Conflict of Laws in Cross-Border Cyber Disputes: An Analysis in Light of International Humanitarian Law

Dr. Mohamed Ahmed Zakaria Shehata

Abstract:
This study addresses the conflict of laws in cross-border cyber hostilities from an international humanitarian law (IHL) point of view. With the growing integration of cyber operations into modern armed conflicts, legal systems are faced with unprecedented challenges of determining applicable laws and competent jurisdictions. Unlike traditional warfare, cyberattacks often transcend physical borders, and it is complex to apply concepts such as lex loci delicti, territoriality, and nationality. The research explains how this traditional conflict of laws rules can be fitted into the intangible and borderless nature of cyberspace. It also addresses the applicability of the principles of IHL-distinction, proportionality, and necessity-to cyber operations, especially if they are against civilian infrastructure or occur in armed conflict. Using a descriptive-analytical approach, the study is based on legal instruments, international jurisprudence, and scholarly debate to examine the adequacy of current regimes. The aim is to provide recommendations that merge private international law mechanisms and IHL frameworks to efficiently govern cyber warfare while safeguarding humanitarian interests. By bridging these two legal fields, the research contributes towards developing a coherent and realistic legal response to the evolving nature of cyber warfare.
Keywords: Conflict of laws, Cyber conflicts, international humanitarian law, Cross-border jurisdiction, Digital warfare.

تنازع القوانين في النزاعات السيبرانية العابرة للحدود: دراسة تحليلية في ضوء القانون الدولي الإنساني

د. محمد أحمد زكريا شحاته

جامعة الازهر – فلسطين

ملخص البحث:

يناقش هذا البحث قضية تضارب القواعد القانونية في الاعمال العدائية التي تتخطى الحدود، وذلك من زاوية القانون الدولي الإنساني. فمع تزايد اعتماد النزاعات المسلحة المعاصرة على الأنشطة الرقمية، تواجه التشريعات صعوبات لم يسبق لها مثيل في تحديد القوانين المطبقة والمحكمة صاحبة الولاية. على عكس المعارك التقليدية، فإن الاعتداءات السيبرانية لا تعترف بالحدود الجغرافية، الأمر الذي يجعل تطبيق مفاهيم مثل القانون الساري في مكان الضرر أو مفاهيم الإقليمية والجنسية أمرًا معقدًا ويوضح البحث عن كيفية تكييف قواعد تداخل القوانين المتبعة حاليًا لتناسب طبيعة المجال الرقمي المفتوحة وغير الملموسة. كما يدرس مدى إمكانية تطبيق أسس القانون الدولي الإنساني، خاصة تلك المتعلقة بالتمييز والتناسب والضرورة العسكرية على العمليات السيبرانية، خاصة عندما تستهدف المنشآت المدنية أو تقع في خضم نزاعات مسلحة. بناءً على منهج تحليلي وصفي، يستند البحث إلى الوثائق القانونية الدولية، وأحكام المحاكم الدولية، والمناقشات الفقهية، لتقييم مدى فعالية الهياكل القانونية الموجودة، ويقدم مقترحات تدعم التوافق بين طرق القانون الدولي الخاص ومبادئ القانون الدولي الإنساني، بما يؤدي إلى تنظيم أفضل لأعمال الحرب السيبرانية وصون الجوانب الإنسانية.

الكلمات المفتاحية: تنازع القوانين؛ النزاعات السيبرانية؛ القانون الدولي الإنساني؛ الاختصاص العابر للحدود؛ الحرب الرقمية.

1. Introduction.

The advent of cyberspace in the recent past has greatly transformed social, economic, as well as legal interactions on a global scale. While the virtual world has ushered in unprecedented space for communication, business, and entrepreneurship, it has also brought complex legal challenges, particularly on how to identify the governing laws in international conflicts. As opposed to traditional territorial spheres, cyberspace does not have a geographical borderline, thereby creating a legal vacuum in which traditional rules of jurisdiction and conflict of laws are liable to fail to provide effective solutions.

In these conditions, the conflict of laws problem in cyberspace has become one of the most pressing issues confronting modern-day international law. The borderless nature of activities ranging from cybercrime and online commerce to data protection and intellectual property disputes does raise questions of whose law is applicable to conflicts and how the states can coordinate their jurisdictional claims. Traditional doctrinal methods grounded in territorial sovereignty and national systems of law are increasingly ill equipped to deal with interaction that occurs across a decentralized and globalized digital world.

The present research seeks to provide a thorough legal analysis of the conflict of laws phenomenon on the Internet, including its intellectual foundations, mechanisms developed by international and regional law systems, and the challenges posed by the unique nature of the virtual space. Through both theory and practice, the research aims to identify trends towards more consistent and efficient regulation reconciling state sovereignty, human rights, and international cooperation in the era of cyberspace.

