



INTERNATIONAL JOURNAL OF LAW AND CONSTITUTION STUDY

Journal home page: <https://jurnal.asrypersadaquality.com/index.php/ijlacos>

A RECONSTRUCTION OF THE PRINCIPLE OF NATIONAL SOVEREIGNTY IN AN ERA OF GLOBAL DIGITAL INTERVENTION

Asti Nurul Puspita¹, Riza Aulia², Risa Siti Fadilah³, Muhammad Rahman Rizqi⁴

Faculty Of Sharia And Law, Department Of Islamic Criminal Law, State Islamic University Of North Sumatra

uulaza1206@gmail.com rizaaulia2323@gmail.com muhammad0205232042@uinsu.ac.id
risasitifadilah@uinsu.ac.id

ABSTRACT

The rapid development of information technology and communication in the digital age has given rise to new modus operandi of global digital interventions that threaten the existence of the state. Traditional state sovereignty, which has been built on the basis of physical territoriality and the principles of conventional non-intervention, has proved insufficient in the face of transcended cyber threat dynamics, nirid, and nirada. Cyberintervention of critical infrastructure hacking, mass disinformation, and data exploitation by multinational tech corporations can descale a country's political, economic, and domestic security authority without the presence of the perpetrators. The study aims to analyze the urgency of the reconstruction of the principles of national sovereignty in international law, to evaluate the various national regulatory models adopted by some areas, and to adopt the ideal dimension of global digital sovereignty. The study employs normative-law research methods with a conceptual and comparative approach. Data used in secondary legal materials obtained through literature studies of books, scientific journals, international law instruments, and associated policy documents. Research indicates that national sovereignty should be interpreted by extending ideas to the digital space. The reconstruction includes three main dimensions: expansion of cyberjurisdiction, reinforcement.

KEYWORDS

National Sovereignty, Digital Interference, Global Law, Sovereignty In The Digital World, Virtual Space.

Corresponding Author: Asti Nurul Puspita				
Article History	Submitted: March 16, 2026	Revision: March 18, 2026	Accepted: March 30, 2026	Published: July 30, 2026
https://doi.org/10.63736/ijlacos.v3i1				

INTRODUCTION

The writing was designed to explore its importance, compare the different models of Settings, and examine the challenges of international law in retailing the principles of national sovereignty amid increasing global digital interventions that are increasingly unbound by physical limitations. The authors understand that the rapid progress of information technology and communication has drastically altered the fabric of international relations. On the one hand, cyberspace presents many opportunities; But on the other hand, there are new asymmed-such as attacks on critical infrastructure, massive misinformation dissemination, and misuse of data that threaten the political power of a country without the presence of a person.

This situation presents a legal dilemma, especially in interpreting article 2 verse (4) the UN charter relating to the restriction of violence, as well as article 2 verse (7) the UN charter concerning the principle of non-intervention in internal affairs, which is now often violated through cross country cyberactivity. Thus, in this text, the writer seeks to reformulate interpretations that include three main dimensions: enlarging diplomatic jurisdictions, strengthening autonomy in national regulations, and the creation of more responsive multilateral legal frameworks in the future. The process of creating this scientific work is not without guidance, support, and collaboration among those who have accomplished it.

RESETACH AND METHOD

The study falls under the category of normative law study, a study aimed at learning and analyzing the principles of law, doctrine, law rules, and harmonizing law regulations at both national and international levels that relate to the concept of state sovereignty in the digital age. The main focus of the study was conceptual studies on understanding conventional international laws in responding to the phenomenon of global cyberintervention.

The legal materials used in this research are categorized into three layers:

- Primary legal materials, consisting of the Universal Declaration of Human Rights (UDHR) 1948, the International Covenant on Civil and Political Rights (ICCPR) 1966, the General Data Protection Regulation (GDPR) 2016, and Law Number 27 of 2022 on Personal Data Protection.

- Secondary legal materials, comprising academic journals, books, and scholarly works addressing personal data protection, international law, and cybersecurity.
- Tertiary legal materials, including legal dictionaries and encyclopedias used to support the interpretation of legal terminology throughout this study.

