Explaining the Challenges of the International Legal System in the Digital Age

1. Akbar Adibi*: Assistant Professor, Department of Law, Payam Noor University, Tehran, Iran

*Correspondence: a.adibi@pnu.ac.ir

Abstract

Technological developments in the 21st century have confronted the traditional structure of the international legal system with unprecedented challenges. The advent of the digital age—characterized by the expansion of cyberspace, the empowerment of global platforms, the transformation of warfare patterns and security threats, and the emergence of new concepts such as "cyber sovereignty" and "digital human rights"—necessitates a serious reconsideration of existing legal concepts and mechanisms. Within this context, six fundamental challenges can be identified: the absence of clear sovereignty in cyberspace, ambiguity in the application of international responsibility rules, the inability to guarantee and protect human rights in the digital environment, the lack of effective regulation over the operation of global platforms, the absence of international consensus regarding behavioral norms in cyberspace, and finally, the fundamental transformation of the concept of war and international security. These challenges not only underscore the relative inefficiency of traditional international law in confronting digital developments, but also highlight the urgent need to revise its principles, sources, and actors. If the international community fails to design new mechanisms to respond to these developments, the risk of eroding international trust, increasing legal inequality, and the emergence of new global tensions will escalate. Accordingly, the future of international law hinges on its ability to adapt to the complex realities of the digital world.

Keywords: Digital Age; Cyber Sovereignty; Open Internet; Global Platforms; Human Rights.

Received: 01 November 2024
Revised: 28 January 2025
Accepted: 05 February 2025
Published: 25 March 2025

Citation: Adibi, A. (2025). Explaining the Challenges of the International Legal System in the Digital Age. *Legal Studies in Digital Age,* 4(1), 1-11.

1. Introduction

The rapid evolution of modern digital technologies in recent decades has significantly disrupted the traditional foundations of many legal, political, economic, and cultural systems. Particularly in the realm of international law, the globalization of information and communication technologies, the emergence of cyberspace as a new domain of transnational interactions, and the expanding role of non-state actors such as tech corporations have introduced unprecedented challenges to legal structures grounded in classical principles of sovereignty, territorial jurisdiction and responsibility, and state-centric relations. Against this backdrop, a fundamental question arises: to what extent has the international legal system been able to adapt to the new conditions of the digital world and respond to its demands? This question not only casts doubt on the sufficiency of existing rules but also calls for a reexamination of concepts such as sovereignty, jurisdiction, security, international responsibility, and even the nature of international legal actors (Kuner, 2015). Technological advances in fields such as artificial intelligence, big data, blockchain, the Internet of Things, and satellite communications have shifted much of human and international interaction into a digital and transnational sphere—a space in which traditional geographic borders are rendered meaningless and unprecedented fluidity in data, power, information, and responsibility has emerged (Schmitt, 2013). Under such conditions, the concept of “territory” in international law—which has historically depended on land and physical borders—faces foundational challenges. For example, cyberattacks originating from an anonymous or untraceable source can disrupt the critical infrastructure of another state without the possibility of accurate attribution or definitive linkage to any state. Does the current international legal system possess the capacity to respond to such scenarios? Furthermore, the digital space has become a novel arena for human rights violations. Digital surveillance tools, internet censorship, behavioral analytics, and the widespread deployment of classification algorithms all present serious challenges to freedom of expression, privacy, and the protection of human dignity (De Hert & Papakonstantinou, 2012). The core question becomes: how can individual rights be protected in a space governed by tech corporations, using rules designed for the era of nation-states? Can non-state actors that shape digital life be held accountable for violations of human rights? Another challenge pertains to jurisdiction and responsibility within international law. In the traditional framework, each state is considered responsible for actions occurring within its territory or originating from it. However, in the digital world, activities may traverse multiple servers across different countries, take place in cloud infrastructure, and be carried out by anonymous actors. Consequently, traditional rules on attribution of unlawful acts to states and the determination of international responsibility have lost much of their effectiveness (Tsagourias & Buchan, 2015). Is there a need to develop new principles for attribution, oversight, or compensation in cyberspace? And can such principles be harmonized with the accepted tenets of the UN Charter and customary international law? In this context, the lack of global consensus on regulatory rules for cyberspace has further intensified the crisis. While some countries advocate for “internet freedom” and the openness of the digital realm, others insist on “cyber sovereignty” and complete state control over domestic data and communications. This dichotomy presents a serious obstacle to the formulation of common and binding international rules for cyberspace governance. With the rising threats of cyber warfare, disinformation campaigns, and electoral interference, the question becomes more pressing: can international law offer the necessary tools for regulating this emerging domain? Thus, interrogating the challenges of international law in the digital age is not merely a technical or marginal concern—it reflects a structural transformation in the nature of international interactions. Identifying and analyzing these challenges is a necessary prerequisite for developing coherent, inclusive, and effective legal responses. What is clear is that failure to address these questions will expose international law to realities that lie beyond the reach of its current frameworks.

