https://doi.org/10.18196/jhi.v11i2.14361

JURNAL HUBUNGAN INTERNASIONAL
VOL. 11, NO. 2 (2023)

The Paradox of Indonesia Cyberspace Policy and Cooperation: Neoclassical Realism Perspective

Muhammad Abdurrohim
International Relations Department, Universitas Satya Negara, Indonesia
abdurrohim.muhm@gmail.com
Indah Kumalasari
International Relations Department, Universitas Gadjah Mada, Indonesia
indahkumaal@mail.ugm.ac.id
Fathur Rosy
Jilin University, China
Submitted: 29 March 2022; Revised: 13 August 2022; Accepted: 30 August 2022

Abstrak

Cyberspace merupakan ancaman baru bagi keamanan negara, khususnya di Indonesia. Peningkatan pengguna internet di Indonesia diikuti dengan beberapa kebijakan yang diambil Jakarta untuk beradaptasi dengan pesatnya tantangan dunia maya. Dalam rangka pengelolaan dunia maya di Indonesia, pemerintah mengembangkan UU ITE yang berusaha mengatur dunia maya Indonesia dan mencegah segala ancaman yang datang dari dalam. Selain itu, menyadari bahwa dunia maya memiliki begitu banyak peluang, pemerintah juga bekerja sama dengan aktor lain seperti ASEAN untuk merumuskan ASEAN Digital Masterplan untuk meningkatkan kontribusi dunia maya terhadap pemulihan ekonomi pasca Covid-19. Namun, terdapat kontradiksi antara UU ITE, khususnya Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 dengan kerjasama dunia maya yang coba diterapkan oleh pemerintah. Fenomena tersebut menimbulkan pertanyaan mengapa pemerintah Indonesia mengambil kebijakan kontradiksi di dunia maya antara tingkat domestik dan internasional. Penelitian ini mencoba menjelaskan alasan di balik kebijakan paradoks pemerintah Indonesia di bawah undang-undang ITE dan masterplan digital ASEAN mengenai kebijakan ruang siber, terutama dari tahun 2016 – 2021. Untuk mencapai tujuan tersebut, penelitian dilakukan dengan menggunakan metode kualitatif dengan beberapa laporan konfiguratif disiplin. dan dokumen pemerintah mengenai kebijakan siber mereka. Data kolektif tersebut kemudian dianalisis dengan menggunakan teori yang sudah mapan, yaitu realisme neoklasik untuk mengidentifikasi perilaku kebijakan dunia maya pemerintah Indonesia di tingkat domestik dan internasional. Situasi paradoks antara pemerintah Indonesia tingkat domestik dan internasional terhadap kebijakan dunia maya ini tercipta dari bagaimana pemerintah Indonesia mengidentifikasi ancaman. Pemerintah di Indonesia masih menghadapi ketidakstabilan di tingkat domestik untuk mengidentifikasi kategori ancaman terhadap rezim karena warisan model pemerintahan rezim otoriter yang dialami oleh pemerintah Indonesia sebelumnya. Respon sebaliknya di tingkat internasional terjadi karena proses sosialisasi dan pelembagaan di kawasan menciptakan budaya strategis. Budaya strategis dunia maya membatasi pemerintah Indonesia untuk menerapkan ide yang sama dari tingkat domestik terhadap kawasan. Pada tingkat internasional, pemerintah Indonesia perlu mengadaptasi budaya strategis populer untuk memastikan prestise.
Kata kunci: Indonesia, cyberspace, politik dalam negeri, dunia ketiga, realisme neoklasik, tatanan internasional.

Abstract

Cyberspace is a new threat to state security, especially in Indonesia. The increase of internet users in Indonesia is followed by several policies Jakarta takes to adapt to the fast pace of cyberspace challenges. To manage cyberspace in Indonesia, the government has developed ITE Law to regulate Indonesia's cyberspace and prevent threats coming from within. Moreover, realizing cyberspace offers many opportunities. The government also cooperates with other actors like ASEAN to formulate ASEAN Digital Masterplan to enhance cyberspace contribution toward economic recovery after the COVID-19 pandemic. However, there is a contradiction between ITE Law, especially the Regulation of the Minister of Communication and Informatics No. 5 of 2020, and the cyberspace cooperation that the government tries to impose. These phenomena raise the question of why the Indonesian government takes contradiction policy on cyberspace between domestic and international levels. This research examined the reason behind the paradoxical policy of the Indonesian government's ITE Law and the ASEAN Digital Masterplan regarding cyberspace policy, especially from 2016 to 2021. A qualitative method was employed to achieve the objective, with disciplined configurative reports and government documents regarding its cyber policy as the data. The data were analyzed using the theory of neoclassical realism to identify the Indonesian government's cyberspace policy behavior on domestic and international levels. This paradoxical situation between the domestic and international levels of the Indonesian government's cyberspace policy was created by how the Indonesian government identified threats. The Indonesian government still faced instability at the domestic level to identify the category of threats toward

the regime due to the inheritance of the authoritarian regime government model it experienced before. The opposite response at the international level occurred because the socialization and institutionalization in the region have created strategic culture. Accordingly, the strategic culture of cyberspace has restricted the Indonesian government from applying the same idea at the domestic level. The Indonesian government should adapt the popular strategic culture at the international level to ensure prestige.
Keywords: Indonesia, cyberspace, domestic politics, third world, neoclassical realism, international order.

