JuSS: **Jurnal Sosial Soedirman**
Vol.6, No. 1, 2023

Comparative Analysis of Cyber Sovereignty: Case from Indonesia and Iran

Lidia Tri Chris Nia Wati, Mahmud Syaltout Syahidullhaq Qudratullah, Bimantoro Kushari Parmono
Universitas Paramadina

Abstrak:
Penilitian ini bertujuan untuk mengetahui perbedaan cyber sovereignty antara Iran dan Indonesia, dimana dunia maya saat ini menjadi faktor penting dalam menentukan kedaulatan suatu negara. Untuk mengetahui perbedaan kedaulatan keda negara, peneliti menggunakan pendekatan Euro-Cyber Sovereignty, dengan teori yang digunakan adalah Theory of Three Perspectives. Untuk menghitung nilai cyber sovereignty, peneliti menggunakan pendekatan Analytical Hierarchy Process (AHP). Sumber data yang digunakan untuk mengetahui sejauh mana cyber sovereignty suatu negara melalui cyber application, infrastruktur siber, dan data inti siber. Dalam penelitian ini terlihat bahwa Indonesia memiliki cyber sovereignty sebesar 46,7%, sedangkan Iran sebesar 46,38%. Kedua negara meningkatkan cyber sovereignty mereka dengan cara yang berbeda : Iran cenderung meningkatkan cyber sovereignty dengan mempelajari serangan siber yang diterima dari saingannya, sedangkan Indonensia meningkatkan cyber sovereignty dengan melakukan kerja sama bilateral dan multilateral dengan kekuatan besar. Dapat dilihat bahwa Indonesia memiliki cyber sovereignty lebih tinggi dibandingkan Iran.

Kata-Kata Kunci: **Cyberspace, Cyber Sovereignty, Iran, Indonesia.**

Abstract:
This study aims to determine the differences in cyber sovereignty between Iran and Indonesia, where cyberspace is currently an important factor in determining the sovereignty of a country. To find out the differences in the sovereignty of the two countries, researchers use the Euro-Cyber Sovereignty Approach, with the theory used being the Theory of Three Perspectives. To calculate the value of cyber sovereignty, researchers use the Analytical Hierarchy Process (AHP) approach. The data sources used to determine the extent of a country's cyber sovereignty are cyber applications, cyber infrastructure, and cyber core data. In this study, it can be seen that Indonesia has 46.7% cyber sovereignty, while Iran has 46.38%. The two countries enhance cyber sovereignty in different ways: Iran tends to enhance its cyber sovereignty by studying cyberattacks received from rivals, while Indonesia improves cyber sovereignty by conducting bilateral and multilateral cooperation with major powers. It is known that Indonesia has higher cyber sovereignty than Iran.

Keywords: **Cyberspace, Cyber sovereignty, Iran, Indonesia**

Korespodensi:
Lidia Tri Chris Nia Wati (lidia.chris@students.paramdina.ac.id)

Introduction

The cyber world is a place where human activities in the real world are carried out virtually. Humans can interact, discuss, and exchange ideas without meeting face to face. Human interaction in cyberspace is represented by data or information that represents that human. Such as email, mobile number, or other unique code. Because the information is the most important thing in the cyber world. Public disclosure of information will bring a threat to society (Dysson, 1994).

Internet, various telecommunication networks, communication systems, transmission systems, radio and television networks, various computer systems, and ICT are all components of the man-made electromagnetic space known as cyberspace. Infrastructures used as the carrier by people to produce, store, update, send, use, and display data as well as perform other tasks with data to carry out particular communication technology activities include embedded processors and controllers in major industrial facilities (Fang, 2018)

Cyber threats take many forms, and if they develop into an attack, they can harm the systems they target. System security measures are necessary to reduce the harm that may arise as a result of an attack. Cybercrime evolves as technology evolves, so attackers, hit targets that are even more impenetrable, and evade the detection for which they are designed. However, the most frequent attacks still come from conventional cyberthreats. Many types of attacks have been identified and researched, among which; A man-in-the-middle attack happens when the attacker gets in the way of communication between two sources, meaning that every message sent from source A to source B first reaches the attacker. Unauthorized access to sensitive information or the potential for the attacker to change the information or message that reaches the target are additional hazards associated with this type of assault; A brute force attack involves making numerous tries to access secured information (such as passwords, encryption, etc.) until the right key is discovered, at which point the information can be accessed; DDoS (Distributed Denial of Service) is a sort of assault that jeopardizes data availability by bombarding the victim (such as a server) with commands, rendering it unusable; The term "malware" refers to various forms of harmful software that an attacker uses to jeopardize the confidentiality, accessibility, and integrity of data; The most prevalent forms of

Korespodensi:
Lidia Tri Chris Nia Wati (lidia.chris@students.paramdina.ac.id)

malware are viruses, worms, trojans, spyware, ransomware, adware, and scareware/rogware; Phishing is a method for stealing users' private information by pretending to be a reliable source (like a website). Social engineering is the umbrella term for methods for obtaining unauthorized access to information through human interaction (Bendovschi, 2015).

Securing information technology resources in order to stop cyber crime is known as cyber security. Information security includes cyber security, which guards against potential cyber attacks on systems connected to the internet, including hardware, software, programs, and data. safeguards against unauthorized electronic access to network integrity. The integrity of the network and any data sent over network devices are protected by network security, a type of cyber security. Technologies, procedures, and procedures used in cyber security are those that guard against attacks, data corruption, and unauthorized access on networks, devices, programs, and data (Arifin, 2021).

Cybercrimes and cyberterrorism, which are raging today, are the most visible symptoms of the increasingly widespread cybersecurity problem. Cybersecurity has emerged as a global challenge and has become a level one security threat for sovereign countries. Fierce debates are raging in international forums about cyberspace rules and systemic and revolutionary challenges to global governance in cyberspace. Cyber sovereignty is bound to be the focus of major controversy in every country (Yeli, 2017). Sovereignty is the keyword in the current era of information technology freedom, especially Cyber Sovereignty. 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, including social media, electronic mail (email), internet storage (clouds), technology grants, servers, and others (Ro'is, 2022) .

In cyberspace, we will also get to know about cyber attacks, cyber security, and cyber sovereignty. Cyber attacks are attacks launched by cyber criminals using one or more computers against one or more computers or networks. Cyber attacks can maliciously disable computers, steal data, or use the compromised computer as a launching point for other attacks. Cyber criminals use a variety of methods to launch cyber attacks, including malware, phishing, ransomware, and denial of service, among others. Cyber security is security carried out in cyberspace because of the fact that there are crime rates in cyberspace, a collection

of tools, policies, security concepts, security protection, guidelines, risk management approaches, measures, training, best practices, guarantees, and technologies that can be used to protect the cyber environment. Cyber sovereignty is a phrase commonly used in the field of internet governance to define the desire of states to exercise and maintain control over the Internet domain within their own borders, including political, economic, cultural, and technological activities.

Due to the threat of the spread of secret information outside the country's territorial boundaries, a country continues to look for ways to keep the cyber world safe. When confidential information is threatened with spreading, the sovereignty of a country can also be threatened. Regarding cyber sovereignty in Indonesia, data sovereignty and security in cyberspace are an important part of the sovereignty of the Indonesian nation which cannot be compromised. What's more, cyber security threats and demands for technological advances continue to overshadow in the current era of digitalization. Even though Indonesia is ranked 24th out of 194 in the Global Cybersecurity Index, Indonesia still faces serious problems in maintaining the security of data protection for activities in the cyber world (Prakoso, 2022).

Indonesia's cyber sovereignty needs a lot of improvement, even though Indonesia has various policies regarding the cyber world that are contained in the Law of the Republic of Indonesia No. 11 of 2008 in Chapter VI, which regulates "domain names, intellectual property rights, and protection of personal rights," and in Chapter VII, "prohibited acts," and has a state body that regulates and secures Indonesia's cyberspace. Indonesia, with its various technological advances, of course, has received various attacks from various parties. Like when the private data of Indonesian secret residents could be accessed and distributed by the well-known hacker Bjorka. This proves that Indonesia is still very vulnerable to attacks in cyberspace, so Indonesia must improve cyber security.

