

International Law and Cyber Technology: Challenges of Global Regulation in the Digital Diplomacy Era

Dewi Triwahyuni^{1*}, Wim Tohari Daniealdi², Iwan Ridwan Zaelani³

^{1*}Universitas Komputer Indonesia

Email: dewi.triwahyuni@email.unikom.ac.id,

²Universitas Komputer Indonesia

Email: wimtohari@email.unikom.ac.id

³Universitas Pasundan

Email: iwanrz@unpas.ac.id

Article Info

Received: 2025-01-12

Revised: 2025-02-21

Accepted: 2025-04-28

Keywords:

international law;
cyberspace; digital
diplomacy; global
regulation; digital
sovereignty

Abstract

The rapid development of information technology has driven a major transformation in international relations, particularly through digital diplomacy. On the other hand, this progress has also posed serious challenges to international law, which has yet to fully regulate cross-border cyber activities. This study aims to examine the main challenges faced by international law in responding to the dynamics of global cyberspace, as well as to evaluate the role of digital diplomacy in shaping fair and inclusive cyber regulations. The research employs a qualitative method using a literature review approach, analyzing scholarly sources, policy reports, and official international documents. The findings reveal a significant legal vacuum in addressing cyberattack attribution, state responsibility, and the protection of human rights in the digital space. Current cyber diplomacy efforts remain hindered by ideological differences between major powers and developing countries, as well as by the dominance of non-state actors such as global technology companies. The conclusion of this study highlights the urgency of establishing a responsive, multistakeholder international legal framework that ensures global digital justice. Without collective efforts and international compromise, cyberspace risks becoming a battlefield of conflict without clear legal boundaries.

I. Introduction

Over the past two decades, the world has witnessed a drastic transformation in how states interact, driven by the rapid advancement of information and communication technologies that have given rise to a new landscape of digital diplomacy. This transformation has not only altered traditional diplomatic practices but has also challenged the structure of international law, which has long served as the main foundation of inter-state relations. Cyber technology enables states, international organizations, and non-state actors to communicate and influence global public opinion within seconds. However, this progress is accompanied by increasing threats to digital security, privacy, and state sovereignty that are not yet fully regulated under existing international law (Kello, 2017).

Incidents such as election system hacking, the spread of disinformation through social media, and cyberattacks on critical infrastructure have become global events that raise widespread concern. Countries like the United States, Russia, and China have been involved in mutual accusations regarding cyber incidents that could trigger diplomatic tensions. However, there is still no legally binding international agreement on the permissible boundaries of actions in cyberspace. Existing legal frameworks such as the UN Charter, the Geneva Conventions, and international humanitarian law do not explicitly address the cyber domain (Schmitt, 2013).

The state of the art (SOTA) shows that academic discourse on cyber regulation in the context of international law continues to evolve. Various studies emphasize the need for a multilateral approach to create a fair and transparent global cyber governance system (Maurer, 2011; Nye, 2014). Several countries and international organizations have pushed for the development of cyber behavioral norms, such as those initiated by the United Nations Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG). However, differences in interests and perceptions of digital sovereignty between Western countries and the Global South often hinder the achievement of global consensus (DeNardis, 2020).

This synthesis reveals a growing gap between the rapid advancement of cyber technology and the sluggish response of international legal systems. Technology is inherently transnational, while law remains tightly bound to state jurisdiction. This tension raises critical questions: how can international law address global challenges without compromising the principles of sovereignty and human rights in digital space? The challenge becomes even more complex as cyber actors now

include not only states but also global technology corporations with power and influence nearly equal to that of states (Bradshaw, Millard & Walden, 2011).

This study aims to examine the main challenges faced by international law in formulating global regulations on cyber activities, and to evaluate the dynamics of digital diplomacy as an arena of contestation between national interests and the need for international cooperation. Thus, this study seeks to provide both theoretical and practical contributions to understanding the paradigm shift in international law in the digital era, which is full of uncertainty and complexity. The method used in this research is a literature review with a descriptive-analytical approach. The literature review focused on relevant academic publications, including reputable international journals, policy reports, and official documents from international organizations. The analysis centered on studies addressing issues of cyber law, global governance, and digital diplomacy. This approach enables the author to identify patterns, gaps, and opportunities in the normative developments at the international level.