INTRODUCTION

Modern society heavily relies on the internet daily, whether for leisure or work-related. This situation has also been accelerated by the COVID-19 pandemic, where people interact virtually. Nugraha and Putri cited Internet Live Stat, revealing that Indonesia ranked the 12th largest internet user worldwide with 53 million users among its 274 million population (Nugraha & Putri, 2016). This number keeps growing, especially after the COVID-19 pandemic hit the world in 2020. Data from the Association of Indonesian Internet Service Providers (APJII) unveiled a 73.7 percent increase in the additional spike of internet users in Indonesia (VOI, 2020). The main contributor to this statistic is social media, a communication platform, e-commerce, and game online, all needing a set of identity registration to sign up.

The 'Big Data' stored on the internet, called cyberspace, has become a hotspot for online criminal activities. State Cyber and Code Agency (BSSN) revealing that 290 million cyber-attacks in Indonesia in 2019, while in January-Mei 2021, it rapidly grew to 448 million cases (Ananda, 2021). Cyber-attack in Indonesia includes information leak from *Tokopedia*, one of the largest and most used e-commerce sites; the data of more than its 15 million users were sold on the dark web. Other cases happened to *Bukalapak* and *BRI Bank*. In addition to the economic sector, cyber threats have also targeted governance, such as the data leak of the General Election Commission (KPU) and COVID-19 patients in 2020. Meanwhile, in 2021, the personal information of 279 million Indonesian Citizens from the Social Security Agency (BPJS) was leaked and found on the internet (Wijayaatmaja, 2021).

Reacted to this, the Indonesian government under Joko Widodo Presidency allocated Rp 30.5 trillion to accelerate digital transformation in information and communication technology in 2021 (Eloksari, 2020). Cyberlaw in Indonesia under the ITE Law of 2008 and the revised version of 2016, in addition to national policy on CRIST, proved ineffective, demonstrated by the rising number of cyber-attacks (Anjani, 2021). Moreover, Cyber Law in Indonesia still lacks requirements due to various challenges. Rizal and Yani in their article, Cyber Security Policy and Its Implementation in Indonesia, argued that cyberspace is relatively common in developed and some developing countries, while Indonesia is new to this topic and considered a new pseudo-industrializing country (Rizal & Yani, 2016). Using realism theory, Rizal and Yani considered cyberspace a world without borders and more likely used to be a criminal space, such as illegal information, hackers, or attacks through media and informational exchange, becoming a threat to national defense. Cyber security is an action to secure information from unauthorized access and other cyber-attacks. The majority of Indonesian cyber policies are under the authority of the Minister of Communication and Information Technology related to Internet-protocol-based telecommunication networks together with the Minister of Defense. Meanwhile, cybercrime evolves rapidly, and national regulation is hard to tackle new challenges.

The Regulation of the Minister of Communication and Informatics No. 5 of 2020 regulates the obligation of all private digital apps and platforms such as Google, Facebook, Twitter, Tiktok, Paypal, and various platforms serving in Indonesia to register their service to the ministry. If the platform does not register its service on the date set by the Ministry of Communication and Information Technology, the government will block it in Indonesia. However, if it registers its service to the government, the ministry is allowed to access its data; the purpose is to filter and block unwanted content that spreads through digital service.

Ministry accessibility to digital data invites debates. The Human Right Watch representative, Linda Lakhdir, stated that the action is a severe violation of freedom of speech, privacy concerns, and free access to information of internet users (Human Right Watch, 2021). The regulation violates the ASEAN Digital Masterplan 2025 that Indonesia is involved in the agenda-setting process. According to the document, the first principle guarantees connectivity within and among society, including freedom of access to information and speech. By the time the Regulation of the Minister of Communication and Informatics entered into force, the connectivity had broken, and the vision to build an excellent digital infrastructure system to support local creative capability was gone (ASEAN, 2021).

The increase of internet users in Indonesia is followed by several policies Jakarta takes to adapt to the fast pace of cyberspace challenges. Accordingly, the Indonesian government has tried to develop international cooperation with other states or regional institutions like ASEAN. However, the international cooperation and cyberspace policy that the Indonesian government formulated has contradicted domestic policy. It raises the question of why the Indonesian government takes contradiction policy on cyberspace between domestic and international levels. This research studied the reason behind the paradox of the Indonesian government's cyberspace policy, especially from 2016 to 2021.

LITERATURE REVIEW

CYBERSPACE AND THE DIFFERENT APPROACHES TO THE CYBERSPACE POLICY MODEL

Current literature reviews the characteristic of cyberspace, creating a new dimension of international actor interaction in an anarchical environment. International actors need to adjust and adapt their interest in the rapid pace of cyberspace. As a new domain of influence between states, cyberspace creates multi-dimensional characteristics that form an environment in which international actors interact. Nazli Choucri proposed seven characteristics of cyberspace becoming a new interaction domain (Choucri, 2012).