2.2 Data Collection

Legal collecting was done by means of literature study methods. This process involves searching, reading, recording, and compiling of academic literature and international documents of cyberlaw that are relevant to the reconstruction issue of state sovereignty.

2.3 Data Analysis

The collected legal material was analyzed using analytic qualitative descriptive methods. Researchers elaborated on the draft of the law, described the differences between the concept of physical sovereignty and digital space, and deductive conclusions to formulate responsive three dimensions of legal reconstruction.

RESULTS AND DISCUSSION

Results

Based on the analysis of various secondary legal materials, international legal instruments, and cyber policy documents, the research findings are divided into three main discoveries: National sovereignty is the highest power a country has to manage and run all matters within its legal jurisdiction without interference from other parties (Shaw, M.N, 2021). However, rapid advancements in the field of information and communication technology in the digital age have created new forms of global digital interventions that threaten the existence of nations. Digital interventions include cyber attacks that damage a country's critical infrastructure, such as power grids, communication systems, and financial sectors. They also involve spreading false information on digital platforms to influence public opinion and election outcomes. Additionally, it includes the control of large amounts of data by foreign multinational technology companies, which can shape economic direction (Balarabe.K, 2025).

Characteristics of Digital Regulation Model Comparisons: In response to challenges in digital interventions, several countries and regions have developed their own regulatory models to reflect the principle of digital sovereignty.

This includes the European model, represented by GDPR and DSA, which focuses on protecting individual rights and ensuring accountability of digital platforms (Pierucci. F, 2025). Next, there is the Asia (China) model through cyber security and data protection laws that encourage the government to tightly control critical infrastructure based on localized data. Finally, countries in Southeast Asia, including Indonesia, use a mixed approach that aims to find a balance between national security, digital economic growth, and the protection of human rights.

Traditional notions of state sovereignty, which have long been based on physical territory and conventional non-intervention principles, are no longer sufficient to address the complexities of cross-border, identityless, and territory-free cyber threats. Therefore, the reconstruction of the principle of national sovereignty must be realized through three main dimensions: expanding the concept of sovereignty to the digital realm (digital sovereignty, which includes data, infrastructure, algorithmic, and normative sovereignty) (Fratini, 2024); strengthening national rules/regulations based on regulatory autonomy; and creating a new international legal framework that is responsive (Santaniello. M, 2025).

Discussion

The findings show that the concept of state sovereignty in classic international law, which is based on the idea of territorial territory, has difficulty in interpretation when faced with the reality of cyberspace. Since the Treaty of Westphalia was signed in 1648, the idea of sovereignty has been understood as the highest power to manage all matters within its jurisdiction without outside interference (Shaw, M.N, 2021). However, when cyber intervention actions damage important infrastructure such as power networks and the financial sector, conventional international law often faces legal gaps due to the difficulty in obtaining physical evidence, making it urgent to update interpretations towards the dimension of digital sovereignty (Santaniello. M, 2025).

The impact of this global digital intervention is uneven and widespread, especially because multinational tech companies control data around the world. This

allows them to influence people's behavior and affect domestic political power without being physically present (Balarabe.K, 2025). A comparison study of different regulatory models shows that the European Union model is best at protecting citizens' rights through the GDPR (2016), but it has a weakness in the complexity of the rules, which can slow down innovation (Pierucci). F, 2025). On the other hand, the Chinese model gives full control to the government through data localization policies, but it is vulnerable to abuse of power that can threaten freedom of expression. A mixed approach, now being used in Indonesia, tries to balance economic growth with data security. This shows that each country must create its own national rules to monitor foreign platforms and protect its citizens' data sovereignty.

Around the world, traditional borders are becoming weaker because of difficulties in working together, caused by differences in country rules and the hidden nature of people in the online world. Academic documents like the *Tallinn Manual* have made important contributions to shaping the understanding of cyber norms, but these documents still cause serious debates about what types of cyber attacks can be classified as the use of force under Article 2(4) of the UN Charter.