In other cases, Iran's cyber sovereignty is weaker than Indonesia's. Even the Iranian government has not been able to control its population through the use of cyberspace. Iran is known to be a country that frequently attacks the cyberspace of major countries such as America, Israel, and Saudi Arabia which are often called cyber offensive wars. These attacks are carried out by Iranian

citizens, who are often unknown to the Iranian government. Therefore, the Iranian government must strengthen Iran's cyber sovereignty.

The increase in Iran's cyber sovereignty cannot be separated from the influence of the many cyber-attacks that Iran has received. It is recorded that the cyber-attacks that Iran received came from various countries that are competitors or countries that are suspected of being hostile to Iran. The attack that never happened and is considered the most sophisticated attack in history where America and Israel in 2007 to secretly sabotage Iran's nuclear infrastructure. Not only was the attack external, but an Iranian hacker also attacked Dutch security firm DigiNotar for fraudulently issuing encryption certificates that allowed Iran to spy on all domestic Gmail users, one of the biggest security breaches in Internet history. The number of cyber-attacks has made Iranians protect their personal data. Iranians protect their personal data by studying every attack they receive. So that Iran's cyber sovereignty is getting stronger, with the motivation of its residents to secure their personal data. This case shows that cyber sovereignty is very close to personal data protection.

Data sovereignty in cyberspace is the physical extension of national sovereignty, including independence and equality, to the absolute right to use infrastructure, entities, actions, and related data and information within the territory of a country. It is also extended to the principle of sovereign equality enshrined in the UN Charter. This principle states that sovereign states have the right to participate equally in global governance in cyberspace and jointly formulate international rules (Octavian, 2021).

However, data is only one aspect of cyberspace. There are still other aspects that affect cyber sovereignty, including data security. In cyber governance, there are several aspects that must be met to ensure cyber sovereignty. In the Three Perspective Theory of Cyber Sovereignty, cyber sovereignty is influenced by various elements. These three elements are the cyber core, cyber application, and cyber-infrastructure (Yeli, 2017). Moreover, these three elements are key components that must be protected by the government in order to presences cyber sovereignty.

The explanation above relates to what aspects must be protected to present cyber sovereignty. However, to regulate cyber sovereignty, it is not enough to determine the aspects that must be protected. An agency protection concept is

needed that determines which elements of government must have cyber sovereignty. Based on The Council of The European Union, security improvements concentrate on the energy, transportation, information, and communication technology sectors. The energy sector is divided into three sections, namely Electricity, Oil, and Gas. In the transportation sector, there are five sections, namely land transportation, rail, air transportation, sea transportation, and shipping and ports (UNION, 2018).

Considering that cyber sovereignty is very important for public security in the information age, this research aims to make a comparison of cyber sovereignty between Indonesia and Iran. By comparing the two countries, this study seeks to see what are the differences in the strengthening of the Cyber world between Indonesia and Iran. Also, to find out which sectors are the focus of Indonesia and Iran in strengthening cyberspace.

Building the capabilities of Indonesian citizens regarding data security is urgently needed. In this case, the state has the responsibility to establish a cyber security system to provide safe and democratic data protection for Indonesian citizens. a people-centered approach by prioritizingThe context of data as labor is a solution to accelerate the development of cybersecurity and data sovereignty in Indonesia (M. Prakoso Aji, 2022).

Cyber sovereignty is very important for an independent country like Indonesia. Indonesia's limitations in maintaining cyber sovereignty can be anticipated by using the concept of Gotong Royong cyber sovereignty. sovereignty involves all citizens, territories and other national resources. The concept of Gotong Royong cyber sovereignty is a concept learned from China's experience regarding its cyber sovereignty. (Nur Ro'is, 2022)With its cyber-offensive operations, Iran has become a country that has many enemies in cyberspace, such as Israel, America, Germany, Saudi Arabia, and the Arab region.The cause of this offensive cyber operation is also due to cyber attacks that are often obtained by Iran. With the many cyber attacks targeted at Iran, it has made Iran learn and develop its cyber defense (Collin anderson and Karinm Sadjadpour, 2018).

In previous research, regarding cyber sovereignty in the two countries and how they maintain and enhance it. Discussion where cyber sovereignty can affect national defense, especially with state secret data. With the number of reports of

cyber attacks received and the amount of damage caused by each attack, the researchers analyzed how vulnerable the two countries' cyber defenses were.
In that research, it was stated that Indonesia has low ability in data security. Therefore, it is hoped that Indonesian citizens can work together with the government to secure personal data in cyberspace. Iran, which is indeed the target of cyber attacks from major powers, cannot continue to survive with the capabilities of its citizens and government. The Iranian government is trying to get its citizens to increase their ability to defend and attack enemy countries in cyberspace.

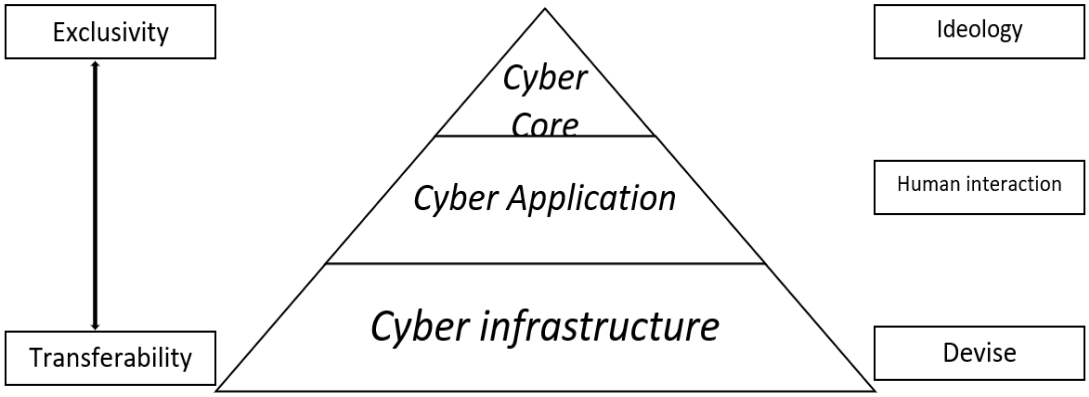
Regarding cyber sovereignty, not many people are aware of how important it is for the country. But in the modern world, where almost all areas of life currently use various technologies that facilitate human work, we cannot ignore cyber sovereignty. Technology is always associated with information that can be known and utilized by everyone. But not everyone has the awareness and responsibility to protect information and use it properly. There are many leaks of misused information that make a country have to increase its cyber sovereignty.
In the era of cyber security information is important. Indonesia and Iran are two countries with low cyber security, as stated by Collin Anderson and Karim Sadjadpour in Iran's Cyber Threat, that Iran only develops its own cyber power and lacks the readiness to face its enemies in cyberspace. Whereas Indonesia is very fond of cyber sovereignty, Indonesia does not yet have the capability to protect confidential data. Both countries take different approaches to increasing cyber security. This study aims to compare the two countries' cyber sovereignty so that the strongest and weakest aspects of each country's critical infrastructure can be identified. With the difference in strength in each critical infrastructure in the two research countries, we can measure how much cyber sovereignty each country possesses (Aji, 2022).

In this research, we discussed how the two countries increased their cyber sovereignty, in order to maintain domestic information. Based on data from the two countries' critical infrastructure obtained through Open-Source Intelligence (OSINT). The data used is mathematical data that has a definite size, so it is different from previous research that has not yet given a measure of the research. With the Analytical Hierarchy Process (AHP) method used in this study, it can find out how much it is to assess the country's cyber sovereignty.

Cyber Sovereignty Concept

This study uses the concept of the Three-Perspective Theory, to compare cyber sovereignty between Iran and Indonesia. Hao Yi, in 2017, put forward the Three Perspective Theory Concept. In A Three-Perspective Theory, the three levels of cyber sovereignty are core, application, and infrastructure. In addition, this theory also divides into nature of sovereignty into two parts, namely transfer (open) and exclusive (closed) as illustrated in Figure 1.1.

Figure 1.1 *Cyber Sovereignty Concept by Three-Perspective Theory*



Source: prism 7, no. 2 By Hao Yeli

In the three-perspective theory, sovereignty is divided into two, categories: exclusive sovereignty and classical sovereignty, which are the principles of a country such as data storage and state information. The second is open and transferable, such as joint technology development cooperation. As an example of innovation and cooperation in making new technology that is balanced and in accordance with the portion. It can also be understood that ideological sovereignty tends to be more exclusive than shared sovereignty which tends to be more open (transferable) to issues of economic development, national and international political issues, knowledge sharing, etc.