One of the main challenges in formulating cyber regulation lies in its highly dynamic and borderless nature. Cyberattacks can be launched from one jurisdiction against systems in another without any physical movement. This presents difficulties in proof, attribution, and the application of state responsibility principles under international law (Tsagourias & Buchan, 2015). In addition, varying security standards, threat definitions, and states' capacities to respond to cyberattacks further complicate the harmonization of legal frameworks.

Digital diplomacy has emerged as a new arena for states to project influence and pursue their interests. However, the dominance of major powers in setting technical standards and cyber protocols also raises concerns about the marginalization of developing countries. In this context, multistakeholder diplomacy involving the private sector, civil society, and the technical community is considered a more inclusive approach (Hintz, Milan & Wahl-Jorgensen, 2019). Nonetheless, this approach still faces challenges in legitimacy and effectiveness in global decision-making processes.

Furthermore, the imbalance between national security protection and freedom of expression in digital space has become a sensitive issue in international cyber law. States often use security concerns as justification to restrict access to information and control digital narratives. In the long term, such practices may threaten the global democratic order and create digital fragmentation, further widening the global digital divide (MacKinnon, 2012).

Disparities in digital capacity and the availability of legal resources between

developed and developing countries are also significant barriers to formulating equitable cyber policies. Developing countries often fall victim to cyberattacks without adequate legal or technical means to respond. Therefore, an international mechanism is needed—one that not only prioritizes security but also promotes global digital justice (UNIDIR, 2021).

Through this study, the author hopes to contribute to enriching the understanding of the relationship between international law, cyber technology, and digital diplomacy. This research is crucial to support efforts to reform international law so it can be more adaptive to the evolving challenges of the digital age. Moreover, the findings of this study can serve as input for policymakers and diplomats in building a global cyber legal architecture that is more responsive, inclusive, and sustainable.

2. Research Method

This study employs a qualitative method using a library research approach to analyze the challenges faced by international law in regulating global cyberspace amidst the dynamics of digital diplomacy. The review is conducted using a descriptive-analytical approach on secondary sources such as international scholarly journals, academic books, reports from international institutions (such as the UN, UNIDIR, and ICANN), as well as relevant policy documents. The selection of literature is based on topic relevance, publisher credibility, and the recency of publications, with a primary focus on the period between 2010 and 2024 to capture contemporary developments.

The data is analyzed using a thematic approach by mapping key issues such as cyber legal norms, digital sovereignty, cyberattack attribution, and the role of multistakeholder diplomacy. The researcher identifies patterns of argumentation, regulatory gaps, as well as points of convergence and conflict within international legal discourse related to cyber technology. This method is selected as it is well-suited for examining an evolving phenomenon that lacks established legal consensus, and for producing a conceptual synthesis that can serve as a foundation for developing the discourse on international cyber law in a global context.

3. Results and Discussion

In this section, the researcher will present the findings and analyze the key issues that are the focus of the study. The analysis covers the gap in international law regarding the regulation of cyberspace, highlighting the weakness of formal regulations in addressing the complex dynamics of cross-border digital activities. The study also examines the challenges of establishing global regulations through cyber diplomacy, where differing interests and ideologies among countries often hinder the achievement of mutual agreements.

Furthermore, the analysis explores the role of non-state actors in international cyber governance, especially major technology companies and civil society organizations that significantly influence the shaping of norms and policies in cyberspace. Finally, the research addresses issues of digital sovereignty, global inequality, and the protection of human rights in the digital realm—critical debates that seek to balance state interests with the rights of individuals in an ever-evolving information technology era.

1. The Void of International Law in Regulating Cyberspace

Although international law has evolved to address global challenges in various sectors such as armed conflict, human rights, and the environment, cyberspace remains a normatively ambiguous domain. There is no single treaty or international convention that comprehensively regulates state behavior in cyberspace. Meanwhile, digital activities—whether by states or non-state actors—are increasingly impacting sovereignty, national security, and international stability. In this context, the legal vacuum becomes even more apparent as cyber threats grow in complexity and frequency (Schmitt, 2017).

