Proceedings of the 3rd International Conference on Social and Islamic Studies
Online ISSN: 2809-6339
Volume: 3, 2023
Publisher: Alauddin University Press

THE URGENCY OF CYBER SOVEREIGNTY RESILIENCE FOR INDONESIA (COMPARATIVE STUDY WITH THE PEOPLE'S REPUBLIC OF CHINA)

Nur Ro'is[1]
[1]Universitas Baturaja
Correspondence Email: nurrois@unbara.ac.id

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 contains jurisdictional authority, but in reality, there are unclear territorial boundaries in cyberspace. Indonesia today still has a dependence on foreign cyber infrastructure which causes a high level of cyber vulnerability along with low cyber sovereignty resilience. In contrast with the People's Republic of China, which has a strong infrastructure and strict cyber policies, it has powerful cyber sovereignty resilience. This study compares the resilience of Indonesia's cyber sovereignty with the People's Republic of China by using a normative legal research methodology, with a comparative law approach, it is hoped that it can determine the urgency of cyber sovereignty strength for Indonesia.

Keywords: Cyber sovereignty; cyber sovereignty strength; Indonesian cyber sovereignty; Chinese cyber sovereignty

1. INTRODUCTION

The development of information technology is growing rapidly and spreading to almost all areas of society. Developments in information technology also affect legal aspects. The boundaries of a country's territory seem meaningless anymore with the development of existing information technology, the relationship between one part of the world and another is done in a matter of seconds. Transactions between regions of the country are carried out remotely and can be done at any time. The parties involved in the transaction only rely on the principle of trust and evidence in the form of existing

electronic data. The use of information technology, media and communication has changed both the behavior of society and human civilization globally. Information technology is currently a double-edged sword because in addition to contributing to the improvement of welfare, progress, and humanity, it is also an effective means of acts against the law (crime) which, according to Mardjono Reksodiputro's term, is known to have a contemporary nature due to the problem of computer use (Reksodiputro, 2007).

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 become overlapping. This chaotic situation is illustrated by the cyber world regulatory model as revealed by Lessig in his book "The Code" that technology can weaken laws and norms, where according to him cyberspace is likened to the dot governed by The Code which consists of law, Norm, Architecture and Market. , the four support each other, a change to one affects the whole (Lessig, 2006).

According to Lessig, (Lessig, 2006) the four influence each other, support or even mutually destroy one another. Technology can undermine laws and norms; but also, can support it. Norms can be a reference for behavior in society, the market through pricing supports the rules, while architecture creates a physical environment that forces the rule of law to be obeyed. According to Lessig, (Lessig, 2006) the regulation of cyberspace depends on the architecture, some architectures cannot be managed, some can be adjusted. The choice on the government to regulate the existing architecture, so that it becomes "The Code" for cyberspace. As for architecture that cannot be regulated, the government can take steps to make rules directly or indirectly. And finally, the government's ability to reorganize depends on the character of "The Code". Regulation will be easier on "code" which has the character "closed code" while on "open code" the power of government regulations becomes less binding. “Closed code” type settings can be found in communist countries such as China and North Korea which tighten internet access for their citizens, while “open code” type settings are found in many liberal countries, one example of which is the United States.

China is one of the countries that are active in implementing cyber sovereignty in their country, especially in the defense and security domain. On December 31, 2015 Chinese officials announced a major 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 has described reforms as essential to modernizing the military. and the reorganization confirmed the PLA's loyalty to the Chinese Communist Party (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, the SSF secures electromagnetic space and cyber space. Chinese military experts hail the SSF as necessary for twenty-first century

warfare. Over the years, the PLA has deployed cyberspace capabilities at various command levels, and the SSF elevated control of cyberspace operations to the highest echelons. ultimately, the PLA uses cyberspace power to ensure cyber sovereignty (wangluo zhuquan) and safeguard the Chinese Dream in all domains (Kolton, 2017).

Sovereignty is a keyword in the current era of information technology freedom, especially Cyber Sovereignty. For Indonesia, Cyber Sovereignty is a new thing, this can be seen from some of the internet infrastructure in terms of hardware and software which still depends on foreign parties, from social media, electronic mail (email), internet storage (clouds), technology grants, servers (servers), and others. This provides a point of vulnerability if the use of social media, e-mail, free clouds is used by state officials and then used to store confidential documents. In simple terms, cyber sovereignty can be interpreted as the ability of the government to control cyber space within the territory of the Republic of Indonesia. (Rahman, n.d.) Similar to the territorial sovereignty of the Republic of Indonesia, the government fully controls all political, economic, cultural and technological activities. This is what makes cyber sovereignty resilience an important matter for the Unitary State of the Republic of Indonesia (NKRI).

Based on the background that has been presented, problems related to the urgency of cyber sovereignty resilience can be drawn, namely; What is the urgency of maintaining cyber sovereignty for Indonesia and how does it compare to cyber sovereignty implemented in the People's Republic of China? The purpose of this research is to see the urgency of Indonesia's cyber sovereignty resilience and a comparison of cyber sovereignty in the People's Republic of China (PRC).

