PANCASILA AND LAW REVIEW

Doktoral Ilmu Hukum, Fakultas Hukum, Universitas Lampung,
Bandar Lampung, Lampung, Indonesia.
Volume 3 Issue 1, January–June 2022: pp: 13-26
http://jurnal.fh.unila.ac.id/index.php/plr
P-ISSN: 2723-262X E-ISSN: 2745-9306

Cyber Sovereignty Gotong Royong, Indonesia'a Way of Dealing with the Challenges of Global Cyber Sovereignty

Nur Ro'is
Universitas Baturaja, Indonesia
nurrois@unbara.ac.id

Submitted: Mar 20, 2022; Reviewed: June 22, 2022; Accepted: June 27, 2022

Article's Information

Keywords:
Cyber, Cyber Sovereignty, Indonesian Cyber Law

DOI :
https://doi.org/10.25041/plr.v3i1.2573

Abstract

Abstract

State sovereignty, in terms of physical territories or cyberspace, is fundamental to a nation's independence. However, cyberspace lacks clear territorial boundaries, complicating the exercise of jurisdictional authority. Indonesia's reliance on foreign cyber infrastructure heightens its cyber vulnerability and weakens its cyber sovereignty. This research examines how Indonesia's traditional concept of "Gotong Royong" (mutual cooperation) could address these cyber sovereignty challenges. Using a normative legal research methodology and a comparative law approach, the research compares Indonesia's cyber sovereignty with that of the People's Republic of China. It argues that adapting the Gotong Royong principle, in line with the Universal People's Defense System outlined in Law Number 3 of 2002 on National Defense, could enhance Indonesia's cyber sovereignty. This approach involves engaging all citizens, regional entities, and national resources in safeguarding cyberspace.

A. Introduction

On October 20, 2021, a website managed by the Indonesian National Cyber and Crypto Agency (BSSN) was hacked by an individual from Brazil who identified as "theMx0nday." The defacement of the www.pusmanas.bssn.go.id site was reportedly in retaliation for Indonesian

hackers targeting Brazilian websites.[1] This incident is particularly ironic, given BSSN's mandate to ensure national cybersecurity, protection, and sovereignty, as outlined in Presidential Regulation Number 28 of 2021 concerning BSSN. The fact that BSSN, tasked with safeguarding national cyber assets, was unable to prevent an international cyber attack highlights significant vulnerabilities.

Indonesia is highly susceptible to cyber-attacks, with approximately 741 million attacks recorded by the end of July 2021, targeting both private and government entities.[2] The widespread use of the internet, with 202.6 million users in 2021[3], exacerbates the challenges to Indonesia's cybersecurity and sovereignty. The integration of information technology, media, and communication has globally transformed societal behavior and human civilization. While information technology has advanced human welfare, progress, and culture, it also serves as a potent tool for unlawful activities, as noted by Mardjono Reksodiputro, who characterizes these crimes as contemporary due to their reliance on computers.[4]

The rapid advancement of information technology has blurred traditional legal boundaries, creating significant challenges in law enforcement, particularly in cases where jurisdictional lines are unclear and national laws overlap. This chaotic legal landscape is reflected in the model of cyberworld regulation described by Lessig in his book "The Code," where cyberspace is governed by a combination of law, norms, architecture, and market forces. These four elements are interdependent, with changes in one influencing the others.[5]

According to Lessig, technology has the power to both undermine and support laws and norms. Norms serve as behavioral guidelines within society, while markets reinforce rules through pricing mechanisms. Architecture, in this context, refers to the physical environment that enforces adherence to legal norms.[6] Different countries approach the regulation of cyberspace differently; for instance, "closed code" systems are prevalent in communist countries like China and North Korea, where internet access is tightly controlled, while "open code" systems are characteristic of liberal countries such as the United States.

China is a prominent actor in the implementation of cyber sovereignty, particularly within the defense and security sectors. On December 31, 2015, Chinese authorities announced a major reorganization of the People's Liberation Army (PLA), marking the most significant overhaul of the armed forces since the 1950s. President Xi Jinping emphasized that these reforms were crucial for modernizing the military, reinforcing the PLA's loyalty to the Chinese Communist Party (CCP). A key outcome of this reorganization was the establishment of a new service branch, the Strategic Support Force (SSF), which stands alongside the Army, Navy, Air Force, and Rocket Force. The SSF is tasked with securing both electromagnetic space and cyberspace, a mission that Chinese military experts regard as essential for twenty-first-century warfare. The elevation of cyberspace operations within the PLA, now under the direct control of the SSF, reflects the importance of cyberspace sovereignty (*wangluo zhuquan*) in achieving the broader objectives of the Chinese Dream across all domains.[7]

---

[1] Nur Ftriatus Saliha, "Situs Milik BSSN Dibobol Peretas, Ini Analisis Dan Saran Pengamat Siber," 2021, https://www.kompas.com/tren/read/2021/10/26/133000565/situs-milik-bssn-dibobol-peretas-ini-analisis-dan-saran-pengamat-siber?page=all.

[2] Emanuel Kure, "2021 Hingga Juli, Ada 741 Juta Serangan Siber Di Indonesia," Investor, 2021, https://investor.id/it-and-telecommunication/260649/2021-hingga-juli-ada-741-juta-serangan-siber-di-indonesia.

