The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History,” *WIRED*, October 17, 2019, <https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>
- ³⁶ Scott J. Shackelford et al., “Cyber Peace and International Cybersecurity Governance,” *Journal of Cybersecurity* 8, no. 1 (2022): tyacoo7, <https://academic.oup.com/cybersecurity/article/8/1/tyacoo7/6695166>
- ³⁷ U.S. Department of Justice, “North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions,” *Office of Public Affairs*, September 6, 2018, <https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>
- ³⁸ Eleonore Pauwels, *Preparing for Next-Generation Information Warfare with Generative AI*, CIGI Paper No. 310 (Waterloo, ON: Centre for International Governance Innovation, December 2024), <https://www.cigionline.org/static/documents/Pauwels-Nov2024.pdf>
- ³⁹ Thomas Copeland, “AI-Generated Iran War Videos Surge as Creators Use New Tech to Cash In,” *BBC Verify*, March 7, 2026, <https://www.bbc.com/news/articles/ckg8wvz427v0>
- ⁴⁰ William K. Lietzau, “Old Laws, New Wars: *Jus ad Bellum* in an Age of Terrorism,” *Max Planck Yearbook of United Nations Law* 8 (2004): 383–455, https://www.mpil.de/files/pdf/mpunyb_lietzau_8.pdf
- ⁴¹ Thomas F. Lynch III, “Forward Persistence in Great Power Cyber Competition,” *The Cyber Defense Review* 9, no. 4 (2024): 81–118, <https://www.jstor.org/stable/48836260>
- ⁴² European Commission, “The Digital Services Act,” *European Commission Digital Strategy*, accessed May 10, 2026, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>
- ⁴³ Michael N. Schmitt, *Trends in International Law for Cyberspace* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2019), https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf
- ⁴⁴ Ashkan Shokri, “Sovereignty in Cyberspace from the Viewpoint of International Law,” *Asian Journal of International Law* 16, no. 2 (2026): 326–356, <https://doi.org/10.1017/S2044251325100556>
- ⁴⁵ Oxford Process on International Law Protections in Cyberspace, *Compendium: Major Existing Legal Instruments and Other Documents Applicable to Cyberspace* (Oxford: ELAC and University of Oxford, 2022), <https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf>
- ⁴⁶ United Nations Institute for Disarmament Research, *Cyberwarfare and International Law* (Geneva: UNIDIR, 1999), <https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf>
- ⁴⁷ Benedict Kingsbury, “The Concept of ‘Law’ in Global Administrative Law,” in *The Exercise of Public Authority by International Institutions: Advancing International Institutional Law*, ed. Armin von Bogdandy et al. (Heidelberg: Springer, 2010), <https://iilj.org/wp-content/uploads/2016/08/Kingsbury-GAL-Dimensions-of-International-Organizations-Law.pdf>
- ⁴⁸ Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change,” *International Organization* 52, no. 4 (1998): 887–917, <https://library.fes.de/libalt/journals/swetsfulltext/5333873.pdf>
- ⁴⁹ International Committee of the Red Cross, “Cyber and Information Operations,” *ICRC Law and Policy*, accessed May 10, 2026, <https://www.icrc.org/en/law-and-policy/cyber-and-information-operations>

-
- ⁵⁰ Beatrice Walton, "Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law," *Yale Law Journal* 126 (2017): 1460–1535, <https://yalelawjournal.org/note/duties-owed-low-intensity-cyber-attacks-and-liability-for-transboundary-torts-in-international-law>
- ⁵¹ European Parliament Research Service, *Artificial Intelligence and Hybrid Threats: AI-Generated Content in Information Warfare* (Brussels: European Parliament, 2025), [https://www.europarl.europa.eu/thinktank/en/document/ECTI_ATA\(2025\)778577](https://www.europarl.europa.eu/thinktank/en/document/ECTI_ATA(2025)778577)
- ⁵² Richard W. West, "Beyond Fighting Words: Reconceptualizing Information Warfare and Its Legal Barriers," *National Security Law Journal* 7, no. 2 (2019): 265–322, <https://www.nslj.org/wp-content/uploads/West.BeyondFightingWords-ReconceptualizingInformationWarefareanditsLegalBarriers-1-2.pdf>
- ⁵³ Guido Perboli, Nadia Simionato, and Serena Pratali, "Navigating the AI Regulatory Landscape: Balancing Innovation, Ethics, and Global Governance," *Economic and Political Studies* 13, no. 4 (2025): 367–397, <https://doi.org/10.1080/20954816.2025.2569584>
- ⁵⁴ Anaïs Tschanz and Tilman Rodenhäuser, "How Harmful Information on Social Media Impacts People Affected by Armed Conflict," *International Review of the Red Cross* 106, no. 926 (2024), <https://international-review.icrc.org/sites/default/files/reviews-pdf/2024-12/how-harmful-information-on-social-media-impacts-people-affected-by-armed-conflict-926.pdf>