2. METHODS

This research was carried out using normative legal research, in normative legal research law is conceptualized as what is written in laws and regulations (law in the books) or law is conceptualized as rules or norms which are benchmarks for human behavior deemed appropriate (Amiruddin & Asikin, 2006). The approach used is qualitative method, namely by looking at and analyzing the norms in 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, that Comparing law is an attempt to find and signal differences and similarities by providing explanations, and researching how the law functions, and how the juridical solution is in practice, as well as which non-legal factors affect it (Hartono, 1988). 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 better understand and develop national law" (Arief, 2010).

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 studied (Soerjono, 1981).

3. RESULTS AND DISCUSSION

The concept of sovereignty in cyberspace cannot be separated from the concept of sovereignty in general. Sovereignty is the highest, absolute power, and there is no other agency that equates it or controls it, which can regulate citizens and also regulate what is the goal of a country, and regulate various aspects of government, and carry out various acti the concept of sovereignty in cyberspace cannot be separated from the concept of sovereignty in general. Sovereignty is the highest, absolute power, and there is no other agency that equates it or controls it, which can regulate citizens and also regulate what is the goal of a country, and regulate various aspects of government, and carry out various factions within a country, including but is not limited to the powers of legislators, implementing and enforcing laws, punishing people, collecting taxes, making peace and declaring war, signing and enforcing treaties, and so on (Fuady, 2013).

Jean Bodin in De La Republique, as quoted by Munir Fuady relates sovereignty as absolute and continuous 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" (Fuady, 2013). Jhon Austin explained that sovereignty is a person or body or state leader who has sovereignty can make positive laws that will be applied to members of an independent political community under the authority of the sovereign, the majority in the community will comply with the wishes of the relevant sovereign (Fuady, 2013).

H. L. A Hart saw the supremacy of a state's sovereignty even to the point that a state does not need to be subject to international law, or be bound by international law or can only be bound by a certain specific form of international law. The meaning of "sovereign" is independent; has enforcement power: a sovereign State is not subject to any particular type of control, and its sovereignty includes areas of action in which it is autonomous (Hart, 2011).

Talking about sovereignty, it definitely involves jurisdiction. In accordance with the applicable rules of international law, territory is a space for a country to exercise its sovereignty. Country network refers to the Information and Computer Technology (ICT) infrastructure consisting of ICT systems built on its own territory. There is no question that a state can use its sovereign power to govern, like any other entity, its own ICT infrastructure. Binxing Fang said regarding cyber sovereignty that "cyberspace sovereignty is a natural extension of state sovereignty in cyberspace guided by ICT infrastructure located on the territory of the country; that is, the state has jurisdiction

(right to intervene in data operations) over ICT activities (concerning the role and operations of the cyber world) that exist in cyberspace, ICT systems in terms of facilities, and data carried by Computer Technology and Informatics systems (virtual assets)(Fang, 2018).

The basic rights of cyberspace sovereignty also directly derive from state sovereignty, namely, the right to cyberspace independence, the right to cyberspace equality, the right to cyberspace defense, and the right to cyberspace jurisdiction. The right to cyberspace independence is embodied in networks within parts of the country that can operate independently without external interference. It is naturally obvious that 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 peculiarities of the centralized operating model of the global Internet result in the subjection of Internet operations in every part of the country to the centralized control positions of the Internet. in terms of domain name resolution (Fang, 2018).

The right to cyberspace equality is a manifestation of the independent condition of the country concerned, making equal power for policy makers with developments in technology and international policies, the right to self-defense is embodied in a network area that is considered a special network of protected area areas (specialized protected area), this has been implemented by the United States in the Manhattan project, a project of the United States military network to protect United States interests in cyber space (Fang, 2018). It is clear here that sovereignty is attached to the rights that exist in the state naturally.

Cyber sovereignty issues are not only legal issues between one country and another, but also related to foreign corporations in other countries. As Lessig describes how the conflict between domestic (French) and foreign interests in the case of Yahoo selling Nazi equipment on the Yahoo site, the legal fact of buying and selling Nazi equipment is prohibited in France, while the Yahoo site that trades it can be accessed in France, the site Yahoo itself is physically the paladin (server) located in the city of New York, United States, where things related to the Nazis are freely traded there. Yahoo then faced demands to stop buying and selling products on its website, Yahoo offered to the French government that they could make access to the trade related to Nazi equipment inaccessible from the French State but failed to prove in court that they could do so 100%, so there is still a possibility that sites that contain trade and content that are prohibited can still be accessed. Yahoo was defeated in a French court to have to remove the content related to the Nazis with a period of 3 months and bear the burden of fines of 100,000 Francs per day for delays in implementation (Lessig, 2006).