These characteristics of cyberspace create a multi-dimensional approach for international actors to adjust themselves in pursuing their interests in an international environment. This co-existence of the virtual domain (cyber) and international politics is often called cyber politics.

Nowadays, there is a bipolarity of power that desires to regulate how cyberspace should operate in an international system; it is between the U.S. and China. The U.S.-led deterrence model over cyberspace is reflected by its experience during the Cold War when each side of major power could destroy each other regardless of which side had more destructive force under their control (Harold, Libicki, & Cevallos, 2016). As a technology originating in the U.S., the internet and cyberspace must imitate U.S. values over the international system and community. The U.S. and its alliance have argued that cyberspace should be a free, transparent, and global environment controlled by a bottom-up approach driven by technical organizations, civil society, and the private sector (Segal, 2020). Because of its origin, cyberspace also promotes a value of the U.S. where the internet and cyberspace value automatic operating system becomes privacy, free speech, information access, and the function of control over it. However, China has tried to resist this operating system in cyberspace because it has seen it as threatening the regime value of the country.

On the other hand, literature regarding Indonesia's cyberspace policy is still limited. As Setiadi, Sucahyo, and Hasibuan mentioned in their article *An Overview of Development Indonesia National Cyber Security,* Indonesia's cyberspace policy consists of five aspects (Setiadi, Sucahyo, & Hasibuan, 2012): (1) legal measures, (2) technical and procedural measures, (3) organizational structures, (4) capacity building, and (5) international cooperation depicting how the Indonesian government tries to develop its cyberspace policy.

The increasing threats from cyberspace security have become a severe issue that the government has been concerned. Muhammad Rizal and Yayan M Yani, an International Relations Professor from Padjajaran University argued that cybersecurity laws and regulations

Table 1. Seven characteristics of cyberspace

Temporality	Replacing near instantaneity for conventional temporality
Physically	Surpassing geography and physical location limits
Permeation	Penetrating authorities and borders
Fluidity	Disclosing sustained adjustments and reconfigurations
Participation	Decreasing obstacles to freedom of speech and activism
Attribution	Obscuring actors' names and connections to actions
Accountability	Bypassing transparency mechanisms

Note. Data adapted from Choucri (2012)

have existed in Indonesia; however, they are too general *(lex generalis),* consequently, non-specific type *(lex specialis)* (Rizal & Yani, 2016). Therefore, the use of cyber security has not been successful. The government must make them specific and regularly socialize them with all stakeholders to be effective.

The ineffective of the Indonesian cyberspace policy has become a serious issue because of the increasing number of internet users in Indonesia. Although cyber connectivity has brought numerous advantageous economic opportunities for Indonesia, it has also given rise to cybercrime issues, exacerbated religious intolerance, and false information. Due to Indonesia's poor legislative framework and lack of enforcement, cybercriminals utilize Indonesia as a haven for their operations. The Indonesian government has declared a small number of efforts to solve these problems, including promoting digital literacy and addressing problems in national cyberspace policy. However, according to Thomas Paterson, even though some of these recommendations for changes to the law are favorable, they also contain an automatic "content moderation" system that, in the absence of adequate monitoring or open implementation procedures, might be used to censor or restrict ostensibly free expression (Paterson, 2019).

RESEARCH METHOD

As highlighted before, this research analyzed the Indonesian contradiction policy on cyberspace law between the domestic and international levels. A qualitative method was applied to achieve the research objective, with disciplined configurative reports and government documents regarding its cyber policy as the data. Documentary analysis of existing documents was performed to comprehend their substantive content and disclose their nature and coverage (Ritchie, 2003). This article addressed official documents from related governments, reputable literature, and multiple news outlets to address the research question.

The data were analyzed using an established theory of neoclassical realism to identify the Indonesian government's cyberspace policy behavior on domestic and international levels. Neoclassical realism emphasizes that states develop their foreign security policies principally with an eye to the threats and opportunities that emerge in the international system, which determine each state's range of policy options (Ripsman, Taliaferro, & Lobell, 2016). How states vision their foreign policy depends on their material capability related to domestic power to support their foreign policy goals. However, domestic power is not the only determinant because systemic influences must be translated through intervening factors at the unit level; the effect of such power capacities on foreign policy is indirect and complicated (Rose, 1998).

When states develop their foreign policy, they will consider every variable they hold and measure how far the variable can influence the output. Foreign policy development, like any other policy, is often influenced by domestic-level intervening variables, including state-society relations, which impact the state's capacity to enact and implement decisions; leader images that interfere with realistic judgments; strategic culture, which shapes all elements of state responses; when state leaders

meet social resistance to policy choices or implementation, and internal political institutions, which can either empower or hinder state leaders (Rose, 1998). As a result of the more complicated domestic decision-making situation, nations do not always choose the best policy response to address systemic limitations; instead, they select from a variety of policy options to balance systemic constraints and domestic political imperatives.

