DEVIANCE JURNAL KRIMINOLOGI
Volume 8 Nomor 2 Desember 2024
Hal: 109-131
DOI: http://dx.doi.org/ 10.36080/djk.3496

Cyber Espionage in Indonesia: Legal Challenges and The Role of Institutions in the Digital Era

Fahlesa Munabari[1], Eko Daryanto[2], Stanislaus Riyanta[3], Margaretha Hanita[4]
[1234]National Resilience Studies, School of Strategic and Global Studies,
Universitas Indonesia
Jakarta, Indonesia
fahlesa.wisa41@ui.ac.id

Abstract: In this digital era, cyber espionage is a serious threat to countries around the world, including Indonesia. This study probes the legal framework governing cyber espionage, especially the challenges and opportunities for law enforcement it faces and its development. Through a qualitative methodology based on institutional theory, this study reveals that the existing legal framework, both internationally and nationally is still not sufficient. Lack of legal clarity and inconsistencies, particularly The Electronic Information and Transactions Law (ITE Law) and Penal Code (KUHP) complicate matters. Other contributing factors to poor law enforcement include limited institutional capacity resulting in the lack of well-trained human resources, insufficient technological infrastructure, and inter-agency collaboration. The process of isomorphism, which is understood in institutional framework as imitation of best practices implemented by other countries to cope with cyber espionage, does not always work because each country has different contexts and needs. This study shows that most literature in cyber espionage underscores the need for comprehensive legal reform, improvement of institutional capacity, quality of cooperation, and better understanding of the role of non-state actors in building an effective cyber security system in Indonesia.

Keywords: Cyber Espionage, Cyber Security, Cyber Resilience, Cyber Legal Framework, Institutional Theory, Indonesia

Abstrak: Dalam era digital ini, spionase siber merupakan ancaman serius bagi negara-negara di seluruh dunia, termasuk Indonesia. Penelitian ini mengkaji kerangka hukum yang mengatur spionase siber, serta tantangan dan peluang yang dihadapi dalam penegakan hukum dan perkembangannya. Melalui metodologi kualitatif yang berbasis pada teori institusional, penelitian ini mengungkapkan bahwa kerangka hukum yang ada, baik di tingkat internasional maupun nasional masih belum memadai. Kurangnya kejelasan dan ketidaksesuaian hukum, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP) semakin memperumit situasi. Faktor lain yang berkontribusi terhadap lemahnya penegakan hukum termasuk kapasitas institusional yang terbatas, yang mengakibatkan kurangnya sumber daya manusia yang terlatih dengan baik, infrastruktur teknologi yang tidak memadai, dan kolaborasi antar lembaga yang kurang efektif. Proses isomorfisme, yang dipahami dalam kerangka institusional sebagai peniruan praktik terbaik yang diterapkan oleh negara lain untuk menghadapi spionase siber, tidak selalu berhasil karena setiap negara memiliki konteks dan kebutuhan yang berbeda. Penelitian ini menunjukkan bahwa sebagian besar literatur dalam spionase siber menekankan perlunya reformasi hukum yang komprehensif, peningkatan kapasitas institusional, kualitas kerja sama, dan pemahaman yang lebih baik tentang peran aktor non-negara dalam membangun sistem keamanan siber yang efektif di Indonesia.

Kata Kunci: Spionase Siber, Ancaman Siber, Ketahanan Siber, Teori Institusionalisme, Kerangka Hukum Siber, Indonesia

Introduction

In a world where we rely on technology for everything from commerce to national security, cyber espionage is an ever more pressing and complicated problem. Advancements in information technology have led to the development of new methods and tools that facilitate espionage, and these are often not easily detected or responded to (Ziolkowski, 2013, p. 12). Cyber espionage, or the illicit collection of information via computer networks, poses a threat to national security as well as to economic and political stability. Incidents in major countries including the United States, Russia, and China have shed light on weaknesses in transport networks, critical infrastructure, and sensitive data. It is important to know how the existing legal framework could respond to the cyber espionage, especially in Indonesia, where the development of regulations and institutional capacity is still underway.

This becomes even more problematic considering that Indonesia, like many other countries, currently lacks appropriate regulations to combat cyber espionage threats. Even with the passage of Law No. 11 of 2008, also known as the Electronic Information and Transactions Law (ITE Law), there are still legal loopholes that cybercriminals could exploit. In order to promote electronic commerce and give participants in e-commerce legal protection, Indonesia's ITE Law governs electronic information and transactions. It covers many things, such as the legality of electronic signatures, protection of electronic data, and penalties for cybercrime-related crimes. Also, challenges include limited public and law enforcement understanding and awareness of the risks and impact of cyber espionage. This environment facilitates the acquisition of strategic knowledge and sensitive data by irresponsible parties through cyberattacks. Hence, it is mandatory to focus on the existing legal framework and the way legal institutions can tackle these challenges.

This study aims to explore the legal framework for cyber espionage by identifying challenges and opportunities for law enforcement at the international and national level using Indonesia as a case study. This study reviews literature in the ways in which international and Indonesia’s legal framework deals with the evolving dynamics of cyber espionage This study addresses the following research questions: “How can the existing legal framework in Indonesia address the challenges of cyber espionage, and what factors affect law enforcement effectiveness in this case?”

By investigating the Indonesian legal framework governing cyber espionage—an area that has not gotten much scholarly attention—this study adds to the body of current material. More specifically, it addresses the gap in understanding how Indonesia's legal and institutional capacities confront the evolving challenges of cyber espionage, particularly in the absence of widely agreed-upon and harmonized international norms. It can help inform better policy for combating the threats of cyber espionage. Through exploring the current hurdles, it is anticipated that such research can suggest beneficial implications for policymakers and law enforcement authorities to devise more robust and adaptive solutions to advancements in technology and espionage methods. Furthermore, such research can augment literature on law and cyber security, and promote public awareness regarding cyber espionage.

This research employs a qualitative methodology, with literature study is used as the primary approach. We systematically collected data by searching the relevant literature using keywords such as "cyber espionage," "cybercrime," "ITE Law," and "Penal Code (KUHP)". Journals, articles, and books about relevant issues were pulled from several academic databases. Using institutional theory to analyze the process of data analysis, it was possible to allow for a deeper insight into understanding how institutions can encompass and set the parameters for the legal frame of cyber espionage (Libicki, 2017, p. 5). This theoretical perspective helps us identify the dynamic relationship between law, policy, and law enforcement practices, particularly in the face of cyber threats.