The existence of US domination of the Internet is also a major problem related to cyber sovereignty, even though its influence is not obvious and is carried out in a "subtle way". The various actors involved in his administration collaborated through their own personal interests to propagate a Western way of governing, especially the idea of a unified world globalized by the interests of the United States. The diplomatic strategy used by China has had some minor wins. The Obama administration's decision to transfer internet authority over domain names issued from the US Department of Commerce, left to the international community is recognized as the result of effective diplomacy from China and Russia. The problem that must be considered is the potential war of approaches by multi-stakeholders to The Internet Corporation for Assigned Names and Numbers (ICANN) as the Institution responsible for naming internet domain names, and the intergovernmental approach to The International Telecommunication Union (ITU), which is UN sub-agency (Calamur, 2018). There has been tentative agreement on the sharing of responsibilities since 2014, but 2016 saw some developments that might 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 (Schia & Gjesvik, 2018a).

In the end, however, the virtual conditions of cyberspace will always require "physical" infrastructure that will be placed within the territory of one/several countries, this is where the key to territorial sovereignty of a country naturally applies to cyberspace, so it does not prevent a country from exercising jurisdiction over cyberspace that is in its territory. territorial, as well as the law of a country that applies to cyber infrastructure in its territorial area, including whether to uphold freedom or to restrain it depends on each country where the cyber infrastructure is located, including data center settings where the information will be accessed within the country concerned (Ro'is, 2022).

How about Indonesia? As mentioned in the introduction, cyber sovereignty for Indonesia is something new, even though its rights have been attached together with the proclamation of independence. The big question is whether we have the sovereignty to control the information that travels in cyberspace today.

Cyber sovereignty in the Cyber Security and Resilience Bill is interpreted 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 to be contrary to the principles of the internet itself, where it is said that the internet does not have centralized governance either in terms of technology implementation or policies for access and use (DPR RI, 2020).

The biggest concern is if the government then monitors all of a person's activities on the internet, including email accounts, social media, discussion groups and others that have the potential to violate the human rights of account owners. However, in terms of the government's interests in the field of national cyber security, especially regarding the security of government data and information that are confidential in nature, 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 who are less qualified, slow internet access, untested applications, to security aspects that are often overlooked. For example, from the application side, the lack of stability of the email service provided by a government agency/institution to state administrators is not difficult to find, where the services provided are often difficult to access or turn off at certain times (DPR RI, 2020).

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, in 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 Indonesian territory with the aim of ensuring 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 protecting this data from theft or manipulation by third parties outside the boundaries of Indonesia, which can have an impact on the company's bad reputation. financial loss. Several countries have implemented data storage localization policies. One of the policies that was busy being discussed by business people in the past year was the GDPR (General Data Protection Regulation), designed by the European Union government (which was implemented in 28 countries in Europe). Under these regulations, every company (especially those domiciled outside the borders of the European Union) is required to provide information to its citizens regarding the use of their personal data, and send notifications within 72 hours in the event of a cyber-attack crisis (TelkomTelstra, n.d.).

It is very unfortunate that 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 be located in Indonesia was also revoked. The revocation of this regulation has direct implications for Indonesia's cyber sovereignty, including:

1. Jurisdictional problems, especially if there is a violation of law while the data center is outside the reach of the Indonesian government.

2. There is a high probability that personal data information, even important and state-secret information, will be leaked to third parties because there is no government control over data stored in data centers.

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 developing, because there is no obligation to use data centers within Indonesia.

The government can block to uphold Indonesia's cyber sovereignty, blocking itself based on Article 40 of Law Number 16 of 2016 concerning Amendments to Law Number 11 of 2008 concerning 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 it can still be a basis for the government to block sites whose content is contrary to laws in Indonesia, for example; prostitution, gambling, pornography, terrorism, and so on.

The law here must play a leading role in regulating development in the field of Information and Communication Technology, as in Mochtar Kusumaatmaja's theory of development law that law is a means of community renewal and law as a tool (regulator) or means of development in the sense of channeling the direction of human activity in the direction desired by development or reform (Mochtar Kusumaatmadja, 2002).

Rapid developments and changes in information and communication technology will require changes in law that are fast as well, as Mochtar Kusumaatmadja argues that these changes can be carried out in an "orderly and orderly manner", otherwise changes will be made forcefully and quickly with the possibility of chaos., which if not controlled can result in a regressive effect which may negate the results of the changes that have been achieved through violence (Mochtar Kusumaatmadja, 2002).

The concept of Indonesia's cyber sovereignty cannot be implemented as full sovereignty over the cyber world due to several obstacles in its implementation, including;

1. The United States which have influence over internet domain names through the ICANN agency as the only non-profit organization that regulates domain names on the internet, this institution is domiciled in Los Angeles, United States of America;

2. Data centers that are outside the jurisdiction in Indonesia limit our ability to close a site that is contrary to the laws and norms that apply in Indonesia;

3. International cooperation related to cyber jurisdiction which is still limited so that it creates limitations in law enforcement related to cybercrimes.

When viewed in comparison with other countries, the People's Republic of China for example can be a model for managing cyber sovereignty, where cyber sovereignty is usually conceptualized differently from the term cyber security, 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. In effect, this will enable states to prevent their citizens from being exposed to ideas and opinions that the regime deems harmful. Another key principle is to move Internet governance from current bodies, which include academia and companies, to international forums such as the United Nations. This move would also require a transfer of power from corporations and individuals to the states only (Schia & Gjesvik, 2018a).