This study uses a quantitative method for measuring a country's cyber sovereignty. The data source comes from data processing using Maltego Paterva software to see the position of the Core, Application, and Infrastructure. For example, if the Core website is an exclusive self-governing domain it will increase the value of the institution's Cyber Core. Conversely, if the domain of

government institutions does not stand alone or participate in the cyber environment of other countries, it will weaken the value of the Cyber Core. Then the value of each aspect is processed in a Microsoft power query.Cyber core concerns state ideology or policies including political ideology and its legal system. Cyber core was Obtained by extracting website data from government agencies of each country. Withdrawing data using SEOquake which is a google extension search tool, by entering cyber keywords in the languages used by that country.

The cyber application concerns human activities in cyberspace including social relations that are integrated into various sectors such as technology, culture, economy, trade, and other aspects of life. Cyber infrastructure concerns the expansion of internet networks, bandwidth, devices, gadgets, wireless, and so on. Cyber infrastructure and cyber applications are obtained by grabbing data using Maltego and using keyword names and domains from selected state institutions. Then the data that has been obtained is entered into the cleansing process, which is done to filter the data based on the name of the institution that corresponds to the country's domain based on the data on the target that has been obtained. Next, the average calculation of the grabbing results is carried out at times 100.

Table 1.1 Cyber sovereignty indicator

Variable	Data Sources	Measurement
Cyber Infrastructure	Data is taken from each official website of critical infrastructure.	See the independence of the sub-website. If an organization has many sub-websites connected to other organizations' servers, then its cyber infrastructure will be rated low.
Cyber Application	Data is taken from each official website of critical infrastructure.	View server independence. If the server used is one that is connected to another organization, then cyber apps will be rated low.

Cyber Core	*Open-source intelligence (OSINT)*	Seeing whether or not there is a cyber policy on the government's official website

Source: *Cyber sovereignty council directive 2008*

Based on the hierarchical level in the Three-Perspective Theory, there is a determination of the value/weight of each element of cyber sovereignty. The determination of weight is based on elements that are considered priorities in the Three-Perspective Theory. After the weight of each level has been known, the next process is calculating the final number of cyber sovereignty of the two countries in each of the selected government agencies.

From the calculation of the three previous components, namely Cyber Infrastructure, cyber application and cyber core, we can calculate the value of Cyber Sovereignty. Where Cyber Sovereignty represents the value of a country's cyber sovereignty. To calculate the value of cyber sovereignty, researchers use the Analytical Hierarchy Process (AHP) approach.

AHP is a decision support model developed by Thomas L. Saaty. This decision support model describes a complex multi-factor or multi-criteria problem in a hierarchy. According to Saaty, a hierarchy is defined as representing a complex problem in a multilevel structure, and objectives, followed by factor levels, criteria, sub-criteria, etc., up to the last alternative level (Saaty, 2012).

AHP sees a hierarchy of degrees of interest or influence of an element (Core, Infrastructure and Application) in cyber sovereignty. Based on the AHP approach, the following formula is obtained as an equation to calculate cyber sovereignty:

Tabel.1 cyber sovereignty calculations

Cyber Sovereignty = (0,42 x Cyber Core) + (Cyber Application x 0,33) + (Cyber Infrastructure x 0.25)

For further analysis, several institutional entities are needed that have a major influence on cyber sovereignty in both countries based on the European Union concept. Some of these institutions are the Ministry of Home Affairs, Ministry of Defense, Ministry of Foreign Affairs, Ministry of Communication and Information, Police, Military, Cyber Authority, State intelligence agency,

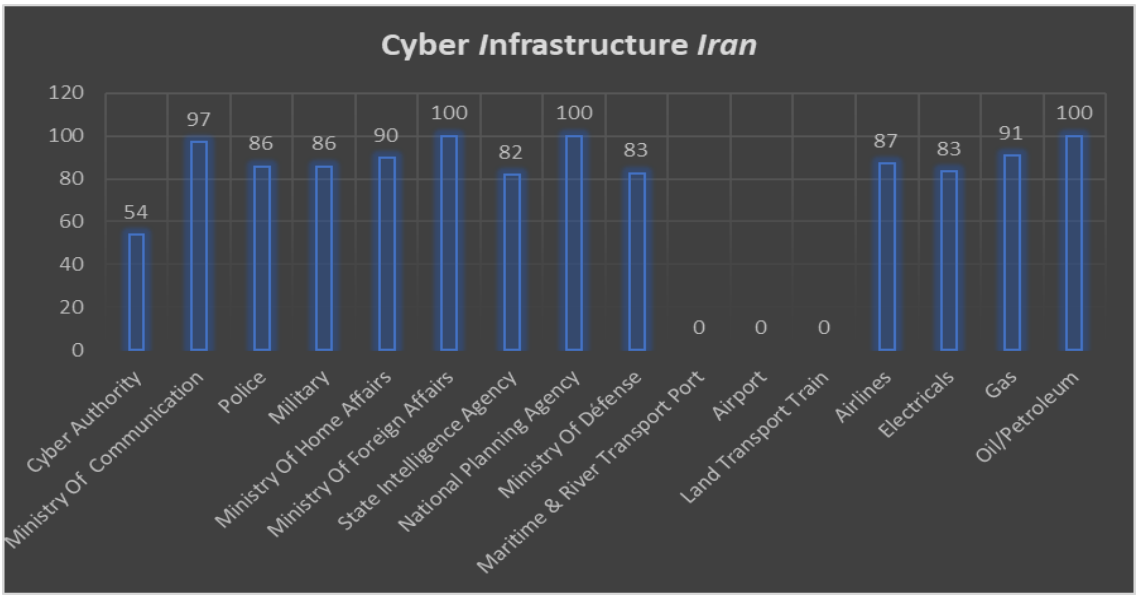
National planning agency, electricity, Gas, Petroleum/oil, Aviation Company, Airport, Maritime and River Transportation, Land transportation.

Iran's Cyber Sovereignty Analysis

The cyber sovereignty of the Iranian state in the context of cyber infrastructure is analyzed based on sixteen main entities giving results as shown in Figure 1.1 below.

Figure 1.1

Cyber Infrastructure Iran



Source: Based on the agency website domain

In the graph above, the vertical line is the value (X) of cyber infrastructure, and the horizontal line is the name of the critical infrastructure being researched (Y). The value of cyber infrastructure is calculated with a range of 0–100 for each critical infrastructure. Critical Iranian infrastructure that is the object of research based on European Union standards, namely the Ministry of Interior, Ministry of Defense, Ministry of Foreign Affairs, Ministry of Communication and Information, Police, Military, Cyber Authority, State Intelligence Agency, National Planning Agency, Electricity, Gas, Petroleum, Aviation Companies, Airports, Sea and River Transportation, and Land Transportation. With these various institutions, researchers have access to every official website of the institution. Ministry of Home Affairs (moi.ir), Ministry of Defense (irangov.ir), Ministry of Foreign Affairs (en.mfa.ir) , Ministry of Communication

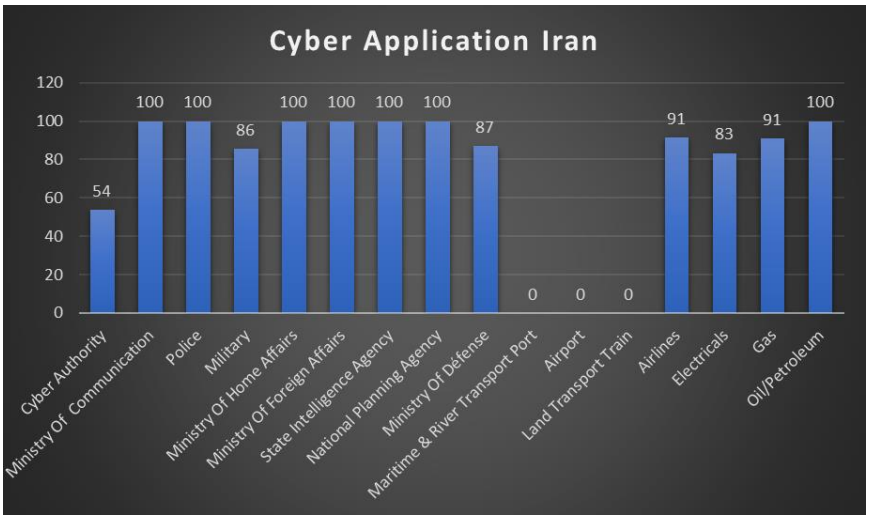
and Information (ict.gov.ir), Police (police.ir), Military (mod.ir), Cyber Authority (cyberpolice.ir/en), State Intelligence Agency (vaja.ir), National Planning Agency (mporg.ir), Electricity (ieicorp.ir), Gas (nigc.ir), Petroleum (icofc. ir), Corporate Aviation (iranair.com), Airport (airport.ir), Sea and River Transportation, Land Transport. Then the researchers used the Maltego application to find out the value of the cyber infrastructure. After the researcher obtained the data from Maltego, the researcher processed the data using Excel, where the cyber infrastructure value was based on the name of each institution's website, averaged, and then multiplied by 100.