One fundamental problem in international cyber law is the ambiguity of attribution. In conventional warfare law, identifying the perpetrator—such as a state—for acts of aggression can be established through intelligence and explicit recognition. However, in cyberspace, attribution is highly complicated. Cyberattacks can be disguised, launched from multiple jurisdictions, and executed through third-party devices without direct traces. This obscures the principle of “state responsibility” because it is difficult to precisely determine which state is accountable for an attack (Tsagourias & Buchan, 2015).

This ambiguity is exacerbated by the lack of uniform interpretation regarding the principles of non-intervention and use of force in cyberspace. For example, can an attack that disables a country's power grid be categorized as a “use of force” under Article 2(4) of the UN Charter? Or is an attack on a state's media and information infrastructure a form of intervention in domestic affairs? There is no global consensus on answering these questions. Consequently, many states interpret international law principles according to their own national interests (Kleffner & Dinniss, 2019).

A concrete example of this legal vacuum can be seen in the Stuxnet incident, aimed at damaging Iran's nuclear facilities in 2010 but only discussed extensively in legal terms years later. Although strongly suspected to involve major states, no international sanctions were imposed, nor was there explicit recognition of legal violations. This case demonstrates that the cyber legal gap creates a space of impunity, where states or other cyber actors can act without fear of international legal consequences (Lin, 2016).

Similarly, attacks on global supply chain systems such as the 2020 SolarWinds incident, which affected government agencies and major companies in the United States, highlight the global scale of risks. However, international legal responses to these events remain reactive and are mostly conducted through diplomatic forums or unilateral sanctions

rather than international courts (Lewis, 2021). This reflects the limitations of collective mechanisms in addressing legal violations in cyberspace.

Some argue that traditional international law principles are sufficiently flexible to be applied in the cyber context. However, without codification and interpretive consensus, this flexibility becomes a weakness as it allows states to justify ethically and politically problematic actions. Normative processes such as the Tallinn Manual 2.0 have attempted to outline international law principles applicable to cyberspace, but they remain non-binding academic guidelines rather than formal legal documents (Schmitt, 2017).

In practice, this legal vacuum directly impacts global political instability. States have begun developing offensive cyber strategies as part of their defense policies without clear international oversight. For example, national security strategy documents of some countries explicitly state capabilities to “launch pre-emptive cyberattacks,” which naturally open the door to escalation of digital conflicts (Buchan, 2018). The absence of a legal framework regulating the boundaries of such actions creates legal uncertainty and increases the potential for conflict.

Furthermore, this legal gap affects developing countries with limited cyber capabilities. These countries are more vulnerable to cyberattacks and digital exploitation but lack strong bargaining power in global forums to advocate for fair regulations. This illustrates that the imbalance in international cyber governance is not only a technological issue but also a matter of global legal justice (Maurer, 2018).

The absence of formal legal instruments also raises ethical implications. For example, the use of cyber technology in intelligence operations, manipulation of public opinion, or interference in foreign elections has become a recurring practice but is rarely legally processed. Such actions clearly affect the integrity of democracy and social stability. In this context, the legal vacuum functions not as a “neutral zone,” but rather as a power gap (DeNardis, 2020).

Therefore, it is urgently necessary to develop specific and binding international legal instruments to regulate cyberspace. This process requires political courage, willingness to compromise among states, and involvement of various non-state actors. Without this, cyberspace will continue to be a free arena for asymmetric conflict, political manipulation, and human rights violations that are beyond the reach of existing legal mechanisms (Kello, 2017).

2. Challenges in Establishing Global Regulation through Cyber Diplomacy

Efforts to establish global governance over cyberspace have been ongoing for more than two decades; however, the results remain very limited and have yet to produce legally binding norms. In many respects, cyber diplomacy occupies a complex position due to the deep ideological clashes between various countries, particularly between Western blocs and countries such as Russia and China.