The international response to China's attempts to put the concept of cyberspace sovereignty in practice has been overshadowed by the West with industrial espionage and hacking in China, though this will assume much greater importance in the future. The concept has attracted more attention over the past few years, with the United States expressing concern that China will use its policies as a cover for censorship, protectionism and espionage. There was a statement noting the concerns, claiming that "In June 2015, China passed the National Security Act with the stated aim of keeping China safe, but including overarching provisions addressing economic and industrial policies. China also drafted a law relating to counterterrorism and cybersecurity in 2015 which, if finalized in its current form, would also impose far-reaching and onerous trade restrictions on imported Information Technology and Computer products and services in China" (Schia & Gjesvik, n.d.).

The introduction of laws that allow the Chinese government to increase control over the Internet is not exclusive to China or any other authoritarian regime. While some other countries, such as Russia, Iran and Saudi Arabia have taken steps in this direction, European countries such as Poland, Hungary and the United Kingdom have pointed out that the clear dictatorship-democracy divide may not have been the norm in recent years. This approach is also popular in developing countries, which see themselves at a digital disadvantage and are vulnerable to globalization. This isn't to say that there aren't distinct lines between countries seeking an open Internet and countries that want it under tighter control, but the gap in some areas may be closing. Some issues, such as companies helping the government when asked, are also high on the agenda in the US. 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 intrusions into their networks (Schia & Gjesvik, n.d.).

Reaction to the Chinese concept has been received with strong skepticism by some NGOs. Prior to the 2015 World Internet Conference, Amnesty International asked the company to make a statement and criticize the position of the People's Republic of China, stating that the talk of freedom 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 world cyber defeat, and how it is implemented, has been positioned as a major factor in why China is considered the worst in its class (Schia & Gjesvik, 2018b).

Fang Binxing, known as the creator of China's Great Firewall, expressed that view in his remarks at the China-Russia forum on Internet sovereignty in 2016. He claimed that the fact that much of the Internet's infrastructure is located in America means that the United States controls today's Internet governance. . Therefore, The point is not to add the concept of government control to today's Internet, but to force America to share existing control. By framing the issues within this issue, China seeks to build a narrative in which state power already exists in cyberspace, but America is the hegemon. Establishing national sovereignty would, therefore not be a matter of Internet censorship, but the inclusion of more actors than the US in its administration. This argument is in line with the broader trend in Chinese foreign policy that calls for a "democratization of international relations". This notion is a move away from perceived Western domination of international affairs towards a more inclusive order with greater respect for autonomy and the internal affairs of states (Schia & Gjesvik, 2018a).

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 external access that automatically stimulates the domestic industry to develop as people enjoy Baidu compared to Google, Weibo compared to Facebook, and WeChat compared to WhatsApp, so the experience of citizens is no different from outside China, only they have very sophisticated filters that can block the private chat application WeChat (Calamur, 2018).

For Indonesia to be able to maintain its cyber sovereignty, it is carried out with the concept of gotong royong. As the meaning of gotong royong means working together (help, helping each other), Cyber Sovereignty Gotong Royong means working together (helping, 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 in the informatics community in Indonesia, including elements from Internet Companies (ISPs), Internet User Communities, Internet Cafes, E-commerce Companies, Telecommunications Companies, even to the scope of the smallest community is the family.

In this mutual cooperation cyber sovereignty system, the government as the regulator and executor in blocking internet content, the community plays an active role in two forms, namely; the first is independent blocking (performed by the people themselves), the second is by reporting to the government on sites/content that violate the laws and norms that apply in Indonesia (Ro'is, 2022).

The model for implementing the "gotong royong" cyber sovereignty system is in line with the Indonesian defense system, namely a defense system that is universal in nature which involves all citizens, territories and other national resources, and is prepared early by the government and implemented in a total, integrated, directed, and continue to uphold state sovereignty, territorial integrity, and the safety of the entire nation from all threats. Against any threats to sovereignty from cyberspace, this universal defense system will be very effective where the government does not play an active role alone but is supported by all citizens and resources in Indonesia.

In Law Number 3 of 2002 concerning National Defense, it is stated regarding the objectives of national defense that the National Defense aims to maintain and protect state sovereignty, the territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of the entire nation from all forms of threats. In the Elucidation it is stated that what is meant by threats is any business and activity, both domestic and foreign, 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 entire nation's safety from all forms of threats, including one threat from the cyber world.

The government's role in terms of regulations includes blocking existing sites with technological efforts, namely with the AIS engine that it already has, it becomes a kind of "Great Firewall of China" which differs from the Indonesian version in that in China internet blocking only relies on "machines" and "internet police". ", in Indonesia it 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 networks and internet provider company (ISP) networks.