The value of Cyber Infrastructure of Iran has three data points worth 100 namely, Ministry of Foreign Affairs, National Planning Agency, and Oil/Petroleum. With these results, the three entities can be declared to have good Cyber Infrastructure values. Three of the Iranian state entities have an entity value of 0, namely Maritime & River Transport Port, Airport and Land Transport Train. With ten entities that score 0-100 namely Cyber Authority, Ministry of Communication, Police, Military, Ministry of Home Affairs, State Intelligence Agency, Ministry of Defense, Airlines, Electricals, and Gas. With this, of all entities from Iran, an average value of 71 is obtained.

The second component in analyzing cyber power in Iran is the application originating from the website obtained in each domain of the selected institutional entities. Following are the results of data processing to find out the value of cyber applications which can be seen in Figure 1.2.

Figure 1.2

Cyber Application Iran



Source: Based on the agency website domain

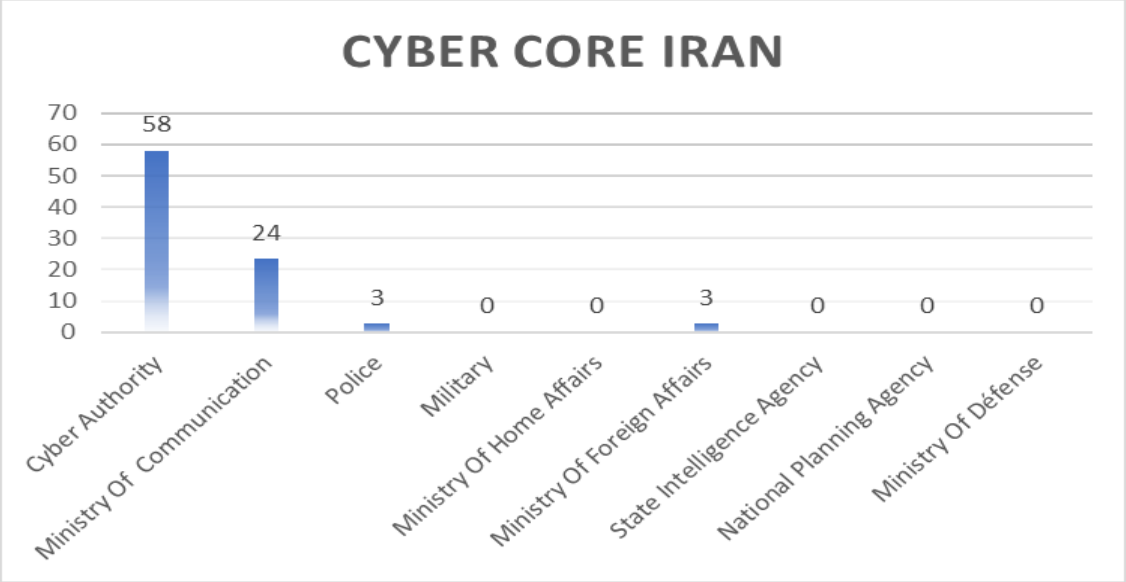
In the graph above, the vertical line is the value (X) of cyber application, and the horizontal line is the name of the critical infrastructure being researched (Y). The value of cyber application is calculated with a range of 0-100 for each critical infrastructure. Critical Iranian infrastructure that is the object of research based on European Union standards, namely the Ministry of Interior, Ministry of Defence, Ministry of Foreign Affairs, Ministry of Communication and Information, Police, Military, Cyber Authority, State Intelligence Agency, National Planning Agency, Electricity, Gas, Petroleum, Aviation Companies, Airports, Sea and River Transportation, Land Transportation. With these various institutions, researchers have access to every official website of the institution. Ministry of Home Affairs (moi.ir), Ministry of Defense (irangov.ir), Ministry of Foreign Affairs (en.mfa.ir), Ministry of Communication and Information (ict.gov.ir), Police (police.ir), Military (mod.ir), Cyber Authority cyberpolice.ir/en), State Intelligence Agency (vaja.ir), National Planning Agency (mporg.ir), Electricity (ieicorp.ir), Gas (nigc.ir), Petroleum (icofc. ir), Corporate Aviation (iranair.com), Airport (airport.ir), Sea and River Transportation, Land Transport. Then the researchers used the Maltego to find out the value of the cyber application. After the researcher obtained the data from Maltego, the researcher processed the data using Excel, where the cyber application value based on the domain of each institution's website was averaged, then multiplied by 100.

From the sixteen cyber application entities, there are seven Iranian government entities with the highest scores covering 100 each, namely the Ministry of Communication, Police, Ministry of Home Affairs, Ministry of Foreign Affairs, State Intelligence Agency, National Planning Agency, and Oil/Petroleum. In addition, there are three entities that have a value of 0, namely Maritime & River Transport Port, Airport, and Land Transport Train. Entities with an index value of 0-100 are Cyber Authority, Military, Ministry of Defense, Airlines, Electricals, and Gas. With an average score of for the country's cyber application 75.

Next is the analysis that is Iran's cyber core. In measuring the cyber core index, only government agencies that can issue policies are analyzed, namely Cyber Authority, Ministry of Communication, Police, Military, Ministry of Home Affairs, Ministry of Foreign Affairs, State Intelligence Agency, National Planning

Agency, and Ministry of Defense. The results of Iran's cyber core analysis can be seen in Figure 1.3.

Figure1.3 Cyber Core Iran



Source: Based on the agency website domain

From the graph above, it can be concluded from the nine components of the Iranian government entities. The most significant score is found in the Cyber Authority government institution with a value of 58. Then followed by the Ministry of Communication which has an index value of 24, then the Police and the Ministry of Foreign Affairs. Meanwhile, the five entities in the Iranian government do not have a cyber core value. Based on these data, the average value of Iran's cyber core is 10. It can be concluded that Iran's institutional entities are not optimal and responsive to cyber policies in their country.

Based on the calculation of the three previous components, namely Cyber Infrastructure, cyber application, and cyber core, the final calculation of the value of Cyber Sovereignty can be carried out. Where Cyber Sovereignty represents the value of Iran's cyber sovereignty.