The literature review reveals that cyber espionage law is a relevant issue in the digital age. International law does not typically govern espionage in an explicit manner, which many countries view as a permissible element of international relations (O'hara, 2010, p. 20). Yet, as the threats from cyber espionage escalate, the demand for clearly articulated legal norms is emerging (Weissbrodt, 2013, p. 15). The study further highlights the key role that institutional capacity plays in law enforcement, where challenges are evident in terms of trained human resources and sufficient infrastructure to properly deal with cyber espionage (Amer, 2024, p. 10; Pun, 2017, p. 22) Indeed, the challenge of international cooperation is one of the more prominent issues arising, as many countries have differing interests in the field of cyber security (Buchan, 2016, p. 8). Skinner (2013) argues that the existing legal system is struggling to cope with advancements in technology by necessitating a more flexible legal framework to adjust to rapid changes in the cyber domain (p. 30), while Yoo (2015) emphasized the need to adopt similar policy paradigms (p. 18).

Employing the framework of institutionalism, this article analyzes the state of the law that relates to cyber espionage both internationally and in Indonesia. It explores the difficulties facing law enforcement and suggest opportunities that could maximize their efficacy. Finally, the article concludes with recommendations for improved policy responses to cyber espionage threats. This article demonstrates a trend in literature in cyber security that supports ways to effectively combat cyber espionage in Indonesia by holistically reforming legal framework concerning cyber espionage and being responsive to contemporary technological developments. Human resource capacity building at the cyber domain; inter-agency collaboration and information sharing; and public awareness are other measures that need consideration to address this scenario. A similar level of international cooperation and dedication to putting in place clear and effective international regulations to ensure national security in a digital age is also necessary.

Methods

This study uses a qualitative method with literature review approach to explore the legal framework of cyber espionage in Indonesia, the challenges and opportunities in law enforcement, and the research trend in legal studies on this issue. The complexity involved in the cyber espionage issue, consisting of intertwined legal, technological, and social factors, influences the selection of a qualitative approach. This allows for more nuanced exploration and richer contextual interpretation than is possible with quantitative approaches, resulting in a deeper understanding. A literature review was selected for this study because, when conducted effectively, it offers a comprehensive, all-inclusive picture of the issue and the development of an issue, in-depth coverage of its context, and highlights differing perspectives.

The data collected was systematically conducted through the search for relevant literature, similarities to the keywords "cyber espionage," "cybercrime," "ITE Law," "Penal Code" and relevant terms in international law. Academic databases (eg, Google Scholar, University of Indonesia Library Database) were used to search journals, articles, and books discussing related issues. This process involved strict literature selection (relevant topics, reputable sources, methodological quality, information completeness, and data currency). Only literature fitting these inclusion criteria were employed in analysis. Apart from scholarly literature, the data sources for this study also included relevant legislation in Indonesia, including the ITE Law and Penal Code.

The data was analyzed through the framework of institutionism theory acting as the main analytical lens. This approach enables a unique understanding of the significant role of formal institutions (such as states, laws, and international organizations) and informal institutions (such as societal norms and cultural practices) in regulating and defining the legal boundaries of cyber espionage. This study adopts an institutional perspective to explore the impact of global and local norms on the behavior of actors. It assesses the ability of Indonesian institutions to address such challenges, the effectiveness of inter-agency cooperation, and the presence of institutional isomorphism in the creation and implementation of laws.

This means a deep contextual understanding of the world and how it interacts with data, but not necessarily raw predictive accuracy. Data collection and thematic analysis of the data sets was carried out to identify emerging themes and patterns. Moreover, the institutional theory framework is utilized to analyze these themes and patterns in a more in-depth manner, resulting in cohesive interpretations of the identified themes that substantiate the research conclusions. This includes descriptions of findings, thematic analysis, and interpretations regarding the research questions. The findings of the study are re-connected to the theory and literature to establish the credibility of the results.

Theoretical Framework

Institutional Theory: Definition and Basic Concepts

Institutional theory is recognized as a highly influential approach in the social sciences, particularly in the areas of public policy analysis, international relations, and organizational studies. This framework highlights the impact of institutions on actor behavior within social systems. Institutions encompass not only formal structures but also norms, values, and practices that shape interactions between individuals and organizations. Consequently, institutions serve as a guiding framework for individual and societal behavior. Institutions can be understood as rules, norms, and practices that shape individuals and groups' behavior. As North (1990, p. 3) defines them, institutions are essentially "the rules of the game in a society" governing social interactions. This means that institutions include not only laws, policies, social practices, and cultural practices. Formal institutions, including laws and regulations, as well as informal institutions, including social norms and traditions, are both critical frameworks for minimizing uncertainty in social interactions. Institutions therefore serve as a distinct class of map, one that provides actors with guidance on how to behave given the uncertainty that complex and dynamic environments engender.

Institutional theory emerged as a critique of conventional social science approaches that primarily focus on individual behavior and economic factors as the main influences on decision-making. This theory posits that human and organizational behavior cannot be fully understood without considering the institutional context in which they operate. Interestingly, institutional theory encompasses multiple streams, offering potentially valuable insights into how institutions function within our specific context and historical experiences. One key thing here is what we call historical institutionalism, which indicates the impact of history or context on institutions.

According to Amenta & Ramsey (2010, p. 45), institutions are influenced not only by modern day considerations but also by historical legacies that shape both present actions and future frameworks. This same approach usually uses longitudinal analysis to capture how institutions change over time. Moreover, we can also argue that institutions move toward other institutions over time whereby they increasingly become similar, as explained by the theory of isomorphism pioneered by DiMaggio and Powell (1983, p. 147). They consider three kinds of isomorphism to prevail: coercive, mimetic, and normative. Constructed from the elements of coercive and mimetic isomorphism, coercive isomorphism refers to a scenario in which institutions face pressures to conform to national and international norms. Normative isomorphism refers to the impact of professional norms and values that guide the conduct of organizations.

The restraining and enabling resources of institutions are, moreover, shaped by the norms and values present within institutions that affect the policy-making process. It explains public policy as the result of the interaction of actors with different interests and values (Sabatier 1988, p. 129). In this respect, institutions are arenas of interaction and negotiations where these actors seek to reach agreement. In addition, institutions also affect the implementation of policy. Policy implementation is often dependent on how well policy initiatives align with existing institutional structures (Pressman and Wildavsky 1973, p. 4).