Blocking by the Government of Indonesia (Ministry of Communication and Information) is carried out with an AIS engine which is used by the AIS Team with two mechanisms. The first way the team will patrol regularly 24 hours a day to monitor and look for negative content on the internet. The second way of taking action is based on community participation in the form of reports coming from the community through various channels such as dukuponten.id. this method is an effort in upholding our cyber sovereignty with the spirit of "gotong royong."

One example of success in 2020 carried out by Kominfo is blocking more than 1 million sites that contain pornography, and blocking 166,853 sites related to gambling and 8,689 fraud 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 blocking more than 600 thousand content from social media. Blocking efforts have continued in the most recent 2021, including the issue of fake news (hoaxes) about Covid-19 which are widely circulating on social media, until 08 August 2021 there were 1,897 findings of hoaxes spread across various social media. The spread of hoaxs is most commonly found on Facebook. There are 1,729 hoaxes about the Covid-19 vaccine. Video sharing sites, such as YouTube and TikTok, are also not spared from being targeted by hoaxes. It was noted that there were 41 hoaxes on YouTube and 17 on TikTok. Then the remaining 11 hoaxes were found by the Ministry of Communication and Information on Instagram (Kominfo, 2021).

Cyber sovereignty in Indonesia can be enforced by blocking policies on content in the cyber world that are against the law, and can be law enforcement in a "non-penalty" way where "penal" efforts cannot even be carried out because they collide with jurisdictional issues (Ro'is, 2020). Jean Bodin in De La Republique, as quoted by Munir Fuady relates sovereignty as absolute and continuous 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" (Fuady, 2013). Jhon Austin explained that sovereignty is a person or body or state leader who has sovereignty can make positive laws that will be applied to members of an independent political community under the authority of the sovereign, the majority in the community will comply with the wishes of the relevant sovereign (Fuady, 2013).

H. L. A Hart saw the supremacy of a state's sovereignty even to the point that a state does not need to be subject to international law, or be bound by international law or can only be bound by a certain specific form of international law. The meaning of "sovereign" is independent; has enforcement power: a sovereign State is not subject to any particular type of control, and its sovereignty includes areas of action in which it is autonomous (Hart, 2011).

Talking about sovereignty, it definitely involves jurisdiction. Under the applicable rules of international law, territory is a space for a country to exercise its sovereignty. The country network refers to the Information and Computer Technology (ICT) infrastructure consisting of ICT systems built on its territory. There is no question that a state can use its sovereign power to govern, like any other entity, its own ICT infrastructure. Binxing Fang said regarding cyber sovereignty that "cyberspace sovereignty is a natural extension of state sovereignty in cyberspace guided by ICT infrastructure located on the territory of the country; that is, the state has jurisdiction (right to intervene in data operations) over

ICT activities (with respect to the role and operations of the cyber world) that exist in cyberspace, ICT systems in terms of facilities, and data carried by Computer Technology and Informatics systems (virtual assets)(Fang, 2018).

The basic rights of cyberspace sovereignty also directly derive from state sovereignty, namely, the right to cyberspace independence, the right to cyberspace equality, the right to cyberspace defense, and the right to cyberspace jurisdiction. The right to cyberspace independence is embodied in networks within parts of the country that can operate independently without external interference. It is naturally obvious that 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 peculiarities of the centralized operating model of the global Internet result in the subjection of Internet operations in every part of the country to the centralized control positions of the Internet. in terms of domain name resolution (Fang, 2018).

The right to cyberspace equality is a manifestation of the independent condition of the country concerned, making equal power for policy makers with developments in technology and international policies, the right to self-defense is embodied in a network area that is considered a special network of protected area areas (specialized protected area), this has been implemented by the United States in the Manhattan project, a project of the United States military network to protect United States interests in cyberspace (Fang, 2018). It is clear here that sovereignty is naturally attached to the rights that exist in the state.

Cyber sovereignty issues are not only legal issues between one country and another, but also related to foreign corporations in other countries. As Lessig describes how the conflict between domestic (French) and foreign interests in the case of Yahoo selling Nazi equipment on the Yahoo site, the legal fact of buying and selling Nazi equipment is prohibited in France, while the Yahoo site that trades it can be accessed in France, the site Yahoo itself is physically the paladin (server) located in the city of New York, United States, where things related to the Nazis are freely traded there. Yahoo then faced demands to stop buying and selling products on its website, Yahoo offered to the French government that they could make access to the trade related to Nazi equipment inaccessible from the French State but failed to prove in court that they could do so 100%, so there is still a possibility that sites that contain trade and content that are prohibited can still be accessed. Yahoo was defeated in a French court to have to remove the content related to the Nazis with a period of 3 months and bear the burden of fines of 100,000 Francs per day for delays in implementation (Lessig, 2006).