2. The Conceptual Framework of Conflict of Laws in Cyberspace.

The rapid expansion of cyberspace as a borderless and decentralized domain has generated unprecedented challenges for the traditional legal order, particularly in the field of private international law. Unlike physical territories, cyberspace does not conform to geographical boundaries or sovereign jurisdictions, thereby complicating the application and enforcement of national legal systems. These complexities have led to the

emergence of intricate questions concerning the determination of applicable law, the identification of competent jurisdiction, and the recognition and enforcement of digital rights and obligations across borders.

This section seeks to provide a conceptual framework for understanding the phenomenon of conflict of laws in cyberspace. It begins by defining cyberspace and highlighting its distinctive legal attributes that differentiate it from conventional territorial domains. It then explores the nature of conflict of laws in the digital environment, tracing the factors that give rise to such conflicts and examining the challenges posed by the dematerialized nature of online interactions. Finally, it addresses the unique transnational character of cyber disputes, emphasizing how their cross-border dimension necessitates a re-evaluation of existing legal doctrines and the development of innovative mechanisms of international cooperation.

2.1. Definition of Cyberspace and Its Legal Characteristics.

Cyberspace is widely understood to be an unusual, intangible, and global space that transcends the traditional territorial boundaries. Unlike physical territories subject to territorial sovereignty, cyberspace is constructed from webbed structures of information systems, data flows, and cyber infrastructures. This virtual space provides instant communication and interactivity beyond borders, raising extraordinary challenges to the enforcement of legal norms (Tsagourias, 2015).

From a legal perspective, cyberspace has aspects that distinguish it from other spaces in which to regulate. First, it is an inherently decentralized space where no one state or entity can possibly exercise total control of its infrastructure or governance mechanisms. Second, its borderlessness complicates the ability to assign jurisdiction since digital activities tend to touch simultaneously across various states. Third, anonymity and the difficulty of attribution mark cyberspace, as identifying who initiated a cyber activity requires advanced technical and legal analysis (Krasikov & Lipkina, 2020).

These attributes have significant implications for international law and conflict of laws. Decentralization of cyberspace challenges the classical theory of sovereignty, as governments are unable to exert jurisdiction on activities outside their geographical confines but with local implications .Similarly, the imprecision of territorial boundaries poses difficulties in choosing the law applicable in a situation, particularly when electronic

transactions or cyber incidents are governed by more than one legal system. Hence, cyberspace requires refashioning established legal concepts to fit its traits and impose effective legal regulation.

2.2. Nature of Conflict of Laws and Its Emergence in the Digital Environment.

Conflict of laws has traditionally delimitated legal scenarios wherein more than one jurisdiction may claim power in a cross-border conflict, thereby resulting in which court and legal system to preside over. With the information age, this issue has become much more severe as web interactions tend to traverse territorial borders, requiring older legal frameworks to struggle to implement. The borderless, decentralized nature of cyberspace itself leads to incessant overlap of the jurisdictions of law, rendering the traditional ideas of territoriality and domicile problematic (Chałubińska-Jentkiewicz, 2022).

The international character of cyberspace means that a single online action—e.g., data leak or e-commerce sale-can give rise to legal consequences in several jurisdictions simultaneously. The multiplicity aggravates jurisdictional disputes and showcases the inadequacy of conventional conflict-of-law principles based on physical location or nationality. Such orthodox theories have the propensity of creating inconsistencies and inconsistency in judicial results(Simón & Lanoszka, 2020) .

Compounding this complexity is the diffusion of private digital spaces and platforms. These platforms commonly exert their own quasi-regulatory institutions in the form of user agreements and algorithmic governance, which can respectively override or interfere with local law. The emergence of these private norms creates a parallel order of law which has the potential to undermine traditional state-based institutions, expanding legal uncertainty and reducing foreseeability (De Miguel Asensio, 2024).

In addition, variation in the regulatory approaches of states, particularly in data protection, consumer protection, and cybercrime, aggravates conflict of laws. For instance, differing use of digital privacy laws and e-commerce practices encourages forum shopping and legal fragmentation. This kind of dissonance in regulation calls for international collaboration and harmonization to neutralize conflicts and maintain legal uniformity (Abdelkarim, 2023).

Consequently, cyberspace pushes conventional conflict-of-law rules to their limits, calling for new mechanisms—such as harmonized arbitration procedures, cross-border regulatory systems, or hybrid governance models—that are appropriate for the digital environment's global, multi-jurisdictional character.