Putting in place the policies above may not be possible if institutions do not support them. Mostly, change at institutions is multi-faceted and highly contextual. Diermeier & Krehbiel (2003, p. 1) indicate that institutional change can be accomplished by two different mechanisms: incremental change or radical change. Gradual change tends to happen in response to unforeseen environmental changes that allow institutions to adjust without changing their fundamental building blocks. In contrast, true change is often catalyzed by major crises or external pressures, resulting in fundamental reforms in institutions, often accompanied by shifts in basic norms and values to institutions' context in cyber security.

Institutional theory can be effectively applied to cyber security. Dewar (2017, p. 15) illustrates how international norms in cyber security, supported by various international organizations, can guide state behavior in response to cyber threats. Major powers play a crucial role in establishing new cyber security norms where necessary. Finnemore & Hollis (2016, p. 5) describe these states as "norm entrepreneurs" who leverage their influence and diplomacy to convince other states to change their policies. Jeyaraj & Zadeh (2020, p. 10) note that significant cyberattacks often lead to shifts in cyber security policies, indicating that institutions adapt in response to environmental demands.

Assessing public policies and different international relations aspects through the lens of institutional theory is a strong framework for analyzing social and political dynamics. Focusing on the importance of institutions in shaping the behavior of actors, this theory allows of the articulation of how norms, values, and practices affect social interactions. This knowledge is valuable for understanding how institutions shape responses to new threats and changes within institutions can influence future policies. Mutual assistance in addressing issues between states (e.g. cyber capabilities), where collaboration in making better policies can result from institutions, is extremely important (Ruohonen & Leppänen, 2016, p. 20).

The institutional theory sheds light on the relationship between institutions and the implications they hold for the development of policies, thereby also providing useful lens through which the wider field of action in facing cyber espionage and wider cyber challenges can be restructured. Policymakers and other relevant actors would be wise to consider these institutional factors as they endeavor to navigate the cyber security minefield in our increasingly interconnected world. Institutional theory aims at elucidating the mechanisms of institutional development, providing a lens through which we can understand how legal structures adapt in response to the complex landscape of cyber threats – a prevailing theme in the evolution of cyber security laws and policies across the globe.

Institutional Theory: Approaches and Perspectives

Institutional theory is one of the most important theories used for analysis in social and political areas, particularly in the field of public policy and international relations. An emphasis on institutions — formal and informal — and their impacts on the behavior of actors in social systems. In this regard, institutions should also not only be seen as bestow, but also with the norms, values, and practices that regulate the relations of individuals and organizations that use them. How these institutions work can best be imagined as a framework which helps guide how the different parts of society -- be they individuals or collectives (think corporations) -- behave.

Historical institutionalism, one of the main strands within institutional theory, highlights the significance of historical context in the formation of institutions and policies. Amenta & Ramsey argues that it is not just current factors that form institutions but also historical consequences that shape present choices and policies (2010, p. 45). At this juncture, longitudinal analysis is common to understand the way institutions grow and how changes in social and political contexts affect those institutions. This camp also shares a notion called "path dependency", where policies and decisions made previously restrict options in the future. According to Diermeier & Krehbiel (2003, p. 1), policy change within institutions is often incremental but can also be initiated by major events that radically shift policy vectors. Analyzing political institutions in response to cyber threats may help shape policies.

Moreover, DiMaggio and Powell (1983, p. 147) proposed another major concept of institutional theory, institutional isomorphism. They delineate three forms of isomorphism: coercive, mimetic, and normative. Coercive isomorphism happens when institutions are compelled to comply with certain norms based on external pressures from other actors, such as governments or international organizations. This, for example, includes countries being forced to implement certain cyber security policies under pressure from international organizations or alliances (eg. NAT): The second form of isomorphism is mimetic, which takes place when institutions copy best practices of other institutions as a means of reducing uncertainty. In this context, countries may replicate what has been successful in other countries around cyber security policies. On the other hand, isomorphism refers to the effect of professional norms and ethics that bind institutional conduct.

Norms that develop in the international sphere can shape how countries design their cyber security plans. Similarly, the constructivism`s angle in institutional theory is important. This perspective highlights that institutions are socially constructed through social interaction and the signification process. According to Finnemore & Hollis (2016), social norms and international norms and their social construction can be explained in terms of the interaction processes among different actors. Certain actors especially major powers are seen as "norm entrepreneurs" which through times seek to shape new norms on specific issues, including cyber security. Norm entrepreneurship is a vital process that brings new issues to the interest of the international system and determines how they should be perceived. For example, United States-led efforts have aimed to create international norms that limit cyber espionage for commercial purposes. When they are able use the right language and frame the problem effectively, they gain attention and can ultimately win the support of other states to either adopt or support these norms (Finnemore & Hollis, 2016, p. 5).

Institutions also structure the growth of public policy. A good part of that is not only about a decision-making framework but also about agenda-setting and policy processes. In this context, institutions can serve as “gatekeepers” that decide the issues that most deserve attention and funding. Policy agenda setting, according to Kingdon (1995, p. 3) is the product of the interplay between three categories of streams: problems, solutions, and politics. In this sense, institutions facilitate the linkage of these three strains, allowing certain issues to receive increased consideration. But within institutions, norms and values also shape the policy-making process. According to Sabatier (1988, p. 129), public policies evolve when the interactions of the different actors with different interests and values come across. To this end, institutions function as spaces in which these actors meet and negotiate their interactions, aiming to find agreements.

Institutions also shape the implementation of policies. Implementation of policies is contingent on the institutional structures that they create, and therefore the formulation of policy must be aligned with its implementation (Pressman & Wildavsky, 1973, p. 4). If the institutions fail to support the proposed policies, their implementation may also be hampered. Change in an institution is a multifaceted phenomenon and is frequently affected by an array of elements. There are two mechanisms for institutional change, these are incremental change and radical change (Diermeier & Krehbiel, 2003, p. 1). Incremental change often responds to unknown environmental change, which allows institutions to adjust without modifying underlying architectures. Emphatic change, on the other hand, is borne out of great crises or external faculties of power that can genuinely reframe institutions. It is also often framed through minimums of norms, values, and ever-changing tensions. Dewar (2017, p. 15) illustrates how global cyber security norms established by various international institutions shape state responses to cyber threats. Additionally, Jeyaraj & Zadeh (2020, p. 10) argue that major events, like significant cyberattacks, are catalysts for changes in cyber security policies, highlighting institutional growth through experience. Therefore, institutional theory provides a robust analytical framework for examining processes in public policy and international relations.