The existence of US domination of the Internet is also a major problem related to cyber sovereignty, even though its influence is not obvious and is carried out in a "subtle

way". The various actors involved in his administration collaborated through their own personal interests to propagate a Western way of governing, especially the idea of a unified world globalized by the interests of the United States. The diplomatic strategy used by China has had some minor wins. The Obama administration's decision to transfer internet authority over domain names issued from the US Department of Commerce, left to the international community is recognized as the result of effective diplomacy from China and Russia. The problem that must be considered is the potential war of approaches by multi-stakeholders to The Internet Corporation for Assigned Names and Numbers (ICANN) as the Institution responsible for naming internet domain names, and the intergovernmental approach to The International Telecommunication Union (ITU), which is UN sub-agency (Calamur, 2018). There has been tentative agreement on sharing responsibilities since 2014, but 2016 saw some developments that might 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 (Schia & Gjesvik, 2018a).

In the end, however, the virtual conditions of cyberspace will always require "physical" infrastructure that will be placed within the territory of one/several countries, this is where the key to territorial sovereignty of a country naturally applies to cyberspace, so it does not prevent a country from exercising jurisdiction over cyberspace that is in its territory. territorial, as well as the law of a country that applies to cyber infrastructure in its territorial area, including whether to uphold freedom or to restrain it depends on each country where the cyber infrastructure is located, including data center settings where the information will be accessed within the country concerned (Ro'is, 2022).

How about Indonesia? As mentioned in the introduction, cyber sovereignty for Indonesia is something new, even though its rights have been attached together with the proclamation of independence. The big question is whether we have the sovereignty to control the information that travels in cyberspace today.

Cyber sovereignty in the Cyber Security and Resilience Bill is interpreted as a term used in the field of internet governance to describe the government's desire to exercise control over the internet within their own territory, including political, economic, cultural and technological activities. For some people, control over the internet is considered to be contrary to the principles of the internet itself, where it is said that the internet does not have centralized governance either in terms of technology implementation or policies for access and use (DPR RI, 2020).

The biggest concern is if the government then monitors all of a person's activities on the internet, including email accounts, social media, discussion groups and others that have the potential to violate the human rights of account owners. However, in terms of

the government's interests in the field of national cyber security, especially regarding the security of government data and information that are confidential in nature, 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 who are less qualified, slow internet access, untested applications, to security aspects that are often overlooked. For example, from the application side, the lack of stability of the email service provided by a government agency/institution to state administrators is not difficult to find, where the services provided are often difficult to access or turn off at certain times (DPR RI, 2020).

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, in 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 Indonesian territory 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 protecting this data from theft or manipulation by third parties outside the boundaries of Indonesia, which can have an impact on the company's bad reputation financial loss.

Several countries have implemented data storage localization policies. One of the policies that was busy being discussed by business people in the past year was the GDPR (General Data Protection Regulation), designed by the European Union government (which was implemented in 28 countries in Europe). Under these regulations, every company (especially those domiciled outside the borders of the European Union) is required to provide information to its citizens regarding the use of their personal data, and send notifications within 72 hours in the event of a cyber-attack crisis (TelkomTelstra, n.d.).

It is very unfortunate that 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 be located in Indonesia was also revoked. The revocation of this regulation has direct implications for Indonesia's cyber sovereignty, including:

1. Jurisdictional problems, especially if there is a violation of law while the data center is outside the reach of the Indonesian government.

2. There is a high probability that personal data information, even important and state-secret information, will be leaked to third parties because there is no government control over data stored in data centers.

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 developing, because there is no obligation to use data centers within Indonesia.

The government can block to uphold Indonesia's cyber sovereignty, blocking itself based on Article 40 of Law Number 16 of 2016 concerning Amendments to Law Number 11 of 2008 concerning 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 it can still be a basis for the government to block sites whose content is contrary to laws in Indonesia, for example; prostitution, gambling, pornography, terrorism, and so on.

The law here must play a leading role in regulating development in the field of Information and Communication Technology, as in Mochtar Kusumaatmaja's theory of development law that law is a means of community renewal and law as a tool (regulator) or means of development in the sense of channeling the direction of human activity in the direction desired by development or reform (Mochtar Kusumaatmadja, 2002).

Rapid developments and changes in information and communication technology will require changes in law that are fast as well, as Mochtar Kusumaatmadja argues that these changes can be carried out in an "orderly and orderly manner", otherwise changes will be made forcefully and quickly with the possibility of chaos., which if not controlled can result in a regressive effect which may negate the results of the changes that have been achieved through violence (Mochtar Kusumaatmadja, 2002).

The concept of Indonesia's cyber sovereignty cannot be implemented as full sovereignty over the cyber world due to several obstacles in its implementation, including;

1. The United States which has influence over internet domain names through the ICANN agency as the only non-profit organization that regulates domain names on the internet, this institution is domiciled in Los Angeles, United States of America;

2. Data centers that are outside the jurisdiction in Indonesia limit our ability to close a site that is contrary to the laws and norms that apply in Indonesia;

3. International cooperation related to cyber jurisdiction which is still limited so that it creates limitations in law enforcement related to cybercrimes.