[3] Pratiwi Agustini, "Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya Di Internet," Aptika Kominfo, 2021, https://aptika.kominfo.go.id/2021/09/warganet-meningkat-indonesia-perlu-tingkatkan-nilai-budaya-di-internet/.

[4]Mardjono Reksodiputro, *Kemajuan Pembangunan Ekonomi Dan Kejahatan (Kumpulan Karangan Buku Kesatu)* , Pusat Pelayanan dan Pengabdian Hukum (d/h Lembaga Kriminologi) Jakarta : UI (2007). p..2.

[5] Lawrence Lessig, *The Code Version 2.0,* New York: Basic Book, (2006). p. 121-123

[6] Lawrence Lessig, *Ibid,* p..124.

[7] Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017). p. 119

Adam Segal has noted that China's cyber sovereignty strategy operates on both domestic and international levels. Domestically, Beijing has developed a comprehensive matrix of interconnected cybersecurity strategies, laws, actions, regulations, and standards. This framework not only includes training for officials in China's internet management model but also encompasses the Cybersecurity Law, Personal Information Security Specifications, and other guidelines that offer alternatives to European and U.S. regulations on data protection, collection, storage, transfer, and analysis. Internationally, China has promoted the concept of cyber sovereignty through diplomatic efforts in multilateral organizations and forums. These efforts are further supported by the Belt and Road Initiative (BRI), other commercial diplomacy tools, and the global activities of Chinese technology companies.[8]

The implementation of these cybersecurity policies has significantly bolstered China's cyber sovereignty in two key areas: capacity and resource development. China's robust cybersecurity framework enables it to protect itself from external interference and resist negotiations on internet policies that may undermine its interests. Additionally, China's governance system is increasingly being viewed as a potential model for other countries in terms of internet regulation and policy.[9] In comparison, Indonesia's cyber sovereignty remains considerably underdeveloped.

The United States' dominance in the internet sphere poses a significant challenge to the concept of cyber sovereignty, particularly because its influence is often exerted subtly and indirectly. Various actors within the U.S. administration collaborate through vested interests to propagate Western governance models, promoting the idea of a unified world aligned with U.S. interests. China's diplomatic strategy, while still facing challenges, has achieved some successes. Notably, the Obama administration's decision to transfer internet authority over domain names from the U.S. Department of Commerce to the international community is widely recognized as a result of effective diplomatic efforts by China and Russia.[10]

In the current era of information technology, sovereignty—especially cyber sovereignty—has become a crucial concept. For Indonesia, however, cyber sovereignty remains a relatively new and evolving issue. This is evident in the country's dependence on foreign entities for much of its internet infrastructure, including hardware, software, social media platforms, email services, cloud storage, technology transfers, and servers.[11] This dependence creates vulnerabilities, particularly if state officials use these foreign-controlled platforms to store confidential documents. In essence, cyber sovereignty can be defined as the government's ability to control and regulate cyberspace within the territory of the Republic of Indonesia, akin to its control over the nation's political, economic, cultural, and technological activities. Strengthening cyber sovereignty is therefore critical to maintaining the resilience of the Unitary State of the Republic of Indonesia (NKRI).

To uphold cyber sovereignty despite these limitations, Indonesia could adopt the concept of *Gotong Royong*—a traditional Indonesian practice of mutual cooperation[12] and communal assistance. *Gotong Royong* in the context of cyber sovereignty implies collective responsibility and collaboration among all stakeholders within Indonesia's information technology

[8] Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," in *An Emerging China-Centric Order, China's Vision for a New World Order in Practice*, ed. Nadège Rolland, Seattle, Washington: The National Bureau of Asian Research (2020). p.88.
[9] *Ibid*. p.94
[10] Harini Calamur, "The Rise Of Cyber Sovereignty: How Do We Balance Security And Privacy On The Net?," Cnbctv18.Com, 2018, https://www.cnbctv18.com/technology/the-rise-of-cyber-sovereignty-how-do-we-balance-security-and-privacy-on-the-net-4734821.htm.
[11] Arif Rahman, 'Indonesia Belum Memiliki Kedaulatan Siber', Cyber Thread, 2019 <https://cyberthreat.id/read/196/Indonesia-Belum-Memiliki-Kedaulatan-Siber>
[12] The definition of gotong royong according to the Big Indonesian Dictionary (KBBI) is working together, https://kbbi.web.id/gotong royong

community. This includes not only the government but also internet service providers (ISPs), internet user communities, internet cafes, e-commerce companies, telecommunications firms, and even families, the smallest unit of society.

This article explores the concept of cyber sovereignty and examines how Indonesia upholds its cyber sovereignty through the traditional concept of *Gotong Royong*, comparing it with the approach taken by the People's Republic of China. The research adopts a normative legal approach, which conceptualizes law as what is codified in legislation ("law in the books") or as a set of rules and norms that serve as standards for acceptable human behavior.[13] The research employs qualitative methods by analyzing the norms present in existing laws, regulations, and relevant court decisions.[14]

Additionally, the research incorporates a comparative law approach. As noted by Sudikno Mertokusumo, and quoted by Sunarjati Hartono, comparative law involves identifying and explaining both the differences and similarities between legal systems, while also examining how the law functions in practice and the influence of non-legal factors on legal outcomes. Similarly, Rene David and Brierly, as cited by Barda Nawawi Arief, emphasize that one of the primary benefits of comparative law is to enhance the understanding and development of national law.[15] The data for this research were collected through a literature review, in which, according to Soerjono Soekanto, only library materials or secondary data are examined in normative legal research.[16]

B. Discussion

1. Cyber sovereignty and its central issue

Some experts have expressed concerns about the complexities of governing cyberspace, a domain that, while intangible, is intricately linked to the physical world. The challenge in cyber governance lies in asserting administrative authority within this logical space. This governance involves both the provisioning system and the broader existence in cyberspace, requiring a blend of subjective and objective perspectives. Decisions in this domain are made by actors based on an objective framework, yet they are influenced by subjective judgments.