This theory helps us understand how norms, values and practices shape social interactions by emphasizing the role of institutions that underline actor behavior. The institutional theory can be helpful in the context of cyber security as it allows for an analysis of how institutions can contribute to the response to new threats as well as how changes within institutions might further influence future policies on cyber security. Thus, the institutional theory is not just relevant for everyday policy analysis but also by necessity in determining how actors in the international system engage with and adapt to constantly changing challenges.

Institutional Theory and Cyber Espionage

As the world becomes more and more digital, one of the most pressing threats facing nations is cyber espionage. Cyber espionage, the illegal gathering of information in order to illicitly exploit it, poses a threat to national security, economic, and political stability. Institutional theory is helpful in allowing us to deliberate the influence of institutions in the responses to the cyber espionage threat as well as the potential of international norms in the behavior of states.

Cyber espionage is an act performed by states, organizations, or individuals seeking strategic, economic, or political advantages. Recently, there has been a notable shift, with an increase in cyberattacks focused on espionage. International institutions in this regard are important because they help outline norms and policies that guide what states can do regarding cyber espionage. Dewar (2017, p. 15) shows how the concept of international norms in cyber security, as proposed by various international organizations, can influence how states respond to cyber threats. An international treaty such as the Budapest Convention on Cybercrime, adopted by the Council of Europe in 2001, also helps bring countries together to cooperatively combat cybercrime like espionage.

According to the institutional theory, the behavior of actors within social systems is shaped by both formal and informal institutions. As part of the framework of cyber espionage, international institutions like NATO, the EU, and the UN also create norms and policies to regulate the behavior of states. NATO, for example, has established a cyber security strategy, which includes cooperation between states to improve resilience against cyberattacks and informational espionage threats (Burton, 2015, p. 10). Institutions also serve as “gatekeepers” that set the agenda for which issues get attention and resources. Policy agendas are the result of the interaction of three streams: problems, solutions, and politics (Kingdon, 1995, p. 3). In this sense, institutions act as boundaries in connecting these three streams, meaning issues regarding cyber espionage can begin to be properly accounted for. In particular, major cyberattacks (e.g. the attack on Estonia’s critical infrastructure in 2007) inspired countries to increase cyber security collaboration; to develop more stringent anti-cyber espionage policies.

In the field of cyber espionage, the idea of institutional isomorphism, as outlined by DiMaggio and Powell (1983, p. 147), can also be of relevance here. They present three kinds of isomorphism: coercive, mimetic, and normative. Coercive isomorphism takes place when institutions are compelled to follow specific norms through external pressures, including those from governments or international organizations. In this context, states might use pressure from international organizations or alliances, such as NATO, to adopt certain cyber security policies. Mimetic isomorphism occurs when these institutions copy best practices from other institutions to alleviate uncertainty. Here, countries can imitate the cyber security policies of successful countries that deal with espionage. On the other hand, normative isomorphism is explained by the impact of professional norms and ethics that influence institutional behavior. In this context, the development of norms within the international community can impact the way in which states craft their cyber espionage policies.

The constructivist aspect of institutional theory provides valuable insights into the formation of norms related to cyber espionage. Finnemore & Hollis (2016) demonstrate that international norms and social practices evolve through interactions among various actors. In this context, influential actors, such as major powers, serve as "norm entrepreneurs" who advocate for new norms on specific issues, including cyber espionage. These norm entrepreneurs are crucial in introducing new topics to the international agenda and shaping perceptions of these issues. For instance, the United States has actively worked to establish international norms against cyber espionage for commercial gain by using appropriate language and framing the issue in a way that attracts attention and support from other countries (Finnemore & Hollis, 2016, p. 5).

Failures within institutions often create a challenging path influenced by numerous factors. Diermeier & Krehbiel (2003, p. 1) define two key mechanisms of institutional change: change can be incremental or radical. Should the current status quo become fundamentally compromised, gradual shifts ensue as institutions respond to unexpected degrees of environmental adaptation, finding their refined methods ultimately incompatible with legacy structures. In contrast, radical reforms are often responses to deep crises or external shocks to the system that cause the nature of institutions to shift fundamentally, including changes to the very norms and values that preside within them. Policy changes in regard to cyber espionage often arise in the wake of major events, such as large-scale cyber attacks. According to Jeyaraj & Zadeh (2020, p. 10), these events can motivate countries to further work together on cooperation in cyber security and the enactment of harsher laws against espionage.

The Law on Cyber Espionage: A Literature Review

Definitions and Legal Context

International law does not explicitly address espionage, which many countries consider a permissible practice in the realm of international relations. Nonetheless, in light of the growing risk of cyber espionage, the necessity of clearer legal standards for these new phenomena is apparent (O’hara 2010, p.20). In this way, cyber espionage should be treated as a serious threat, because it is a more powerful and destructive form compared to traditional espionage (Skinner, 2013, p. 30).

In the context of cyber espionage law, a major distinction needs to be drawn between espionage conducted by states and that of non-state actors. State espionage is commonly understood as a component of foreign policy and national security strategy, while espionage perpetrated by individuals or non-state groups can be framed as criminogenic activity (Weissbrodt, 2013, p. 15). This poses challenges for law enforcement because states often hesitate to take effective action against espionage conducted by other states, even when such activities are detrimental to their national interests (Buchan, 2016, p. 8). At the international level, there is a dispute over whether cyber espionage performed by other nations constitutes a breach of international law. According to some researchers, espionage actions violating the sovereignties of other states should be regarded as breaches to the international law, particularly if such actions result in long-term economic injury (Banks, 2016, pg 25). Hence, there is a need to create an international legal instrument that could help regulate cyber espionage and clarify state responsibilities in this regard (Libicki, 2017, p. 12; Weissbrodt, 2013, p. 15).

Regarding domestic law, a few countries have created laws governing cyber espionage. For instance, they note that the US Economic Espionage Act criminalizes the theft of trade secrets yet fails to meaningfully enforce this law against foreign actors, because enforcement of laws generally becomes difficult when jurisdiction falls beyond the domestic sphere (Amer, 2024, p. 10; Pun 2017, p. 22). Conversely, states such as China and Russia adopt an alternative methodology, often leveraging cyber espionage as a mechanism for geopolitical advantage (Yoo, 2015, p. 18).