When viewed in comparison with other countries, the People's Republic of China for example can be a model for managing cyber sovereignty, where cyber sovereignty is usually conceptualized differently from the term cyber security, 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. In effect, this will enable states to prevent their citizens from being exposed to ideas and opinions that the regime deems harmful. Another key principle is to move Internet governance from current bodies, which include academia and companies, to international forums such as the United Nations. This move would also require a transfer of power from corporations and individuals to the states only (Schia & Gjesvik, 2018a).

The international response to China's attempts to put the concept of cyberspace sovereignty in practice has been overshadowed by the West with industrial espionage and hacking in China, though this will assume much greater importance in the future. The concept has attracted more attention over the past few years, with the United States expressing concern that China will use its policies as a cover for censorship, protectionism and espionage. A statement noted the concerns, claiming that "In June 2015, China passed the National Security Act with the aim of keeping China safe, but including overarching provisions addressing economic and industrial policies. China also drafted a law relating to counterterrorism and cybersecurity in 2015 which, if finalized in its current form, would also impose far-reaching and onerous trade restrictions on imported Information Technology and Computer products and services in China" (Schia & Gjesvik, n.d.).

The introduction of laws that allow the Chinese government to increase control over the Internet is not exclusive to China or any other authoritarian regime. While some other countries, such as Russia, Iran and Saudi Arabia have taken steps in this direction, European countries such as Poland, Hungary and the United Kingdom too, have pointed out that the clear dictatorship-democracy divide may not have been the norm in recent years. This approach is also popular in developing countries, which see themselves at a digital disadvantage and are vulnerable to globalization. This isn't to say that there aren't distinct lines between countries seeking an open Internet and countries that want it under tighter control, but the gap in some areas may be closing. Some issues, such as companies helping the government when asked, are also high on the agenda in the US. 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 intrusions into their networks (Schia & Gjesvik, n.d.).

Reaction to the Chinese concept has been received with strong skepticism by some NGOs. Prior to the 2015 World Internet Conference, Amnesty International asked the company to make a statement and criticize the position of the People's Republic of China, stating that the talk of freedom 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 world cyber defeat, and the way in which it is implemented, has been positioned as a major factor in why China is considered the worst in its class (Schia & Gjesvik, 2018b).

Fang Binxing, known as the creator of China's Great Firewall, expressed that view in his remarks at the China-Russia forum on Internet sovereignty in 2016. He claimed that the fact that much of the Internet's infrastructure is located in America means that today's Internet governance is under the control of the United States. . The point is therefore not to add the concept of government control to today's Internet, but to force America to share control that already exists. By framing the issues within this issue, China seeks to build a narrative in which state power already exists in cyberspace, but America is the hegemon. Establishing national sovereignty would therefore not be a matter of Internet censorship, but the inclusion of more actors than the US in its administration. This argument is in line with the broader trend in Chinese foreign policy that calls for a "democratization of international relations". This notion is a move away from perceived Western domination of international affairs towards a more inclusive order with greater respect for autonomy and the internal affairs of states (Schia & Gjesvik, 2018a).

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 external access that automatically stimulates the domestic industry to develop as people enjoy Baidu compared to Google, Weibo compared to Facebook, and WeChat compared to WhatsApp, so the experience of citizens is no different from outside China, only they have very sophisticated filters that can block the private chat application WeChat (Calamur, 2018).

For Indonesia to be able to maintain its cyber sovereignty, it is carried out with the concept of gotong royong. As the meaning of gotong royong means working together (help, helping each other), Cyber Sovereignty Gotong Royong means working together (helping, 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 in the informatics community in Indonesia, including elements from Internet Companies (ISPs), Internet User Communities, Internet Cafes, E-commerce Companies, Telecommunications Companies, even to the scope of the smallest community is the family.

In this mutual cooperation cyber sovereignty system, the government as the regulator and executor in blocking internet content, the community plays an active role in two forms, namely; the first is independent blocking (performed by the people

themselves), the second is by reporting to the government on sites/content that violate the laws and norms that apply in Indonesia (Ro'is, 2022).

The model for implementing the "gotong royong" cyber sovereignty system is in line with the Indonesian defense system, namely a defense system that is universal in nature which involves all citizens, territories and other national resources, and is prepared early by the government and implemented in a total, integrated, directed, and continue to uphold state sovereignty, territorial integrity, and the safety of the entire nation from all threats. Against any threats to sovereignty from cyberspace, this universal defense system will be very effective where the government does not play an active role alone but is supported by all citizens and resources in Indonesia.

In Law Number 3 of 2002 concerning National Defense, it is stated regarding the objectives of national defense that the National Defense aims to maintain and protect state sovereignty, the territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of the entire nation from all forms of threats. In the Elucidation it is stated that what is meant by threats is any business and activity, both domestic and foreign, 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 in order to ensure the safety of the entire nation from all forms of threats, including one threat from the cyber world.

The government's role in terms of regulations includes blocking existing sites with technological efforts, namely with the AIS engine that it already has, it becomes a kind of "Great Firewall of China" which differs from the Indonesian version in that in China internet blocking only relies on "machines" and "internet police". ", in Indonesia it 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 networks and internet provider company (ISP) networks.