Table 1. Comparison of Cyber Governance Paradigms Between Western Countries and Russia & China

Aspect	Western Countries	Russia & China
Paradigm	Multi-stakeholder	Digital sovereignty
Main Focus	Transparency, freedom of information	Control of domestic information
Involvement of Non-State Actors	Very open	Tend to be closed
International Regulation	Promote global norms	Promote state-based norms
Main Challenges	Fragmentation, corporate dominance	Lack of global legitimacy

Western countries tend to promote a multi-stakeholder governance model that upholds the principles of freedom of information, transparency, and private sector involvement. Conversely, China and Russia prioritize the concept of digital sovereignty, where states have full control over their domestic digital space, including censorship policies and information surveillance (Segal, 2018).

These differing paradigms have directly contributed to stagnation in international forums attempting to develop cyber law norms. Two primary forums often cited are the United Nations Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG). Although both have successfully formulated several general principles regarding state responsibility in cyberspace, no agreement has yet been reached on a legally binding international treaty. A key issue remains disagreement over whether existing international legal principles are sufficient to govern cyberspace or if a new legal regime is required (UNIDIR, 2021).

In diplomatic negotiations, geopolitical factors pose significant obstacles. Major powers view cyberspace as a strategic element in global competition, thus are reluctant to make concessions that would restrict their digital maneuverability. For example, the United States is cautious about signing agreements that could impede its cyber intelligence operations. Meanwhile, Russia and China reject broad involvement of non-state actors, viewing them as instruments of Western cultural and political dominance. The result is deadlock, where cyber diplomacy more often produces non-binding normative documents (Carr, 2016).

This phenomenon shows that digital diplomacy often serves more as a contest of interests than as collaboration toward global governance. Amidst this fragmentation, various regional initiatives frequently overlap. The European Union developed the General Data Protection Regulation (GDPR), which has a broad global impact, while China designed a stringent Cybersecurity Law to protect domestic data. Although these policies are legally valid domestically, their implications for interstate relations and global actors cause jurisdictional conflicts and diplomatic tensions (Bradshaw, Millard & Walden, 2017).

Such tensions are also reflected in difficulties drafting norms on responsible state behavior in cyberspace. For example, while Western countries emphasize that attacks on critical infrastructure should be considered serious violations, some other countries stress the importance of protecting domestic information stability. Failure to reach a consensus on definitions of “cyberattack” and “information intervention” has led cyber diplomacy to revolve around normative discussions without implementation certainty (Finnemore & Hollis, 2016).

Beyond states, the presence of non-state actors such as major technology companies complicates diplomatic processes. Companies like Google, Microsoft, and Meta hold global influence and cross-border infrastructure that sometimes do not fully comply with national laws. States advocating for technology company involvement are often accused of politicizing cyberspace for economic gain. Conversely, countries that exclude corporate participation risk stifling innovation and the multistakeholder engagement needed to build inclusive governance (Mueller, 2017).

Another challenge is the disparity in capacity among countries to understand and respond to digital diplomacy issues. Developing countries often lack the technical and diplomatic resources to participate actively in global forums. Consequently, the narratives and norms developed tend to be dominated by major powers with vested interests. This imbalance creates the risk of an elitist cyber governance that does not represent broader global needs fairly (Riordan, 2020).

Moreover, digital diplomacy faces linguistic, cultural, and political barriers in drafting legal terminology acceptable to all parties. Terms such as “digital sovereignty,” “information stability,” or “information manipulation” may carry very different meanings across countries. Without shared understanding of these key concepts, it is impossible to draft an international agreement with universal legitimacy (Betz & Stevens, 2016).

Some suggest a hybrid approach between hard law and soft law as a middle ground. This model allows states to gradually engage in consensus building without immediate legal bindingness. However, this approach is criticized for being too weak to provide legal certainty, especially on crucial issues such as critical infrastructure protection or cyber weapons non-proliferation (Peters, 2020).