2. Materials and Methods

This study employs a descriptive-analytical method and relies on library-based sources to develop the article.

3. Lack of Clear Sovereignty in Cyberspace

The transformation brought by digital technologies, especially the expansion of cyberspace, has revolutionized communication, economic exchanges, information transfer, and even political power. However, alongside these changes, international law—which is built upon classical principles such as territorial sovereignty, state jurisdiction, and international responsibility—faces a fundamental challenge: the absence of clearly defined sovereignty in cyberspace. This absence has not only created legal instability in international relations but has also increased the opportunity for abuse by malicious actors—both state and non-state (Schmitt, 2013). The following sections examine various dimensions of this challenge, its legal implications, and ongoing efforts to address it.

3.1. The Concept of Sovereignty in International Law and the Challenge of Cyberspace

In traditional international law, sovereignty is defined as a state's exclusive authority to exert power, legislate, and exercise jurisdiction within its territorial boundaries (Crawford, 2006). This notion relies on the principle of independence and the equality of states, and it derives meaning from fixed geographic borders. However, due to its decentralized, borderless, and global structure, cyberspace fundamentally disrupts this premise. Data are transmitted across global networks; servers may be located in multiple countries; and actors can operate from anywhere in the world, often anonymously (Kulesza, 2017). Under these conditions, it becomes exceedingly difficult to determine which state exercises sovereignty over what segment of cyberspace, or which actions constitute violations of sovereignty. For instance, if a cyberattack is launched by an anonymous actor using infrastructure in State A to target the critical infrastructure of State B, does State A violate State B's sovereignty? Answering such a question requires clear rules regarding the attribution of cyber activities to states and the scope of cyber sovereignty—issues that remain highly contested (Tsagourias & Buchan, 2015).

3.2. Cyberspace: A Borderless Realm with No Clear Ownership?

One of the main reasons for the lack of clear sovereignty in cyberspace lies in the inherently transnational and borderless nature of this domain. Unlike air, sea, or outer space—which are governed by specific international legal regimes such as the Law of the Sea Convention or the Outer Space Treaty—cyberspace has yet to fall under any comprehensive and binding legal framework. Consequently, countries have adopted divergent approaches to the concept of "cyber sovereignty." States such as China and Russia emphasize national cyber sovereignty, arguing that every government should have full control over the data and digital infrastructure within its territory. In contrast, countries like the United States promote an open and global internet model in which the digital space is viewed as a global public good. This divergence in outlook has significantly hindered international efforts to develop shared principles governing sovereignty in cyberspace (Segal, 2017).

3.3. Cyberattacks and the Concept of Sovereignty Violation

Cross-border cyberattacks are one of the most illustrative manifestations of the sovereignty dilemma in cyberspace. While Article 2(4) of the United Nations Charter prohibits the use of force against the territorial integrity or political independence of states, the question remains whether a cyberattack constitutes a use of force or a violation of sovereignty. The influential Tallinn Manual, which explores the application of international law to cyberspace, represents one of the earliest systematic attempts to address this issue. It posits that certain cyber operations may amount to sovereignty violations if they cause significant material effects within the victim state's territory (Schmitt, 2017). Nonetheless, as these interpretations lack legal binding force and rely on non-obligatory commentary, the legal status of such operations remains ambiguous.

3.4. The Problem of Attribution and the Erosion of Accountability

A major obstacle to the effective exercise of sovereignty in cyberspace is the difficulty in accurately attributing cyber actions to states or other actors. Unlike physical attacks, which often leave concrete evidence of origin and perpetrator, cyber operations tend to be anonymous, dispersed, and deceptive. Attackers may use proxy servers, generate fake IP addresses, or even impersonate other states. This reality makes it extremely challenging to establish state responsibility for internationally wrongful acts in cyberspace (Jensen, 2015). As a result, victims of cyberattacks are left with a growing sense of legal helplessness, given that clear pathways for pursuing accountability are lacking. In the absence of established mechanisms for assigning responsibility, trust in international law is undermined, and the door opens for unilateral or retaliatory measures.