So, the most important step in rebuilding international norms is to strengthen multilateral forums like the Internet Governance Forum (IGF), the United Nations Group of Governmental Experts (GGE), and the Open-Ended Working Group (OEWG). By strengthening this multilateral platform, the international community can create new universal behavior norms for cyberspace, clarify attribution mechanisms to deal with anonymous actors, and agree that digital sovereignty violations are real breaches of the non-intervention principle (Chatinakrob, T.2024).

CONCLUSION

Rapid growth in the field of information and communication technology in the digital age has created new ways, in the form of global digital interventions, that threaten the existence of nations. This progress creates a big opportunity for international relations, but at the same time, the significant global reliance on the digital ecosystem introduces new vulnerabilities that threaten the traditional foundations of nations. Therefore, the reconstruction of the principle of state sovereignty has become an urgent issue in contemporary international law to better face the challenges of the times with greater adaptability. In classical international

law, the concept of state sovereignty is rooted in the 1648 Westphalia Treaty, which defined sovereignty based on physical territorial boundaries and the traditional principle of non-intervention. However, the classic international legal framework struggles with interpretation and often faces legal gaps when dealing with the reality of the cyberspace environment, which is borderless, identityless, and territory-free.

This situation requires updating the traditional concept of sovereignty to include the dimension of digital sovereignty. In the age of global digital intervention, achieving digital sovereignty involves strengthening the ideal aspects, such as national regulatory autonomy that covers control over data (data sovereignty), independence in network infrastructure, oversight of artificial intelligence algorithms (algorithmic sovereignty), and the right to set normative regulatory standards.

These dimensions aim to ensure that countries have strong regulatory autonomy to protect their national interests in the digital world while still actively participating in global digital connectivity. Countries play a key role in strengthening national regulations and developing independent digital ecosystems within their own borders.

On the other hand, multilateral forums such as the Internet Governance Forum (IGF), the United Nations Group of Governmental Experts (GGE), and the Open-Ended Working Group (OEWG) help shape the behavior rules that countries follow in the cyber space. Working together between a country's own control and strengthening international groups is important for creating a global and legally secure cyber management system.

Even though national regulatory autonomy is being worked on, there are still major challenges that threaten the country's sovereignty in the cyber space. The challenges include asymmetric actions such as hacking critical infrastructure, spreading organized disinformation to manipulate democratic processes, and the dominance of data capitalism by foreign multinational technology companies. This situation is made worse by the anonymity of cyber criminals and the limitations of traditional territories, which make it difficult to provide physical evidence in conventional international law.

Therefore, expanding cyber jurisdiction, strengthening national regulations based on cyber autonomy, and creating a new international legal framework that is

fully responsive are all necessary. These strategic steps will help rebuild national sovereignty effectively in the global digital age, allowing for clear accountability in cyberspace through well-defined attribution mechanisms, ensuring domestic security, and maintaining the nation's presence and independence in the virtual world.

REFERENCES

- Andika, T. (2018). Information sovereignty in the digital age: A theoretical and international law review. *International Law Journal*.
- Balarabe, K. (2025). Digital intervention and the development of digital power in international relations. *Global Governance Review*.
- Chatinakrob, T. (2024). Strengthening multilateral frameworks for universal cyber norms: The roles of GGE and OEWG. *Journal of Cyber Policy and International Law*.
- Darmawan, A. B., et al. (2022). National sovereignty in digital data ownership: Strategic steps by Australia in response to Facebook and Google. *International Relations Journal*.
- Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty as regulatory autonomy in the connectivity era. *Philosophy & Technology*.
- Pierucci, F. (2025). Accountability and transparency in the European model for digital sovereignty: Examining the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA). *European Law Journal*.
- Santaniello, M. (2025). Rebuilding national control: Understanding international law rules in the cyber world. *Digital Policy Studies*.
- Shaw, M. N. (2021). *International law* (9th ed.). Cambridge University Press.
- Tallinn Manual. (2013). *The Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.
- United Nations. (1945). *Charter of the United Nations*. United Nations.