2.3. The Role of Blockchain in Intellectual Property Registration and Management.

Blockchain technology represents a significant advance in intellectual property (IP) law, especially in registration and rights management. Unlike centralized and vulnerable registries that can be manipulated or inefficient, blockchain provides a decentralized, tamper-resistant ledger that ensures transparency, authenticity, and record durability. Once the information on authorship, invention, or ownership is entered, it cannot be altered, thus offering unprecedented reliance for legal application(Bodó et al., 2018).

One of the central features of blockchain is that it has the capacity to create tamper-proof, time-stamped evidence of creation or ownership. This ability addresses age-old legal challenges in IP conflicts, particularly establishing priority of rights. Courts and arbitral bodies are prone to deciding cases largely on the basis of the date of invention or authorship and blockchain offers a trustworthy tool for such verification, which could reduce litigation costs and enhance legal certainty (Savelyev, 2018). Furthermore, the development of smart contracts in blockchain systems makes it possible for automatic enforcement of licensing terms, royalty payments, and usage tracking, thus simplifying rights management and minimizing the risk of human mistakes (O'Dair & Beaven, 2017).

International institutions are increasingly realizing the importance of blockchain in intellectual property (IP) governance. World Intellectual Property Organization (WIPO), for example, has debated the application of blockchain to IP protection, highlighting that it has the power to transform current systems by offering more secure, less expensive, and borderless solutions (World Intellectual Property Organization (WIPO). Blockchain Whitepaper: Opportunities and Challenges for IP. WIPO; 2020., n.d.). It captures the essence of blockchain as something more than a technical innovation but as an agent of legal and institutional transformation in global IP.

Yet, there are hurdles. Interoperability among blockchain networks, jurisdictional acceptance of blockchain records, and compliance with data

protection regimes such as the GDPR pose significant hurdles to universal adoption. But the benefits-chiefly, increased trust, reduced cost, and verifiable authenticity-suggest that blockchain can have a pivotal role in rethinking how IP rights are registered, enforced, and protected across borders(Finck, 2017) .

3. General Principles of Conflict of Laws in Cyber Disputes.

The development of cyberspace has presented unprecedented challenges to the conventional principles of private international law, especially those relating to conflicts of laws. In contrast to physical territories, cyberspace is characterized by its decentralized and borderless nature, which complicates jurisdiction identification as well as the applicable law. The rules traditionally established to solve conflicts with extra-territorial implications were designed in the context of tangible interactions between sovereign states, whereas cyber conduct tends to cross numerous jurisdictions simultaneously, thereby making traditional thought moot.

This section tries to examine how the fundamental principles of conflict of laws can be adapted to the unique features of cyber disputes. It discusses how far territoriality, traditional connecting factors, and existing legal doctrines can be exported or reinterpreted in the virtual environment. Besides, it sheds light on the actual issues which arise when courts seek to ascertain jurisdiction or the governing law in cases of online behavior. This way, the discourse highlights the restrictions of current frameworks and the pressing need for innovative solutions which strike a balance between regard for state sovereignty and efficient regulation of cyberspace.

3.1. The Principle of Territoriality in Cyberspace and Its Challenges.

The theory of territoriality has been a pillar of conflict-of-laws thinking for centuries, premised on the idea that states have exclusive legal authority over their physical domains. Within the realm of cybercrime, this maxim is brought under a great deal of strain. Cyber activity is likely to occur in virtual, geographical space, which complicates adherence to a territorially based model of jurisdiction. The principle becomes operationally difficult, as one can practically be unable to identify the "locus delicti" of a cyber operation if data is originated, transits, and impacts multiple states simultaneously (Maillart, 2019).

Moreover, digitalization pushed legal scholars to reject the practicability of strict territoriality. One such study argues that even though territoriality as

the default model still prevails, its application in cyberspace is diminishing, with increasingly clamorous demands for a multifactor "reasonableness" test-one that assesses jurisdictional claims on the grounds of connection, effect, and fairness, not just locus (Ryngaert, 2023). On the other hand, other strategies maintain that territoriality remains fundamental, particularly in relation to the defense of sovereign rights, but emphasize the need for complementary principles like effects-based jurisdiction or nationality to counter digital realities (Pierucci, 2025).

This conflict highlights a wider conceptual dilemma: how can the law maintain the state's legitimate interest in governing conduct where the activity can't be situated within its physical space? The answer lies in a hybrid approach-one that maintains territoriality as the default rule but completes it with loose, case-by-case norms appropriate to cyber conditions.

3.2. Applying Traditional Choice-of-Law Rules to Cyberspace.

In private international law, the selection of the applicable jurisdiction traditionally depends on well-established connecting factors, such as the place where a contract was formed (lex loci contractus), where a wrongful act occurred (lex loci delicti), or the parties' domicile. However, the inherently borderless and decentralized character of cyberspace significantly undermines the functionality of these doctrines. Digital interactions—including online contracts, defamation, or data breaches-manifest across multiple territories simultaneously, rendering the concept of a singular legal locus often ambiguous or unworkable (F. F. Wang, 2010).