3.5. Absence of a Binding Legal Regime

At present, no global binding treaty specifically governs cyberspace. Initiatives such as United Nations expert working groups have produced a number of behavioral principles, but these are largely voluntary and lack universal consensus (United, 2021). Moreover, some states have accepted norms like "non-intervention" and "non-destructive use of technology" as voluntary behavioral codes, but the lack of enforcement mechanisms has weakened their effectiveness. Meanwhile, treaties such as the Budapest Convention on Cybercrime—adopted by the Council of Europe in 2001—represent a significant step in addressing cybercrime, but they are primarily focused on criminal aspects and inter-police cooperation. They do not explicitly address cyber sovereignty as understood under public international law (Council of, 2001).

3.6. Legal and Political Consequences of the Lack of Clear Sovereignty

The absence of a shared understanding and binding rules regarding sovereignty in cyberspace has serious implications for international peace and security. On the one hand, this condition has created a legal grey zone in which states can justify aggressive actions or deny responsibility. On the other hand, it has heightened the risks of geopolitical rivalry in the digital sphere and increased the likelihood of unintended or mistaken conflicts (Lewis, 2014). In the absence of clear sovereignty, even foundational principles such as non-intervention in internal affairs, freedom of information, and human rights are at risk of being eroded. For this reason, the international community must move toward developing a legal regime specific to cyberspace—one that simultaneously guarantees the legitimate sovereignty of states while also preventing the suppression of fundamental freedoms under the pretext of cybersecurity.

4. Ambiguity in Applying International Responsibility Rules

The digital transformation has profoundly altered the structure of international interactions. Emerging technologies such as the internet, decentralized communication networks, artificial intelligence, and big data have ushered the world into a new era in which traditional notions of geography, time, and even the actors of power have been redefined. Yet, international law—rooted in inter-state relations, sovereignty, and classical notions of responsibility—has not fully aligned itself with these emerging realities. One of the most pressing challenges in this context is the ambiguity in applying international responsibility rules to activities taking place in digital and cyber domains, where attribution, breach identification, and harm assessment are fraught with unprecedented complexities (Tsagourias & Buchan, 2015).

4.1. State Responsibility in International Law: Classical Concepts

International responsibility is a legal mechanism by which states are held accountable when they breach their international obligations, requiring them to provide reparations and restore the situation to its prior state. This system was structurally codified in the International Law Commission's 2001 Draft Articles on the Responsibility of States for Internationally Wrongful Acts (International Law, 2001). According to this document, three core elements are required for establishing state responsibility: the attribution of a wrongful act to a state, a breach of an international obligation, and the occurrence of damage. However, each of these elements encounters obstacles in the digital context. Data can traverse multiple countries, servers may be scattered across jurisdictions, and the identities of attackers may be falsified or remain anonymous. These conditions undermine the applicability of traditional legal rules.

4.2. The Challenge of Attribution in Digital Space

One of the most fundamental problems in the digital environment is determining who is responsible for a particular act—that is, the problem of attribution. In traditional international law, an act can be attributed to a state when it is carried out by official state organs or by groups operating under the effective control of the state. In the cyber domain, however, it is exceedingly difficult to determine whether a cyberattack was launched by a state or by a non-state actor, and if the latter, whether it was under the control of a state. The Tallinn Manual explicitly acknowledges that cyber attribution should follow existing international law standards, but in practice, there is often insufficient evidence to make such attributions (Schmitt, 2017). Moreover, cyberattacks can be conducted using proxy networks, botnets, or anonymizing tools, making it nearly impossible to trace the true origin (Jensen, 2015). In the absence of attribution transparency, the application of responsibility rules stalls. Victims cannot identify a responsible state from which to seek reparations, while perpetrators operate with impunity.

4.3. The Concept of "Breach" in Cyberspace

The second pillar of international responsibility involves the breach of an international obligation. In traditional contexts, state obligations are clearly defined through treaties or customary law. In cyberspace, however, there is still no global consensus on what types of cyber conduct constitute violations of international law. For instance, does unauthorized access to classified government data through cyber means constitute a breach of sovereignty? Do intrusions into a foreign banking system or energy grid amount to aggression? Some analyses argue that cyberattacks resulting in significant material harm could qualify as uses of force under Article 2(4) of the UN Charter (Tsagourias, 2016). Yet the boundary between a "hostile act" and a "breach" remains blurred, especially when such attacks originate from non-state actors whose state affiliations are unclear. Additionally, activities such as the spread of disinformation or data manipulation have serious consequences but are difficult to classify under traditional legal categories of breach. This conceptual gap leaves states without effective legal tools to respond to such harmful actions.