In conclusion, cyber diplomacy faces serious challenges in realizing a global regulatory framework that is fair, inclusive, and effective. Ideological differences, geopolitical conflicts, domination by certain actors, and a lack of enforcement mechanisms are real obstacles that must be overcome. Without a transformation toward more open, collaborative, and interest-based diplomatic approaches, global cyberspace regulation will remain a discourse without concrete legal substance.

3. The Role of Non-State Actors in International Cyber Governance

In the governance of international cyberspace, non-state actors play an increasingly central and complex role. Global technology companies such as Google, Meta (formerly Facebook), Microsoft, and Huawei are no longer just business entities but also geopolitical actors that influence the direction of policies, norms, and even global laws in cyberspace. For example, Meta's decisions on content moderation or Google's steps to restrict access to certain information have widespread impacts on the digital rights of citizens worldwide. These companies control critical global information infrastructure—from search engines and cloud servers to communication platforms—making them key players in the architecture of digital security and international cyber policy (DeNardis, 2014).

However, the dominance of these global corporations raises fundamental dilemmas regarding legitimacy and accountability. Unlike states that hold democratic mandates through constitutions or elections, technology companies operate based on shareholder interests and business models. This raises questions: who oversees these companies as they manage data of billions of users? What mechanisms ensure their accountability over algorithm policies, data security, or blocking decisions? When companies like Huawei engage in digital infrastructure projects across developing countries, concerns about cross-border political influence and cybersecurity increase (Maurer, 2018). This illustrates that the involvement of non-state actors is often politically charged, embedded with economic considerations and the national strategies of their countries of origin.

Table 2. Roles and Challenges of Non-State Actors in Cyber Governance

Non-State Actor	Main Role	Challenges
Technology Companies (Big Tech)	Provide infrastructure, content regulation	Accountability, market dominance, conflicts of interest
NGOs & Technical Communities	Advocate for digital rights, develop technical protocols	Limited representation, resource constraints
Cybersecurity Vendors	Detect and mitigate threats	Security privatization, limited legal authority

Technical communities and civil society organizations (NGOs) also contribute significantly to shaping norms and advocating for digital rights. Organizations such as the Internet Society (ISOC) and the Electronic Frontier Foundation (EFF) play roles in developing technical protocols and defending civil liberties in the digital realm. However, their presence in international forums like the Internet Governance Forum (IGF) or the Global Commission on the Stability of Cyberspace (GCSC) still faces challenges regarding representation and effectiveness. Many of these NGOs come from developed countries, while civil actors from developing countries often struggle to participate due to resource limitations, information access, or language barriers. This raises the risk that globally agreed norms are neither inclusive nor reflective of the diversity of global interests (Hofmann, Katzenbach & Gollatz, 2017).

On the other hand, the privatization of digital security by private companies also creates new tensions between states and the private sector. In many cases, states no longer have full control over cyber incident detection and response tools, as these are managed by private vendors or third-party infrastructure. For example, in many ransomware attacks or major data breaches, the first responders and public communicators are cybersecurity companies like FireEye or Kaspersky, not government agencies. This raises dilemmas: to what extent can states rely on private parties to maintain national security in cyberspace? Can states mandate private sector involvement in security policies without violating principles of market freedom or innovation? (Carr, 2016).

Meanwhile, in the Indonesian context, Indonesia has demonstrated a significant role for non-state actors in cyber governance through the active involvement of digital communities, NGOs, and the private sector in both national and international cyber policy forums. Organizations such as the Indonesian Telematics Society (MASTEL) and ICT Watch actively participate in the Internet Governance Forum (IGF) and ASEAN discussions on internet governance and cybersecurity, contributing local perspectives that strengthen Indonesia's position in global norm formation (Putra, 2018; Pratama, 2019). This role reflects an inclusive multistakeholder approach, where, besides the government, private sector and civil society actors actively participate in regulation and digital advocacy processes.

A concrete example is the involvement of non-state actors in drafting the Personal Data Protection Act (PDP Law) enacted in 2022. The regulatory formulation process involved open dialogue among the government, NGOs, digital communities, and academics to ensure policies responsive and appropriate to societal needs in the digital era (Nugroho & Susanti, 2021). This approach shows that strengthening cyber governance in Indonesia relies not only on state instruments but also on active participation by non-state actors, making resulting regulations more inclusive and adaptive to technological developments (Sari et al., 2022).