RESULTS AND ANALYSIS

INTERNATIONAL SYSTEM OF CYBER OPERATION AND REGIONAL CONDITION

The increasing number of internet users in Indonesia is also followed by several vulnerabilities of cyberattacks. Despite the penetration of internet users increasing every year, digital literacy among Indonesian people remains low (Harsono 2022). The poor digital literacy among internet users in Indonesia affects how Indonesian people conduct internet safety and identify hoaxes or misleading information on the internet. Besides, low digital literacy also affects businesses, which the Indonesian government estimates to cost more than USD 1.5 Million (Eloksari, 2021). According to Indonesia's National Cyber and Crypto Agency (BSSN), from January to December 2021, 1.65 billion cyber traffic anomalies were recorded. Those numbers were 62% caused by malware infection and 10% Trojan activity, and 9% data leaked. The targets of the cyber-attacks were 36% higher education sites, 25% private sites, and 18% local government sites (Nasution, 2022).

Previously, the Indonesian government published Law No.11 of 2008 about Information and Electronic Transaction (ITE). Then, it was revised to Law No.19 of 2016 to prevent the spreading unwanted 'negative' content. The law is expected to ensure Indonesia's cyberspace security and defense (Tashia, 2016). Unfortunately, it has proven not to tackle cyber-attacks, especially regarding social media etiquette (MKRI, 2022). The high cyber-attacks were responded to with the stipulation of the Regulation of the Ministry of Communication and Informatics (MoCI) No. 5 of 2020 to prevent any threat from cyberspace.

The 2020 COVID-19 pandemic has accelerated the government and businesses to transform their operation to digital. This condition becomes a wake-up call for the government in ASEAN to cooperate more deeply in cyberspace. The International Criminal Police Organization (Interpol) report revealed several major cyber-attacks in ASEAN (Tan et al., 2021).

- Data Breach. 1.1 million accounts on Redmart were compromised.
- Ransomware. Targeting Bussiness and hospitals in Thailand
- Ransomware. 1.5 terabytes of sensitive data were stolen from a subsidiary of ST Engineering Aerospace
- Data Breach. Indonesia's e-commerce Tokopedia's 91 million user data leak
- Cyber Fraud. "Macau Scam" that attacked people in Malaysia with 5,218 cases and a total loss of over MYR 256 million

The high number of cyber-attacks in the region has become a concern for ASEAN members to form serious cooperation to mitigate the impact of an increasing number of internet users and cyber attacks. ASEAN Digital Masterplan appeared as one of the fragments to establish cyber cooperation in the region. However, cyber cooperation remains complex because of the different principles of the ASEAN members.

ASEAN Digital Masterplan becomes the fragmented part of regional cooperation in cyberspace between ASEAN members. This cyber cooperation has envisioned ASEAN as a leading digital community and economic bloc powered by secure and transformative digital services, technologies, and ecosystems (ASEAN, 2021).

As a fragmented part of the power institution in the region, ASEAN Digital Masterplan has a mission to connect ASEAN member states through underlying telecommunications infrastructure and safe and relevant services and remove the barriers to users in the region (ASEAN, 2021). To achieve the vision of the ASEAN Digital Masterplan, its members have agreed to reduce online affordability and accessibility to ensure the creation of a digitally inclusive society in ASEAN. As the biggest country in the region, Indonesia needs to adapt to regional cyber cooperation to ensure the objective of the

ASEAN Digital Masterplan.

INDONESIA'S CYBER POLICY AND THE PARADOX OF INTERNATIONAL CYBER COOPERATION

The COVID-19 pandemic has augmented the request for digital services in Indonesia more than before. People are obliged to be more virtually connected daily for commerce, education, health care, politics, socializing, and others. Indonesia had at least 196.7 million internet users between 2019 and 2020. These numbers increased from 64.8% in 2018 – 2019 to 73.7% in 2019 – 2020 (APJII, 2020). The states follow the increasing number of internet users to ensure the security of internet users in Indonesia. The ASEAN Digital Masterplan serves as a guideline for cooperating on this issue in the region.

One of the essential aspects of this cooperation is ensuring that cybersecurity and digital data governance best practices are widely followed, both to reduce the direct effect of a breach on businesses and customers and to create confidence (ASEAN, 2021). This aspect is crucial to ensure the economic recovery from the COVID-19 pandemic by accelerating the digital economy in the region.

As a guideline for the states in the region to cooperate in cyberspace, the ASEAN Digital Masterplan aims to achieve the following goals (ASEAN, 2021).

1. Accelerating economic recovery in the region through digital service
2. Improved fixed and mobile broadband infrastructure quality and coverage
3. Providing dependable digital services for internet users
4. Creating a competitive and sustainable market for the supply of digital service
5. Improving the quality and use of e-government services
6. Connecting businesses and facilitating cross-border trade using digital services
7. Improving business and people's capacity to engage in the digital economy
8. Developing a digitally inclusive society in ASEAN

The objective of the ASEAN Digital Masterplan has a similar value inherited from the American value of cyberspace. Washington sees cyberspace as a sphere to anchor American values, such as individual liberty, free expression, free markets, and privacy (The White House, 2018). Despite inheriting American values in regional cyber cooperation, not all ASEAN member states, including Indonesia, aim to apply the same value at the domestic level.