Challenges in Law Enforcement

One of the primary issues associated with the enforcement of laws against cyber espionage relates to jurisdiction and state responsibility. Some States like China, engage in cyber espionage activities against others; unfortunately, they might not be prosecuted due to the absence of international cooperation and legal ambiguities (Weissbrodt, 2013, p. 15; Buchan, 2016, p. 8). Moreover, the differences in the legal systems of the various states are barriers for the law enforcement too. Because countries have different legal systems, the definition, methods used, and punishment of cyber espionage can differ that can create confusion and uncertainty in law (Skinner, 2013, p. 30).

Some states might consider cyber intelligence an accepted activity that falls within the bounds of competing with one another in the international arena, whereas others might consider it to be a grave breach of international law (Yoo, 2015, p. 18). A case in point is large corporations being targeted for cyber espionage. There are also laws concerning data protection and trade secrets, but enforcement remains difficult where the perpetrators and their locations are not easily identifiable (Amer, 2024, p. 10). Additionally, because of reputation concerns, many firms do not disclose cyber espionage incidents, and the data are not available for law enforcement purposes (Pun, 2017, p. 22).

Conducting cyber espionage is also done through advanced and unknown way such as the use of malware and phishing attack, which is generally difficult to prove or identify before the court (O'hara, 2010, p. 20). This multi-layered complexity arises from the challenges forensic investigators face in proving that a specific cyber espionage operation occurred, as perpetrators may have access to potential evidence and can easily delete or conceal it (Skinner, 2013, p. 30). Additionally, international cooperation faces challenges due to conflicting interests among states in the field of cyber security. Many states are reluctant to actively engage in investigating or prosecuting cyber espionage cases involving actors from other countries (Buchan, 2016, p. 8). This complicates the development of effective and collaborative international laws to address cyber espionage.

International Law Approaches

Due to its greater reach and potential damage, some researchers hold that cyber espionage demands more serious attention than traditional espionage (Skinner, 2013, p. 30). Scholarship like Yoo (2015, p. 18), for example, indicates that acts of cyber espionage that violate the sovereignty of other states can at least in principle constitute such violations of international law, especially where such acts inflict significant economic harm (Banks, 2016, p. 25). In these circumstances, an international legal framework becomes important to govern cyber espionage. Others suggest revision of existing international legal norms (including those of sovereignty and non-intervention) to account for the risks associated with cyber espionage (Libicki, 2017, p. 12; Weissbrodt, 2013, p. 15).

Coupled with these, which is also mediated by verification and enforcement mechanisms, some specialists on international law suggest the establishment of multilateral treaties governing cyber espionage (Buchan, 2016: 8), mirroring existing treaties governing conventional weapons and weapons of mass destruction. These types of agreements may focus on enhancing transparency, increasing governmental information sharing capacity, and developing agreed-upon dispute resolution mechanisms that may alleviate tensions between affected nation-states participating in cyber intelligence (Amer, 2024, p. 10).

In addition, international organizations, such as the United Nations, should be involved in creating international standards and restrictions regarding cyber espionage. In this way, by including countries, technology companies, and civil society, a more effective and inclusive legal framework can be reached (Weissbrodt, 2013, p. 15). Some researchers also note the importance of teaching people at the international level how to avoid them and their dangers through education and training. Doing so can help countries to be more equipped to work together in addressing the challenges posed by cyber espionage (Libicki, 2017, p. 12).

Gaps in International Law

The absence of comprehensive international law governing cyber espionage is becoming increasingly critical. Despite existing legal rules for inter-state relations, international law fails to clearly address many aspects of cyber espionage, creating opportunities for malicious activities like data theft and the acquisition of sensitive information without clear legal repercussions (Banks, 2016, p. 25). A primary reason for this gap is that espionage, whether traditional or cyber, is not directly regulated by conventional international law. Since espionage is often viewed as part of a state's foreign policy, there is widespread reluctance among states to legally bind or directly address this practice (see Yoo, 2015, p. 18). As a result, cyber espionage acts are often not prosecutable in international courts, yet they can significantly harm the targeted states (O'hara, 2010, p. 20).

In addition, even where there are various international treaties governing various aspects of cyber security, not all of them address cyber espionage specifically. An example of this is the fact that data protection and privacy-based agreements often do not include acts of foreign state espionage (Libicki, 2017, p. 12). This calls for updates and more succinct international legal norms to adapt with the challenges of cyber espionage. Here, some scholars call for the international community to begin codifying a clearer and more comprehensive legal framework regarding cyber espionage. This acknowledgment led to the view that some cyber espionage activities can violate core norms of international law (sovereignty and non-interference) (Weissbrodt, 2013, p. 15) An such, clarity in legal norms constitute a step towards addressing the legal vacuum by establishing a stronger foundation for international prosecution of cyberespionage offenders. It is essential to consider the impact of emerging technologies such as artificial intelligence and big data analytics, which may exacerbate the legal gap. As cyber espionage techniques become increasingly sophisticated with advanced technology, there is a pressing need for a more adaptable and responsive legal approach (Skinner, 2013, p. 30). Consequently, developing a legal framework that can swiftly adapt to technological advancements and cyber espionage practices is imperative.

Results and Discussion

Cyber Espionage Legal Framework in Indonesia

Indonesia has enacted several cybercrime laws, including cyber espionage. The main reference for this is Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE). Based on Article 31 paragraph 1, the ITE law can impose sanctions on anyone who, intentionally and without rights, intercepts or taps information electronically (Dewi, 2022, p. 5). However, explicit regulations concerning cyber espionage are written only in Law Number 1 of 2023 on the matter of Penal Law (KUHP) concerning illegal interception and illegal data retrieval (Rusman & Kamaludin, 2024, p. 1580).

The ITE Law represents Indonesia's initial attempt to regulate cyberspace activities, providing a legal foundation for addressing actions that cause harm via information technology, particularly in relation to cyber espionage. However, despite offering a legal basis, researchers argue that the ITE Law has deficiencies in terms of definition clarity and precision. Terms such as "interception" and "unlawfully" are not clearly defined, which may affect law enforcement effectiveness (Hastri, 2021, p. 15). The enactment of Law Number 1 of 2023 concerning the Penal Code marked a significant development in Indonesian criminal law by including provisions on cyber espionage. Articles related to illegal interception and information acquisition offer a stronger legal basis for prosecuting cyber violations. Nevertheless, this progress is hindered by challenges in existing law enforcement and effective implementation (Pratama, 2023, p. 105).