Ultimately, although the involvement of non-state actors has enriched the global cyber governance landscape with new perspectives and capacities, questions of accountability, representation, and power distribution remain. To create fair and sustainable cyber governance, a collaborative framework recognizing the roles of all actors is necessary, while prioritizing the protection of citizen rights and state sovereignty. Balancing the technocratic efficiency offered by the private sector with the democratic principles upheld by states is crucial to addressing future challenges in cyber governance (Floridi, 2020).

4. Digital Sovereignty, Global Inequality, and Human Rights

In the digital era, the concept of state sovereignty faces fundamental challenges. Cyberspace has become a new domain that transcends geographical boundaries, making state efforts to protect territorial integrity, political systems, and populations from digital threats increasingly complex. Developing countries often fall victim to cross-border cyberattacks—whether criminal, economic, or geopolitical—without having sufficient

technical capacity or legal frameworks to respond effectively. For example, many government systems in Africa, South Asia, and Latin America are attacked by unidentified malware or hackers, while these countries lack robust digital forensic tools or national cybersecurity teams to respond adequately (Tanczer et al., 2018). This imbalance creates a worrying dependency on private security firms from developed countries, which in turn places developing states in subordinate positions within the global cyber governance system.

This gap also reflects global disparities in digital infrastructure and regulatory capacity. Developed countries such as the United States, the United Kingdom, and some European Union members possess advanced digital security systems, established privacy regulations, and active participation in international negotiations concerning cyber norms. Conversely, many developing countries still struggle with building basic internet infrastructure, fragmented data regulations, and limited human resources in technology. This has serious consequences for establishing fair global cyber governance. Countries most affected by cyberattacks or digital inequality are often the least heard in international forums due to diplomatic, technical, or political limitations (Broeders & Dunn Cavelt, 2020).

In this context, the protection of human rights—especially digital rights—becomes a highly critical issue. In various authoritarian regimes, digital technology is used to expand mass surveillance, restrict freedom of expression, and censor information. Such practices violate civil liberty principles and create tensions between international human rights norms and the principle of digital sovereignty claimed by states. For example, in recent years, China, Iran, and Russia have actively strengthened domestic information control systems under the guise of digital sovereignty, yet these steps often lead to restrictions on internet freedom and individual privacy (Hintz & Milan, 2019). When sovereignty principles are used to justify human rights violations, the urgency for global regulation balancing state rights and citizen rights becomes paramount.

Furthermore, the current international legal architecture lacks a universal instrument explicitly regulating human rights protection in cyberspace. Although human rights principles in the UN Charter and the Universal Declaration of Human Rights are considered applicable online, their implementation is often hindered by jurisdictional challenges, encryption technology, and states' unwillingness to submit to international oversight mechanisms. Disparities in states' capacity to enforce these principles make citizens in developing countries more vulnerable to privacy violations and suppression of opinion. Therefore, developing international norms that unite the spirit of human rights protection and the principle of digital sovereignty is a strategic agenda in global diplomacy (Kerry, 2021).