However, Jakarta has taken an opposite step toward the liberalism and connectivity value of cyberspace with several policies reflected in ITE Law, the Regulation of the Minister of Communication and Informatics No. 5 of 2020. This law was formulated to revoke the Regulation of the Minister of Communication and Informatics No. 19 of 2014 about websites with negative content. Following the new regulation, every digital service needs to register its platform with the government. Otherwise, the ministry will block or take down its service in Indonesia.

The Regulation of the Minister of Communication and Informatics No. 5 of 2020 consists of seven articles and 49 chapters, described in the following table.

As Chapter 2 stated, the government emphasizes that every platform, even private electronic system, needs to register its service to the government. In Chapter 3, the government tries to monetize the content of the platform. Both chapters reflect the paradoxical policy that the Indonesian government tried to formulate in the ASEAN Digital Masterplan.

Southeast Asia Freedom of Expression Network (SAFEnet) noted that the Regulation of the Minister of Communication and Informatics No. 5 of 2020 includes 65 keywords about access termination, whether about blocking or take-down access (SAFE net, 2020). This law reflects that the government has tried to obtain complete control of every content and platform having service in Indonesia. The government has the power to terminate the platform not meeting its standards. However, this law becomes more problematic in Chapter 3, Article 9.

- The electronic system operator must ensure that (a) the electronic system does not contain any prohibited electronic information and/or electronic documents

Table 2. The Regulation of the Minister of Communication and Informatics No. 5 of 2020

Chapter	Content	Article
Chapter 1	General Requirements	Article 1
Chapter 2	Registration of Private Electronic System	Article 2 - 8
Chapter 3	Management and Governing Electronic Information and/or Electronic Document	Article 9 - 12
Chapter 4	Application for Termination of Access to Electronic Information and/or Prohibited Electronic Document	Article 13 - 20
Chapter 5	Granting Access to Electronic and/or Electronic Systems for Supervision and Enforcement of Criminal Law	Article 21 - 46
Chapter 6	Transition Terms	Article 47
Chapter 7	Closing Terms	Article 48 - 49

Note. Data adapted from SAFE net (2020)

and (b) the electronic system does not facilitate the dissemination of prohibited electronic information and documents.

- Prohibited electronic information and documents, as referred to in paragraph (3), are classified as (a) violating the provisions of laws and regulations, (b) disturbing the public and public order, and (c) notifying the way or providing access to prohibited electronic information and documents.

This article will become the basis for the government to control every content in cyberspace, making it too powerful. During COVID-19, the government tried to monitor every issue circulating among its people. Despite the government's efforts to accelerate cyberspace in the region with the ASEAN Digital Masterplan, it becomes an obstacle for the government to connect regional policy with domestic policy.

Following freedomhouse.org, a non-profit organization advocating the development of democracy, political freedom, and human rights, noted three issues emerging in cyberspace during the COVID-19 pandemic (Shahbaz & Funk, 2020). First, political leaders use the pandemic as a pretext to restrict access to information. Second, COVID-19 was used by governments to justify increased surveillance powers and the deployment of new technologies previously considered too intrusive. Third, the systematic "splintering" of the internet into a full-fledged race for "cyber sovereignty", with each government enacting its internet laws that limit the flow of information across national borders.

SafeNet report noted that several policies of the Indonesian government are comparable to China's cyberspace model of taking control of the virtual world. Several policies reflecting the Beijing model are ITE Law, Law No. 1 of 1946 Chapter 14 - 15, and the Regulation of the Minister of Communication and Informatics No. 5 of 2020 about private electronic system operators. These laws become draconian for states to limit users' behavior in cyberspace, especially ITE Law and the Regulation of the Minister of Communication and Informatics. From 2019 to 2020, ITE Law was used for 84 cases, an increase from 24 cases in the previous year (Sanjaya et al., 2021). Moreover, the Regulation of the Minister of Communication and Informatics No.5 of

2020 also tries to empower states to restrict people's activities in cyberspace by forcing digital platforms to accept local jurisdiction in their content and providing the government access to their user data.

How the Indonesian government at the international level takes the side of the American model of cyberspace, yet at the domestic level applies an opposite cyber model similar to China's cyberspace model has been influenced by the assumption that developing country like Indonesia has the perception of threat could be non-military in characters (Collins, 2000). This perception comes from the influence of military or authoritarian rule that the Indonesian government still inherit from the previous regime. The developing military has established a considerably more enormous political influence, a relationship that might hamper the state-building process (Tilly, 1990).

Like the core idea of realism, the regime develops a policy to survive. Regimes focus on their security. Thus, it is natural for them to spend precious resources on military equipment, consider threatening opposition groups demanding more public discourse, and regard harmful community activities that promote alternative identities and loyalties (Job, 1992). Within the anarchical world of cyberspace, the discord of distrust toward regimes always emerges because of the free expression and anonymity of users in cyberspace.

Different domestic situations make developing countries have more insecurity within their domestic problems and security issues in developed states. As Job (1992) asserted, the insecurity of the developing states includes, one of which, the dominant sense of threat—a domestic threat to and from the predominate regime. In this case, the Indonesian government tries delegitimizing any group or power seen as a threat to the existing regime. For example, the Indonesian government has managed separatism groups, such s the Sunda Empire, with Law No. 1 of 1946, Chapter 14 - 15. The Sunda Empire was identified as a group that could delegitimize government authority toward its people.