Consequently, contemporary legal scholarship advocates for a more contextual and pragmatic method to determine the governing law. Instead of rigidly applying territorial norms, courts and legal practitioners should evaluate where the essential elements of the dispute occurred—such as where the data was accessed, communications were exchanged, or the harm was felt in the most substantial manner. This adaptable approach aligns legal reasoning with functional realities rather than outdated geographical presumptions (De Miguel Asensio, 2024).

Moreover, the principle of party autonomy has emerged as a stabilizing force in cyberspace-related disputes. When parties deliberately and fairly agree on the governing law and competent court in their digital transaction, courts are increasingly recognizing and honoring such agreements. This

offers much-needed legal certainty in a domain where jurisdiction is often diffuse. Yet, especially in consumer contexts or instances of unequal bargaining power, autonomy must be balanced with protective principles to uphold fairness (Gillies, 2007).

In summary, while traditional choice-of-law principles remain conceptually instructive, their practical application in cyberspace requires reinterpretation and flexibility. A hybrid legal model-rooted in classical foundations, yet responsive to digital realities—provides the most viable path for fair and predictable dispute resolution in the cyber age.

3.3. Practical Challenges in Determining the Applicable Law in Cyber Disputes.

Perhaps the most pressing problem concerning cyber warfare is determining what national law will govern online conduct, since cyberspace does not sit inside traditional territorial boundaries. Such traditional connecting factors as for example lex loci delicti (where the offense was perpetrated) or lex loci contractus (where the agreement was formed) become obscure inside cyberspace because transactions and offending activities can occur simultaneously within different jurisdictions (Goldsmith & Wu, 2006).

Consider, for example, the Yahoo! Inc. v. LICRA judgment, wherein French courts mandated stripping off Nazi-themed material from Yahoo!'s website, even though the servers were located in the United States-demonstrating the built-in difficulty of applying models of jurisdiction to cyber events (Goldsmith & Wu, 2006).

Another instance is YouTube (Google) v. CNIL, in which the French Conseil d'État sought CJEU guidance on whether de-referencing obligations (like the "right to be forgotten") must apply worldwide or must be geo-limited. The Court ultimately held large EU data protection concepts over territorially limited implementations (Kowalik-Bańczyk & Pollicino, 2016). That decision points to how cyberspace defies national borders and makes applicable law determinations difficult.

Widescale cyberattacks like the WannaCry ransomware assault (2017) targeted over 150 countries simultaneously. The attack is the best illustration of how crimes with no physical place challenge jurisdictional certainty and expose the inadequacies of classical conflict-of-laws rules in addressing anonymous, transnational offenses (Batarseh, 2022).

Secondly, the Budapest Convention on Cybercrime (2001) attempts to provide mechanisms for cross-border harmonization and cooperation. Differences in participation and interpretation among states, as well as opposition from non-members, undermine its implementation, creating continuities of enforcement gaps across cyberspace legal governance (Ragavan, 2013).

In short, cyberspace needs a sophisticated legal response. The dispersed and intangible character of cyber conduct denies many conventional law assumptions, compelling responsive, coordinated systems that respect sovereignty while ensuring effective cross-border cyber justice.

4. International Humanitarian Law and the Conflict of Laws in Armed Cyber Conflicts

The rapid evolution of cyberspace as a new domain of warfare has raised complex questions regarding the applicability and scope of international humanitarian law (IHL). Unlike traditional battlefields, cyber operations are characterized by their transnational nature, anonymity, and potential for widespread impact on civilian infrastructure. This raises critical concerns about how established rules of IHL—such as the principles of distinction, proportionality, and necessity-should be interpreted and applied in the context of cyber armed conflicts.

This section seeks to explore the interplay between IHL and the challenges posed by cyber warfare through three main subsections. The first examines the extent to which IHL applies to cyberspace and the legal debates surrounding its applicability. The second addresses the principle of distinction, focusing on the protection of civilian objects and the difficulties in distinguishing between civilian and military targets in cyberspace. The third subsection discusses state responsibility and international accountability for damage caused by cyber operations during armed conflicts, highlighting the gaps and potential reforms needed to strengthen compliance with IHL in this emerging domain.

4.1. The Applicability of International Humanitarian Law to Cyberspace .

The advent of cyber warfare in armed conflicts requires a careful reconsideration of whether International Humanitarian Law (IHL) is still applicable in such non-conventional situations. Although IHL was

originally formulated in terms of physical combat, the essential principles of distinction, necessity, and proportionality are held to be technologically neutral and therefore potentially adaptable to cyber warfare that reaches the level of armed hostilities ("International Humanitarian Law and Cyber Operations during Armed Conflicts," 2020).