Iran's Cyber Sovereignty = (0,42x10) + (0,33x71) + (0,25x75)

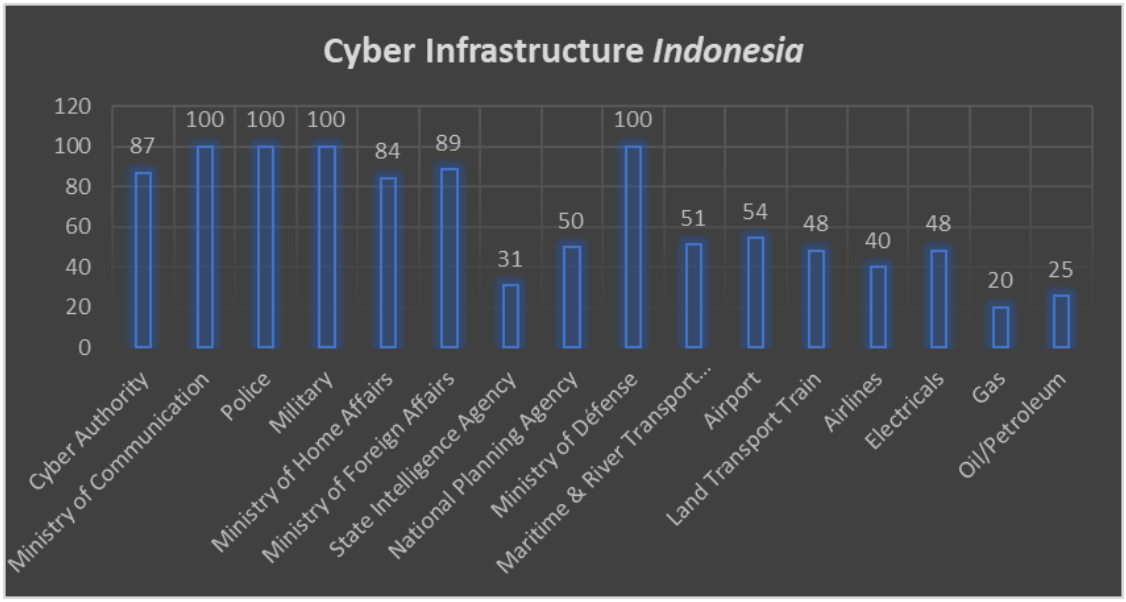
Based on data processing, the average value of the Cyber Core is 10, the cyber application is 71, and the cyberinfrastructure is 75. So, the cumulative index of Iran's cyber sovereignty is 46.38.

Indonesia Cyber Sovereignty

In Indonesia's cyber infrastructure, there are sixteen main entities to be analyzed. The calculation of Cyber Infrastructure Indonesia can be seen in Figure 2.1 below.

Figure 2.1

Cyber Infrastructure Indonesia



Source: Based on the agency website domain

In the graph above, the vertical line is the value (X) of cyber infrastructure, and the horizontal line is the name of the critical infrastructure being researched (Y). The value of cyber infrastructure is calculated on a scale of 0-100 for each critical infrastructure. Critical Indonesian infrastructure that is the object of research based on European Union standards, namely the Ministry of Interior, Ministry of Defense, Ministry of Foreign Affairs, Ministry of Communication and Information, Police, Military, Cyber Authority, State Intelligence Agency, National Planning Agency, Electricity, Gas, Petroleum, Aviation Companies, Airports, Sea and River Transportation, and Land Transportation. With these various institutions, researchers have access to every official website of the institution. Ministry of Home Affairs (kemendagri.go.id), Ministry of Defense (kemhan.go.id), Ministry of Foreign Affairs (kemlu.go.id), Ministry of Communication and Information (kominfo.go.id), Police (polri.go. id), Military (tni.mil.id), Cyber Authority (bssn.go.id), State Intelligence Agency (bin.go.id), National Planning Agency (bappenas.go.id), Electricity (pln.co. id), Gas

(pgn.co.id), Petroleum (pertamina.com), Corporate Aviation (garuda-indonesia.com), Airports (ap1.co.id and jasapura2.co.id), Sea and River Transport (jict.co.id and pelindo.co.id), Land Transportation (kai.id). Then the researchers used the Maltego application to find out the value of the cyber infrastructure. After the researcher obtained the data from Maltego, the researcher processed the data using Excel, where the cyber infrastructure value based on the name of each institution's website, averaged, and then multiplied by 100.

The value of Cyber Infrastructure in Indonesia does not have a data point that is worth 100, so the institution that has the highest score is the Military at 90. With these results, an entity can be declared to have a good entity. Three entities from Indonesia have an entity value of 0 namely Cyber Authority, State Intelligence Agency, and Electricals. Ten entities with a score of 0-90 namely the Ministry of Communication, Police, Military, Ministry of Home Affairs, Ministry of Foreign Affairs, National Planning Agency, Ministry of Defense, Maritime & River Transport Port, Airport, Land Transport Train, Gas, and Oil/Petroleum. With this from all entities from Indonesia, an average value of 66 is obtained.

The second component in analyzing cyber power in Indonesia is the Application which is calculated from websites obtained in each domain of Indonesian cyber institutional entities. The following are the results of data processing to find out the value of the cyber application as shown in Figure 2.2.

Figure 2.2

Cyber Application Indonesia

Source: Based on the agency website domain

In the graph above, the vertical line is the value (X) of the cyber application, and the horizontal line is the name of the critical infrastructure being researched (Y). The value on the cyber application is calculated with a range of 0-100 in each critical infrastructure. Critical Indonesian infrastructure, which is the object of research based on European Union standards, namely the Ministry of Home Affairs, Ministry of Defense, Ministry of Foreign Affairs, Ministry of Communication and Information Technology, Police, Military, Cyber Authority, State Intelligence Agency, National Planning Agency, Electricity, Gas, Petroleum, Aviation Companies, Airports, Sea and River Transportation, and Land Transportation. With these various institutions, researchers have access to every official website of the institution. Ministry of Home Affairs (kemendagri.go.id), Ministry of Defense (kemhan.go.id), Ministry of Foreign Affairs (kemlu.go.id), Ministry of Communication and Information (kominfo.go.id), Police (polri.go. id), Military (tni.mil.id), Cyber Authority (bssn.go.id), State Intelligence Agency (bin.go.id), National Planning Agency (bappenas.go.id), Electricity (pln.co. id), Gas (pgn.co.id), Petroleum (pertamina.com), Corporate Aviation (garuda-indonesia.com), Airports (ap1.co.id and jasapura2.co.id), Sea and River Transport (jict.co.id and pelindo.co.id), Land Transportation (kai.id). Then the researchers used the Maltego application to find out the value of the cyber infrastructure. After the researcher obtained the data from Maltego, the researcher processed the data using Excel, where the cyber value of the application based on the domain of the website of each institution was averaged and multiplied by 100.

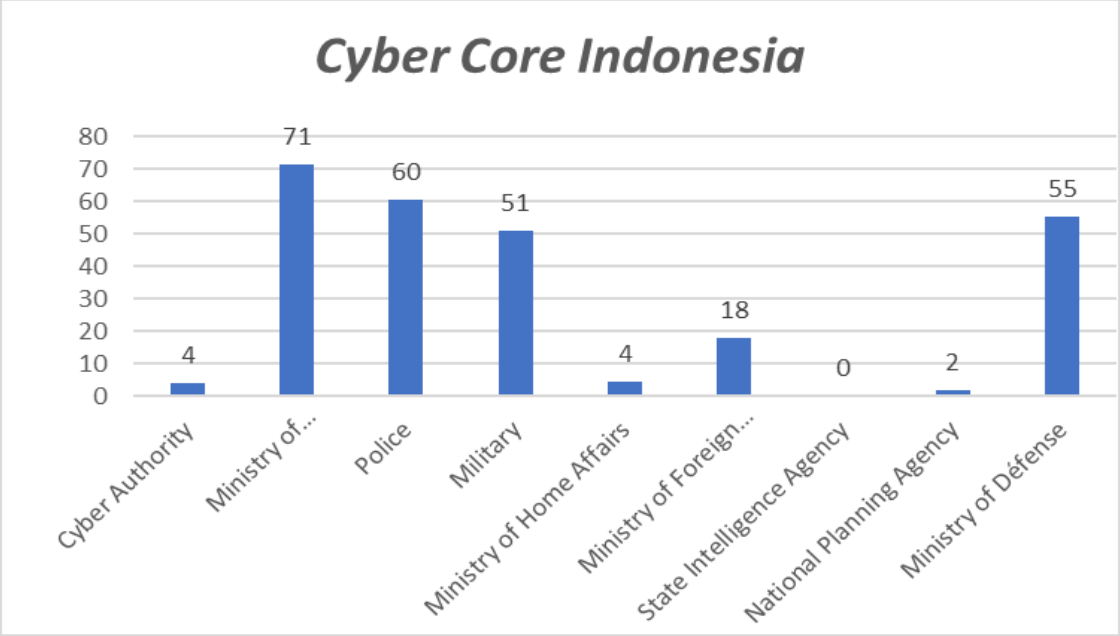
From the cyber application entities, there are six Indonesian entities that have the highest scores covering 100 each, namely the Ministry of Communication, Police, Ministry of Home Affairs, Ministry of Foreign Affairs, National Planning Agency, and Land Transport Train. And there are three entities with a value of 0 namely Cyber Authority, State Intelligence Agency, and Electricals, with an index value of 0-100 namely Military, Ministry of Defense, Maritime & River Transport Port, Airport, Airlines, Gas, and Oil/Petroleum, and electricals. With an average score of for the country's cyber application 74.