In addition, the state lacks effective competence for maintaining internal peace and order; separatism. The Indonesian government has constantly faced separatism groups, especially in Papua, with its human rights issues and unequal development, placing the Indonesian government in an uncomfortable situation. The resistance movement of the existing regime also works in a virtual world where the Indonesian government cannot create a single narration over the conflict. This situation of conflict on the ground, supported in the virtual world, demands the Indonesian government to minimize internet access in Papua, even constantly turning it off if the conflict escalates.

Furthermore, popular support for the regime is low; its existence and security interests are not seen as legitimate. In this case, the Indonesian government has continually faced cyber resistance toward regime policy. During the pandemic, the Indonesian government passed an omnibus bill with considerable resistance from several civil groups, including student and labor unions. This considerable resistance appeared in the street and the virtual world, making the narration against regime policy grow bigger. In the middle of the protest, there was a leaked telegram from police describing how the police used an intelligence approach to de-escalate the demonstration. This leaked telegram was met with a more negative view of the regime in the virtual world, causing the police to arrest several people sharing "hoaxes" escalating resistance to the regime policy.

Lastly, there existed primary identification with community groups fighting for their security. Papua has become the hotspot for the Indonesian government to manage. A decade of unequal development followed by violent territory gave the resistance group momentum against the Indonesian army. The decade-long conflict has led the Indonesian government to identify this area as a sensitive domain causing limited internet users and every narration against the government to be faced with imprisonment.

Despite developing a draconian model of cyberspace at the domestic level, the Indonesian government has agreed to cooperate in cyber development in the region. The opposite response at the international level happened as a result of the socialization and institutionalization in the region creating strategic culture. Political leaders, domestic elites, and even the general public's strategic thinking are shaped by this strategic culture. These collective assumptions and

expectations become deeply entrenched through socialization and institutionalization (in rules and norms) and constrain a state's behavior and freedom of action by defining acceptable and unacceptable strategic choices, even in an anarchic self-help environment (Ripsman, Taliaferro, & Lobell, 2016). In other words, the strategic culture of cyberspace has limited the Indonesian government from applying the same idea at the domestic level.

The Indonesian government must adapt popular strategic culture to ensure prestige at the international level. Power and prestige have a moral and functional grounding when together, especially in the international arena. The acceptance of the Indonesian government toward the American cyber model is due to the strategic culture in the established system and partly to its preference for the certainty of the status quo over the uncertainty of change (Gilpin, 1981). The established American cyberspace model at the international level has influenced states to apply it within international cooperation. By following the existing order, the Indonesian government would be accepted in the international arena for having a similar strategic culture to the existing system.

This paradoxical situation between the domestic and international levels of the Indonesian government regarding cyberspace policy was created by how the Indonesian government identified threats. To ensure the survival of the regime, the Indonesian government took a draconian approach to cyberspace at the domestic level and a liberalism approach at the international level. The researchers argue that the contradictory policy of the Indonesian government on cyberspace at the domestic and international level happened because of the regime's existing need to ensure its survival with the limited resource to identify the emerging threats. Limited resources cover the power to implement the policy, the information obtained, and the strategic culture or norms flourishing at the domestic or international level.

The Indonesian government has replicated the problem of developing countries where international powers, whether military, political, economic, or technical, have a significant and meaningful impact on the fortunes of the state-making enterprise as well as the broader security issues that developing countries face (Ayoob, 1991). The Indonesian government is still facing instability at the domestic level to identify the category of threats toward the regime because of the inheritance of the authoritarian regime government model it experienced before. Cyberspace, as a new sphere of influence of states, has become the technological part of neoclassical realism, believed to be a structural modifier to distribute power.

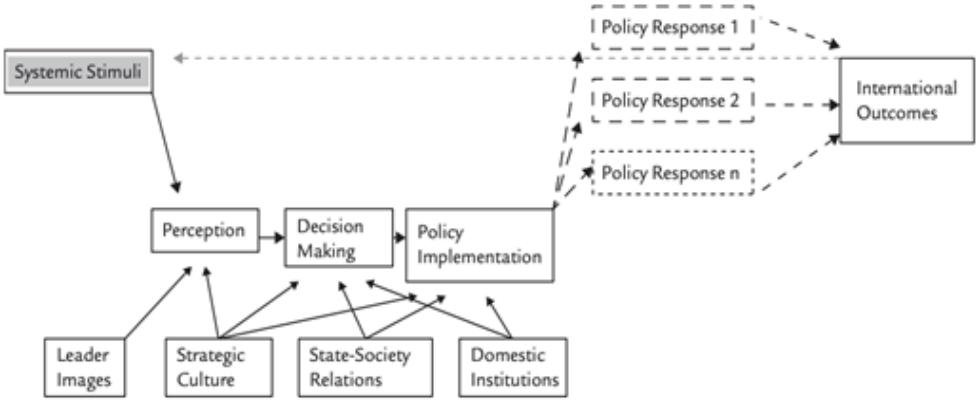

Figure 1. Neoclassical Realism Model (Ripsman, Taliaferro, & Lobell, 2016)

This paradoxical situation between the domestic and international levels of the Indonesian government regarding cyberspace policy was created by how the Indonesian government identified threats. To ensure the survival of the regime, the Indonesian government took a draconian approach to cyberspace at the domestic level and a liberalism approach at the international level. The researchers argue that the contradictory policy of the Indonesian government on cyberspace at the domestic and international level happened because of the regime's existing need to ensure its survival with the limited resource to identify the emerging threats. Limited resources cover the power to implement the policy, the information obtained, and the strategic culture or norms flourishing at the domestic or international level.