In 2005, a United Nations report highlighted that the control of the DNS Zone was effectively under the authority of the United States government. This prompted calls for reforms in internet governance based on the principles of equality.[17] China's role in advocating for and defining cyber sovereignty emerged from this context. President Xi Jinping has frequently used the term "cyber sovereignty," which can be understood through several key components: first, it refers to the state's sovereignty in managing information flow within its borders; second, it affirms each country's right to independently formulate cyber-related policies; third, it emphasizes that all nations should have equitable rights in shaping the rules, norms, and codes of conduct governing global cyberspace; and finally, respect for national sovereignty should be a fundamental principle in addressing international cyber-related issues.[18]

Numerous studies have examined President Xi Jinping's efforts to uphold China's cyber sovereignty. For instance, Yi Sen's article, "Cyber Sovereignty and the Governance of Global

[13] Amiruddin and Zainal Asikin, *Pengantar Metode Penelitian Hukum* , Rajawali Press, (2006). p..118.
[14] Sunarjati Hartono, *Kapita Selekta Perbandingan Hukum* , Bandung: Citra Aditya Bakti (1988). hal.54
[15] Barda Nawawie Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjaratle* , Yogyakarta: Genta Publishing (2010).
[16] Soekanto Soerjono, *Pengantar Penelitian Hukum* , Jakarta: UI-Press (1981). p..52
[17] Yi Shen, "Cyber Sovereignty and the Governance of Global Cyberspace," *Chinese Political Science ReviewChina Political Science Review* 1 (2016), https://doi.org/10.1007/s41111-016-0002-6. p.85-86.
[18] *Ibid*

Cyberspace," focuses on China's leadership in resisting U.S. dominance in cyberspace.[19] Additionally, Jinghan Zen, Tim Stevens, and Yaru Chen, in their work "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty,'" explore how Chinese cyberspace policies have bolstered the legitimacy and security of the Chinese Communist Party (CCP) regime, aligning with both domestic and international objectives.[20]

Yu Hong's research delves into China's strategic use of cyber power during critical moments in the global political economy, demonstrating how the party-state has asserted its sovereignty in the cyber realm. This development of national virtual sovereignty is seen as a countermeasure against the multifaceted influences of global capitalism.[21]

The research in the article is distinctive in its comparative analysis of cyber sovereignty in Indonesia and China, particularly emphasizing Indonesia's unique approach through the local wisdom method of "*Gotong Royong*." This approach contrasts with China's more centralized and state-driven model of cyber sovereignty.

The concept of sovereignty in cyberspace is inherently linked to the broader notion of sovereignty, which represents the highest and absolute authority within a state. Sovereignty is characterized by its ability to regulate citizens, achieve national goals, oversee various governmental functions, and carry out actions within a country. This authority includes, but is not limited to, legislating, enforcing laws, punishing offenders, collecting taxes, making peace, declaring war, and entering into and enforcing treaties.[22]

Jean Bodin, in his work *De La Republique*, as quoted by Munir Fuady, describes sovereignty as an absolute and perpetual power within a state that stands above positive law. Bodin defines sovereignty as "supreme power over citizens and subjects, unrestrained by the laws," placing sovereignty above the law itself. According to Bodin, sovereignty not only possesses supremacy but also immortality, meaning it persists over time.[23]

John Austin further elaborates on sovereignty by identifying it as the authority vested in a person, body, or state leader who has the power to create positive laws applicable to members of an independent political society under their control. Austin asserts that the majority within the society will obey the sovereign's will, reinforcing the idea of the sovereign's supreme authority.[24]

H.L.A. Hart offers another perspective on state sovereignty, highlighting its supremacy to the extent that a state need not be subject to international law or be bound by it unless it chooses to be.[25] Hart interprets "sovereign" as synonymous with independence[26], asserting that a sovereign state possesses enforcement powers and operates autonomously within its domain.[27]

In the Island of Palmas case, Max Huber highlighted the crucial link between sovereignty and territory, emphasizing that sovereignty can only be exercised over areas where a state can effectively exert its power through the right to perform state functions. This principle underlines

[19] Ibid. p.91.
[20] Jinghan Zeng, Tim Stevens, and Yaru Chen, "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty,'" *Politics & Policy* 45, no. 2 (2017), https://doi.org/10.1111/polp.12202. p.452-453
[21] Yu Hong and G. Thomas Goodnight, "How to Think about Cyber Sovereignty: The Case of China," *Chinese Journal of Communication*, 2019, https://doi.org/10.1080/17544750.2019.1687536. p.14-15.
[22] Munir Fuady, *Teori-Teori Besar Dalam Hukum,* Jakarta: Kencana (2013). p.. 92.
[23] Wm. A Dunning, "Jean Bodin on Sovereignty," *Political Science Quarterly* 11, no. 1 (1896), http://www.jstor.org/stable/2139603. hal.. 93. Diakses pada 12 Desember 2015.
[24] Munir Fuady, *Op.cit.* hal..92.
[25] H.L.A. Hart, *The Concept of Law ; Penerjemah: M Khozim* , Bandung: Nusa Media, 2011, hal., 344.
[26] Huala Adolf, *Filsafat Hukum Internasional,* Bandung: Keni Media (2020). hal..80
[27] *Ibid*

the notion that sovereignty is not just a theoretical claim but requires actual control and the ability to govern within a defined geographical area.[28]