Next is the calculation of the cyber core. In measuring the cyber core index, only government agencies that can issue policies are analyzed, namely the Cyber Authority, the Ministry of Communication, the Police, the Military, the Ministry

of Home Affairs, the Ministry of Foreign Affairs, the State Intelligence Agency, the National Planning Agency, and the Ministry of Defense. The results of Indonesia's cyber core analysis can be seen in Figure 2.3.

Figure 2.3

Cyber Core Indonesia



Source: Based on the agency website domain

From the graph above, it can be concluded that the most significant figure is in the Police government agency, with a value of 18. This is followed by the Cyber Authority, which has an index value of 11. Then there are three institutions with the same score of 10, namely the Ministry of Communication, the Ministry of Home Affairs, and the Ministry of Foreign Affairs. While none of the four Indonesian government entities have a cyber core value, based on these data, the average value of Indonesia's cyber core is 7. It can be concluded that Indonesian institutional entities are not yet optimally responsive to cyber policies in their country.

From the calculation of the three previous components, namely Cyber Infrastructure, cyber application and cyber core, the final score for Cyber Sovereignty Indonesia is obtained. Where Cyber Sovereignty represents the quality of Indonesian cyber sovereignty. Indonesia's Cyber Sovereignty = (0,42x10) + (0,33x75) + (0,25x71). The average value of Cyber Core is 10, the cyber

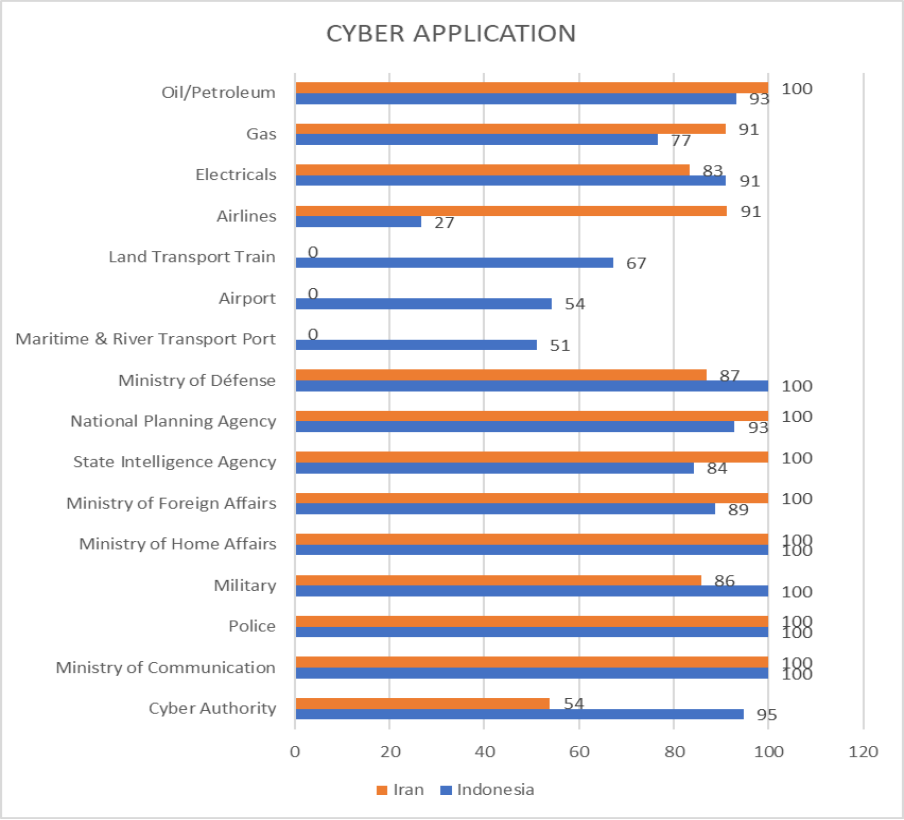
application is 75, and the cyberinfrastructure is 71. So, the value of Indonesia's cumulative cyber sovereignty index is 46.7.

Cyber Sovereignty Comparison

The following is a comparison of cyber applications between Indonesia and Iran.

Figure 3.1

Cyber Application comparison



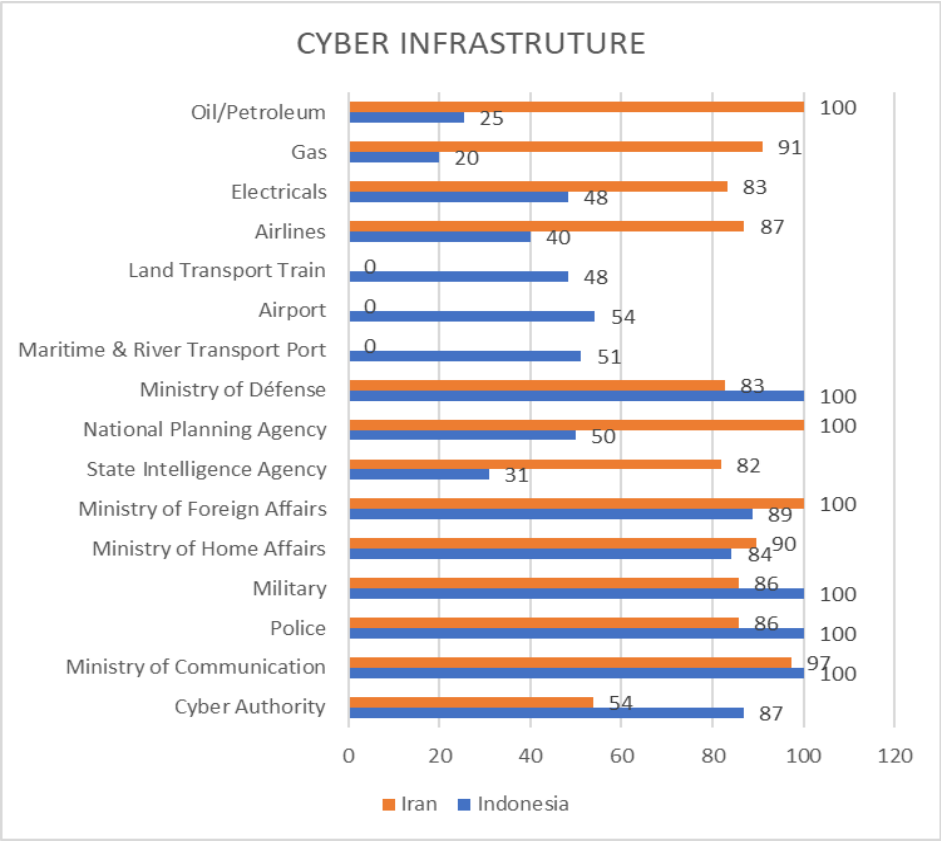
Source: *Based on the agency website domain*

Comparison of Indonesia's cyber applications with Iran, from the Cyber Authority to the Indonesian oil/petroleum sector is superior to that of Iran. However, Iran has cyber applications in six agencies and sectors that are superior to Indonesia.

Meanwhile, we can see Cyber Infrastructure Indonesia and Iran in Figure 3.2.