4.4. Damage and Reparation: Ambiguity in the Digital Environment

The third component of international responsibility is proving damage and executing reparations. In the digital realm, it is often difficult to define the extent and nature of harm. Many cyberattacks may result in data leaks, temporary disruptions, or non-material harm to reputation and public trust. But are such harms compensable? What forms of reparation are appropriate? Should the responsible party be required to restore lost data, provide financial compensation, or issue a formal apology? In traditional international law, there are well-established principles for reparation, including restitution, compensation, and satisfaction (Crawford, 2006). Yet applying these principles in cyber cases requires clarity about the nature and severity of the harm—something frequently lacking in both legal and technical terms. Furthermore, identifying the responsible party and securing reparations may require transnational cooperation, but most states are reluctant to act transparently regarding their cyber operations, particularly when national security is at stake (Kleffner & Dinniss, 2013).

4.5. Responsibility of Non-State Actors: Theoretical and Practical Gaps

Another major challenge in adapting international responsibility to the digital space concerns the role and status of non-state actors. In cyberspace, technology companies, hacker groups, and even individual users can exert global influence. Yet the traditional framework of international responsibility is primarily concerned with inter-state conduct. A key question arises: can such actors be held accountable under international law? Some scholars have attempted to expand the scope of state responsibility by invoking concepts such as "indirect participation" or "sponsoring states," thereby linking state accountability to private actors' conduct (Wilde, 2004). However, a binding legal framework that would clearly establish such responsibility for non-state actors in the digital domain has yet to be developed.

4.6. International Responses and Initiatives

In recent years, efforts have been made at the UN level to develop principles for responsible state behavior in cyberspace. Among these initiatives is the work of the Group of Governmental Experts (GGE), which has articulated norms such as respect for sovereignty, non-intervention, and the upholding of human rights in the digital space. However, these principles often lack enforcement mechanisms and continue to suffer from diverging interpretations and implementation. Additionally, the "Tallinn Manual 2.0" has sought to adapt existing international law to cyberspace, but since the manual is non-binding, it cannot definitively resolve the conceptual and legal gaps that persist (Schmitt, 2017).

5. Protection of Human Rights in the Digital Space

In the digital age, human rights have encountered challenges that are unprecedented in previous decades. Cyberspace has not only transcended geographical and political borders but also created a new realm for social, cultural, political, and economic interactions. While this deep transformation has provided opportunities to realize certain human rights—such as freedom of expression, access to information, and political participation—it has also introduced new threats to privacy, personal security, freedom of information, and even the right to identity (McGregor, 2021). The fundamental question remains whether the international legal system has provided an adequate, comprehensive, and realistic response to digital transformations, particularly in the area of human rights protection. Indications suggest that this question continues to be met with serious skepticism.

One of the most pressing concerns relates to privacy in the digital realm. With the expansion of tracking tools, behavioral data analytics, facial recognition technologies, and AI-driven algorithms, the traditional notion of "privacy" has been severely destabilized. States and tech companies alike are now capable of collecting and analyzing vast amounts of personal data without clear legal frameworks governing informed consent, usage limitations, or transparency in data processing (Kuner, 2015). Although international documents—such as Article 17 of the International Covenant on Civil and Political Rights—explicitly protect privacy, the mechanisms for enforcing this right in digital spaces remain ineffective or incomplete.

Another significant issue is digital surveillance by governments. In recent years, both democratic and authoritarian states have implemented mass surveillance programs that pose not only a threat to privacy but also constitute direct violations of freedom of expression and assembly (Deibert, 2019). While some of these practices are justified on security grounds, the absence of effective international oversight and transparency has left internet users without even minimal human rights protections. This is particularly acute in states lacking independent oversight structures, where rights violations are widespread and often immune to international accountability (Bradshaw et al., 2015).

Moreover, technology companies—as powerful non-state actors—play a critical role in shaping how human rights are exercised in digital spaces. Platforms such as Google, Meta, X (Twitter), and Amazon make decisions on content regulation, censorship, and content prioritization through complex algorithms—decisions that directly impact freedom of expression, access to information, and even political participation. However, these companies are not formally bound by international human rights law, and existing frameworks such as the UN Guiding Principles on Business and Human Rights remain largely voluntary in nature (Ruggie, 2013). Consequently, there is a growing accountability gap between the immense influence of these corporations and the legal responsibilities they bear.

The right to internet access has also emerged as a central issue in digital rights discourse. In a world where access to public services, educational opportunities, and forms of political participation increasingly depends on internet connectivity, internet shutdowns or platform restrictions may constitute violations of fundamental rights. Nevertheless, in some countries, such shutdowns occur for political or security reasons without any regulatory oversight (Tufekci, 2017). The international legal system has yet to establish a binding and universal norm ensuring the "right to connectivity."