It is supported by authoritative counsel from learned academic institutions specializing in cyber conflict. The Tallinn Manual 2.0 on International Law Applicable to Cyber Operations, prepared by leading experts in the field, states that IHL is applicable to cyber operations whenever the escalation to an armed conflict occurs, be it a kinetic or a digital operation(Schmitt, 2017) . This stance has also been given institutional support in the reaffirmation of an institution's stance by the International Committee of the Red Cross (ICRC), which openly states that cyber operations must be placed under the same IHL limitations as conventional warfare ("Reports," 2020).

Despite such reaffirmation, there are operational and doctrinal uncertainties. A key challenge is how to determine when a cyber operation can be an "armed attack"–i.e., whether disrupting civilian infrastructure such as hospitals, power grids, or communications infrastructure should be equivalent in law to their destruction (Biggio, 2025). This uncertainty creates diverging opinions among jurisdictions and threatens the cohesion of IHL's regulatory framework in cyberspace.

Moreover, the dual-use character of the majority of cyber systems—both military and civilian purposes-increases legal categorization's complexity. Determining the moment at which a digital item stops being "lawful military objective" and turns into a civilian object under the protection of laws is complex and risks being inconsistently applied IHL protections to civilians.

Lastly, since IHL undoubtedly binds in principle to cyber operations, putting its norms into effective practice in cyberspace requires more nuanced interpretation. The doctrine must be tailored to provide improved clarity on essential thresholds, attain legal consistency, and prevent erosion of civilian protection amid rapid technological developments.

4.2. The Principle of Distinction and Protection of Civilian Objects in Cyber Attacks.

The principle of distinction is one of the key pillars of international humanitarian law, which mandates parties to a conflict to always

distinguish between civilian objects and combatant targets. Cyber warfare presents new challenges in applying this principle since most of these digital infrastructures have dual use, meaning that they have both civilian and military purposes simultaneously (Mamiya & Vestner, 2022).

Military objectives are objectives which by their function, location, use, or purpose make a important contribution to military activity, and whose destruction in whole or in significant part offers a clear military advantage. In cyberspace, infrastructures in the cyber world such as communication networks and data centers can serve civilian and military purposes. Hence, decision-making on legitimate targets is a careful assessment of the function being performed at the time of attack and the expected military advantage (Mamiya & Vestner, 2022).

Cyber attacks against civilian targets, like hospitals, electricity grids, or banking systems, can have indirect but significant consequences. Even if direct physical damage does not happen, disrupting such services may have significant humanitarian consequences, challenging respect for the principle of distinction ("International Humanitarian Law and Cyber Operations during Armed Conflicts," 2020). Those attacks which fail to make a distinction between civilian and military objectives are a violation of international humanitarian law. For example, attacking a power grid that supplies both civilians and the military without precision constitutes an indiscriminate attack, breaching the basic requirement of distinction.

The use of autonomous cyber weapons presents additional complicating variables. Such systems can be programmed to strike at specific military targets but have the unintended effect of spreading into civilian infrastructure, causing disproportionate damage in relation to anticipated military gain. This circumstance presents the challenge of applying classic principles of distinction to modern cyber operations (Biggio, 2025).

In conclusion, cyber warfare development calls for a robust legal framework that effectively protects civilian objects, establishes unambiguous boundaries for defining military targets in cyberspace, and establishes mechanisms for surveillance and enforcement of compliance with the principle of distinction. The determination of the peculiarities of cyber operations ensures international humanitarian law is contemporary and efficient in the cyber battlefield.

4.3. International Responsibility for Damages Resulting from Cyber Attacks in Armed Conflicts

The attribution of responsibility for cyber warfare in armed conflict poses difficult questions under international humanitarian law (IHL). States and non-state actors may employ cyberattacks that cause massive harm, including physical destruction, economic disruption, and loss of civilian life. Attribution entails a careful examination of the identity of the attacking party, the scale and effect of the attack, and the pertinent legal frameworks (Madubuike-Ekwe, 2021).

In IHL, states have an obligation to be responsible for internationally wrongful acts that are breaches of their legal obligations, including those under the Geneva Conventions and customary international law. Cyberattacks on civilian infrastructure, disruption of essential services, or indiscriminate effects may constitute such breaches of obligations, thereby engaging the principle of state responsibility (Mačák, 2021). The principle is also applied to non-state actors where activities are state directed or controlled, hence the state becomes liable for resulting damage (Parron et al., 2022).