Figure 3.2

Cyber Infrastructure Comparison

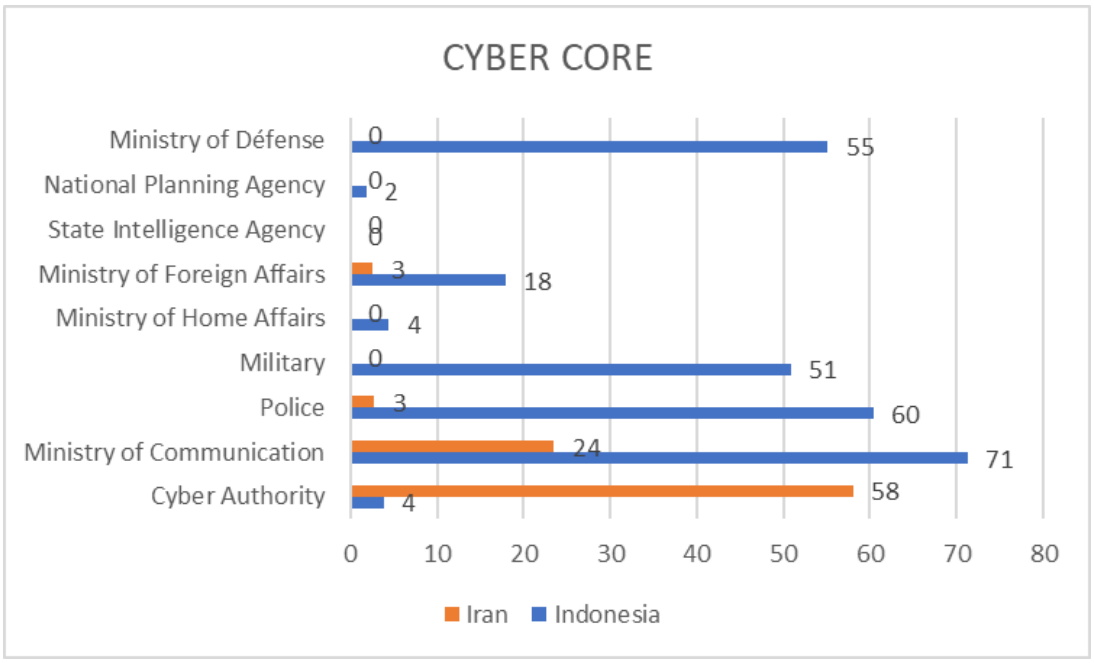


Source: Based on the agency website domain

Comparison of Indonesia's cyber infrastructure with Iran, from the Cyber Authority to the oil/petroleum sector, Indonesia is superior than Iran. Iran has cyber infrastructure aimed at institutions and sectors that are superior to Indonesia. Next is the Cyber core which represents policies regarding cyberspace issued from every government agency. The following is a comparison of Indonesian and Iranian cyber cores in Figure 3.3.

Figure 3.3

Cyber Core Comparison



Source: processed by researchers

It can be seen that many policies regarding cyberspace are issued by Indonesian government agencies. Indonesia and Iran have the same values in the policies of their State Intelligence Agency, in this agency, both countries do not have cyberspace policies. Iran's policies have the highest score for Cyber Authority agencies, namely 58 while Indonesia only has 4. But seven out of nine Indonesian agencies issue more policies in cyberspace. From various comparisons, it can be concluded that Indonesia has better cyber sovereignty compared to Iran. Where Indonesia has cyber sovereignty of 46.7% while Iran has 46.38%. So, it can be concluded that Indonesia has better cyber sovereignty than Iran.

Cyber Activities Pattern : Indonesia and Iran

In recent years, the Internet and cyberspace have had an impact on relations between countries. Big countries, trying to outperform other countries in technology, which has positive implications for the progress of the Internet, but at the same time the Internet has created a new atmosphere of competition, even hostility. Based on council directive 2008/114/EC regarding the identification and support of critical European infrastructure, the European Union Council benefits from enhancing its security system. The Council of the

European Union stated that a first step that could be secured through critical infrastructure concentrating on the energy and transport sectors was reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology sector.

With an increase in the sovereignty of critical infrastructure, of course there are disturbing threats to critical infrastructure. Because critical infrastructure currently uses information and communication technology for the progress of a country. So the cyber space that is used contains a lot of information that can be used by irresponsible parties, so it will experience a lot of cyber attacks. This threat can cause a lot of losses to the country, both financially and in terms of the technology recovery time used.

In order to prevent all cyber attacks aimed at critical infrastructure, the government or state must have sufficient cyber security to withstand the attacks it receives. Each country has its own strategy to improve cybersecurity in order to maintain their cyberspace sovereignty and secure any information that can be misused. Therefore, the comparison between Indonesia and Iran is different because each country has a different strategy for increasing its cyber sovereignty. Where Iran is increasing its cyber sovereignty by attacking many major countries and the Middle East Region with offensive cyber movements. Meanwhile, Indonesia prefers to cooperate with big countries to increase its cyber sovereignty.

Although in terms of infrastructure and internet network, Iran is not superior to Indonesia. But Iran itself is recorded to have received many attacks in cyberspace. This makes Iran continue to develop its cyber capabilities. Iranian cyber actors are continuously improving their offensive cyber capabilities. Iran has used its increasingly sophisticated cyber capabilities to suppress certain social and political activities, to the detriment of regional and international adversaries. They continue to engage in conventional offensive cyberspace activities ranging from website tampering, spear phishing, distributed denial-of-service (DDOS) attacks, and theft of personally identifiable information, to more sophisticated activities including destructive malware, and influence-driven operations. social media, and, potentially, cyber attacks intended to cause physical consequences (CISA, n.d.).

According to Robert Jervis in Medvedev (2015) is the first variable figured out when the tension situation of other countries is assessed as a threat. It is assumed that action is both offensive and defensive in nature. Both are used as a means of arming the country with strategy politics and interests to be achieved by the country. Following the 2010 Stuxnet attack on Iran's nuclear program, Iran quickly began investing in and increasing its offensive cyber warfare capabilities, resulting in increasingly sophisticated attacks. In September 2011, an Iranian hacker claimed credit for an attack that compromised Dutch certificate authority DigiNotar. Iranian hackers have the ability to access Gmail accounts and spy on the encrypted communications of 300,000 Iranian users. The attack was claimed by a hacker who claimed to have acted alone and who chose to help the government monitor the communications of its fellow citizens, but it appears that Iranian intelligence was also involved in one of the biggest security breaches in internet history (Army, 2022)

In the wake of numerous cyber attacks on Iran, a group calling itself the Iranian Cyber Army began vandalizing websites linked to Iran's political opposition, Israeli businesses, independent Persian-language media, and social media platforms, posting pro-government messages. (Anderson, 2018). This group often attacks countries such as America and Israel. Iran's cyberspace operations are unlike those of the United States and Israel, which are run by professional intelligence services backed by billions of dollars in budgets. In addition, Iran's offensive and defensive capabilities are not simply organized and funded and only have modest technological sophistication. Iran also uses cyberspace to carry out attacks, as opposed to diplomacy. Iran reportedly attacked Albania's defense twice, this made Albania decide to end diplomatic relations with Iran (Gritten, 2022).

Unable to effectively challenge or deter more powerful adversaries, Iran has demonstrated its ability to retaliate, using opportunistic subversive attacks. Especially in the Middle East, Iran can implicitly threaten cyber operations against poorly maintained economic resources and the infrastructure of adversaries. Disclosures of targets and victims of cyber operations often include industries such as banks and airports that appear to have no purpose other than establishing a foothold in a competing country.

Iran carried out offensive attacks on American financial institutions using DDoS, the perpetrators have exploited vulnerabilities in the software of thousands of websites to bring the attack platform under their control. This is Iran's most costly attack on America because America needs millions of dollars to restore its servers. These attacks were retaliation for Western activities against Iran's nuclear sector and senior officials in the Iranian government were aware of these attacks. Then Iran through malware is reported to have harmed up to 800 victims during the year 2013. The targeted countries and entities are harbingers of future Iranian cyber operations in attacking, oil companies, US think tanks, government agencies, engineering firms, financial institutions, and academics.

In Iran's foreign policy, there is a policy of opposing the existence of Israel and supporting anti-Israeli military groups. With this, Iran carried out an offensive cyberattack against Israeli institutions, but this attack was not successful. Then, in the war between Israel and Gaza, many Israeli defense institutions were attacked by DDoS, one of them by Iran. The attacks carried out by Iran against Israel are getting weaker and weaker because Israel's cyber security capabilities are getting more and more sophisticated.

Iran's offensive attacks were also widely reported by Saudi Arabia; various industrial sectors and political institutions were attacked by Iran. The attack carried out by Iran on Saudi Arabia uses malware that aims to find out passwords for data theft. This dispute between Iran and Saudi Arabia is likely due to the deep geopolitics and ideologies of both countries and Saudi Arabia's ongoing vulnerability in cyberspace (opportunity). In every attack carried out by Iran, it will definitely incur large repair costs (Andeson, 2018).