A further challenge stems from the clash of cultural interpretations of human rights in the digital age. While Western countries tend to emphasize freedom of expression and access to information, many Asian and African states prioritize national security or cultural values. These conflicting approaches have prevented international bodies such as the UN Human Rights Council from reaching a clear consensus on binding digital norms (Gorwa, 2019). Thus, international law faces a dual challenge: it must preserve the universality of human rights while also respecting cultural and political sensitivities—an endeavor that has proven to be deeply complex.

From an institutional perspective, the lack of specialized international courts for digital rights has left victims of online human rights violations without effective legal remedies. Aside from regional mechanisms like the European Court of Human Rights, most international judicial bodies lack jurisdiction to adjudicate cases concerning digital rights violations. This is despite the rising prevalence of harms such as online harassment, algorithmic discrimination, and the digital suppression of dissent (Perry & Olsson, 2021).

Ultimately, the core problem in protecting human rights in the digital sphere lies not merely in the absence of rules, but in the misalignment between traditional legal norms and the structures and realities of the digital era. Most foundational human rights instruments were developed between the 1940s and 1970s—a period that predates the internet, artificial intelligence, or big data. Accordingly, revising human rights instruments—or at the very least, reinterpreting them through a dynamic and context-sensitive lens—is a necessary condition for addressing today's evolving challenges.

6. Regulation of Global Platforms

In the digital era, global platforms such as Google, Meta (Facebook), Amazon, Twitter (X), and TikTok have become key actors in the realms of communication, economy, and politics. These companies, by providing digital infrastructure for social interaction, e-commerce, advertising, and information circulation, exert significant influence over how individuals interact with each other and with states. However, their growing dominance in the global digital ecosystem presents a fundamental challenge to international law: the lack of a coherent and binding framework for regulating transnational actors that operate beyond the reach of individual states. This challenge not only highlights the limitations of state sovereignty in the digital domain but also reflects a broader crisis in the capacity of traditional legal systems to govern contemporary realities (Gorwa, 2019).

Through their algorithmic architectures, global platforms influence public discourse and even shape political and social realities. Decisions about content removal, censorship, or information prioritization confer powers on these companies akin to sovereignty over public space—yet without democratic legitimacy or meaningful legal accountability (Kaye, 2019). This has raised widespread concerns about infringements on free speech, access to information, algorithmic discrimination, and the weakening of democratic processes.

One of the key difficulties in regulating global platforms under international law lies in their private and transnational nature. Traditional international law was designed to regulate the conduct of states, and its tools are limited when it comes to applying legal obligations to private corporate entities across borders. Although documents like the UN Guiding Principles on Business and Human Rights underscore corporate social responsibility, they are non-binding and lack effective enforcement mechanisms (Ruggie, 2013). As a result, platform companies often exploit legal loopholes and regulatory disparities across jurisdictions to evade accountability.

Another major issue is the lack of global consensus on the extent and nature of platform regulation. For instance, the European Union has adopted an active regulatory approach focused on user protection, exemplified by laws such as the Digital Services Act and the Digital Markets Act, which represent coordinated efforts to rein in platform power (Bradford, 2020). In contrast, the United States generally adheres to principles of self-regulation and internet freedom, maintaining caution about governmental interference in platform content. Meanwhile, some authoritarian regimes use platform regulation as a pretext for political censorship and control. This regulatory fragmentation has led to the splintering of the global digital space and introduced new risks to the coherence of international legal norms.

In addition, the unprecedented economic power of platforms enables them to resist regulatory efforts or extract concessions from states. Many of these corporations are wealthier than entire countries and exploit diverse legal systems to minimize tax obligations or circumvent restrictive laws (Zuboff, 2019). This not only exacerbates global economic inequalities but also undermines the capacity of states to exert legal authority over platforms.

At the global level, initiatives to regulate platforms are beginning to emerge. The UN Human Rights Council has issued reports highlighting the impact of platforms on human rights and has called for greater transparency and adherence to international standards. Organizations such as the OECD and ITU have also initiated discussions on international frameworks for platform regulation. However, no binding or effective global consensus has yet emerged, and platforms continue to operate primarily under self-imposed rules.

This makes the need for a comprehensive legal regime for global platform regulation increasingly urgent. Such a regime must uphold core human rights standards while addressing platform-specific challenges such as information manipulation, discriminatory algorithms, monopolistic dominance, and content responsibility. Furthermore, international cooperation, civil society participation, and corporate transparency must be integral to the regulatory process to establish a balanced, multi-actor, and accountable governance system (Suzor, 2019).