Moreover, apart from the ITE Law and the Penal Code, several other regulations provide additional legal basis for cyber espionage in Indonesia. For instance, the protection of information and personal data is regulated under the Government Regulation Number 82 of 2012 regarding the Implementation of Electronic Systems and Transactions. In cyber espionage, where personal data and sensitive information are often the objects, this is essential. Sandy et al. (2023, p. 55) argue for the need to elevate sensitive data protection within the legal hierarchy to prevent the misuse of information.

Table 1: Strengths and Weaknesses of Indonesia's Cyber Espionage Legal Framework

Feature	Strengths	Weaknesses
ITE Law (2008**)**	Provides a legal basis for addressing cybercrimes, including data interception.	Lacks clarity in definitions (e.g., "access," "unlawfully"); insufficiently comprehensive to address complex modern cyber espionage techniques; difficult enforcement.
Penal Code (KUHP, 2023)	Includes articles on illegal interception and information retrieval, offering a more comprehensive legal basis for prosecution.	Still lacks a clear definition of "cyber espionage"; challenges remain in effective implementation and enforcement; ambiguities may hinder prosecution.
Government Regulation 82/2012	Addresses information security and personal data protection.	May not adequately address state-sponsored cyber espionage; insufficient to prevent misuse of information.

Feature	Strengths	Weaknesses
International Legal Framework	Some international norms exist (e.g., Budapest Convention); increasing calls for clearer standards.	Significant gaps exist; lack of harmonization and standardized norms; differing national interests and interpretations hinder global consensus; difficulty in cross-border enforcement.

Sources: Compiled from various relevant references in this article.

Challenges in Cyber Espionage Law Enforcement in Indonesia

In the era of rapidly evolving digital information, law enforcement of cyber espionage in Indonesia is facing various complex challenges. Among various challenges, one significant challenge is the scarcity of trained and competent human resources in cyber domain. Cases that involve information technology require not only understanding of the law but also deep technical skills to conduct effective law enforcement. Improved civil law enforcement tools in the cyber domain can be achieved through enhanced human resource capacity (Dewi, 2022, p. 20). When officers have not been sufficiently trained, they may not identify and address existing threats, which can result in enforcement failures.

In addition, the lack of appropriate infrastructure and technology are also major barriers. Many of Indonesia's law enforcement agencies do not yet have adequate access to the most up-to-date technologies needed to detect and analyze cyberattacks. According to Pratama (2023, p. 105), law enforcement will be unable to enforce the law without the right technological assistance. Sandy et al. (2023, p. 55) argue that building information and communications technology (ICT) infrastructure is an essential step in improving detection and response capabilities. As a result, without good infrastructure, law enforcement agencies will struggle to gather evidence and perform forensic analysis to support the effective prosecution of violations of law. Moreover, there is lack of integration among information systems of various government agencies that hampers the response against cyber espionage incidents.

On top of all these issues, weak coordination among various relevant governmental bodies like Indonesian National Armed Forces (TNI), National Intelligence Agency (BIN), and National Police (POLRI) further aggravates the problems. In the absence of synergy, pertinent information is not shared in a timely manner, leading them to formulate responses to e-crimes slowly. Sandy et al. (2023, p. 60) also highlight the importance of collaboration between the public and private sectors for creating a better cybersecurity ecosystem. Therefore, establishing strict protocols and policies for cooperation between law enforcement agencies is essential for improving investigations into cyber espionage incidents.

Even though multiple laws govern cyber espionage, countless researchers and legal practitioners argue that the existing regulations are insufficient. The existing regulation is generally dormant without any responsiveness to the rapidly advancing technology as well as the practices of cyber espionage. Accordingly, this creates gaps, weaknesses, or even loopholes in the regulation that are described by Susila and Salim (2020, p. 10) as being largely unresponsive. Therefore, amendments and updates in the suitability of the regulations are necessary to ensure that the law is capable of effectively addressing new threats.

Analyzing Cyber Espionage in Indonesia through an Institutional Lens

Employing institutional theory as the primary analytical framework, the following discussion highlights how both formal (such as government, legal bodies, and international organizations) and informal (such as social norms and cultural practices) institutions affect the legal framework, law enforcement, and overall responses to cyber espionage in Indonesia. Legal, technological, and social elements contributing to this issue have been extensively discussed in the literature as affecting, and being affected by, national security, economic stability, and public trust in Indonesia.

Due to the advanced nature of contemporary cyber technology, cyber espionage—which entails the unlawful acquisition of information through cyber methods for strategic or economic gain—poses a significant and evolving threat in today's digital era. Advancements in information technology have made it easier to carry out while making detection and mitigation more difficult. Examples of these are data theft at great scale, such as the Tokopedia data leak in 2020, when personal records of millions were misused by unauthorized persons (*CNN Indonesia*, 2020). Other real-world threats include monitoring of critical infrastructure — attacks that can impact electricity generation systems that can bring down the energy supply of an entire country. For example, WannaCry was a ransomware attack that crippled computer systems in multiple countries. Various other hacking methods, like malware (malicious software) and phishing, also target individuals and organizations. Private companies, government agencies, and public infrastructure have all fallen victim to attacks, with extremely high economic and reputational impacts. One example is ransomware attacks, which can halt company operations and result in heavy financial loss (Mohurle & Patil, 2017).

The law on cyber espionage at the international level is neither comprehensive nor universal. Most countries, especially developed ones, consider cyberespionage (especially initiated by other states) as acceptable behavior in the framework of geopolitical and economic competition. As the growing threats and their repercussions have triggered debates and demands for more transparent and effective legal standards, varying interpretations of cyber espionage, a divergence of national priorities and complex geopolitical dynamics are obstacles that remain in reaching a global consensus on the matter. Unfortunately, there are some international law experts who contend that the violation of a state's sovereignty through cyber espionage would breach international law if it has the potential of producing significant economic damage or undermining its national security and stability (Libicki, 2017, p. 12; Weissbrodt, 2013, p. 15).