Iran, which is often subject to cyber-attacks from its enemies, cannot continuously defend itself, but when Iran takes revenge, it will cause damage that will cost a lot to repair. Iran's biggest enemy is America. If Iran cannot attack America during the conflict, it will attack its allies. This mutual attack between Iran and America's allies has made Iran's cyber sovereignty stronger. Unlike Iran, Indonesia prefers to cooperate with big countries to overcome cyberspace. Through the Cyber Authority, Indonesia cooperates with the Netherlands. This collaboration includes various information in the fields of law, legislation, various national policies, institutions, and technological development in the field of cyber security. As well as cooperation in the field of education and training in

defense and cyber-attacks. Indonesia is also working with America to promote and build capacity in cyberspace. This collaboration includes national incident management capabilities, capacity, and cyber-crime prevention, cyber security is disseminated in various forums as needed (Chotimah, 2019).

Indonesia is also working with Australia in cyber security. Australia is considered to have good cyber security. Indonesia and Australia underscore the importance of capable and strong national law enforcement agencies, as well as international partnerships involving governments, international organizations, and the digital industry sector. Both Participants emphasized the importance of international and regional mechanisms to build a more stable and secure cyberspace. This collaboration between Indonesia and Australia is by organizing skills development, including through the Cyber Boot Camp (Public Communication, 2020).

Indonesia also has bilateral cooperation with the United Kingdom in increasing its capabilities in dealing with cyber-attacks and increasing cyber sovereignty. Cooperation between the two countries includes training and the exchange of information to assist and develop understanding. related to cybersecurity when managing data, systems, and assets, including human resources. It is hoped that this collaboration will be able to identify, detect, provide protection and defense, and respond or determine attitudes in taking action before and when an attack occurs in cyberspace, as well as support cyber-attack recovery in order to minimize the impact of an attack. cyber done (Weu, 2020).

Cooperation in the context of overcoming cybercrime and increasing Indonesia's cyber sovereignty to become a member of the International Telecommunication Union (ITU), Indonesia carries a vision and agenda of increasing equitable connectivity for all through capacity building, empowering women, and connecting the unconnected. The vision and agenda are things that are the main issues not only for Indonesia but also for developing and less developed countries at the ITU. Indonesia's re-election as a member of the ITU Council is not only proof of recognition of the progress of efforts and achievements in the field of information, communication, and technology, but also proof of the trust ITU member countries have in Indonesia, which is

considered a country that has cyber sovereignty and has made consistent progress in fighting for the interests of sovereign states in the ITU (Dunia, 2022).

Indonesia became a member of the Asia Pacific Computer Emergency Response Team (APCERT) steering committee after being selected to be the Asia Pacific internet monitoring team. Being a member of the world's cyber security community is considered very important because you will have access to information, resources, and cooperation support in various matters from other countries. The benefits that can be felt in real terms are expert sharing, training, knowledge materials, tools, and assistance for capacity building, as well as lessons learned that we cannot learn from other sources or books (admin, 2012). Indonesia not only carries out bilateral diplomacy in cyber cooperation but also has multilateral cooperation, namely with ASEAN. Indonesia is the largest country among friends that uses Internet facilities, so Indonesia cannot be separated from various cyber threats. ASEAN is collaborating with Japan in an online cyber training program, in this program, is expected to increase development capacity and share cyber information. The aim of this program is to increase capability and readiness in coordinating responses to cyber security incidents at the national level in each ASEAN country (Saputri, 2020).

Indonesia, as part of ASEAN, collaborates with America in the development of the cyber world. ASEAN's cooperation with America is not only joint training but also the construction of infrastructure to support cyber sovereignty in ASEAN. This cooperation is to strengthen and share the vision of "an open, interoperable, reliable, and secure information communication technology (ICT) environment that drives efficiency, innovation, communication, and economic prosperity." between Asia and America (Parameswaran, 2019).

Conclusion

Comparison between Indonesian and Iranian cyber powers, in which Indonesia and Iran have taken different steps to increase their cyber sovereignty. Iran, which has low and underdeveloped infrastructure and expertise, Iran also lacks cooperation in enhancing its cyber sovereignty Indonesia, on the other hand, has a good infrastructure and expertise in dealing with cyber sovereignty.Indonesia also carries out bilateral and multilateral cooperation with

various major countries, such as America, Australia, and Japan, to increase its cyber sovereignty. Iran's way of increasing its cybersovereignt is to defend itself from the attacks of its enemies, such as America, Israel, and Saudi Arabia. With various attacks, Iran will learn about them and improve its cyber defense. Therefore, Indonesia is better at cybersovereignty compared to Iran, where Indonesia has collaborated a lot to bind its cyber sovereignty.

Bibliography

admin. (2012, march 27). *Id-SIRTII Jadi Punggawa Pengawas Internet Asia Pasifik*. Retrieved from m.kominfo.go.id: https://m.kominfo.go.id/content/detail/1805/id-sirtii-jadi-punggawa-pengawas-internet-asia-pasifik/0/sorotan_media

Andeson, C. &. (2018). Iran's Cyber Threat. *Carnegie Endowment*.

Aji, M. P. (2022). Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective (Case Study of Personal Data Protection). *Politica* .

Arifin, Z. (2021). Keamanan dan Ancaman . *MSIM4404*.

Army, I. C. (2022). *The Iranian Cyber Threat*. Iran: United AGAINST NUCLEAR Iran.

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *ResearchGate*.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber DAN Diplomasi Siber Indonesia. *Political Vol 10*.

Cisa. (N.D.). *Iran Cyber Threat Overview AND Advisories*. Retrieved from cisa.gov: https://www.cisa.gov/uscert/iran

Dyson, E. G. (1994). Cyberspace and the american dream: a magna carta for the knowledge age. *Future Insight*.

Fang, B. (2018). Cyberspace Sovereignty. *China Science Publishing & Media Ltd (Science Press).*

Gritten, D. (2022). *Albania Severs Diplomatic Ties With Iran Over Cyber-Attack*. Retrieved From Bbc News: https://www.bbc.com/news/world-europe-62821757

Komunikasi Publik, B. H.–B. (2020). *Bssn Inisiasi Lanjutan Kerja Sama Keamanan Siber Indonesia-Australia dalam 3RD Indonesia-Australia Cyber Policy Dialogue*. Retrieved from https://bssn.go.id/bssn-inisiasi-lanjutan-kerjasama-keamanan-siber-indonesia-australia-dalam-3rd-indonesia-australia-cyber-policy-dialogue/

Medvedev, S. A. (2015). Offense-Defense Theory Analysis Of Russian Cyber Capability. Naval Postgraduate School Monterey Ca

Octavian, A. (2021, April 02). *Rektor Unhan Ri Tegaskan Pengingnya Kedaulatan Data DAN Keamanan Siber DI Era Internet OF Things (Iot)*. Retrieved FROM

www.idu.ac.id: https://www.idu.ac.id/berita/rektor-unhan-ri-tegaskan-pentingnya-kedaulatan-data-dan-keamanan-siber-di-era-internet-of-thingsiot.html#:~:text=kedaulatan%20data%20di%20ruang%20siber,wilayahnya%20mencakup%20kemerdekaan%20dan%20kesetaraan.

Parameswaran, P. (2019). *What's Behind the New US-ASEAN Cyber Dialogue?* Retrieved from thediplomat.com: https://thediplomat.com/2019/10/whats-behind-the-new-us-asean-cyber-dialogue/

Prakoso, A. (2022). Sistem Keamanan Siber dan Kedaulatan Data DI Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi). *Politica*.

Saaty, T. &. (2012). Models, Methods, Concepts & Applications Of The Analytic Hierarchy Process: Springer Science & Business Media. *Academia.EDU*.

Saputri, D. P. (2020). Indonesian Cyber Diplomacy: Asean-Japan Online Cyber. *Indonesian Cyber Diplomacy: Asean-Japan Online Cyber*.

Telecommunication Union (ITU) Wilayah E Periode 2023-2026. Retrieved from kemlu.go.id: https://kemlu.go.id/portal/id/read/4035/berita/indonesia-terpilih-kembali-sebagai-anggota-dewan-international-telecommunication-union-itu-wilayah-e-periode-2023-2026

UNION, T. C. (2018). Council Directive 2008/114/EC. *Official Journal of the European Union*.

Weu, M. R. (2020). Kerjasama Pemerintah Indonesia Dan Pemerintah Kerajaan Inggris . *Global Political Studies Journal*.

Yeli, H. (2017). A Three-Perspective Theory of Cyber Sovereignty. *Prism*.