Schwarzenberger, as quoted by Huala Adolf, elaborates on sovereignty, defining it as the ultimate power or omnipotence that resides solely within the state. This sovereignty embodies the state's autonomy and its authority to create and enforce legal rules (national law) within its territory, as well as to establish and maintain state institutions.[29] Sovereignty, therefore, is a fundamental aspect of statehood, granting the state the supreme power to govern itself and its affairs.

When applied to the cyber realm, sovereignty extends to the state's control over cyberspace infrastructure and activities within its territory. This concept of cyber sovereignty implies that a state has the authority to regulate and manage its Information and Communication Technology (ICT) infrastructure, including networks, data centers, and other cyber-related assets located (virtual assets) within its national borders.[30] This includes the sovereignty over infrastructure found in inland areas, internal waters, territorial seas, archipelagic waters, and national airspace, all of which are considered part of the state's territorial domain.

In discussing sovereignty, the issue of jurisdiction inevitably arises. International law recognizes that a state's territory is the space where it exercises its sovereignty, including its jurisdiction over ICT infrastructure. A state network refers to the ICT infrastructure built and operated within its territory, and there is no doubt that a state can use its sovereignty to govern this infrastructure, just as it does with other entities within its borders.

Binxing Fang, a prominent scholar on cyber sovereignty, posits that "cyberspace sovereignty is a natural extension of state sovereignty in cyberspace, guided by ICT infrastructure located within the country's territory." According to Fang, this means that the state has jurisdiction, or the right to intervene, in data operations and other cyber activities occurring within its borders. This jurisdiction extends to ICT systems, facilities, and the data they carry, which are considered virtual assets under the state's control. In essence, cyberspace sovereignty is an extension of the state's authority to govern all aspects of its territory, including the digital domain.

The fundamental rights of cyberspace sovereignty are directly derived from state sovereignty and include cyberspace independence rights, cyberspace equality rights, cyberspace self-defense rights, and cyberspace jurisdiction rights. Cyberspace independence rights are manifested in networks within a country's territory that can operate independently without external interference. This principle is evident in many existing network models, such as radio and television networks and industrial control networks. However, the centralized operating model of the global Internet results in Internet operations being subject to centralized control, particularly in domain naming resolution.[31]

Cyber sovereignty issue is not only a legal matter between countries but also involves foreign corporations. As Lessig described, the conflict between domestic (French) interests and foreign interests is illustrated by the case of Yahoo selling Nazi-related equipment on its site. Trading Nazi equipment is prohibited in France, yet Yahoo's site, which sells such items, can still be accessed from France. Yahoo's servers are physically located in New York City, United States, where such trading is permitted.[32] Yahoo faced a lawsuit in France and offered to block access to the prohibited content from France but failed to prove that it could do so completely.

---

[28] Michael N. Schmitt, *Tallinn Manual On The International Law Applicable To Cyber Warfare,* Cambridge: Cambridge University Press, (2013). p.13

[29] Huala Adolf, *Hukum Ekonomi Internasional Suatu Pengantar*, Bandung: Keni Media (2019). p..224

[30] Binxing Fang, *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace*, Beijing: Science Press, (2018). p.83

[31] *Ibid.* p.84

[32] Lessig, *The Code Version 2.0*. p.294-295

As a result, Yahoo was ordered by a French court to remove the offending content within three months and faced a daily fine of 100,000 francs for non-compliance.[33]

The United States' dominance of the Internet is also a significant issue regarding cyber sovereignty, although its influence is subtle. Various actors involved in its administration have collaborated to promote Western governance models and U.S. interests. However, China's diplomatic strategy has achieved some minor victories. For instance, the Obama administration's decision to transfer internet authority over domain names from the U.S. Department of Commerce to the international community is seen as a result of effective diplomacy by China and Russia.[34] Issues to consider include the potential conflicts between the multi-stakeholder approach of the Internet Corporation for Assigned Names and Numbers (ICANN) and the intergovernmental approach of the International Telecommunication Union (ITU), a UN sub-agency. There has been tentative agreement on dividing responsibilities since 2014, but developments in 2016 suggest a more uncertain future.

Another pressing issue with uncertain consequences is the ongoing debate about alleged election hacking in the United States and its impact on perceptions of information sovereignty in the West. [35] The virtual conditions of cyberspace always require a "physical" infrastructure within the territory of one or more countries. This is where a country's territorial sovereignty applies to cyberspace, allowing it to exercise jurisdiction over cyberspace within its territory. The laws of a country apply to cyberinfrastructure within its borders, including decisions about whether to uphold or restrict freedom, depending on the location of the cyberinfrastructure, such as data centers, where information is accessed.

2. Indonesian solution for cyber sovereignty with its local wisdom is called "*Gotong Royong*."

As mentioned in the introduction, cyber sovereignty is a relatively new concept for Indonesia, despite the fact that its rights have been implicitly attached since the proclamation of independence. A key question is whether Indonesia possesses the sovereignty to control the information circulating in today's cyber world.

In the Cyber Security and Resilience Legal Plans, cyber sovereignty is defined as a term used in internet governance to describe the government's desire to exercise control over the Internet within its territory, including political, economic, cultural, and technological activities. Some argue that this control contradicts the fundamental principle of the Internet, which is characterized by its decentralized nature in both technology and policy implementation.[36]

The major concern is that government monitoring of internet activities, including email accounts, social media, discussion groups, and others, may infringe on individuals' human rights. Nonetheless, in the realm of national cyber security, particularly concerning the protection of confidential government data and information, it is undeniable that Indonesia's cyber infrastructure requires significant improvement. Challenges include inadequate human resources, slow internet access, untested applications, and often neglected security aspects. For instance, instability in email services provided by government agencies frequently results in difficulties accessing or maintaining these services.[37]

[33] *Ibid*. p. 295
[34] Calamur, "The Rise Of Cyber Sovereignty: How Do We Balance Security And Privacy On The Net?" diakses pada 20 Mei 2020
[35] Niels Nagelhus Schia and Lars Gjesvik, "The Chinese Cyber Sovereignty Concept (Part 1)," The Asia Dialogue, 2018, https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/. Diakses pada 10 Mei 2020
[36] DPR RI, "Naskah Akademik Rancangan Undang-Undang Keamanan Dan Ketahanan Siber," DPR RI, 2020, http://www.dpr.go.id/dokakd/dokumen/RJ1-20190617-025848-5506.pdf. p.59
[37] *Ibid,* p. 33

The Government of the Republic of Indonesia implemented Government Regulation (PP) No. 82 of 2012, which regulated the implementation of electronic systems and transactions. According to Article 17, paragraph (2), electronic system operators providing public services were required to establish data centers and disaster recovery centers within Indonesia. This regulation aimed to ensure law enforcement, protection, and the enforcement of state sovereignty over citizen data.

The purpose of locating these data centers in Indonesia was to protect the personal data of Indonesian citizens by enhancing transparency in data usage (e.g., customer data) and safeguarding against theft or manipulation by third parties outside Indonesia. Such data breaches could negatively impact a company's reputation and lead to financial losses.

Several countries have adopted data localization policies. For example, the General Data Protection Regulation (GDPR), enacted by the European Union and implemented across 28 European countries, requires companies, including those based outside the EU, to inform citizens about data usage and notify them within 72 hours in the event of a cyber-attack.[38]

However, Government Regulation (PP) No. 82 of 2012 was revoked and replaced by Government Regulation (PP) No. 71 of 2019, which removed the requirement for data centers to be located in Indonesia. This revocation has significant implications for Indonesia's cyber sovereignty, including:

1. Jurisdiction issues, especially if there is a violation of the law while the data center is outside the reach of the Indonesian government;
2. There is a high possibility related to personal data information; even essential and state secret information will be leaked to third parties because there is no government control over the data stored in the data center;
3. Content from the cyber world in Indonesia will become increasingly out of control by the government;
4. Domestic industries related to data centers will stop growing because there is no obligation to use data centers in Indonesia.

The Indonesian government has the authority to enforce cyber sovereignty through blocking measures, as outlined in Article 40 of Law Number 16 of 2016, which amends Law Number 11 of 2008 concerning Electronic Transactions, published in the State Gazette of 2016 Number 251. Although such measures raise concerns about human rights violations related to freedom of speech, they serve as a basis for blocking websites with content deemed contrary to Indonesian laws, such as those related to prostitution, gambling, pornography, and terrorism.

In this cooperative framework, known as *Gotong Royong*, cyber sovereignty involves both government and community roles. The government acts as the regulator and executor in blocking internet content, while the community contributes in two ways: first, through independent blocking by individuals, and second, by reporting websites or content that violate Indonesian laws and norms. Cyber sovereignty is a shared responsibility among all stakeholders in the Indonesian informatics community, including Internet Service Providers (ISPs), internet user communities, internet cafes, e-commerce companies, telecommunications companies, and even families.

This collaborative approach to cyber sovereignty aligns with the concept of "universal people's defense" as defined in Article 4 of Law Number 3 of 2002 concerning National Defense. The law states that national defense aims to maintain and protect the sovereignty of the state, the territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of the nation from various threats. The Elucidation further explains that "threats" encompass any activities, whether domestic or international, that endanger state sovereignty, territorial

[38] TelkomTelstra, "PP No. 82, Revisinya Dan Dampaknya Bagi Perusahaan Di Indonesia," n.d., https://www.telkomtelstra.co.id/id/insight/blog/481-revisi-pp-no-82-menguntungkan-perusahaan-di-indonesia.

integrity, or national safety. In the context of cyber sovereignty, this includes controlling cyber infrastructure within Indonesia to safeguard against cyber threats.

The government's regulatory role involves blocking problematic sites through technological measures, utilizing the Automated Information System (AIS) engine. This system functions similarly to the "Great Firewall of China," although it differs in its implementation. In China, internet blocking relies heavily on automated systems and internet police, while Indonesia employs the AIS machine, the AIS team, and community involvement through reporting and independent blocking such as aduankonten.id.[39] This includes installing filters on private networks, local networks, and ISP networks.

The Indonesian government, through the Ministry of Communication and Information (*Kominfo*), implements content blocking using the Automated Information System (AIS) machine. This approach is managed by the AIS Team and involves two primary mechanisms. First, the team conducts continuous 24-hour patrols to monitor and identify harmful online content. Second, the team responds to community reports submitted through various channels, such as aduankonten.id. This cooperative approach reflects the principle of *Gotong Royong*, or mutual cooperation, in enforcing cyber sovereignty.

In 2020, *Kominfo* successfully blocked over 1 million websites related to pornography, 166,853 gambling sites, and 8,689 fraudulent sites. Additionally, sites containing defamatory content, issues related to SARA (ethnic, religious, racial, and inter-group relations), separatism, and information security violations were also blocked. The total count of blocked sites and content reached 1,203,948, excluding more than 600,000 pieces of content removed from social media platforms.[40]

Efforts continued into 2021, focusing on combating misinformation, particularly concerning Covid-19. As of August 8, 2021, the Ministry identified 1,897 hoaxes across various social media platforms, with Facebook hosting the majority (1,729 hoaxes). Video-sharing sites, such as YouTube and TikTok, were also targets, with 41 hoaxes found on YouTube and 17 on TikTok. Additionally, Instagram had 11 hoaxes identified by the Ministry.[41] The enforcement of cyber sovereignty in Indonesia involves blocking unlawful content in the digital realm, operating as a form of "non-penal" law enforcement when traditional penal measures are hindered by jurisdictional challenges.

3. China's Experience in Cyber Sovereignty

The People's Republic of China, with over 600 million internet users, has implemented some of the world's strictest internet controls, which are central to the government's extensive surveillance of information flow, including media and cultural content. According to a recent Freedom House report, the Chinese government employs sophisticated techniques to enforce information control. This includes strategic management of key information nodes, outsourcing censorship tasks, reinforcing party ideology, and cracking down on social media platforms.[42]

In China, the concept of cyber sovereignty is distinct from cybersecurity, which focuses on the protection of infrastructure and processes connected to the internet. Instead, cyber

[39] Leski Rizkinaswara, "Kepoin Mesin AIS Kominfo," Dirjen Aptika, 2019, https://aptika.kominfo.go.id/2019/02/kepoin-mesin-ais-kominfo/#:~:text=Jakarta%2C Ditjen Aptika – Mesin Pengais,9 Lantai 8 Gedung Kominfo.%3E,.

[40] Kominfo, "Kominfo Blokir 11.803 Konten Radikalisme Dan Terorisme, Siaran Pers NO. 63/HM/KOMINFO/03/2019," 2019, https://kominfo.go.id/content/detail/17274/siaran-pers-no-63hmkominfo032019-tentang-kominfo-blokir-11803-konten-radikalisme-dan-terorisme/0/siaran_pers#:~:text=Kementerian Komunikasi dan Informatika telah,tahun 2009 sampai tahun 2019.

[41] Kominfo, "Kominfo Turunkan 1.897 Konten Hoaks Seputar Vaksin Covid-19," Kominfo, 2021, https://aptika.kominfo.go.id/2021/08/kominfo-turunkan-1-897-konten-hoaks-seputar-vaksin-covid-19/.

[42] Samson Yuen, "Becoming a Cyber Power China's Cybersecurity Upgrade and Its Consequences," *China Perspectives* 1, no. 2 (2015), https://doi.org/10.4000/chinaperspectives.6731. p.53

sovereignty pertains to controlling the information and content accessible online. China's approach to cyber sovereignty is grounded in two primary principles: First, it seeks to restrict foreign influences within its "information space," thereby preventing exposure to ideas and opinions deemed harmful by the regime. Second, it aims to shift internet governance from existing bodies, including academic institutions and corporations, to international forums like the United Nations, thereby centralizing power within states rather than with private entities or individuals.[43]

The international response to China's implementation of cyber sovereignty has often been overshadowed by concerns about espionage and industrial hacking attributed to China. However, the concept of cyber sovereignty is gaining increasing attention. The United States, in particular, has expressed apprehensions that China may use its policies for censorship, protectionism, and espionage. For instance, in June 2015, China enacted the National Security Law, intended to enhance national security but encompassing broad provisions affecting economic and industrial policies. Additionally, China's 2015 draft laws on counterterrorism and cybersecurity, if enacted in their proposed forms, could impose extensive trade restrictions on imported information technology and computer services in China.[44]

The introduction of laws designed to increase governmental control over the internet is not unique to China or authoritarian regimes. Countries such as Russia, Iran, and Saudi Arabia have adopted similar measures, reflecting a broader trend that also includes European democracies like Poland, Hungary, and the United Kingdom. Recent developments suggest that the distinction between democratic and authoritarian approaches to internet governance may be narrowing. This trend is also evident in developing nations, which often perceive themselves as disadvantaged in the digital realm and vulnerable to the effects of globalization.[45]

While there are still notable differences between nations advocating for an open internet and those seeking greater control, the gaps in regulatory approaches are diminishing in some areas. For instance, issues such as governmental requests for corporate assistance have become prominent in the United States. A notable example is the Apple-FBI case, where the FBI sought Apple's help to access the phones of captured terrorists. Additionally, American companies are increasingly relying on the U.S. government for protection against foreign cyber intrusions.[46]

The Chinese approach to cyber sovereignty has faced significant criticism from non-governmental organizations (NGOs). Prior to the 2015 World Internet Conference, Amnesty International called on companies to oppose China's stance, labeling the concept of sovereignty as an "all-out attack on internet freedom." Freedom House has consistently ranked China among the worst countries in terms of internet freedom, attributing this to its aggressive cyber sovereignty policies.

Fang Binxing, the architect of China's Great Firewall, articulated this perspective during the China-Russia forum on Internet sovereignty in 2016. He argued that since much of the internet's infrastructure is based in the United States, internet governance is effectively controlled by the U.S. Fang's remarks suggested that the objective of China's cyber sovereignty is not merely to impose government control but to challenge the existing U.S. dominance. By framing the issue this way, China aims to shift the narrative from internet censorship to advocating for a more balanced global control of cyberspace. This aligns with China's broader foreign policy goal of promoting the "democratization of international relations," which seeks to move away from perceived Western hegemony towards a more inclusive international order that respects state sovereignty and internal affairs.[47]

---

[43] Yuen. *Opcit*
[44] Hong and Goodnight, "How to Think about Cyber Sovereignty: The Case of China." p.10.
[45] Schia and Gjesvik, "The Chinese Cyber Sovereignty Concept (Part 1)."
[46] *Ibid.*
[47] Schia and Gjesvik.

Ultimately, the central issue is who controls the internet and how that control is exercised. China's approach, embodied by the Great Firewall, restricts outbound access to encourage the development of domestic industries. For instance, Baidu serves as an alternative to Google, Weibo to Facebook, and WeChat to WhatsApp. While these domestic platforms offer similar services, they are subject to sophisticated filters that can block applications like WeChat's private chat.[48]

China's strategy for achieving cyber sovereignty has resulted in significant contradictions both domestically and internationally. The Chinese government is aware of these tensions. Hao Yeli, a Major General in the Chinese People's Liberation Army, has identified three main conflicts.[49] First, there is a clash between cyber sovereignty and the fundamental nature of the internet, which relies on unlimited interconnectivity. Emphasizing cyber sovereignty could lead to a fragmented internet, where each country creates its own isolated cyberspace. Second, there is a tension between cyber sovereignty and human rights, particularly regarding free speech. The imposition of cyber sovereignty often results in restrictions on information flow, evident in China's internet firewalls. Third, there is a conflict between cyber sovereignty and the multi-stakeholder approach to governance. The implementation of cyber sovereignty challenges traditional governance models, especially when a single-party government encounters the multi-party systems present in other countries.[50]

The Chinese internet policies, driven by concerns about regime security, reflect both domestic and international dimensions. Domestically, censorship aims to suppress political dissent and limit foreign influence, which could undermine the legitimacy of the Chinese Communist Party (CCP) and destabilize the state. Internationally, the pursuit of internet sovereignty serves as both a justification for domestic policies and an attempt to fend off foreign interference, encompassing both "hard" and "soft" elements[51] This approach aims to bolster the CCP's domestic legitimacy while pursuing broader foreign policy objectives. However, the global discourse on these cyber norms remains underdeveloped, lacking the convincing or practical application needed for widespread governance of global cyberspace.[52]

C. Conclusion

Cyber sovereignty is crucial for an independent nation including Indonesia. However, several challenges impede Indonesia's ability to fully exercise this sovereignty. First, the dominance of the United States over global internet infrastructure creates dependencies that limit Indonesia's control. Second, the lack of mandatory data center regulations within Indonesian territory weakens the country's ability to enforce its cyber laws. Additionally, international cooperation issues related to cyber jurisdiction further hinder effective law enforcement.

To address these limitations, Indonesia can adopt the concept of *Gotong Royong* cyber sovereignty, which aligns with the Universal People's Defense System as outlined in Law Number 3 of 2002 concerning National Defense. This approach involves a collaborative effort from all citizens, regions, and national resources to strengthen cyber sovereignty.

China's "Great Firewall" serves as a model of stringent cyber sovereignty enforcement, allowing the country to regulate all internet activities within its borders. However, this policy is not directly applicable to Indonesia due to constitutional protections for freedom of speech under the 1945 Constitution. Nevertheless, Indonesia can implement targeted blocking

[48] Calamur, "The Rise Of Cyber Sovereignty: How Do We Balance Security And Privacy On The Net?"
[49] Hao Yeli, "A Three-Perspective Theory of Cyber Sovereignty," *Prism* 7, no. 2 (2017). p.109 - 110
[50] *Ibid*
[51] Zeng, Stevens, and Chen, "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty.'" p.452
[52] *Ibid*. p.453.

measures within the constraints of existing laws. Unlike China's approach, which relies heavily on automated systems and internet police, Indonesia's cyber sovereignty efforts are managed through the AIS machine, the AIS Team, and active community participation. This includes reporting, independent blocking, and the installation of filters on private, local, and internet service provider networks.

References

A. Book

Adolf, Huala. *Filsafat Hukum Internasional*. Bandung: Keni Media, 2020.

———. *Hukum Ekonomi Internasional Suatu Pengantar*. Bandung: Keni Media, 2019.

Amiruddin, and Zainal Asikin. *Pengantar Metode Penelitian Hukum*. Rajawali Press, 2006.

Arief, Barda Nawawie. *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjaratle*. Yogyakarta: Genta Publishing, 2010.

Fang, Binxing. *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace*. Beijing: Science Press, 2018.

Fuady, Munir. *Teori-Teori Besar Dalam Hukum*. Jakarta: Kencana, 2013.

Hart, H.L.A. *The Concept of Law ; Penerjemah: M Khozim*. Bandung: Nusa Media, 2011.

Hartono, Sunarjati. *Kapita Selekta Perbandingan Hukum*. Bandung: Citra Aditya Bakti, 1988.

Lessig, Lawrence. *The Code Version 2.0*. New York: Basic Book, 2006

Reksodiputro, Mardjono. *Kemajuan Pembangunan Ekonomi Dan Kejahatan (Kumpulan Karangan Buku Kesatu)*. Pusat Pelayanan dan Pengabdian Hukum (d/h Lembaga Kriminologi) UI, 2007.

Soerjono, Soekanto. *Pengantar Penelitian Hukum*. Jakarta: UI-Press, 1981.

Schmitt, Michael N. *Tallinn Manual On The International Law Applicable To Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

Yeli, Hao. "A Three-Perspective Theory of Cyber Sovereignty." *Prism* 7, no. 2 (2017).

B. Journal

Dunning, Wm. A. "Jean Bodin on Sovereignty." *Political Science Quarterly* 11, no. 1 (1896). http://www.jstor.org/stable/2139603.

Hong, Yu, and G. Thomas Goodnight. "How to Think about Cyber Sovereignty: The Case of China." *Chinese Journal of Communication*, 2019. https://doi.org/10.1080/17544750.2019.1687536.

Kolton, Michael. "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence." *The Cyber Defense Review* 2, no. 1 (2017).

Segal, Adam. "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace." In *An Emerging China-Centric Order, China's Vision for a New World Order in Practice*, edited by Nadège Rolland. Seattle, Washington: The National Bureau of Asian Research, 2020.

Shen, Yi. "Cyber Sovereignty and the Governance of Global Cyberspace." *Chinese Political Science ReviewChina Political Science Review* 1 (2016). https://doi.org/10.1007/s41111-016-0002-6.

Yuen, Samson. "Becoming a Cyber Power China's Cybersecurity Upgrade and Its Consequences." *China Perspectives* 1, no. 2 (2015). https://doi.org/10.4000/chinaperspectives.6731.

Zeng, Jinghan, Tim Stevens, and Yaru Chen. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty.'" *Politics & Policy* 45, no. 2 (2017). https://doi.org/10.1111/polp.12202.

C. Website

Agustini, Pratiwi. "Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya Di Internet." Aptika Kominfo, 2021. https://aptika.kominfo.go.id/2021/09/warganet-meningkat-indonesia-perlu-tingkatkan-nilai-budaya-di-internet/.

Calamur, Harini. "The Rise Of Cyber Sovereignty: How Do We Balance Security And Privacy On The Net?" Cnbctv18.Com, 2018. https://www.cnbctv18.com/technology/the-rise-of-cyber-sovereignty-how-do-we-balance-security-and-privacy-on-the-net-4734821.htm.

DPR RI. "Naskah Akademik Rancangan Undang-Undang Keamanan Dan Ketahanan Siber."

DPR RI, 2020. http://www.dpr.go.id/dokakd/dokumen/RJ1-20190617-025848-5506.pdf.

Kominfo. "Kominfo Blokir 11.803 Konten Radikalisme Dan Terorisme, Siaran Pers NO. 63/HM/KOMINFO/03/2019," 2019. https://kominfo.go.id/content/detail/17274/siaran-pers-no-63hmkominfo032019-tentang-kominfo-blokir-11803-konten-radikalisme-dan-terorisme/0/siaran_pers#:~:text=Kementerian Komunikasi dan Informatika telah,tahun 2009 sampai tahun 2019.

———. "Kominfo Turunkan 1.897 Konten Hoaks Seputar Vaksin Covid-19." Kominfo, 2021. https://aptika.kominfo.go.id/2021/08/kominfo-turunkan-1-897-konten-hoaks-seputar-vaksin-covid-19/.

Kure, Emanuel. "2021 Hingga Juli, Ada 741 Juta Serangan Siber Di Indonesia." Investor, 2021. https://investor.id/it-and-telecommunication/260649/2021-hingga-juli-ada-741-juta-serangan-siber-di-indonesia.

Rahman, Arif. "Indonesia Belum Memiliki Kedaulatan Siber." Cyber Thread, 2019. https://cyberthreat.id/read/196/Indonesia-Belum-Memiliki-Kedaulatan-Sibe.

Rizkinaswara, Leski. "Kepoin Mesin AIS Kominfo." Dirjen Aptika, 2019. https://aptika.kominfo.go.id/2019/02/kepoin-mesin-ais-kominfo/#:~:text=Jakarta%2C Ditjen Aptika – Mesin Pengais,9 Lantai 8 Gedung Kominfo.%3E,.

Saliha, Nur Ftriatus. "Situs Milik BSSN Dibobol Peretas, Ini Analisis Dan Saran Pengamat Siber," 2021. https://www.kompas.com/tren/read/2021/10/26/133000565/situs-milik-bssn-dibobol-peretas-ini-analisis-dan-saran-pengamat-siber?page=all.

Schia, Niels Nagelhus, and Lars Gjesvik. "The Chinese Cyber Sovereignty Concept (Part 1)." The Asia Dialogue, 2018. https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/.

TelkomTelstra. "PP No. 82, Revisinya Dan Dampaknya Bagi Perusahaan Di Indonesia," n.d. https://www.telkomtelstra.co.id/id/insight/blog/481-revisi-pp-no-82-menguntungkan-perusahaan-di-indonesia.