The Indonesian government has replicated the problem of developing countries where international powers, whether military, political, economic, or technical, have a significant and meaningful impact on the fortunes of the state-making enterprise as well as the broader security issues that developing countries face (Ayoob, 1991). The Indonesian government is still facing instability at the domestic level to identify the category of threats toward the regime because of the inheritance of the authoritarian regime government model it experienced before. Cyberspace, as a new sphere of influence of states, has become the technological part of neoclassical realism, believed to be a structural modifier to distribute power.

CONCLUSION

Modern society relies on the internet daily, whether for leisure or work-related. The 'Big Data' stored on the internet, commonly known as cyberspace, has become a hotspot for online crimes. Cyberattacks in Indonesia include information leaks of its citizen data on the dark web. In response, the Indonesian government under the Joko Widodo Presidency has allocated IDR 30.5 trillion to accelerate Indonesia's digital transformation. The increase in internet users in Indonesia is followed by several policies Jakarta takes to adapt to the fast pace of cyberspace challenges. To further develop Indonesian cyberspace policy, the government tried to formulate international cooperation to enhance cyberspace opportunities, whether with another state or a regional institution like ASEAN. This research seeks to analyze contradictory Indonesian policy on Cyberspace Law under ITE Law, especially the Regulation of the Minister of Communication and Informatics No. 5 of 2020 as domestic policy and the ASEAN Digital Masterplan at the international level. This utilized official documents from governments, reputable literature, and multiple news outlets to address the research question. The collective data were analyzed using the neoclassical realism theory to identify the Indonesian government's cyberspace policy behavior on the domestic and international levels.

The contradiction response at the international level occurred because socialization and institutionalization created strategic culture. The strategic culture of cyberspace has confined the Indonesian government to apply the same idea at the domestic level. In contrast, at the international level, the Indonesian government needs to adapt popular strategic culture to ensure prestige. The established American cyberspace model at the international level has influenced states to apply it in international cooperation. This paradoxical situation between the domestic and international levels of the Indonesian government regarding cyberspace policy emerged due to how the Indonesian government identified threats. The Indonesian government has replicated the problem of developing countries where international powers, encompassing military, political, economic, and technical, have significantly impacted the fortunes of the state-making enterprise and the broader security issues developing countries face (Ayoob, 1991). Cyberspace, as a new influential sphere of states, has eventually become the technological part of neoclassical realism, considered a structural modifier for power distribution.

REFERENCE

Ananda, P. (2021). "Serangan Ciber Di RI Terus Meningkat, Capai 448 Juta Kasus." *Media Indonesia.* https://mediaindonesia.com/politik-dan-hukum/414225/serangan-siber-di-ri-terus-meningkat-capai-448-juta-kasus (August 14, 2022).

Anjani, N. H. (2021). Center for Indonesian Policy Studies (CIPS) *Perlindungan Keamanan Siber Di Indonesia.*

APJII. (2020). "Laporan Survei Internet APJII 2019 – 2020." *Asosiasi*

Penyelenggara Jasa Internet Indonesia 2020: 1–146. https://apjii.or.id/survei.

ASEAN. (2021). *ASEAN DIGITAL MASTERPLAN 2025.*

Ayoob, Mohammed. 1991. "The Security Problematic of the Third World." *World Politics* 43(January): 257–83.

Choucri, N. (2012). *Cyberpolitics in International Relations.* Cambridge, Massachusetts: The MIT Press.

Collins, A. (2000). *The Security Dilemmas of Southeast Asia.* Singapore: Institute of Southeast Asian Studies.

Eloksari, E. A. (2020). "Indonesian Internet Users Hit 196 Million, Still Concentrated in Java: APJII Survey - Business - The Jakarta Post." *Jakarta Post.* https://www.thejakartapost.com/news/2020/11/11/indonesian-internet-users-hit-196-million-still-concentrated-in-java-apjii-survey.html (August 14, 2022).

The Jakarta Post. (2021). "Cyberattacks Cost Indonesian SMEs Dearly in Terms of Revenue, Reputation - Business - The Jakarta Post." https://www.thejakartapost.com/news/2021/10/23/cyberattacks-cost-indonesian-smes-dearly-in-terms-of-revenue-reputation.html (February 13, 2022).

Gilpin, R. (1981). Cambridge University Press *War and Change in World Politics.* Cambridge, United Kingdom.

