PANCASILA AND LAW REVIEW

Doktoral Ilmu Hukum, Fakultas Hukum, Universitas Lampung,
Bandar Lampung, Lampung, Indonesia.
Volume 3 Issue 1, January–June 2022: pp: 15-30
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,
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, Indonesia Cyber Defence, Sovereignty,

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

Abstract

Abstract

State sovereignty is born together with the independence of a country, as well as sovereignty in cyberspace. The state has sovereignty in cyberspace as in its territorial space so that it has jurisdictional authority, but in reality, there are unclear territorial boundaries in cyberspace. Indonesia today still has a dependence on foreign cyberinfrastructure, which causes a high level of cyber vulnerability and low cyber sovereignty resilience. Indonesia has local wisdom known as "Gotong Royong," this conception of local wisdom can be applied to face the global challenges of cyber sovereignty. This study also compares the resilience of Indonesia's cyber sovereignty with the People's Republic of China using a normative legal research methodology with a comparative law approach. Indonesia's limitations in maintaining its cyber sovereignty can be anticipated by using the concept of Gotong Royong cyber sovereignty, which is the implementation of the Universal People's Defense System as regulated in Law Number 3 of 2002 concerning National Defense. The implementation of Cyber Gotong Royong sovereignty involves all citizens, regions, and other national resources.

A. Introduction

On October 20, 2021, one of the sites managed by BSSN (Indonesian National Cyber and Crypto Agency) was hacked by a Brazilian who used the nickname theMx0nday, the www.pusmanas.bssn.go.id site was defaced in response to the Indonesian hacker attack in some website in Brazil[1], BSSN is an institution responsible for national cyber security, protection and sovereignty as stated in Presidential Regulation (PERPRES) Number 28 of 2021 concerning the National Cyber and Crypto Agency (BSSN). What happened to the site managed by BSSN is an irony. This institution is responsible for National cyber security but cannot protect its assets against international cyber attacks.

Indonesia is one of the countries that are vulnerable to cyber-attacks. Until the end of July 2021, there have been around 741 million cyber attacks aimed at Indonesia, both private and government entities[2], The widespread use of the Internet in Indonesia in 2021 reaches 202.6 million people[3], which adds to the vulnerability of Indonesia's cyber security and sovereignty. The utilization of information technology, media, and communication has changed society's behavior and human civilization globally. Information technology is currently a double-edged sword. After all, improving human welfare, progress, and culture is also an effective means of unlawful acts (crime). According to Mardjono, Reksodiputro is known to have a contemporary nature because it involves computers.[4]

The vague boundaries caused by advances in information technology have created problems in the field of law, especially those related to law enforcement. Jurisdiction becomes blurred, laws between countries overlap. This situation of chaos is illustrated by the model of cyber world regulation as revealed by Lessig in his book "The Code" that technology can weaken laws and norms, according to which cyberspace (cyber world) is likened to the dot (dots) governed by The Code which consists of law (law), Norms (Norm), Architecture (Architecture) and Market (Market), the four support each other, changes to one of them will affect the whole. [5]

According to Lessig, the four mutually influence, support, or even destroy one another. Technology can undermine laws and norms; but also can support them. Norms can be a reference for behavior in society. The market through price determination supports the rules, while architecture creates a physical environment that enforces the rule of law to be obeyed. [6] Setting the type of "closed code" can be found in communist countries such as China and North Korea, which tighten internet access for its residents. In contrast, the setting with the type of "open code" is found in liberal countries. One example is the United States.

China is one of the countries active in implementing cyber sovereignty, especially in the defence and security domain. On December 31, 2015, Chinese officials announced a significant reorganization of the armed forces. The reforms cut across the entire People's Liberation Army (PLA) and were the most dramatic reorganization of China's armed forces since the 1950s. President Xi Jinping described reforms as essential to modernizing the military. Moreover, the reorganization underscores the PLA's loyalty to the Chinese Communist Party

[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.