7. Lack of International Consensus on Cyber Norms

In the digital age, cyberspace has become one of the most important arenas for international interaction, economic exchange, and political activity. With the expansion of the internet, concepts such as freedom of information, borderless communication, and digital globalization have flourished. At the same time, mounting concerns regarding national security, foreign interference, cybercrime, and the protection of cultural values have prompted some states to adopt policies under the banner of "cyber sovereignty." This situation has led to one of the central challenges for the international legal system in the digital era: the lack of global consensus on legal norms governing cyberspace (DeNardis, 2014).

According to the liberal approach—championed primarily by Western countries, particularly the United States and the European Union—the internet should remain an open, free, and global space. These states emphasize principles such as freedom of expression, the free flow of information, healthy competition, and the prevention of state censorship (Kleinwächter, 2004). Within this framework, state intervention to control online content or restrict user access is seen as a threat to digital human rights and the rules-based international order. In contrast, countries such as China, Russia, Iran, and other authoritarian states emphasize the concept of "cyber sovereignty," arguing that each state has the right to exert full control over infrastructure, data, and internet content within its borders—just as it does with territorial sovereignty (Segal, 2017). From this perspective, unrestricted internet freedom poses national security risks, fosters cultural interference, incites domestic unrest, and weakens state sovereignty.

The absence of agreement between these two perspectives has impeded the development of a binding global framework for cyber governance. Although bodies like the UN Group of Governmental Experts and the Open-Ended Working Group have attempted to formulate common principles, deep political divisions have stalled significant progress. While the reports emerging from these sessions affirm norms such as the prohibition of the use of force, non-intervention, and state responsibility in cyberspace, national interpretations of these concepts remain sharply divergent (Tikk & Kerttunen, 2020).

A prominent manifestation of this tension lies in disputes over control of internet infrastructure. Global technical organizations such as ICANN, IETF, and W3C—which are responsible for internet standardization and domain name management—are predominantly influenced by Western actors and advocate for a multi-stakeholder model. Conversely, proponents of cyber sovereignty advocate for transferring authority to intergovernmental bodies where states play the leading role (Mueller, 2010). This division has impacted not only theoretical debates but also practical power struggles over cyberspace governance.

The result is the phenomenon of “internet fragmentation,” whereby states implement strict national laws, restrict cross-border data flows, and impose firewalls—effectively transforming the global internet into isolated national networks (Chander & Le, 2015). This condition disrupts digital commerce, innovation, and international cooperation, and poses a threat to the coherence of global legal order. From the standpoint of international law, the lack of consensus on cyber norms has left fundamental principles—such as sovereignty, non-intervention, and lawful use of force in digital space—without comprehensive and reliable interpretation. For example, it remains unclear under what criteria a cyberattack constitutes “force” or whether a countermeasure in response to a cyber operation is legally permissible (Schmitt, 2017). These ambiguities heighten the risk of states exploiting vague rules to justify aggressive behavior under the guise of defending cyber sovereignty.

To address this situation, some scholars have called for a comprehensive international treaty on cybersecurity and cyber norms—one that updates general principles of international law and addresses issues such as state responsibility, the role of non-state actors, protection of digital human rights, and international cooperation (Hathaway et al., 2012). However, geopolitical rivalries and mutual distrust among major powers have impeded such initiatives. In sum, the lack of global consensus on cyber legal norms—and the tension between internet freedom and cyber sovereignty—represents a complex and multifaceted challenge for contemporary international law. The future of legal order in digital space will depend on the international community’s ability to find a balance between freedom and security, participation and sovereignty, and cooperation and competition.

8. The Changing Nature of Warfare and International Security

The transition to the digital age has profoundly transformed the nature of threats, the tools of conflict, and the fundamental concepts of international security. War is no longer confined to physical battlefields; instead, it has extended into cyberspace through cyberattacks, information operations, infrastructure sabotage, and cognitive warfare. This shift poses a serious challenge to the international legal system, particularly the laws of war and collective security, as many traditional legal norms were not designed to address the characteristics of digital warfare (Schmitt, 2017).

One of the most significant changes in this realm is the rise of cyber threats from state actors, non-state groups, and even individuals. Operations such as the attack on Ukraine’s power grid (2015), cyber interference in the U.S. elections (2016), and ransomware assaults on healthcare infrastructure during the COVID-19 pandemic exemplify silent, borderless wars with impacts equal to or greater than conventional conflicts (Healey, 2011).

Under traditional international law, war or the use of force requires an armed attack that results in loss of life or significant physical destruction. However, in the digital context, an attack that merely disables a banking system or disrupts urban transportation may not be recognized as "force" within the current legal framework. This ambiguity constitutes one of the most serious legal gaps in responding to cyber warfare (Tsagourias & Buchan, 2015).