Cyber operations are extremely challenging to attribute due to the anonymity of cyberspace. The identity of the attacker could remain concealed from cyberattacks, proxies, or using third-party infrastructure, making direct attribution challenging (Madubuike-Ekwe, 2021). Despite such hurdles, states are liable to take due diligence to prevent misuse of their territory for activities causing injury to other states and their citizens. The WannaCry ransomware attack of 2017 that occurred in more than 150 nations illustrates the transnational effects of cyber operations and substantiates the practical challenges in holding parties accountable (Mačák, 2021).

The assessment of damages extends beyond the initial physical harm. Cyberattacks may trespass upon significant digital infrastructure, financial networks, or health services to exert cascading effects that erode civilian populations. Legal analysis must therefore consider both physical and indirect harm to determine the level of liability and adequate reparations under international law (Parron et al., 2022).

Having in place efficient mechanisms for accountability ensures that IHL remains effective in regulating state and non-state behavior on the evolving digital battlefield. Establishing international legal regimes that cater to the

unique challenges posed by cyber operations is required to maintain the principles of distinction, proportionality, and precaution in armed conflict (Madubuike-Ekwe, 2021).

5. Prospects for Developing International Law Rules to Address Conflicts of Laws in Cyberspace

The rapid expansion of cyberspace has outpaced the evolution of traditional legal frameworks, exposing significant gaps in regulating cross-border digital interactions. Current conflict-of-laws principles, primarily designed for territorial disputes, struggle to accommodate the borderless, fluid nature of cyberspace. This legal asymmetry not only generates uncertainty for states and private actors but also complicates efforts to prevent, investigate, and resolve cyber disputes. Consequently, there is an increasing scholarly and policy-driven emphasis on adapting international law to better manage these emerging challenges.

This section examines the prospects for developing international legal rules that effectively address conflicts of laws in cyberspace. It begins by analyzing the deficiencies inherent in existing frameworks, including fragmented national regulations, lack of harmonized principles, and difficulties in jurisdictional enforcement. It then explores proposals aimed at enhancing international cooperation, emphasizing mechanisms for shared regulatory standards, mutual legal assistance, and coordinated dispute resolution. Finally, the discussion highlights the potential for negotiating a comprehensive international convention designed to unify the legal approach to cross-border cyber conflicts, ensuring both the protection of state sovereignty and the maintenance of legal certainty.

By focusing on these dimensions, the study not only identifies the structural weaknesses of current legal instruments but also anticipates pathways for a more cohesive, globally recognized set of rules capable of mitigating the challenges posed by cyber disputes. Such forward-looking legal development is crucial to safeguarding the stability and predictability of international digital interactions in an increasingly interconnected world.

5.1. Deficiencies in Existing Legal Frameworks.

The existing international legal framework that regulates cyberspace has notable deficiencies when responding to conflicts of laws in cross-border cyber disputes. Ancient conflict-of-laws principles, mainly designed for

tangible, territorial affairs, are poorly suited to the intangible and boundary-less nature of cyber activities (Janssen et al., 2021). Uncertainty of jurisdiction occurs since cyber activities can affect several states simultaneously so one cannot determine the applicable law or the competent forum to adjudicate the case. This kind of situation exposes a high risk of conflicting claims in law and disproportionate judicial decisions, which undermine legal certainty (H. Wang et al., 2021).

Existing global instruments, such as the Budapest Convention on Cybercrime (2001), attempt to harmonize specific bits of cyber regulation. However, their effectiveness is limited to signing states and does not cover the latest technologies such as cloud computing, AI, or financial cyber operations across borders (Council of Europe. Convention on Cybercrime (Budapest Convention). Strasbourg; 2001, n.d.). Furthermore, voluntary adherence and differences in interpretation across states hinder the establishment of consistent rules, leading to extensive regulatory voids.

Last but not least, the deficiencies of existing legal regimes—viz., jurisdictional ambiguities, fragmented national legislations, and few international instruments—accentuate the need for reform. The establishment of these weaknesses is the foundation for developing more harmonious and effective rules to govern cross-border cyber interactions with legal certainty, accountability, and protection of both state and personal interests.

5.2. Proposals to Strengthen International Cooperation in Solving Cyber Conflicts.

The international nature of cyber activities necessitates vigorous international cooperation to resolve conflicts of laws effectively. Existing national and regional arrangements are usually deficient in providing consistent cross-border mechanisms of enforcement, exchange of information, and harmonized legal standards (Janssen et al., 2021). Building up international cooperation is therefore significant for discouraging jurisdictional disputes, reducing legal uncertainty, and achieving uniform protection of rights in cyberspace.

A few initiatives have been proposed to enhance inter-state cooperation. One of them centers on creating multilateral conventions establishing standardized procedures for mutual legal assistance, information exchange, and coordinated enforcement of cybercrime laws (H. Wang et al., 2021). These conventions can include provisions for expedited exchange of

electronic evidence, simultaneous investigations, and recognition and enforcement of foreign judgments, thereby allowing for a more cohesive legal response across jurisdictions.