Blocking by the Government of Indonesia (Ministry of Communication and Information) is carried out with an AIS engine which is used by the AIS Team with two mechanisms. The first way the team will patrol regularly 24 hours a day to monitor and look for negative content on the internet. The second way of taking action is based on community participation in the form of reports coming from the community through various channels such as dukuponten.id. this method is an effort in upholding our cyber sovereignty with the spirit of "gotong royong."

One example of success in 2020 carried out by Kominfo is blocking more than 1 million sites that contain pornography, and blocking 166,853 sites related to gambling

and 8,689 fraud 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 blocking more than 600 thousand content from social media. Blocking efforts have continued in the most recent 2021, including the issue of fake news (hoaxes) about Covid-19 which are widely circulating on social media, until 08 August 2021 there were 1,897 findings of hoaxes spread across various social media. The spread of hoaxs is most commonly found on Facebook. There are 1,729 hoaxes about the Covid-19 vaccine. Video sharing sites, such as YouTube and TikTok, are also not spared from being targeted by hoaxes. It was noted that there were 41 hoaxes on YouTube and 17 on TikTok. Then the remaining 11 hoaxes were found by the Ministry of Communication and Information on Instagram (Kominfo, 2021).

Cyber sovereignty in Indonesia can be enforced by blocking policies on content in the cyber world that are against the law, and can be law enforcement in a "non-penalty" way where "penal" efforts cannot even be carried out because they collide with jurisdictional issues (Ro'is, 2020).

CONCLUSION

Cyber sovereignty is important for an independent country like Indonesia, but the realization of Indonesia's cyber sovereignty is hampered by several factors, including the US domination of the world's internet infrastructure, the absence of an obligation for data centers to be placed within Indonesia's territory and the lack of international cooperation related to cyber jurisdiction makes law enforcement weak in cyberspace.

China can be an example of enforcing cyber sovereignty using a policy known as the "Great Firewall of China" so that the country can control all internet activity within its sovereign territory. The policy model "Great Firewall of China" cannot be applied in Indonesia because it relates to the right to freedom of speech protected by the 1945 Constitution, but blocking can still be carried out within the limits set by existing laws. In contrast to the "Great Firewall of China" policy in China internet blocking only relies on "machines" and "internet police", in Indonesia the AIS engine carries it out, 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 provider company network (ISP). This model of implementing mutual cooperation sovereignty is in accordance with the universal defense system mandated by Law Number 3 of 2002 concerning National Defense.

REFERENCES

Amiruddin, & Asikin, Z. (2006). *Pengantar Metode Penelitian Hukum*. Rajawali Press.

Arief, B. N. (2010). *Kebijakan Legislatif Dalam Penanggulangan Kejahatan dengan Pidana Penjaratle*. Genta Publishing.

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

DPR RI. (2020). *Naskah Akademik Rancangan Undang-Undang Keamanan dan Ketahanan Siber*. DPR RI. http://www.dpr.go.id/dokakd/dokumen/RJ1-20190617-025848-5506.pdf

Fang, B. (2018). *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace*. Science Press.

Fuady, M. (2013). *Teori-Teori Besar Dalam Hukum*. Kencana.

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

Hartono, S. (1988). *Kapita Selekta Perbandingan Hukum*. Citra Aditya Bakti.

Kolton, M. (2017). Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. *The Cyber Defense Review*, *2*(1).

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

Lessig, L. (2006). *The Code Version 2.0*. Basic Book.

Mochtar Kusumaatmadja. (2002). *Konsep-Konsep Hukum Dalam Pembangunan* (O. S. S. & E. Damian, Ed.). Alumni.

Rahman, A. (n.d.). *Indonesia Belum Memiliki Kedaulatan Siber*. https://cyberthreat.id/read/196/Indonesia-Belum-Memiliki-Kedaulatan-Siber

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

Ro'is, N. (2020). *Kebijakan Kriminal Menghadapi Gelombang Baru Terorisme (Cyberterrorism) untuk Mempertahankan Kedaulatan dan Yurisdiksi Negara kesatuan Republik Indonesia (NKRI)*. Universitas Padjadjaran.

Ro'is, N. (2022). Cyber Sovereignty Gotong Royong, Indonesia'a Way of Dealing with the Challenges of Global Cyber Sovereignty. *Pancasila and Law Review*, *3*(1), 15–30. https://doi.org/10.25041/plr.v3i1.2573

Schia, N. N., & Gjesvik, L. (n.d.). *The Chinese Cyber Sovereignty Concept (Part 2)*. Asia Dialogue, 2018. Retrieved May 10, 2021, from https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-2/

Schia, N. N., & Gjesvik, L. (2018a). *The Chinese Cyber Sovereignty Concept (Part 1)*. Asia Dialogue. https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/

Schia, N. N., & Gjesvik, L. (2018b). *The Chinese Cyber Sovereignty Concept (Part 1)*. The Asia Dialogue. https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/

Soerjono, S. (1981). *Pengantar Penelitian Hukum*. UI-Press.

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