The theft of intelligence or state secrets by other nations, such as alleged Russian infiltrations to hack critical infrastructures in various countries, is considered a severe act of aggression. However, there is a notable absence of a comprehensive and universally accepted international legal framework for cyber espionage. This issue is exacerbated by the lack of effective frameworks for judicial cooperation and extradition in transnational cases. The absence of standardized international laws also complicates the prosecution of offenders outside the victim state's jurisdiction (Susila & Salim, 2020, p. 10). Indonesia has enacted several laws to address these challenges. The ITE Law (Law No. 11 of 2008) serves as a strong legal basis for regulating crimes related to information technology, including eavesdropping and data interception. However, the definitions of many terms in the ITE Law, such as "interception" and "access," are vague or not clearly defined, which limits its comprehensiveness in addressing complex cyber espionage cases (Hastri, 2021, p. 15). Modern cyber espionage often employs sophisticated methods that may fall outside the ITE Law's jurisdiction (Ziolkowski, 2013, p. 12).

One significant issue with the ITE Law is its vague definitions of "interception" and "unlawfully," which complicate law enforcement, especially with advanced technology and elusive methods. The 2023 Penal Code (KUHP) includes new articles on illegal interception and information retrieval, aiming to provide clarity and a legal basis. However, challenges remain in the consistent implementation and regulation of these laws. Additionally, the ambiguous language in several articles and the lack of specific provisions on cyber espionage further complicate enforcement. Currently, the KUHP does not clearly define "cyber espionage," leading to prosecutions based on broad interpretations rather than strict legal definitions. Furthermore, Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions also promotes information security and personal data protection (Sandy et al., 2023; Susila & Salim, 2020).

In general, Indonesia's legal framework still does not fully accommodate these developments and is considered less responsive to the dynamics of technological developments and cyber espionage practices. Hence there is a need for periodic and continuous revision and update in the regulations. One of the theoretical perspectives that have been widely used to analyze the cyber espionage issues is institutional theory (Amenta & Ramsey, 2010; Dewar, 2017). At this juncture, the institutional theory shows how institutions, formal and informal, structure and influence actor behavior and social dynamics. This theory is elaborated in terms of cyber espionage as it explains the factors leading to the development of laws, enforcement mechanisms, and challenges as represented in the following aspects:

1. Norms and Regulations

In studying empirical phenomena in the context of cyber espionage, the analysis of norms and rules as it relates to institution is the clearest lens from which to understand how international and domestic norms govern the behavior of actors. In fact, the lack of clear, well-defined, and universal international norms leaves much to interpretation in the gray area, and cyber espionage is rarely seen as a breach of international law in this context, especially when it comes to strong states with larger capabilities and resources. China and Russia, for example, are accused regularly of engaging in cyber espionage for geostrategic gain, but they rarely suffer international sanctions. Such behavior highlights the impotence of international norms and regulations in tackling state-backed espionage. The broad interpretation of ambiguous norms in the ITE Law and Penalty Code in Indonesia makes the law difficult to enforce. The deficiencies are further aggravated by the lack of national-level legal harmonization and poor inter-agency coordination and response towards incidents of cyber espionage (Weissbrodt, 2013).

2. Institutional Capacity

Another important point through the lens of institutionalism is the limitation of institutional capacity in Indonesia. There is a shortage of trained and experienced human resources in the cyber domain such as digital forensics, intelligence analysis, etc., and deficiencies in infrastructure and technology (specialized software and hardware) that does not facilitate the effective implementation of law enforcement and responses against cyberattacks. Cyberattacks that are high in sophistication and low in visibility are often difficult for law enforcement agencies to detect and respond to, requiring specialized technologies and domain expertise that are not always available.

For example, without skilled digital forensics experts, investigations into complex cyber espionage cases may suffer and important traces of digital evidence may not be collected or analyzed properly. Poor training and education of the public about threats from cyber espionage compounds this issue. In this phase, an institutionalist analysis focuses on existing institutional capacities, available resources as well as internal and external factors reflecting the impact and performance of institutions to respond to cyber espionage risks. This will then be related to factors of institutional structure and bureaucracy within Indonesia itself, such as budgetary limitations, difficulties in coordinating between agencies, and, most importantly, a lack of effective planning and budgeting processes (Ohara, 2010; Buchan, 2016).

3. Inter-Agency Collaboration
As described by institutional theory, many agencies must work together to react to cyber espionage threats. Ineffective cooperation from agencies within the government (TNI, BIN, POLRI, BSSN) and across the public and private sectors delays responses to threats. Incident management is often hampered by the fact that relevant information is not shared quickly and efficiently. This highlights the importance of developing clear protocols and policies to enable more effective collaboration.

One of the examples is when the National Cyber and Crypto Agency (BSSN) coordination with the police does not run well, leading to inefficient and ineffective responses to cyber espionage cases. An institutionalist analysis examines the agency structures and processes, the interagency cultures of collaboration and barriers to collaboration. This may reflect the nature of cyber espionage, but the level of inter-agency cooperation in addressing cyber threats does depend on how the agencies differ in their interests and priorities. For instance, different priorities and focuses of security and law enforcement agencies can hinder investigations and prosecution of cyber espionage cases (Susila and Salim, 2020).

4. Institutional Isomorphism
The idea of isomorphism (coercive, mimetic, normative) helps explain how institutions tend to model themselves after one another. On the other hand, with cyber espionage, states are trying to learn from the laws and policies of other nations with better capabilities, especially those of developed countries with better infrastructures. However, the imitation process is not always successful as each country has different contexts and needs. As an example, Indonesia could be trying to copy-paste the cyber security strategy that the United States or Singapore could have, but copying and pasting these strategies need to be contextualized in Indonesia where the environment and resources are very limited. Institutionalist analysis looks at how isomorphism domestically shapes the two processes of law generation and law implementation on Indonesian legal and cyber espionage policy (Finnemore & Hollis, 2016).

5. Role of Non-State Actors
The institutional theory can be applied to understanding the position of non-state actors (such as private companies, civil society organizations, and intellectuals) concerning cyber espionage. Private businesses are often the targets of cyber espionage but can also range from actors carrying out espionage to actors targeted by it. For instance, state or non-state actors may pursue large technological

companies in Indonesia for their data theft or espionage. Non-governmental organizations can help improve awareness and policies. Civil society organizations, for example, can lobby for tougher, more transparent laws. Academics play a role in understanding this issue through researching and analyzing it. Academic research, for instance, can be a rich source of empirical knowledge to inform the design of policy responses. An institutionalist approach analyzes the interactions of state and non-state actors, from which the influence on legal framework and law enforcement of cyber espionage is examined (Dewar, 2017).