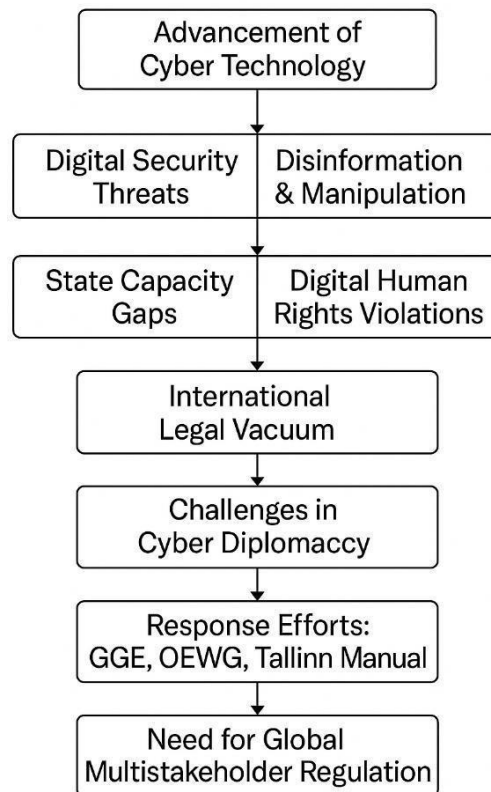


Figure 1. Model of Digital Sovereignty Challenges, Global Inequality, and Human Rights in Cyberspace

The rapid development of cyber technology significantly impacts various aspects of global security and governance. On one hand, this progress creates increasingly complex digital security threats, including cyberattacks targeting critical infrastructure and personal data. On the other hand, the emergence of disinformation and information manipulation presents new challenges threatening the integrity of digital communication and socio-political stability.

The insufficient capacity of states to face these cyber challenges widens the gap in protection and law enforcement capabilities in the digital domain. This is exacerbated by digital human rights violations that are difficult to address without adequate international legal frameworks. Such conditions create an international legal vacuum that weakens global coordination and response efforts to cyber issues.

To address this complexity, cyber diplomacy becomes an important arena for building international consensus and norms. Various initiatives such as the Group of Governmental Experts (GGE), Open-ended Working Group (OEWG), and the Tallinn Manual guidelines serve as initial responses attempting to fill the legal vacuum and strengthen cyber governance. However, the biggest challenge remains the need for inclusive,

multistakeholder global regulation that can respond to technological dynamics and maintain a balance of interests among states and non-state actors.

4. Conclusion

The conclusion of this study asserts that the existence of cyberspace as a new arena in international relations presents fundamental challenges to the international legal system, which has traditionally been oriented toward physical territories and state actors. The absence of legally binding norms to regulate cross-jurisdictional cyber activities, the difficulty of attributing cyberattacks, and disparities in states' capacities to respond to digital threats demonstrate that current legal instruments have yet to keep pace with the rapid development of information technology. Although digital diplomacy has become an important forum for formulating norms of state behavior in cyberspace, it remains hindered by ideological differences, geopolitical interests, and the dominance of certain actors, including major states and global technology corporations. In this context, a more inclusive and accountable multistakeholder approach is needed to ensure that global cyber regulations do not merely serve the interests of a few powerful actors but also reflect the needs and protections of developing countries and the digital rights of global citizens. Reforming the international legal system must include the codification of clear norms, strengthening mechanisms for international cooperation, and integrating human rights principles into global cyber governance so that cyberspace can become a safe, just, and sustainable domain for all humanity.

References

- Betz, D. & Stevens, T. 2016. *Cyberspace and the State: Toward a Strategy for Cyberpower*. Routledge.
- Bradshaw, S., Millard, C. & Walden, I. 2011. Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. *International Journal of Law and Information Technology*, 19(3), pp. 187–223.
- Bradshaw, S., Millard, C. & Walden, I. 2017. Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 21(3), pp. 187–222.
- Broeders, D. & Dunn Cavelty, M. 2020. Security by Proxy: The Shifting Role of the State in Cybersecurity Governance. *Science and Public Policy*, 47(1), pp. 55–66.
- Buchan, R. 2018. *Cyber Espionage and International Law*. Oxford: Hart Publishing.
- Carr, M. 2016. Public–Private Partnerships in National Cyber-Security Strategies. *International Affairs*, 92(1), pp. 43–62.
- DeNardis, L. 2014. *The Global War for Internet Governance*. Yale University Press.
- DeNardis, L. 2020. *The Internet in Everything: Freedom and Security in a World with No Off Switch*. Yale University Press.
- Finnemore, M. & Hollis, D. 2016. Constructing Norms for Global Cybersecurity. *American*