Harold, S., Libicki, M., & Cevallos, A. (2016). *Getting to Yes with China in Cyberspace.* Santa Monica, Calif: RAND Corporation.

Harsono, N. (2022). "Despite Improvements, Indonesia's Digital Literacy Remains Low - Economy - The Jakarta Post." https://www.thejakartapost.com/business/2022/01/20/despite-improvements-indonesias-digital-literacy-remains-low.html (February 13, 2022).

Job, B. L. (1992). *The Insecurity Dilemma: National Security of Third World States.* Boulder: Lynne Rienner.

MKRI. (2022). "Sejumlah Pencipta Konten Persoalkan Unsur Pencemaran Nama Baik Dalam UU ITE | Mahkamah Konstitusi Republik Indonesia." *Mahkamah Tinggi Republik Indonesia.* https://www.mkri.id/index.php?page=web.Berita&id=18118# (August 14, 2022).

Nasution, R. (2022). "BSSN Records 1.65 Billion Cybersecurity Traffic Anomalies in 2021 - ANTARA News." *Antara News.* https://en.antaranews.com/news/214077/bssn-records-165-billion-cybersecurity-traffic-anomalies-in-2021 (August 14, 2022).

Nugraha, L. K., & Putri, D. A. (2016). *Mapping the Cyber Policy Landscape: Indonesia.* London. https://www.gp-digital.org/wp-content/uploads/2017/04/mappingcyberpolicy_landscape_indonesia.pdf.

Paterson, T. (2019). "Indonesian Cyberspace Expansion: A Double-Edged Sword." *Journal of Cyber Policy* 4(2): 216–34. https://doi.org/10.1080/23738871.2019.1627476.

Ripsman, N. M., Taliaferro, J. W. & Lobell, S. E. (2016). *Neoclassical Realist Theory of International Politics.* New York: Oxford University Press.

Ritchie, J. (2003). "The Applications of Qualitative Methods to Social Research." In *QUALITATIVE RESEARCH PRACTICE: A Guide for Social Science Students and Researchers,* eds. Jane Ritchie and Jane Lewis. London: SAGE Publications Ltd.

Rizal, M., & Yani, Y. (2016). "Cybersecurity Policy and Its Implementation in Indonesia." *JAS (Journal of ASEAN Studies)* 4(1): 61.

Rose, G. (1998). "Neoclassical Realism and Theories of Foreign Policy." *World Politics* 51(1): 144–72.

SAFE net. (2020). "Analisis Peraturan Menteri Komunikasi Dan Informatika (Permenkominfo) No. 5 Tahun 2020 Tentang Penyelenggaraan Sistem Eletronik Lingkup Privat." *SAFE net.*

Sanjaya, A. R., et al. (2021). Southeast Asia Freedom of Expression Network (SAFEnet) *Laporan Situasi Hak-Hak Digital Indonesia 2020: Represi Digital Di Tengah Pandemi.* Denpasar. https://koran.tempo.co/read/cover-story/459058/tahun-represi-digital.

Segal, A. (2020). "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace." In *An Emerging China-Centric Order: China's Vision for a New World Order in Practice,* ed. Nadège Rolland. Washington: The National Bureau of Asian Research, 85–100. https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/.

Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. (2012). "An Overview of the Development Indonesia National Cyber Security." *International Journal of Information Technology & Computer Science (IJITCS)* 6: 106–14.

Shahbaz, A., & Funk, A. (2020). Freedomhouse.org *FREEDOM ON THE NET 2020.* https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow.

Tan, J., Tee, W. X., Parsons, A., & Radlett, A. (2021). Interpol *Asean Cyber Threat Assessment 2021.* https://www.interpol.int/content/download/16106/file/ASEANCyberthreatAssessment2021-final.pdf.

Tashia. (2016). "Kebijakan Keamanan Dan Pertahanan Siber – Ditjen Aptika." https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/ (August 14, 2022).

The White House. (2018). "National Cyber Strategy of the United States of America." (September): 1–40. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf%0Ahttps://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.

Tilly, C. (1990). *Coercion, Capital, and European States: AD 990 - 1990.* Oxford: Blackwell Pub. http://www.ncbi.nlm.nih.gov/pubmed/11445135%5Cnhttp://www.ncbi.nlm.nih.gov/pubmed/16914980%5Cnhttp://www.ncbi.nlm.nih.gov/pubmed/18381770%5Cnhttp://www.ncbi.nlm.nih.gov/pubmed/11322980%5Cnhttp://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2323975&t.

VOI. (2020). "APJII: Pandemi COVID-19 Buat Pengguna Internet Di Indonesia Meningkat Hampir 200 Juta." https://voi.id/teknologi/19331/apjii-pandemi-covid-19-buat-pengguna-internet-di-indonesia-meningkat-hampir-200-juta (August 14, 2022).

Wijayaatmaja, Y. P. (2021). "Soal Kebocoran Data BPJS Kesehatan, Polri Dalami Peran IT." *Media Indonesia.* https://mediaindonesia.com/politik-dan-hukum/409284/soal-kebocoran-data-bpjs-kesehatan-polri-dalami-peran-it (August 14, 2022).