Conclusion

This paper analyzed the cyber espionage legal framework in Indonesia by taking a close look at the law enforcement challenges and opportunities and tracing it back to the international legal development. Using a qualitatively-based institutional theory perspective, this study exposed the complexity of the cyber espionage issue, which transcends the purely technical. Beyond being a mere contest of technology, cyber espionage offers a theatre of interactive legal, political, and social antagonisms, creating a vibrant and frequently unpredictable terrain.

The main research question of this article is, "To what extent does the existing legal framework in Indonesia adequately address the challenges posed by the phenomenon of cyber espionage and what factors determine the effectiveness of law enforcement in dealing with the phenomenon of cyber espionage?" — offers the insight that the current legal landscape, despite the recent introduction of the ITE Law and KUHP, is still ill-equipped to realize the complexities of cyber espionage threats. Ambiguities in definitions, unclear legal articles, and a lack of harmonization with international legal norms create a gray area that perpetrators exploit. But with major gaps in international law, the fact that even regulations governing cyber espionage remain widely unstandardized worldwide make things only worse. National interests, divergent interpretations, and complex geopolitics further obstruct international attempts to build consensus.

This study highlights that the challenges are not solely due to an evolving legal system but also stem from institutional capacity limitations. These include a lack of trained personnel and technological infrastructure, weak coordination among government agencies, and poor integration of information systems, all of which hinder the effective detection, investigation, and prosecution of cybercrimes. Ineffective coordination between law enforcement, the private sector, and civil society further delays responses to cyberattacks. Isomorphism, the practice of adopting successful strategies from other contexts, is not very effective since each country has different contexts and resources. Indonesia should develop strategies tailored to its unique circumstances and capabilities rather than imitating its neighbors. It is also important to consider the roles of non-state actors—private companies, civil society organizations, and academia. Effective cooperation and coordination among these entities can establish a robust and proactive legal framework.

A comprehensive and collaborative approach is needed to address the challenges of cyber espionage, which must involve legal, technological, social, and political dimensions. To build a strong and sustainable cyber security system in Indonesia, a holistic legal reform, institutional capacity revival, inter-agency coordination reinforcement, and a comprehensive understanding of non-state actors roles are needed. The responsiveness of human rights and ethical considerations in the cyber domain must also be addressed. By establishing clearer norms, strengthening capacities, and fostering strong collaboration within society, Indonesia will approach a more sovereign and secure cyberspace that better protects national sovereignty and national security in this digital era.

References

Amenta, E., & Ramsey, K. M. (2010). Institutional theory. *Handbook of politics: State and society in global perspective*, 15-39.

Amer, N. (2024). Espionage activities in the perspective of international law. *Journal of Law Science*, 6(1), 110-117.

Banks, W. C. (2016). Cyber espionage and electronic surveillance: Beyond the media coverage. *Emory LJ*, 66, 513.

Buchan, R. J. (2016). The international legal regulation of cyber espionage. In Osula, A.-M. & Rõigas, H. (Eds.), *International cyber norms: Legal, policy & industry perspectives* (pp. 65–86). NATO CCD COE Publications. https://eprints.whiterose.ac.uk/98791/10/Russell_The%20International%20Legal%20Regulatio

Burton, J. (2015). NATO's cyber defence: Strategic challenges and institutional adaptation. *Defence Studies*, 15(4), 297-319.

CNN Indonesia (2020). *Kronologi lengkap 91 juta akun Tokopedia bocor dan dijual*. 3 May. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual. (accessed 1 December 2024).

Dewar, R. S. (2017). Cyber security in the European Union: An historical institutionalist analysis of a 21st century security concern (Doctoral dissertation, University of Glasgow).

Dewi, M. C. (2022). Cyber espionage in national and global perspective: How Indonesia deals with this issue?. *International Law Discourse in Southeast Asia*, 1(1), 1-22.

Diermeier, D., & Krehbiel, K. (2003). Institutionalism as a methodology. *Journal of Theoretical Politics*, 15(2), 123-144.

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, 110(3), 425-479.

Jeyaraj, A., & Zadeh, A. (2020). Institutional isomorphism in organizational cybersecurity: A text analytics approach. *Journal of Organizational Computing and Electronic Commerce*, 30(4), 361-380.

Libicki, M. (2017, May). The coming of cyber espionage norms. In *2017 9th International Conference on Cyber Conflict (CyCon)* (pp. 1-17). IEEE.

Mohurle, S., & Patil, M. (2017). A brief study of WannaCry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), 1938-1940.

North, D. C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge University Press.

O'Hara, G. (2010). Cyber-espionage: A growing threat to the American economy. *Commlaw Conspectus*, 19, 241.

Pratama, Y. A. (2023). Legal framework publication of state secrets via cyberspace in Indonesia. *Constitutionale*, 4(2), 99-110.

Pun, D. (2017). Rethinking espionage in the modern era. *Chicago Journal of International Law*, 18(1), 10. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1727&context=cjil

Rusman, R., & Kamaludin, A. (2024). Investigation of cyber crime in the Indonesian legal framework. *Journal La Sociale*, 5(6), 1576-1586.

Sandy, M. R. A., Ras, A. R., Yusnaldi, Y., Widodo, P., & Suwarno, P. (2023). The impact of cyber espionage issue on maritime security cooperation between Indonesian National Police and Australian Federal Police. International Journal of Humanities Education and Social Sciences*, 3(2).

Skinner, C. P. (2013). An international law response to economic cyber espionage. *Conn. L. Rev.*, 46, 1165.

Susila, M. E., & Salim, A. A. (2020). Cyber espionage policy and regulation: A comparative analysis of Indonesia and Germany. *Computers & Electrical Engineering*, 81, 1.

Weissbrodt, D. (2013). Cyber-conflict, cyber-crime, and cyber-espionage. *Minn. J. Int'l L.*, 22, 347.

Yoo, C. S. (2015). Cyber espionage or cyberwar?: International law, domestic law, and self-protective measures. *Cyberwar: Law and Ethics for Virtual Conflicts* (Jens David Ohlin, Kevin Govern, Claire Finkelstein, eds., 2015), U of Penn Law School, Public Law Research Paper, (15-3).

Ruohonen, J., Hyrynsalmi, S., & Leppänen, V. (2016). An outlook on the institutional evolution of the European Union cyber security apparatus. *Government Information Quarterly*, 33(4), 746-756.