- Journal of International Law*, 110(3), pp. 425–479.
- Floridi, L. 2020. Ethics of Information and the Internet Governance. *Philosophy & Technology*, 33(1), pp. 1–5.
- Hintz, A. & Milan, S. 2019. *Digital Citizenship in a Datafied Society*. Wiley-Blackwell.
- Hintz, A., Milan, S. & Wahl-Jorgensen, K. 2019. *Digital Citizenship in a Datafied Society*. Polity Press.
- Hofmann, J., Katzenbach, C. & Gollatz, K. 2017. Between Coordination and Regulation: Finding the Governance in Internet Governance. *New Media & Society*, 19(9), pp. 1406–1423.
- Kementerian Komunikasi dan Informatika Republik Indonesia 2022. *Undang-Undang Perlindungan Data Pribadi: Proses dan Implikasi*. Jakarta: Kominfo.
- Kello, L. 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press.
- Kerry, C.F. 2021. The Global Race to Regulate Artificial Intelligence: A Comparative Analysis. *Brookings Institution*.
- Kleffner, J.K. & Dinniss, H.A.S. 2019. Applicability of International Law in Cyberspace: Challenges and Developments. *International Law Studies*, 95(1), pp. 1–25.
- Lewis, J.A. 2021. The SolarWinds Cyberattack: Lessons for International Cooperation. *Center for Strategic and International Studies (CSIS)*.
- Lin, H. 2016. Attribution of Malicious Cyber Incidents: From Soup to Nuts. *Journal of National Security Law & Policy*, 8(2), pp. 289–310.
- MacKinnon, R. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. Basic Books.
- Maurer, T. 2011. Cyber Norm Emergence at the United Nations. *Belfer Center for Science and International Affairs*. Available at: <https://www.belfercenter.org>
- Maurer, T. 2018. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press.
- Mueller, M. 2017. *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Polity Press.
- Nye, J.S. 2014. The Regime Complex for Managing Global Cyber Activities. *Global Commission on Internet Governance Paper Series*, No. 1.
- Peters, A. 2020. Soft Law as a New Mode of Governance. *Swiss Review of International and European Law*, 30(4), pp. 415–433.
- Putra, D. & Santosa, B. 2023. Multistakeholder Approach dalam Regulasi Data Pribadi di Indonesia. *Jurnal Hukum dan Teknologi*, 7(1), pp. 80-95.
- Ramdani, F. 2020. Peran Komunitas Digital Indonesia dalam Forum Tata Kelola Internet. *Jurnal Teknologi Informasi*, 12(3), pp. 45-57.

- Riordan, K. 2020. Cyber Diplomacy: The Making of an International Cyber Regime. *Global Society*, 34(1), pp. 1–18.
- Schmitt, M.N. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.
- Schmitt, M.N. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
- Segal, A. 2018. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. PublicAffairs.
- Sari, M.P., Dewi, N.K. & Wulandari, S. 2022. Multistakeholder Engagement in Indonesian Cyber Law Reform. *Indonesian Journal of Cyber Governance*, 3(1), pp. 20-34.
- Tanczer, L.M., Lopez-Neira, I. & Wachter, S. 2018. Technologically Facilitated Abuse: The Intersection of Cybersecurity and Domestic Violence. *Crime, Law and Social Change*, 72(3), pp. 249–271.
- Tsagourias, N. & Buchan, R. 2015. *Research Handbook on International Law and Cyberspace*. Cheltenham: Edward Elgar Publishing.
- UNIDIR 2020. The Role of International Law in the Context of State Use of ICTs. Geneva: United Nations Institute for Disarmament Research.
- UNIDIR 2021. Cybersecurity and International Norms: Findings and Recommendations. Geneva: United Nations Institute for Disarmament Research.
- UNIDIR 2021. International Law and Cyber Stability. Geneva: United Nations Institute for Disarmament Research.
- Widyanto, A. 2019. Advokasi Kebijakan Siber dan Keamanan Data di Indonesia. *Indonesian Journal of Cyber Policy*, 5(1), pp. 23–38.
- Zwitter, A. & Boisse-Despiaux, M. 2020. Blockchain for Humanitarian Action and Development Aid. *Journal of International Humanitarian Action*, 5(16), pp. 1–8.