Moreover, principles such as proportionality and necessity become difficult to apply in cyberspace. For example, is it lawful to respond to an act of information espionage by attacking government servers? Do cyber interventions that damage civilian data or healthcare services comply with the principle of distinction between military and civilian targets? Traditional humanitarian law offers no clear answers to these emerging scenarios (Kello, 2017).

Another critical aspect of this transformation is the expanding role of non-state actors in digital warfare. While states were the main parties in conventional armed conflict, today's cyber wars involve tech firms, hacker collectives, private security contractors, and even ordinary citizens. This complicates attribution and undermines the principle of state responsibility, as identifying the true perpetrators of cyberattacks is often extremely difficult and may restrict lawful response options (Lin, 2012).

Additionally, existing international security institutions—such as the UN Security Council—lack the tools and readiness to confront digital threats. To date, the Council has not adopted any binding resolutions regarding the use of information technologies in military conflicts (Tikk & Kerttunen, 2020). As a result, cyberspace has become a largely unregulated domain, increasing the likelihood of conflict escalation. Simultaneously, emerging technologies such as artificial intelligence, lethal autonomous systems, and algorithmic warfare are shifting the nature of conflict toward automation and non-human decision-making. This not only raises ethical concerns about humanitarian principles like individual accountability and avoidance of unnecessary suffering but also disrupts the balance of classical deterrence (Boulanin & Verbruggen, 2017).

In general, security threats in the digital era have shifted from the visible and tangible to the invisible, diffuse, and unpredictable. This transformation demands a thorough revision of international legal structures, concepts, and norms—including redefining the concept of war, expanding responsibility rules for cyber operations, clarifying legitimate responses, and establishing mechanisms for international cooperation in cyber defense. In the absence of such reforms, the risk of growing instability, strategic misunderstandings, and ultimately full-scale digital warfare will increase—wars without bullets, but with devastating consequences that will reshape the future of international security.

9. Conclusion

The digital age has brought about fundamental transformations in the structure and function of international legal order—transformations that not only challenge existing rules but also question the foundational premises of traditional international law. What initially appeared to be technological opportunities for expanding international cooperation has increasingly become a source of tension, normative inconsistency, and legal fragmentation. Throughout this discussion, the multifaceted nature of these challenges has been examined—from the absence of clear sovereignty in cyberspace to the difficulties in attributing responsibility, the weaknesses in protecting digital human rights, the regulatory limitations regarding global platforms, the lack of international consensus on cyber norms, and, ultimately, the evolving concept of war and security.

The first major challenge lies in the absence of clearly defined sovereignty in cyberspace. Unlike traditional domains such as land, sea, or air, cyberspace lacks clear geographic borders and ownership regimes. As a result, states are embroiled in conflicts over jurisdiction and control, while existing international legal principles regarding territory and sovereignty fail to account for the structural and technical complexities of the digital realm. This has heightened the tension between national sovereignty and the principle of free information flow, whereby some states invoke cyber sovereignty to justify extensive control measures, while others emphasize internet openness and borderlessness.

The second challenge concerns the ambiguity in applying international responsibility rules in digital contexts. In many instances, the difficulty of attributing a cyberattack to a specific state prevents the realization of international responsibility. Even when responsibility is established, traditional legal criteria—such as wrongful acts, harm, and causality—become obscure in cyberspace. The absence of a defined system for accountability and reparation in response to cyber operations has created a lawless environment in which states may resort to offensive or retaliatory actions, thereby posing risks to international peace and security.

The third challenge involves the growing crisis of human rights in the digital domain. While digital technologies can empower individuals, they are frequently used by states and corporations to restrict freedom of expression, violate privacy, and implement algorithmic discrimination. The inability of traditional human rights frameworks to regulate the conduct of both governments and powerful tech companies has left fundamental rights in cyberspace vulnerable. The lack of oversight mechanisms, ineffective binding frameworks, and the blurred line between legitimate surveillance and rights violations have exacerbated this crisis.

The fourth challenge is the international legal system's limited ability to regulate global platforms. Companies like Google, Meta, Twitter, and other major platforms have evolved into not only economic entities but also political and cultural decision-makers with global influence. They wield the power to remove content, restrict access, and shape global public opinion—yet they operate outside any binding international legal framework. The absence of a global legal regime to oversee their expansive power has enabled a form of transnational private governance that remains largely unaccountable but profoundly impactful.