In conclusion, proposals for international cooperation are based on multilateral agreements and universalized procedures. The application of such practices facilitates the resolving of the shortcomings of the current system and forms a foundation for uniform, harmonized, and efficient resolution of transnational cyber disputes.

5.3. Towards a Comprehensive International Convention on Cyber Disputes.

The increasing frequency and complexity of cross-border cyber disputes highlight the urgent need for a consolidating international legal framework. Current legal instruments, such as the Budapest Convention on Cybercrime and regional agreements, provide patchwork and sometimes conflicting solutions. This fragmentation gives rise to jurisdictional gaps, enforcement challenges, and legal uncertainty, undermining the effectiveness of conflict-of-law solutions in cyberspace (Janssen et al., 2021).

A proposed international treaty would attempt to harmonize substantive rules on cyber operations, have uniform procedures for the resolution of disputes, and interpret relevant law for cross-border disputes. The treaty could define basic concepts, like cyberattack, unauthorized access, and electronic evidence, to ensure consistent interpretation by various jurisdictions (H. Wang et al., 2021). The treaty could also contain provisions for mutual legal assistance, cross-border investigations, and harmonized sanctions, reducing possibilities for conflicting legal obligations.

The development of a global treaty requires careful negotiation to balance state sovereignty with the collective interest in regulation. States must reconcile differences in national legal systems, data protection strategies, and approaches to cybercrime liability. In addition, the treaty must incorporate flexible mechanisms to accommodate the rapid technological evolution of cyberspace in order for the legal regime to remain relevant and effective in the long term (H. Wang et al., 2021).

A practical example of this requirement is found in large-scale ransomware attacks across multiple countries where the lack of a unified legal framework impedes investigation, prosecution, and asset recovery. A comprehensive international treaty would enable concerted responses with

fewer duplications of effort and enhanced accountability for cyber actors across borders.

Overall, the establishment of an inclusive international treaty is a forward-looking solution to the issues of cross-border cyber disputes. With harmonized norms, standardized processes, and evolutionary mechanisms, such a framework would foster legal certainty, enable inter-state cooperation, and ensure more effective dispute settlement in cyberspace.

6. Conclusion

This article has demonstrated that cross-border cyber conflicts raise unique challenges to the traditional system of conflict of laws and international humanitarian law (IHL). Cyberspace's nonmaterial and boundary-free nature complicates how one can establish the governing law, jurisdiction, and responsibility, especially in armed conflicts where cyber activities could have humanitarian consequences. The review reiterated that although certain IHL principles-e.g., distinction, proportionality, and necessity—are unchanged, their application to cyber war is not consistent nor properly codified. Moreover, the absence of a binding international convention on cyber wars enhances legal ambiguity and weakens mechanisms for accountability. Therefore, bridging the chasm between private international law and IHL becomes a dire necessity to ensure effective regulation of cyber war and protection of civilian populations.

Recommendations.

1. International Legal Development: States should negotiate an extensive international convention on cyber war which harmonizes conflict of laws principles with humanitarian considerations.
2. Interpretation of IHL Norms: There is a need for international institutions such as the International Committee of the Red Cross (ICRC) to provide authoritative interpretation of the application of underlying IHL rules to cyber operations.
3. Judicial Cooperation: Improved cross-border judicial cooperation and mutual legal assistance mechanisms should be developed to address issues of attribution and enforcement.

4. Capacity Building: Governments must invest in technical and legal capacity that will enable their institutions to investigate, attribute, and prosecute cyber incidents up to international standards.
5. Academic Involvement: Further interdisciplinary research will be required to study the overlap of private international law and IHL in the context of cyberspace, particularly as related to the newly developing technology of artificial intelligence-driven cyber tools.

References .

Abdelkarim, Y. (2023). Jurisdiction Conflicts in Cyberspace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4410115

Batarseh, F. A. (2022). *Cybersecurity Law: Legal Jurisdiction and Authority* (Version 3). arXiv. https://doi.org/10.48550/ARXIV.2206.09465

Biggio, G. (2025). Regulating non-kinetic effects of cyber operations: The 'Loss of Functionality' approach and the military necessity-humanity balance under International Humanitarian Law. *Journal of Conflict and Security Law*, *30*(2), 241–263. https://doi.org/10.1093/jcsl/kraf008

Bodó, B., Gervais, D., & Quintais, J. P. (2018). Blockchain and smart contracts: The missing link in copyright licensing? *International Journal of Law and Information Technology*, *26*(4), 311–336. https://doi.org/10.1093/ijlit/eay014

Chałubińska-Jentkiewicz, K. (2022). Cyberspace as an Area of Legal Regulation. In K. Chałubińska-Jentkiewicz, F. Radoniewicz, & T. Zieliński (Eds.), *Cybersecurity in Poland* (pp. 23–31). Springer International Publishing. https://doi.org/10.1007/978-3-030-78551-2_3

Council of Europe. Convention on Cybercrime (Budapest Convention). Strasbourg; 2001. https://www.coe.int/.../cybercrime/the-budapest-convention

De Miguel Asensio, P. (2024). *Conflict of Laws and the Internet: Second Edition*. Edward Elgar Publishing. https://doi.org/10.4337/9781035315130

Finck, M. (2017). Blockchains and Data Protection in the European Union. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3080322

Gillies, L. E. (2007). Addressing the "Cyberspace Fallacy": Targeting the Jurisdiction of an Electronic Consumer Contract. *International Journal of Law and Information Technology*, *16*(3), 242–269. https://doi.org/10.1093/ijlit/ean002

Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press. https://doi.org/10.1093/oso/9780195152661.001.0001

International humanitarian law and cyber operations during armed conflicts: ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context

of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019. (2020). *International Review of the Red Cross*, *102*(913), 481–492. https://doi.org/10.1017/S1816383120000478

Janssen, H., Cobbe, J., Norval, C., & Singh, J. (2021). Decentralized data processing: Personal data stores and the GDPR. *International Data Privacy Law*, *10*(4), 356–384. https://doi.org/10.1093/idpl/ipaa016

Kowalik-Bańczyk, K., & Pollicino, O. (2016). Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information. *German Law Journal*, *17*(3), 315–337. https://doi.org/10.1017/S2071832200019799

Krasikov, D. V., & Lipkina, N. N. (2020). Sovereignty in Cyberspace: A Scholarly and Practical Discussion: *Proceedings of the XIV European-Asian "The Value of Law" (EAC-LAW 2020)*. XIV European-Asian Congress "The value of law" (EAC-LAW 2020), Ekaterinburg, Russia. https://doi.org/10.2991/assehr.k.201205.028

Mačák, K. (2021). Unblurring the lines: Military cyber operations and international law. *Journal of Cyber Policy*, *6*(3), 411–428. https://doi.org/10.1080/23738871.2021.2014919

Madubuike-Ekwe, J. N. (2021). Cyberattack and the Use of Force in International Law. *Beijing Law Review*, *12*(02), 631–649. https://doi.org/10.4236/blr.2021.122034

Maillart, J.-B. (2019). The limits of subjective territorial jurisdiction in the context of cybercrime. *ERA Forum*, *19*(3), 375–390. https://doi.org/10.1007/s12027-018-0527-2

Mamiya, R., & Vestner, T. (2022). Revisiting the Law on UN Peace Operations' Support to Partner Forces. *Journal of Conflict and Security Law*, *27*(2), 211–227. https://doi.org/10.1093/jcsl/krac010

O'Dair, M., & Beaven, Z. (2017). The networked record industry: How blockchain technology could transform the record industry. *Strategic Change*, *26*(5), 471–480. https://doi.org/10.1002/jsc.2147

Parron, L. M., Villanueva, A. J., & Glenk, K. (2022). Estimating the Value of Ecosystem Services in Agricultural Landscapes Amid Intensification Pressures: The Brazilian Case. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4031123

Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*, *4*(1), 27. https://doi.org/10.1007/s44206-025-00189-4

Ragavan, S. K. (2013). Developing Ethical Values through a Mentoring Scheme. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2438644

Reports. (2020). *International Review of the Red Cross*, *102*(913), 495–509. https://doi.org/10.1017/S181638312000048X
Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, *24*(3), 537–550. https://doi.org/10.1017/glj.2023.24
Savelyev, A. (2018). Copyright in the blockchain era: Promises and challenges. *Computer Law & Security Review*, *34*(3), 550–561. https://doi.org/10.1016/j.clsr.2017.11.008
Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524
Simón, L., & Lanoszka, A. (2020). *The Post-Inf European Missile Balance: Thinking About NATO's Deterrence Strategy (Summer 2020)*. Texas National Security Review. https://doi.org/10.26153/TSW/10224
Tsagourias, N. (2015). The legal status of cyberspace. In N. Tsagourias & R. Buchan (Eds.), *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing. https://doi.org/10.4337/9781782547396.00010
Wang, F. F. (2010). *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* (1st ed.). Cambridge University Press. https://doi.org/10.1017/CBO9780511762826
Wang, H., Dong, T., Ye, M., Yang, D., Jiang, L., & Wu, R. (2021). Modeling Genome-Wide by Environment Interactions Through Omnigenic Interactome Networks. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3765612
World Intellectual Property Organization (WIPO). Blockchain Whitepaper: Opportunities and Challenges for IP. WIPO; 2020.