(CCP). The reforms also established a new service branch called the Strategic Support Force (SSF) on par with the Army, Navy, Air Force, and Rocket Force. Among its many missions, SSF secures electromagnetic space and cyberspace. Chinese military experts praise the SSF as necessary for twenty-first-century warfare. Over the years, the PLA has fielded cyberspace capabilities at various command levels, and the SSF elevates cyberspace operations control to the highest echelons. In the end, the PLA uses the power of cyberspace to ensure cyberspace sovereignty (*wangluo zhuquan*) and safeguard the Chinese Dream in all domains. [7]

Adam Segal said that China's cyber sovereignty efforts have both domestic and international components. Beijing has developed a matrix of interrelated cybersecurity strategies, laws, actions, regulations, and standards at home. Officials were not only trained in China's internet management model. Still, they were also trained on Cybersecurity Laws, Personal Information Security, Specifications, and other guidelines as an alternative to European and US efforts to regulate data protection, collection, storage, transfer, and analysis. Internationally, Beijing has used diplomatic efforts to perpetuate and expand the concept of cyber sovereignty in multilateral organizations and forums. This multilateral effort is supported by the Belt Road Initiative (BRI) and other commercial diplomacy tools, and the global activities of Chinese technology companies.[8]

The implications for China with the implementation of cyber security policies have strengthened its cyber sovereignty, at least in two contexts, namely, capacity and resource development, because China cannot protect itself from interference and negotiations on internet policies without solid cyber security. The two Chinas have shown their governance system as a potential technical and substantive model for other countries regarding internet regulation and regulation.[9] When compared with China, it is clear that Indonesia's cyber sovereignty lags far behind.

The United States' internet dominance is also a significant issue regarding cyber sovereignty, although its influence is not visible and is carried out in a "subtle way." The various actors involved in his administration collaborated through their vested interests to propagate the Western way of governing, more so the idea of a unified world globalized by US interests. The diplomatic strategy employed by China has had some minor victories. The Obama administration's decision to transfer internet authority over domain names issued from the US Department of Commerce to the international community is recognized as the result of effective diplomacy from China and Russia. [10]

Sovereignty is the keyword in the current era of information technology freedom, especially Cyber Sovereignty. For Indonesia, Cyber sovereignty is a new thing, and this can be seen from some of the internet infrastructures in terms of hardware and software, which are still dependent on foreign parties, from social media, electronic mail (email), internet storage (clouds), technology grants, servers, and others. [11] This provides a point of vulnerability if the use of free social media, email, clouds is used by state officials and then used to store confidential documents. In simple terms, cyber sovereignty can be defined as the government's ability to control cyberspace within the territory of the Republic of Indonesia. Similar to the

[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

[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>

territorial sovereignty of the Republic of Indonesia, the government has complete control over all political, economic, cultural, and technological activities. This makes cyber sovereignty resilience important for the Unitary State of the Republic of Indonesia (NKRI).

For Indonesia to maintain its cyber sovereignty with all its limitations, it can be done with the concept of gotong royong. The meaning of gotong royong means working together (helping each other).[12] Cyber sovereignty Gotong Royong means working together (helping each other) in upholding cyber sovereignty. Cyber sovereignty is not only the responsibility of the government alone, but also the responsibility of all stakeholders of the informatics community in Indonesia, which includes elements of Internet Companies (ISPs), Internet User Communities, Internet Cafes, E-commerce Companies, Telecommunication Companies, even to the scope of The smallest community is the family.

This article discusses the meaning of cyber sovereignty and how Indonesia maintains its cyber sovereignty with the concept of gotong royong and its comparison with the cyber sovereignty of the People's Republic of China.

This research is carried out using normative legal research; in normative legal research, the law is conceptualized as what is written in the legislation (law in the books), or the law is conceptualized as a rule or norm that is a benchmark for human behavior considered appropriate. [13] The approach taken by the qualitative method is by looking at and analyzing the norms in the existing laws and regulations and related court decisions.

This study also uses a comparative law approach (comparative law). According to Sudikno Mertokusumo, as quoted by Sunarjati Hartono, comparing the law is an attempt to find and signal the differences and similarities by providing explanations and researching how the law functions and how the juridical solutions are in practice, as well as which non-legal factors are involved. Affect it. [14]

In line with this statement, Rene David and Brierly, as quoted by Barda Nawawi Arief, stated, "One of the benefits and significance of comparative law is to understand better and develop national law."[15]

In collecting data, the tool used in this research is a literature study where according to Soerjono Soekanto in normative legal research, only library materials or secondary data are examined. [16]

B. Discussion

Some experts express their opinion regarding "cyberspace," a logical space that is difficult to perceive and manage accurately, "cyberspace" would not exist without the physical world. The difficulty in cyber governance is demonstrating administrative authority in cyberspace. This perception can be about the provisioning system. It can also be about existence in cyberspace; this perspective must combine subjectivity and objectivity, and the results are made by actors based on an objective framework and subjective judgments. In 2005, based on a UN report which stated that basically, the control of the DNS Zone was under the authority of the United States government, since then Internet governance reforms have been encouraged to use the principles of equality.[17]

[12] The definition of gotong royong according to the Big Indonesian Dictionary (KBBI) is working together, https://kbbi.web.id/gotong royong

[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.

It is from here that China's role in realizing sovereignty and what is meant by cyber sovereignty and how to guarantee sovereignty in the world, President Xi Jinping has used the term several times in which several critical components of the definition of cyber sovereignty can be understood: the first essential part of cyber sovereignty refers to on state sovereignty to manage the flow of information within the region; second is that each country has the power to make cyber-related policies independently; third is that every country should have roughly equal rights to participate in the decision-making process of the rules, norms or codes of conduct that govern global cyberspace; and respect for sovereignty should be one of the most important guiding principles for dealing with cyber-related issues internationally.[18]

Many research discusses President Xi Jinping's steps in upholding China's cyber sovereignty. Yi Sen discusses in his article entitled "Cyber Sovereignty and the Governance of Global Cyberspace" his article focuses on the role of China in leading the world movement against the domination of the United States to cyberspace.[19] Jinghan Zen Tim Stevens and Yaru Chen in "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty." Chinese cyberspace has increased the legitimacy and security of the CCP's regime's power, China's domestic and international goal.[20]

Research conducted by Yu Hong reviewing how China's power during a critical situation in cyberspace related to the global political economy has made the party-state have sovereignty in the cyber world. The development of the country's virtual sovereignty is aimed at countering the multi-influence of global capitalism.[21]

The research in the article has its characteristics, namely by comparing the implementation of cyber sovereignty in Indonesia with that in China, wherein Indonesia uses the local wisdom method known as "Gotong Royong."

C. Cyber sovereignty, Gotong Royong as Indonesian way of sovereignty, and Chinese cyber sovereignty

1. Cyber sovereignty and its central issue

The concept of sovereignty in the cyber world cannot be separated from sovereignty in general. Sovereignty is the highest, absolute power. No other agency equates it or controls it, which can regulate citizens and regulate the country's goal, regulate various aspects of government, and perform various actions in a country. Including but not limited to powers to legislate, implement and enforce laws, punish people, collect taxes, make peace and declare war, sign and enforce treaties, and others.[22]

Jean Bodin in De La Republique, as quoted by Munir Fuady, relates sovereignty as absolute and sustainable power in a country that is above positive law. Bodin defines sovereignty as "Sovereignty is supreme power over citizens and subjects, unrestrained by the laws," sovereignty is positioned above the law. According to him, besides having supremacy, sovereignty also has immortality. [23]

---

[18] *Ibid*
[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.

John Austin explained that sovereignty is a person or body or state leader who has sovereignty and can make positive laws that will be applied to members of an independent political society under the authority of the holder of the sovereignty, the majority in the community will obey the will of the sovereign concerned. [24]

H.L.A Hart sees the supremacy of a state's sovereignty even to the point that the State does not need to be subject to international law or be bound by international law or only a specific form of international law. [25] The meaning of "sovereign" is independent; it has enforcement powers: a sovereign State is not subject to certain types of control. Its sovereignty covers areas of action in which it is autonomous.[26]

In the Island of Palmas case, Max Huber emphasized that the relationship between sovereignty and territory, sovereignty can only be exercised over areas where the State can exercise its power in the form of the State's right to carry out State functions. [27]

Schwarzenberger talks about sovereignty as quoted by Huala Adolf as having the meaning of supreme power (omnipotence), which the State only owns; this sovereignty is used to describe the autonomy and power of the State to make legal rules (national law) that apply in its territory and create state institutions. [28]

Sovereignty in the cyber world is the sovereignty a country enjoys over its territory, which gives it the right to control cyberinfrastructure and cyber activities within its territory. Thus, cyberspace infrastructure located in inland areas, internal waters, territorial seas (including layers and layers of land), archipelagic waters, or national airspace is subject to the sovereignty of the territorial State. [29]

Speaking of sovereignty, it involves jurisdiction. Following applicable international law, the territory is a space for a country to exercise its sovereignty. A state network refers to an Information and Computer Technology (ICT) infrastructure consisting of an ICT system built on its territory. There is no question that a State can use its sovereignty to govern its ICT infrastructure like any other entity. Binxing Fang said regarding cyber sovereignty (cyberspace) that "cyberspace sovereignty is a natural extension of state sovereignty in cyber/cyberspace guided by ICT infrastructure located in the country's territory; that is, the State has jurisdiction (right to intervene in data operations) over ICT activities (about the role and operations of the cyber world) existing in the cyber world, ICT systems in terms of facilities, and data carried by computer technology and information systems (virtual assets). [30]

The fundamental rights of cyberspace sovereignty are also directly derived from state sovereignty, namely, cyberspace independence rights, cyberspace equality rights, cyberspace self-defense rights, and cyberspace jurisdiction rights. Cyberspace independence rights are manifested in networks within the country's territory that can operate independently without external interference. It is as natural as in the majority of existing network models, such as radio and television networks, industrial control networks, but as far as the Internet is concerned, the peculiarity of the centralized operating model of the global Internet results in being subject to Internet operations in

[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] *Ibid*
[27] Huala Adolf, *Filsafat Hukum Internasional*, Bandung: Keni Media (2020). hal..80
[28] Huala Adolf, *Hukum Ekonomi Internasional Suatu Pengantar*, Bandung: Keni Media (2019). p..224
[29] Michael N. Schmitt, *Tallinn Manual On The International Law Applicable To Cyber Warfare*, Cambridge: Cambridge University Press, (2013). p.13
[30] Binxing Fang, *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace*, Beijing: Science Press, (2018). p.83

every part of the country by the position of centralized control of the Internet, In the domain naming resolution.[31]

The problem of cyber sovereignty is not only a legal issue between one country and another but also between foreign corporations in other countries as Lessig described how the conflict between domestic (French) interests and foreign interests in the case of Yahoo selling Nazi equipment on the Yahoo site, the legal fact is that trading Nazi equipment is prohibited in France. In contrast, Yahoo sites that sell it can be accessed in France. Yahoo itself is physically a server located in New York City, United States, where things related to the Nazis are freely traded there.[32] Yahoo then faced a lawsuit by stopping buying and selling products on its site. Yahoo offered to the French government that they could make access to buying and selling related Nazi equipment inaccessible from France but failed to prove in court that they were able to do it 100% so that there is still the possibility that the site containing the prohibited trade and content can still be accessed. Yahoo was defeated in a French court that must remove the charge related to the Nazis with a period of 3 months and bear the burden of a fine of 100,000 francs per day for delays in its implementation.[33]

The United States' internet dominance is also a significant issue regarding cyber sovereignty, although its influence is visible and carried out in a "subtle way." The various actors involved in his administration collaborated through their vested interests to propagate the Western way of governing, more so the idea of a unified world globalized by US interests. The diplomatic strategy employed by China has had some minor victories. The Obama administration's decision to transfer internet authority over domain names issued from the US Department of Commerce to the international community is recognized as the result of effective diplomacy from China and Russia.[34] Issues that must be considered are the potential for war on the multi-stakeholder approach to The Internet Corporation for Assigned Names and Numbers (ICANN) as the agency responsible for naming internet domain names and the intergovernmental approach to The International Telecommunication Union (ITU), which is the UN sub-agency. There has been tentative agreement on the division of responsibilities since 2014, but 2016 saw some developments that may hint at a more uncertain future.

Another pressing issue, with uncertain consequences, is the ongoing debate about alleged election hacking in the United States and how this will affect perceptions of information sovereignty in the west. [35]

In the end, however, the virtual conditions of cyberspace will always require a "physical" infrastructure that will be placed within the territory of one/several countries; this is where the key to a country's territorial sovereignty naturally applies to cyberspace so that it does not prevent a country from exercising jurisdiction over cyberspace within its territory. Its territory, as well as the law of a country, applies to cyberinfrastructure within its territory, including whether to uphold freedom or to curb it depending on the respective country where the cyberinfrastructure is located, including setting up the data center (data center) where the information will be accessed—in the country concerned.

---

[31] *Ibid.* p.84
[32] Lessig, *The Code Version 2.0*. p.294-295
[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

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

As mentioned in the introduction, cyber sovereignty for Indonesia is new, even though its rights have been attached with the proclamation of independence. The big question is whether Indonesia has the sovereignty to control the information circulating in the cyber world today.

Cyber sovereignty in the Cyber Security and Resilience Legal Plans is defined as a term used in internet governance to describe the government's desire to exercise control over the Internet within their territory, including political, economic, cultural, and technological activities. For some people, control over the Internet is considered contrary to the principle of the Internet itself, where it is said that the Internet has no centralized governance both in the implementation of technology and policies for access and use.[36]

The biggest concern is if the government then monitors a person's activities on the Internet, including email accounts, social media, discussion groups, and others that can violate the account owner's human rights. However, in terms of the government's interest in the field of national cyber security, especially regarding the security of government-owned data and information that is confidential, we cannot deny that currently, Indonesia's cyber infrastructure is not very good; there are still many things that need to be improved related to various aspects. Starting from the condition of human resources that are less qualified, slow internet access, applications that have not been tested, to the security aspect that is often not paid attention to. For example, from the application side, the lack of stability in the email service provided by a government agency/institution to state administrators is not difficult to find, where often the services provided are difficult to access or shut down at certain times. [37]

The Government of the Republic of Indonesia has implemented Government Regulation (PP) No. 82 of 2012, which regulates the Implementation of Electronic Systems and Transactions, Article 17 paragraph (2), it is stated that electronic system operators for public services are required to place data centers and disaster recovery centers in the territory of Indonesia to ensure law enforcement, protection, and enforcement of state sovereignty over the data of its citizens.

The purpose of the location of this data center is to protect the personal data of Indonesian citizens by creating transparency in the use of data (for example, customer data) and safeguard the data from theft or manipulation by third parties outside the borders of Indonesia, which can have an impact on the company's lousy reputation up to the financial loss.

Some countries have implemented data storage localization policies. One of the policies that business people discussed last year was the GDPR (General Data Protection Regulation), drafted by the European Union government (implemented in 28 countries in Europe). In the regulation, every company (especially those domiciled outside the European Union's borders) is required to provide information to its citizens regarding the use of their data and send notifications within 72 hours in a cyber-attack crisis. [38]

Unfortunately, Government Regulation (PP) No. 82 of 2012 was revoked by Government Regulation (PP) No. 71 of 2019, so that the obligation for Data Centers to

[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

[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.

be located in Indonesia was also canceled. The revocation of the regulation has direct 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 government can block to enforce Indonesia's cyber sovereignty, the blocking itself is based on Article 40 of Law Number 16 of 2016 concerning Amendments to Law Number 11 of 2008 regarding Electronic Transactions in the State Gazette of 2016 Number 251 even though it has issues of human rights violations related to freedom of speech but can still be the basis for the government to block sites whose content is contrary to the laws in Indonesia, for example; prostitution, gambling, pornography, terrorism, and so on.

In this cooperation (Gotong Royong) cyber sovereignty system, the government as a regulator and executor in blocking internet content, the community plays an active role in two forms, namely; the first is independent blocking (performed by themselves), the second is by reporting to the government on sites/contents that violate the laws and norms that apply in Indonesia.

Cyber sovereignty is not only the responsibility of the government alone, but also the responsibility of all stakeholders of the informatics community in Indonesia, which includes elements of Internet Companies (ISPs), Internet User Communities, Internet Cafes, E-commerce Companies, Telecommunication Companies, even to the scope of The smallest community is the family.

The concept of cooperation cyber sovereignty is in line with the concept of "universal people's defense," which is regulated in Article 4 of Law Number 3 of 2002 concerning National Defense which states about the purpose of state defence 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. Indonesia, and the safety of the entire nation from all forms of threats. In the Elucidation, it is stated that what is meant by "threat" is every business and activity, both from within the country and abroad, which is considered to endanger the sovereignty of the State, the territorial integrity of the State, and the safety of the entire nation. If it is related to cyber sovereignty, it includes control over cyber infrastructure within the territory of the Unitary State of the Republic of Indonesia to ensure the safety of the entire nation from all forms of threats, including threats from the cyber world.

The government's role in terms of regulation includes blocking existing sites with technological efforts, namely with the AIS engine that it already has, becoming a kind of "Great Firewall of China" which distinguishes it from the Indonesian version is that in China, internet blocking relies on "machines" and "internet police." In Indonesia, this is carried out by the AIS machine, the AIS team, and the community's active role in the form of reports or independent blocking by installing filters on private networks, local networks, and internet provider company networks (ISPs).

Blocking by the Government of Indonesia (Ministry of Communication and Information) is carried out with the AIS machine, used by the AIS Team with two

mechanisms. The first method is that the team will regularly patrol 24 hours a day to monitor and look for harmful content on the Internet. The second way is to take action based on community participation in the form of reports from the community through various channels such as aduankonten.id.[39] This method is an effort to enforce our cyber sovereignty in the spirit of cooperation. (Gotong Royong).

One example of the success in 2020 carried out by Kominfo was the blocking of more than 1 million sites containing pornography and 166,853 gambling-related sites, and 8,689 fraudulent sites. Several other negatively charged sites that were successfully blocked were related to defamatory content, SARA, separatism, and information security violations. In total, there are 1,203,948, not to mention the blocking of more than 600 thousand content from social media.[40] Blocking efforts will continue in the latest 2021, including on fake news issues (hoaxes) about Covid-19, which are widely circulating on social media, until August 8, 2021, there were 1,897 hoaxes spread on various social media. The distribution of hoaxes is most often found on Facebook. There was 1,729 hoax content about the covid-19 vaccine. Video sharing sites, such as YouTube and TikTok, were also targeted by hoaxes. There are 41 hoaxes on YouTube and 17 on TikTok. Then the remaining 11 hoaxes were found by the Ministry of Communication and Informatics on Instagram.[41]

Cyber sovereignty in Indonesia can be enforced by blocking content in the cyber world contrary to the law. It can be law enforcement in a "non-penal" way where "penal" efforts cannot even be carried out because they collide with jurisdictional issues.

3. China Experience in Cyber Sovereignty

The people's Republic of China has the world's largest online population with more than 600 million Internet users. The People's Republic of China is also known for its highly tight internet controls, which are integral to the government's extensive surveillance of the flow of information, from media to culture. A recent Freedom House report detailed the Chinese government's sophisticated technical ability to enforce information control, including strategic control over crucial information nodes, outsourcing of censorship, party and ideological reinforcements, and a crackdown on social media.[42]

Cyber sovereignty in China is commonly conceptualized differently from cybersecurity, which concerns the protection of infrastructure and processes connected to the Internet. Cyberspace sovereignty, on the other hand, relates to the information and content that the Internet provides. China's concept of cyber sovereignty is based on two main principles: The first is that unwanted influence in a country's "information space" should be prohibited. As a result, this would allow states to prevent their citizens from being exposed to ideas and opinions that the regime deems harmful. Another fundamental principle is to move Internet governance away from current bodies,

[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

including academia and corporations, to international forums such as the United Nations. The move would also require the transfer of power from companies and individuals to the states only.[43]

The international response to China's efforts to implement the concept of cyberspace sovereignty in practice has been overshadowed by the Western world with espionage and industrial hacking in China. However, it will have much greater importance in the future. The concept has attracted more attention over the past few years. The United States expressed concern that China will use its policies to cover censorship, protectionism, and espionage. There was a statement noting those concerns, claiming that "In June 2015, China passed the National Security Law with the stated aim of keeping China's security in check, but including overarching provisions addressing economic and industrial policies. China also drafted laws relating to counterterrorism and cybersecurity in 2015 which, if finalized in their current form, would also impose far-reaching and onerous trade restrictions on imported Information Technology and Computer services in China."[44]

Introducing laws that would allow the Chinese government to increase control over the Internet is not exclusive to China or other authoritarian regimes. While several other countries, such as Russia, Iran, and Saudi Arabia, have taken steps in this direction, European countries such as Poland, Hungary, and the UK have also pointed out that the gap between democracy and dictatorship may have been unusual in recent years. This approach is also popular in developing countries, which see themselves at a digital disadvantage and are vulnerable to globalization. This is not to say that there are no distinct lines between countries seeking an open Internet and countries wanting it under tighter control, but the gaps in some areas may be closing. Some issues, such as companies helping the government, are also high on the US agenda. An example of this is the Apple-FBI case, where the FBI wanted a company to help hack the phones of captured terrorists. American companies are also increasingly turning to the United States government to protect them from foreign intrusion into their networks.[45]

The reaction to the Chinese concept has been met with intense skepticism by some NGOs. Before the 2015 World Internet Conference, Amnesty International asked companies to make a stand. It denounced the position of the People's Republic of China, declaring that talk of sovereignty was an "all-out attack on internet freedom." Freedom House has consistently ranked China as one of the worst countries when it comes to internet freedom. The strategy of gaining cyber sovereignty and its implementation has been cited as a significant factor in why China is considered the worst in its class.[46]

Fang Binxing, China's Great Firewall creator, expressed that view in his remarks at the China-Russia forum on Internet sovereignty in 2016. He claimed that much of the Internet's infrastructure is located in America means that Internet governance today is under the control of the United States. Therefore, the point is not to add the concept of government control to the Internet today but to force America to share control that already exists. By framing the problem in this issue, China seeks to build a narrative where state power already exists in cyberspace, but America is the hegemon. Therefore, establishing national sovereignty would not be a matter of Internet censorship but more actors than the US in its administration. This argument is in line with the broader trend in China's foreign policy calling for the "democratization of international relations." This idea is a step away from perceived Western dominance over international affairs

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

towards a more inclusive order with more respect for states' autonomy and internal affairs.[47]

In the end, the main problem is back to who controls the Internet and how the Internet is controlled, whether with China's conception of the Great Firewall of China, which does not allow outbound access which automatically stimulates domestic industries to develop as people enjoy Baidu compared to Google, Weibo reached to Facebook. Wechat is compared to WhatsApp, so the experience of its citizens is no different from outside China. It is just that they have very sophisticated filters that can block the WeChat private chat application.[48]

What China has implemented to gain cyber sovereignty has been met with contradictions both domestically and internationally. The China government itself also realizes this. Hao Yeli, one of the Major Generals who served in the Chinese People's Liberation Army, revealed at least three conflicts.[49]

The first is the conflict between cyber sovereignty and the spirit of the Internet; The exclusivity of classical state sovereignty contradicts the nature of the Internet, which rests on the concept of unlimited interconnectivity. If the emphasis is placed on cyber sovereignty, this can lead to each country forming its cyberspace, resulting in the fragmentation of the Internet. This makes conflicts between cyber sovereignty and human rights. It reflects the tension between the principle of free speech on the internet and state intervention in the name of cyber sovereignty, which limits the free flow of information. Such criticism is primarily aimed at the establishment of an internet firewall in China. The third is the conflict between cyber sovereignty and the involvement of various stakeholders in governance. It is argued that cyber sovereignty will spark controversy on internet governance patterns; that is, a government led by a sovereign (one-party) government will be challenged by a multi-party (existing in a foreign country) pattern of government.[50]

Chinese Internet policies have domestic and international aspects, each intimately tied to concerns about regime security. From the perspective of the CCP, threats to regime security derive from domestic sources and external influence, the latter mainly mediated by the Internet. Domestic Internet censorship is geared both to suppressing indigenous political dissent and restricting the influx of foreign ideas corrupting the Chinese populace, either of which or both in combination, could lead to the delegitimization of the CCP and the destabilization of the Chinese State. In this context, the pursuit of Internet sovereignty is both a justification of its domestic policies and an attempt to ward off foreign interference, both "hard" and "soft."[51]

Chinese government's attempt to reshape cyber norms also helps to improve the CCP's domestic legitimacy and improve regime security. In this way, Internet sovereignty serves both domestic and foreign policy goals, united by a fundamental concern with maintaining the Chinese State. In the global arena, however, the relevant discourse is not yet sufficiently developed to be either convincing or practical, let alone widely applied in governing global cyberspace. [52]

D. Conclusion

[47] Schia and Gjesvik.
[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.

Cyber sovereignty is essential for an independent country like Indonesia. However, Indonesia's cyber sovereignty is hindered by several factors; first, the dominance of the United States over the world's internet infrastructure, second, the absence of a data center obligation to be placed within the territory of Indonesia, and at least international cooperation related to cyber jurisdiction make lack of law enforcement. Indonesia's limitations in maintaining its cyber sovereignty can be anticipated by using the concept of Gotong Royong cyber sovereignty, which is the implementation of the Universal People's Defense System as regulated in Law Number 3 of 2002 concerning National Defense. The implementation of Cyber Gotong Royong sovereignty involves all citizens, regions, and other national resources.

China can be an example of enforcing cyber sovereignty using a policy known as the "Great Firewall of China," which allows the country to control all internet activities within its sovereign territory. The "Great Firewall of China" policy model cannot be applied in Indonesia because it relates to the freedom of speech protected by the 1945 Constitution. However, blocking can still be carried out within limits set by existing laws. In contrast to the "Great Firewall of China" policy in China, internet blocking, which only relies on "machines" and "internet police," in Indonesia is carried out by the AIS machine, the AIS Team, and the active role of the community in the form of reports or independent blocking by installing filters on private networks, local network, and internet service provider company network.

Bibliography

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

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

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/.

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.

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.

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

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.

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).

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.

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

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

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

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/.

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

P-ISSN 2723-262X
E-ISSN 2745-9306

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.

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

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.

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

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.