The fifth issue stems from the absence of international consensus on cyber norms—particularly regarding the balance between internet freedom and cyber sovereignty. While Western states typically advocate for a free and open digital order, other governments emphasize strict control over data and online content. This conceptual and political divide hinders the development of a coherent and binding legal framework and obstructs cooperation in the face of shared cyber threats.

Finally, perhaps the most profound transformation of the digital age lies in the changing nature of warfare and international security. Cyber wars, information operations, cognitive warfare, and autonomous weapons have disrupted the traditional framework of the laws of armed conflict. Concepts such as “force,” “hostilities,” “military objective,” and “proportionality” have acquired new meanings in digital environments, while international humanitarian law has yet to develop mechanisms capable of addressing the novel challenges posed by digital warfare.

In summary, the digital age constitutes a major test for the legitimacy and effectiveness of international law. If this legal system fails to adapt to technological transformations and deliver appropriate normative and structural responses, it risks eroding the trust of states and societies in the global legal order—leading to increased instability, inequality, and conflict in new and unpredictable forms. Therefore, the international community must urgently mobilize the capacities of multilateral institutions, technical expertise, and collaboration among states and private actors to redefine and renew international law in response to digital challenges. The future of international law hinges on its ability to respond to these profound and transformative changes.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Boulanin, V., & Verbruggen, M. (2017). *Mapping the Development of Autonomy in Weapon Systems*. Stockholm International Peace Research Institute.

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Bradshaw, S., Millard, C., & Walden, I. (2015). Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. *International Journal of Law and Information Technology*, *19*(3).

Chander, A., & Le, U. P. (2015). Data Nationalism. *Emory law Journal*, *64*(3).

Council of, E. (2001). *Convention on Cybercrime (ETS No. 185)*.

Crawford, J. (2006). *The Creation of States in International Law*. Oxford University Press.

De Hert, P., & Papakonstantinou, V. (2012). The proposed data protection regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*, *28*(2).

Deibert, R. (2019). The road to digital unfreedom: Three painful truths about social media. *Journal of Democracy*, *30*(1).

DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

Gorwa, R. (2019). The platform governance triangle: Conceptualising the informal regulation of online content. *Internet Policy Review*, *8*(2).

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Perdue, W., & Spiegel, A. (2012). The Law of Cyber-Attack. *California Law Review*, *100*(4).

Healey, J. (2011). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.

International Law, C. (2001). *Draft Articles on Responsibility of States for Internationally Wrongful Acts*.

Jensen, E. T. (2015). Cyber sovereignty: The way ahead. *Texas International Law Journal*, *50*(3).

Kaye, D. (2019). *Speech Police: The Global Struggle to Govern the Internet*. Columbia Global Reports.

Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

Kleffner, J. K., & Dinniss, H. M. (2013). Targeting in cyberspace: Legal challenges. *Israel Yearbook on Human Rights*, *43*.

Kleinwächter, W. (2004). Beyond ICANN vs. ITU? How WSIS Tries to Enter the New Territory of Internet Governance. *COMMUNICATIONS & STRATEGIES*, *56*(4).

Kulesza, J. (2017). Due diligence in cyberspace: A comparative law perspective. *Netherlands International Law Review*, *64*(1).

Kuner, C. (2015). *Transborder data flows and data privacy law*. Oxford University Press.

Lewis, J. A. (2014). *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*. United Nations Institute for Disarmament Research.

Lin, H. (2012). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy*, *4*(1).

McGregor, L. (2021). Data-driven discrimination at work. *International & Comparative Law Quarterly*, *70*(1).

Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press.

Perry, A., & Olsson, J. (2021). The future of human rights in the digital age: Challenges and opportunities. *Human Rights Review*, *22*.

Ruggie, J. G. (2013). *Just Business: Multinational Corporations and Human Rights*. W. W. Norton & Company.

Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press. https://doi.org/10.1017/9781316822524

Segal, A. (2017). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. Public Affairs.

Suzor, N. (2019). *Lawless: The Secret Rules That Govern Our Digital Lives*. Cambridge University Press. https://doi.org/10.1017/9781108666428

Tikk, E., & Kerttunen, M. (2020). *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*.

Tsagourias, N. (2016). Non-intervention, sovereignty and cyber operations. In N. Tsagourias & R. Buchan (Eds.), *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing. https://doi.org/10.4337/9781782547396

Tsagourias, N., & Buchan, R. (2015). *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing. https://doi.org/10.4337/9781782547396

Tufekci, Z. (2017). *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press.

United, N. (2021). *Report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (A/75/816)*.

Wilde, R. (2004). The accountability of international organizations and human rights. In M. Ragazzi (Ed.), *The Responsibility of International Organizations*. Martinus Nijhoff Publishers.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs.