# Cyber Espionage Policy and Regulation: A Comparative Analysis of Indonesia and Germany

**Muh. Endriyo Susila*, Andi Agus Salim****

**DOI: https://doi.org/10.22304/pjih.v11n1.a6**

**Submitted: July 13, 2023 | Accepted: February 1, 2024**

**Abstract**

This study explores the policy and regulatory frameworks concerning cyber espionage within Indonesia and Germany. Given the considerable threats cyber espionage poses to national security and economic interests, it is crucial for nations to formulate thorough strategies to mitigate such risks. Through a comparative analysis of Indonesia and Germany—two countries with distinct geopolitical stances and methodologies regarding cybersecurity and espionage—the research delves into the legal, political, and technological factors influencing their cyber espionage policies. The methodology includes a comprehensive review of legislative measures, governmental strategies, and the response of institutions to cyber espionage in both nations. The objective is to discern the similarities, differences, and effectiveness of the policies and regulations of these countries. This comparison sheds light on the adequacy of Indonesian legislation in combating cybercrime, especially cyber espionage. The study reveals that Indonesia's legal infrastructure for cybercrime is markedly underdeveloped compared to Germany's, where stringent and well-articulated regulations are in place, facilitating precise and efficient management of cyber issues. Thus, the study underscores an urgent need for Indonesia to reform its cybercrime laws, focusing on cyber espionage, among other cyber threats, while continuing to enhance the quality of its human resources.

**Keywords**: cybercrime, cyber espionage, cybersecurity.

## A. Introduction

As technology evolves, it supersedes traditional forms of communication and information technology with newer, often more efficient, media.[1] Among the positive impacts is the enhancement of speed and convenience across various domains. For instance, technology facilitates business owners in revenue generation this is through the utilization of diverse marketing tools, including social media

[*] Lecturer of the Faculty of Law, Muhammadiyah Yogyakarta University, Jl. Brawijaya, Geblagan, Tamantirto, Kec. Kasihan, Kabupaten Bantul, Daerah Istimewa Yogyakarta 55183, S.H. (Diponegoro University), MCL. (International Islamic University), Ph.D. (International Islamic University), endriosusilo@umy.ac.id.

[**] Lecturer at the Faculty of Law, Jambi University, Jl. Jambi – Muara Bulian, KM. 15, Mendalo Indah, Kec. Jambi Luar Kota, Kabupaten Muaro Jambi, Jambi 36657, S.H. (Muhammadiyah Yogyakarta University), LL.M. (Asia University), agussalim.ndi@gmail.com.

[1] Catur Nugroho, *Cyber Society: Teknologi, Media Baru, dan Disrupsi Informasi* (Jakarta: Prenada Media, 2020), 9-11.

platforms.[2] Furthermore, innovative devices such as smartphones and tablets have simplified the way parents maintain contact with distant relatives.[3] Moreover, technology has empowered individuals to communicate with others globally, breaking geographical barriers and fostering global connectivity.[4]

However, the advent of new technologies introduces new challenges for society.[5] As reliance on information technology grows, the incidence of Internet-based crimes, commonly referred to as cybercrime, is anticipated to increase.[67] These criminal activities utilize information technology as a medium for execution. With technological advancements, the scale and impact of cybercrime are expanding swiftly, affecting individuals, groups, and nations alike.[8] Cyber espionage is an illicit activity that utilizes internet networks to surveil other entities by penetrating their computer networks. This form of crime often targets business competitors to access crucial documents or data stored within their computational systems.[9]

Additionally, cyber espionage frequently involves a nation acting as the perpetrator, aiming to steal vital and confidential information from another country. It represents a modern iteration of traditional espionage, conducted to gather sensitive data or intelligence from adversary nations. The information acquired is used to predict the actions of the opposing country, especially during conflicts, making such operations commonplace. The advancement in information technology has facilitated the ease and prevalence of wiretapping for espionage purposes across countries.[10] This form of cyber espionage has become increasingly widespread,

[2] Edna Maeyen Solomon and Aaron Van Klyton, "The Impact of Digital Technology Usage on Economic Growth in Africa," *Utilities Policy* 67 (2020): 3, https://doi.org/10.1016/j.jup.2020.101104.

[3] Michelle Drouin (et.al.) "How Parents and Their Children Used Social Media and Technology at the Beginning of the COVID-19 Pandemic and Associations with Anxiety," *Cyberpsychology, Behavior, and Social Networking* 23, no. 11 (2020): 732, https://doi.org/10.1089/cyber.2020.0284.

[4] Danping Lin (et.al.), "Strategic Response to Industry 4.0: An Empirical Investigation on the Chinese Automotive Industry," *Industrial Management & Data Systems* 118, no. 3 (2018): 591, https://doi.org/10.1108/IMDS-09-2017-0403.

[5] W.Z. Khan (et.al.), "Industrial Internet of Things: Recent Advances, Enabling Technologies and Open Challenges," *Computers & Electrical Engineering* 81 (2020): 1, https://doi.org/10.1016/j.compeleceng.2019.106522.

[6] M. Caldwell (et.al.), "AI-Enabled Future Crime," *Crime Science* 9, no. 1 (2020): 14, https://doi.org/10.1186/s40163-020-00123-8.

[7] Shipley, Todd G., and Art Bowker, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace* (Oxford: Syngress Publishing, 2013), 375.

[8] Harjinder Singh Lallie (et.al.), "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic," *Computers & Security* 105 (2021): 102248, https://doi.org/10.1016/j.cose.2021.102248.

[9] Maskun (et.al.) *Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional* (Makassar: CV Nas Media Pustaka, 2020), 27.

[10] Hafidz L. Botua, Chloryne Trie Isana Dewi, and R. Achmad Gusman Catur Siswandi, "Wiretapping on Submarine Communications Cable: Questioning Its Legality Amidst Long Standing Practice," *Padjadjaran Journal of International Law* 6, no. 1 (2022): 20–42, https://doi.org/10.23920/pjil.v6i1.772.

partly due to the inadequacy of regulations governing wiretapping activities. It is crucial to distinguish between espionage conducted through armed conflict and wiretapping-based espionage that occurs outside the context of physical warfare. The Indonesian government's lack of a definitive stance and comprehensive policy on cyber espionage underscores a significant shortfall in effectively addressing this issue.[11]

Wiretapping, particularly in the modern era, is regarded as a form of espionage due to its relatively low detection risk by the target, underscoring the inherent dangers associated with foreign espionage. It poses a significant threat to national security and defense by potentially causing harm and destabilization.[12] Instances of espionage include actions taken by the United States and Australia against the Indonesian government. Marciano Norman, the Head of the Indonesian State Intelligence Agency (*Badan Intelijen Negara*-BIN), reported that Australia had wiretapped phone conversations of several Indonesian leaders from 2007 to 2009.[13]

The phenomenon of espionage is not unique to Indonesia; other nations, including Germany, have encountered similar challenges. In 2020, Nobelium, a group associated with the Russian government, initiated an advanced phishing campaign targeting German government ministries and critical infrastructure entities. Through a combination of spear-phishing emails and supply chain attacks, APT29 successfully infiltrated systems, exfiltrating sensitive information such as government documents and strategic plans.[14]

Beyond governmental bodies, German corporations and research institutions have been the focus of Ocean Lotus, a cyberespionage group believed to be operating under the auspices of the Chinese government. Utilizing tactics such as spear-phishing attacks, malware, and phishing emails, Ocean Lotus aims to misappropriate intellectual property and trade secrets. In 2018, APT32 was implicated in a cyber assault on the German pharmaceutical giant Bayer, leading to the compromise of their confidential data.[15] The case underscores the intricate challenges presented by global competition in the digital age, where the advanced capabilities of information and communication technology can be harnessed by various actors, including espionage agents.

[11] Maharani Chandra Dewi, “Cyber Espionage in National and Global Perspective: How Indonesia Deal with This Issue?” *International Law Discourse in Southeast Asia* 1, no. 1 (2022): 9, https://doi.org/10.15294/ildisea.v1i1.56874.

[12] Romil Rawat (et.al.), “Artificial Cyber Espionage Based Protection of Technological Enabled Automated Cities Infrastructure by Dark Web Cyber Offender,” in *Intelligence of Things: AI-IoT Based Critical-Applications and Innovations*, Fadi Al-Turjman (et.al.) (ed.) (Cham: Springer International Publishing, 2021), 171.

[13] Hamdan Mustameer, “Penegakan Hukum Nasional Dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0,” *Jurnal Yustika: Media Hukum Dan Keadilan* 25, no. 1 (2022): 40–53. https://doi.org/10.24123/yustika.v25i01.5090.

[14] BBC News, “German Cyber Officials Defend Handling of Mass Data Attack,” accessed on January 5, 2019, https://www.bbc.com/news/world-europe-46768990.

[15] Vicky Ray and Kaoru Hayashi, “Tracking Ocean Lotus’ New Downloader, KerrDown,” accessed on February 1, 2019, https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/.

This scenario further reveals Indonesia's vulnerabilities as a potential espionage target, attributed largely to deficiencies in its legal frameworks.[16] Espionage facilitated by wiretapping and leveraging technology renders national borders irrelevant, thus blurring the lines of sovereignty. Sensitive information and data become accessible without spatial or temporal constraints, posing a significant threat to national sovereignty.[17] Consequently, critical questions arise regarding the adequacy of Indonesian law in addressing cyber espionage and the measures Indonesia is implementing to counteract such threats, which could potentially compromise the nation's defense and security stability.

Previously, there have been studies of cyberspace security. For instance, Iqbal and Jaya discussed the evolution of cybercrime in Indonesia alongside the existing regulations in place.[18] Raharjo (et.al.) emphasized the bureaucracy of law enforcement against cybercrime in Indonesia, especially the weaknesses of existing and integrated crime prevention models in the criminal justice system.[19]

In a more specific exploration of cyber espionage, Mustameer has conducted a study on National Law Enforcement and International Law on Cyber Espionage Crimes in the Society 5.0 Era. Mustameer elaborated on how cyber espionage poses a threat to defense and security in the Society 5.0 era and the readiness of Indonesia's international and national legal frameworks to confront such threats.[20] Another related study, conducted by Dewi, explored the legal dimensions of cyber espionage, including national and international cases and their legal frameworks.[21]

The present study seeks to compare Indonesia's legislative framework and its strategies in countering cyber-attacks, especially cyber espionage, with those of Germany. This comparison is pivotal to assessing the effectiveness of Indonesia's current legal regulations and strategies against cybercrimes. The choice of Germany as a comparative subject stem from its advanced status and frequent exposure to cyber-attacks from nations like Russia, China, North Korea, and others.

[16] Muhammad Iqbal and Nyoman Serikat Putra Jaya, "Development of Cyber Crime and Its Regulations in Indonesia," *International Journal of Social Science and Human Research* 4, no. 2 (2021): 143, https://doi.org/10.47191/ijsshr/v4-i2-04.

[17] Federica Cristani, "Economic Cyber-Espionage in the Visegrád Four Countries: A Hungarian Perspective," *Politics in Central Europe* 17, no. 4 (2021): 705, https://doi.org/10.2478/pce-2021-0037.

[18] Muhammad Iqbal and Nyoman Serikat Putra Jaya, 141-147.

[19] Agus Raharjo (et.al.), "The Legal Policy of Criminal Justice Bureaucracy Cybercrime," *BESTUUR* 10, no. 2 (2022): 105, https://doi.org/10.20961/bestuur.v10i2.64498.

[20] Hamdan Mustameer, "Penegakan Hukum Nasional Dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0," *Jurnal Yustika: Media Hukum Dan Keadilan* 25, no. 1 (2022): 46, https://doi.org/10.24123/yustika.v25i01.5090.

[21] Maharani Chandra Dewi, "Cyber Espionage in National and Global Perspective: How Indonesia Deal with This Issue?" *International Law Discourse in Southeast Asia* 1, no. 1 (2022): 1-22, https://doi.org/10.15294/ildisea.v1i1.56874.

Through this analysis, the study aims to highlight Indonesia's legislative shortcomings by using Germany's experience as a benchmark. This study employed normative legal methodology, utilizing a multifaceted problem approach that includes Statute, Conceptual, and Comparative Approaches. The legal materials supporting this study are categorized into primary and secondary types. Primary legal materials comprise statutory regulations and judicial decisions that serve as jurisprudence, while secondary legal materials encompass unofficial legal publications such as books, magazines, law journals, and pertinent legal research. The collection of legal materials is conducted through library research, with the processing of these materials adhering to deductive methods. The analysis within this study is performed using qualitative descriptive techniques for legal material analysis, which involve systematic and comprehensive interpretation to elucidate the research findings.

With the swift progression of cyberspace or the digital realm, criminal activities have transcended the physical boundaries to permeate the digital domain. While technological advancements yield positive outcomes, cyberspace remains susceptible to various forms of attacks, including viruses and hacking perpetrated by individuals or groups harboring malicious intentions.

Cybercrime has emerged as a significant challenge, primarily due to the difficulty in identifying perpetrators who often operate under the veil of anonymity. Specialized expertise is essential to navigate the complexities of cyberspace and detect cybercrimes effectively. The challenge of curbing these crimes has contributed to a consistent increase in cybercrime rates, as reported by the Indonesian State Intelligence Agency.

## B. The Phenomenon of Cyber Espionage

With the rapid progression of cyberspace or the digital realm, criminal activities have transcended the physical boundaries to permeate the digital domain.[22] While technological advancements yield positive outcomes, cyberspace remains susceptible to various forms of attacks, including viruses and hacking perpetrated by individuals or groups harboring malicious intentions.

Cybercrime has emerged as a significant challenge, primarily due to the difficulty in identifying perpetrators who often operate under the veil of anonymity. Specialized expertise is essential to navigate the complexities of cyberspace and detect cybercrimes effectively.[23] The challenge of curbing these crimes has

[22] Priyanka Datta (et.al.), "A Technical Review Report on Cyber Crimes in India," *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)* (2020): 269–270, https://doi.org/10.1109/ESCI48226.2020.9167567.

[23] Olena V. Sviatun (et.al.), "Combating Cybercrime: Economic and Legal Aspects," *WSEAS Transactions on Business and Economics* 18 (2021): 758, https://doi.org/10.37394/23207.2021.18.72.

contributed to a consistent increase in cybercrime rates,[24] as reported by the Indonesian State Intelligence Agency.

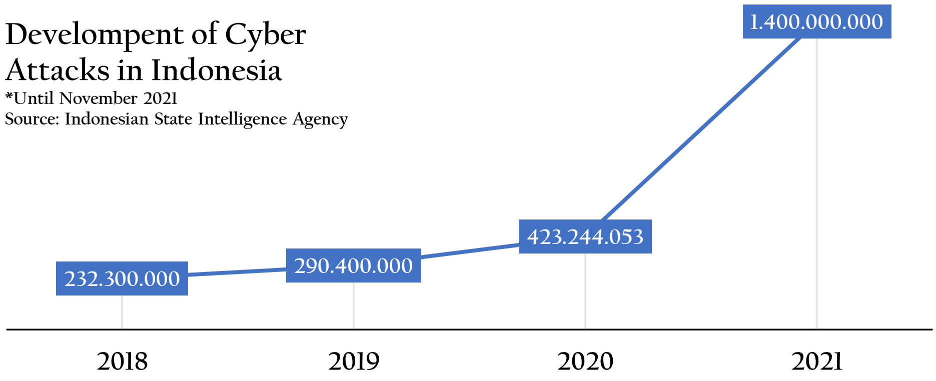

**Figure 1.** Development of Cyber Attacks in Indonesia

Based on the aforementioned data, it is evident that cybercrime attacks in Indonesia have consistently increased year after year, with the most significant surge observed in 2021, experiencing a fourfold increase compared to the previous year. The variety of cybercrimes occurring in the digital realm is vast, encompassing attacks by individuals and groups, as well as those orchestrated by one nation against another. Similarly, the methods employed in these cyber-attacks are diverse, often utilizing various forms of malware. Worms, Trojans, and Spyware are among the most frequently employed malware types targeting individuals, government institutions, or companies. A Worm is a type of malware akin to a computer virus that can inflict internal damage on a computer system. It operates autonomously, spreading to other parts of the system without needing external commands.[25]

Conversely, a Trojan is a form of malware designed to infiltrate and compromise data stored on the infected computer. Trojans can be hidden in unexpected places, such as emails or downloads from untrusted sources.[26] Spyware, true to its name, is a type of malware that secretly collects information about an individual's or organization's browsing habits and surreptitiously transmits it to third parties

[24] Timur Keldeshevich Yerjanov (et.al.), “Legal Issues Related to Combating Cybercrime: Experience of the Republic of Kazakhstan,” *Journal of Advanced Research in Law and Economics* 8, no. 7 (2017): 2279, https://doi.org/10.14505/jarle.v8.7(29).29.

[25] Retno Adenansi and Lia Ayu Novarina, “Malware Dynamic,” *JoEICT (Journal of Education and ICT)* 1, no. 1 (2017): 38, https://doi.org/10.29100/.v1i1.91.

[26] Muhammad Rijal, Amil Ahmad Ilham, and Ady Wahyudi Paundu, “Evaluasi Algoritma Klasifikasi Dengan Berbagai Metode Seleksi Fitur untuk Mendeteksi Aktivitas Trojan,” *Jurnal Pekommas, 7.2* (2022): 86.

without detection by the affected companies, institutions, or countries through various means, including email,[27] and is primarily used for espionage purposes, causing harm to the target country.[28]

Cyber espionage constitutes a form of criminal activity, frequently perpetrated by one nation against another, and often involves the use of spyware-type malware.[29] To elucidate the term, it is helpful to dissect the components "cyber" and "espionage" separately. "Cyber" pertains to the digital or online domain where such criminal activities transpire, while "espionage" encompasses the act of gathering information by individuals or states. Therefore, cyber espionage can be defined as the unauthorized exploitation of cyberspace by individuals to collect both broad and detailed information, as mandated by a governing body, aimed at specific targets.[30]

According to NATO's definition, cyber espionage encompasses “any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party”.[31] This delineation suggests that espionage consists of covert operations designed to acquire sensitive information from an adversary, thereby presenting substantial risks including possible conflicts and threats to the national security, sovereignty, and integrity of the targeted nation.

Cyber espionage crimes, often witnessed in the context of international relations, stem from intensified global competition. This rivalry prompts nations to resort to unfair tactics and deploy diverse strategies to fortify their own positions while weakening their adversaries. Espionage, comprising secretive operations designed to collect confidential information and data from a targeted nation, serves as one of these strategies. The confidential information and data obtained through espionage are used to discern the vulnerabilities of the targeted nation, thus allowing the perpetrators to devise and execute attack strategies with enhanced effectiveness.[32] Traditionally, collecting confidential information from a targeted country through espionage required physical entry into restricted zones. In these

[27] Danial Javaheri, Mehdi Hosseinzadeh, and Amir Masoud Rahmani, “Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines,” *IEEE Access* 6 (2018): 78327. https://doi.org/10.1109/ACCESS.2018.2884964.

[28] Abel Yeboah-Ofori, J Abdulai, and Ferdinand Katsriku, “Cybercrime and Risks for Cyber Physical Systems,” *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* 8, no. 1 (2019): 46. https://doi.org/10.17781/P002556.

[29] Esma Dilek and Ozgur Talih, “Overview of Cyber Espionage Incidents and Analysis of Tackling Methods,” *2022 15th International Conference on Information Security and Cryptography (ISCTURKEY)*, 2022: 57. https://doi.org/10.1109/ISCTURKEY56345.2022.9931893.

[30] Hamdan Mustameer, “Penegakan Hukum Nasional Dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0,”42-43.

[31] Sara Poli and Emanuele Sommario, “The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions,” *German Law Journal* 24, no. 3 (2023): 528, https://doi.org/10.1017/glj.2023.25.

[32] Somosri Hore and Kumarshankar Raychaudhuri, “Cyber Espionage—An Ethical Analysis,” in *Innovations in Computational Intelligence and Computer Vision*, Manoj Kumar Sharma (et.al.) (Singapore: Springer, 2021): 37, https://doi.org/10.1007/978-981-15-6067-5.

areas, designated individuals known as spies or espionage agents would collect classified data and insights, including information on the strengths and weaknesses of the target country.[33] However, these traditional methods have become less effective; they are time-consuming, offer limited access to data and confidential information, and elevate the risk of detection for the spies.[34]

Owing to the swift progress of technology, the conventional methodology was eventually forsaken for a contemporary and more versatile approach that utilizes sophisticated electronic devices. With these devices, espionage agents or spies can execute sabotage and wiretapping activities through cyberspace. By leveraging malware systems, they are capable of breaching and attacking these systems to harvest confidential data and information from the targeted nation. This transition to the use of cyberspace facilitates espionage operations that are both more efficient and covert.[35]

Cyber Espionage emerges from the integration of three interrelated offenses: wiretapping (interception), telematics crime (information technology), and espionage (spy action). This domain has witnessed a substantial evolution, moving from traditional espionage, which involved physical infiltration, to a sophisticated form of crime conducted within the realms of cyberspace. This evolution has fundamentally altered the characteristics of espionage. The framework for cybercrime encompasses three primary elements as follows.[36]

### 1. Computer

Computers are pivotal in enabling access to the internet, allowing users to manipulate networks to their preferences through keyboard inputs and the Central Processing Unit (CPU), which executes commands and processes software data. Moreover, computers act as repositories for vital information that can be disseminated through websites administered by individuals. This instrumental role of computers in internet access has given rise to the term "computer crime," which refers to unlawful activities undertaken using computers as a conduit to the internet.

### 2. Telematics

Telematics, a blend of telecommunications and informatics, has given rise to various legal domains resulting from the convergence of telecommunication law, media law,

[33] Sastya Hendri Wibowo (et.al.), *Cyber Crime di Era Digital* (Padang: PT Global Eksekutif Teknologi, 2022), 161-162.

[34] Wicaksana Prakasa Satria Unggul and PE Noviandy, “Analysist of Cyber Espionage in International Law and Indonesian Law,” *Humanities & Social Sciences Reviews* 7, no. 3 (2019): 40.

[35] Evi Dwi Hastri, “Cyber Espionage sebagai Ancaman Terhadap Pertahanan dan Keamanan Negara Indonesia,” *Law & Justice Review Journal* 1, no. 1 (2021): 13–14, https://doi.org/10.11594/lrjj.01.01.03.

[36] Evi Dwi Hastri, 14.

and informatics law. This interdisciplinary field facilitates the transmission of data via Dial-Up Systems connected to the internet network, encompassing telephone lines, computer systems, specialized wireless antennas, wireless systems, and all forms of telecommunications media. It enables the dissemination of information in both unidirectional and reciprocal manners through digital systems. Consequently, the emergence of Telematics Law, often referred to as Convergence Law, represents the legal response to this integrated technological landscape.

### 3. Internet

The term internet originates from the phrase "Interconnection Networking," denoting the use of interconnected computer networks that operate on the Internet Protocol (IP) or Transmission Control Protocol (TCP). This network houses a virtual realm known as cyberspace or Cyber Space, comprising a vast array of features and content closely tied to contemporary technology. However, this digital expanse has also become a breeding ground for various forms of cybercrimes, largely attributable to a lack of user ethics. As a result, this evolution has necessitated the advent of cyber law, encompassing regulations specific to the domain of cyberspace.

The three aforementioned elements underscore the intricate interrelationship among computers, information technology, and the internet. The escalating use of the internet brings to the fore critical issues related to the stability and harmony of societal order, chiefly stemming from a prevailing deficit of moral and ethical values among Internet users. Additionally, the absence of judiciousness in harnessing this potent tool amplifies the concerns associated with its swift and widespread adoption.

## C. Indonesian Policies and Regulations on Cyber Espionage

Indonesia has enacted a range of policies and regulations to combat the escalating threat of cyber espionage and safeguard national security. These measures include a comprehensive legal framework, strategic policy initiatives, and regulatory mechanisms designed to bolster cybersecurity capabilities and deter cyber espionage activities.[37, 38, 39] The following is the overview of the policies and regulations.

### 1. Legal Framework

[37] Hidayat Chusnul Chotimah, “Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency],” *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 10, no. 2 (2019): 117, https://doi.org/10.22212/jp.v10i2.1447.

[38] Andysah Putera Utama Siahaan, “Pelanggaran Cybercrime dan Kekuatan Yurisdiksi di Indonesia,” *Jurnal Teknik dan Informatika*, 5.1 (2018): 7.

[39] Damar Apri Sudarmadi and Arthur Josias Simon Runturambi, “Strategi Badan Siber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber di Indonesia,” *Jurnal Kajian Stratejik Ketahanan Nasional*, 2.2 (2019): 161–164.

The primary legal framework governing cyberspace in Indonesia is Law Number 11 of 2008, in conjunction with Law Number 16 of 2019 on Electronic Information and Transactions, commonly known as the Electronic Information and Transactions Law (the EIT Law).

The EIT Law plays a pivotal role in the digital era, overseeing electronic information use and strengthening privacy and personal data protection.[40] This comprehensive legislation addresses various aspects of electronic transactions and cyber activities, including cyber espionage provisions.[41] It criminalizes cyber activities such as unauthorized computer system access, data interception, and obtaining classified information.[42] Cyber espionage was indirectly referenced in Article 31 of the EIT Law. However, with the introduction of Law Number 1 of 2023 on the Indonesian Penal Code, cyber espionage is now explicitly regulated under Articles 258 and 259 of this new code.

The provisions state that any individual who unlawfully listens to, records, redirects, alters, obstructs, and/or documents the transmission of non-public Electronic Information and/or Electronic Documents is subject to a penalty of up to ten years imprisonment or a fine of up to 200 million Indonesian *Rupiahs*.[43] In addition, individuals who broadcast or disseminate the results of the aforementioned recordings are subject to up to seven years imprisonment or a fine of up to 200 million Indonesian *Rupiahs*.[44]

The aforementioned articles continue to be relevant in the context of cyber espionage, given that such espionage commonly involves capturing and monitoring the actions and conversations of targeted individuals. Recording can be executed through a variety of methods, employing sophisticated technologies. For example, one method spies use involves deploying spyware onto the target device, enabling them to access and retrieve recorded information. This spyware then transmits the collected data back to the espionage actor.

In addition to capturing the activities and conversations of the target, cyber espionage can be executed by forcefully penetrating or compromising the victim's information systems. Through these systems, perpetrators steal crucial confidential data, which is then processed and analyzed for specific objectives.[45] These actions,

[40] Manuel Lambi, *Sistem Informasi Manajemen Al (Artificial intelligence) as the Future Management Information System* (Ponorogo: Uwais Inspirasi Indonesia, 2023), 85.

[41] Bambang Tri Bawono, "Reformation of Law Enforcement of Cyber Crime in Indonesia," *Jurnal Pembaharuan Hukum* 6, no. 3 (2019): 332-335, https://doi.org/10.26532/jph.v6i3.9633.

[42] Sumiaty Adelina Hutabarat (et.al.) *CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0* (Jambi: PT. Sonpedia Publishing Indonesia, 2023), 121.

[43] Article 258 Law Number 1 of 2023 on Indonesian Penal Code.

[44] Article 259 Law Number 1 of 2023 on Indonesian Penal Code.

[45] Ilker Kara, "Cyber-Espionage Malware Attacks Detection and Analysis: A Case Study," *Journal of Computer Information Systems* 62, no. 6 (2022): 1261, https://doi.org/10.1080/08874417.2021.2004566.

described as the second method of cyber espionage, are regulated in the Indonesian Criminal Code of 2023, specifically within Articles 332-335. According to Article 332, unauthorized access to someone else's computer or electronic system is strictly prohibited. Individuals who intentionally and unlawfully access such systems could face a penalty of up to six years in prison or a fine of up to 500 million Indonesian *Rupiahs*. Furthermore, if the purpose of the system access is to acquire electronic information or documents, the penalty increases to a maximum of seven years in prison or a fine of up to 500 million Indonesian *Rupiahs*.[46] Article 333 stipulates that any individual who, without proper authorization or beyond their granted authority, utilizes or accesses a computer or electronic system with the intention of obtaining, altering, damaging, or deleting information related to national defense or international relations—thereby potentially disrupting or harming the state or its relations with international legal entities—shall face a penalty of up to seven years in prison or a fine of up to IDR200.000.000 (200 million Indonesian *Rupiahs*).

This includes unauthorized actions leading to the damage of state-protected computers or electronic systems through the transmission of programs, information, codes, or commands. It also covers unauthorized or excessive use or access to nationally protected computer or electronic systems, both domestic and foreign, for the purpose of acquiring information. Additionally, this article addresses unauthorized use or access to government-owned computers or electronic systems and any activities that interfere with or disrupt computers or electronic systems used by the government.

Those who disseminate, trade, or exploit access codes or similar information that can be used to compromise and misuse government-protected computers or electronic systems, or those who target foreign-protected computers or electronic systems within Indonesian jurisdiction with the intention of causing damage, will also be held accountable.[47]

There can be ten-years imprisonment or a fine of up to 200 million Indonesian *Rupiahs* for any person who: (1) without proper authorization or beyond their authority, uses or accesses a computer or electronic system with the aim of gaining financial benefits or acquiring financial information from the central bank, banking institutions, financial institutions, credit card issuers, or payment card providers, including customer report data; (2) without proper authorization, utilizes data or accesses another individual's credit card or payment card in electronic transactions for personal gain; (3) without proper authorization or beyond their authority, uses or accesses the protected computer or electronic system of the central bank, banking institutions, or financial institutions with the intention of misusing it or obtaining benefits from it; and (4) distributes, trades, or exploits access codes or similar information capable of breaching a computer or electronic system with the intention

[46] Article 332 Law Number 1 of 2023 on Indonesian Penal Code.

[47] Article 333 Law Number 1 of 2023 on Indonesian Penal Code.

of misuse, potentially impacting the electronic systems of the central bank, banking institutions, financial institutions, as well as domestic and international businesses. Furthermore, Article 335 stipulates that any individual who, without proper authorization, uses or accesses a computer or electronic system by any means, with the intention of obtaining, altering, damaging, or erasing government that is classified or protected due to its significance, shall face a maximum imprisonment of twelve years or a fine of up to five billion Indonesian *Rupiahs.*[48]

## 2. National Cybersecurity Strategy

The Indonesian National Cybersecurity Strategy, introduced in 2019, presents a holistic approach to safeguarding the nation's digital infrastructure, countering cyber threats, and bolstering national security within the cyber realm.[49] This comprehensive strategy articulates a series of objectives, initiatives, and action plans designed to fortify cybersecurity measures across diverse sectors. Its principal goal is to boost Indonesia's resilience against cyber threats and shield critical infrastructures. The strategy seeks to establish a secure and reliable digital ecosystem conducive to economic development, innovation, and societal stability.[50]

The strategy to effectively navigate the digital era focuses on multiple pivotal areas. Firstly, it highlights the necessity of efficient governance and coordination among governmental bodies, private sector entities, and additional stakeholders. To facilitate this, the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*-BSSN) has been designated as the primary coordinating entity for cybersecurity issues. Secondly, the strategy accentuates the critical role of risk management in combating cyber threats. It advocates for the utilization of risk-based methodologies and the execution of cybersecurity strategies tailored to the specific threats and vulnerabilities identified.[51]

The strategy also prioritizes the protection of critical national infrastructure. It aims to bolster the security of vital services including telecommunications, energy, transportation, and financial systems, by employing advanced technologies, establishing secure architectures, and implementing incident response mechanisms. Recognizing the importance of a proficient cybersecurity workforce, the strategy outlines initiatives for capacity building, comprising training programs, certifications, and educational partnerships to elevate the expertise of cybersecurity professionals.

[48] Article 335 Law Number 1 of 2023 on Indonesian Penal Code.

[49] Anang Setiyawan, "National Cybersecurity Policy in the US and Indonesia," *UNTAG Law Review* 3, no. 1 (2019): 77, http://dx.doi.org/10.56444/ulrev.v3i1.1071.

[50] Anggoro Yulianto, "Cybersecurity Policy and Its Implementation in Indonesia," *Law Research Review Quarterly* 7, no. 1 (2021): 73, https://doi.org/10.15294/lrrq.v7i1.43191.

[51] Leonardus K Nugraha and Dinita A Putri, *Mapping the Cyber Policy Landscape: Indonesia* (London: Global Partners Digital, 2016), 21-24.

It encourages research and development activities to stimulate innovation in cybersecurity. Collaboration and cooperation are pivotal elements of the strategy, advocating for partnerships between government entities, the private sector, academia, and international collaborators. Through the exchange of information, sharing of best practices, collaborative intelligence efforts, and participation in joint exercises, the strategy seeks to fortify cybersecurity measures on both regional and global scales.[52]

Finally, the strategy underscores the importance of increasing public awareness regarding cybersecurity threats and fostering responsible digital conduct. It accomplishes this through awareness campaigns, educational initiatives, and outreach activities directed at various segments of society, including government officials, business entities, and the general populace.[53] The execution of the National Cybersecurity Strategy incorporates precise action plans and schedules. These documents detail the activities, assign responsibilities, and establish milestones necessary for accomplishing the strategic aims. These plans undergo periodic reviews and updates to accommodate changing cyber threats and technological developments. The strategy acknowledges the importance of continuous evaluation and the assessment of its efficacy. It integrates mechanisms for tracking implementation progress, gauging the impact of initiatives, and pinpointing opportunities for enhancement. This evaluative approach facilitates the refinement of policies, the reallocation of resources, and the adjustment of strategies to confront new challenges effectively.[54]

While the National Cybersecurity Strategy establishes a robust framework for cybersecurity in Indonesia, several challenges remain to be overcome. These include a scarcity of skilled cybersecurity professionals, the swift evolution of cyber threats, the necessity for ongoing updates to regulations and policies, and the coordination among diverse stakeholders. Future endeavors may further enhance public-private partnerships, foster cybersecurity technology innovation, and intensify international collaboration.[55] In conclusion, the Indonesian National Cybersecurity Strategy signifies the nation's dedication to safeguarding its digital infrastructure and fortifying cybersecurity resilience. Indonesia is poised to address cyber threats effectively through a comprehensive strategy that includes governance, risk management, protection of critical infrastructure, capacity building, collaboration,

[52] Noor Halimah Anjani, “Cybersecurity Protection in Indonesia,” *Policy Brief Center for Indonesian Policy Studies (CIPS) Jakarta,* no. 9 (2021): 2-3.

[53] Abraham Ethan Martupa Sahat Marune and Brandon Hartanto, “Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective,” *International Journal of Business, Economics, and Social Development* 2, no. 4 (2021): 149. https://doi.org/10.46336/ijbesd.v2i4.170.

[54] Elva Azzahra Puji Lestari, “Complex Interdependence Between Indonesia-Australia Through Cybersecurity Cooperation Post Indonesia Australia Cyber War in 2013,” *Jurnal Hubungan Internasional UMY* 9, no. 2 (2021): 185-186, https://doi.org/10.18196/hi.v9i21.10522.

[55] Sarah Safira Aulianisa and Indirwan Indirwan, “Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia,” *Lex Scientia Law Review* 4, no. 1 (2020): 35, https://doi.org/10.15294/lesrev.v4i1.38197.

and awareness. Continuous evaluation and adaptation are imperative to navigate emerging challenges and ensure the strategy remains effective against the backdrop of rapidly evolving cyber risks.

## 3. Indonesian Cybersecurity Infrastructure

Indonesia has undertaken substantial initiatives to enhance its cybersecurity infrastructure and safeguard its digital assets, critical infrastructure, and overall cybersecurity posture. Central to these efforts is the National Cyber and Crypto Agency, which acts as the primary coordinator for national cybersecurity matters. The BSSN is responsible for policy formulation and spearheads collaborations with government agencies, law enforcement bodies, private sector entities, and international counterparts to bolster Indonesia's cybersecurity capabilities.[56, 57]

Indonesia has prioritized securing critical information infrastructure sectors, including telecommunications, energy, transportation, finance, and government services. It has developed and implemented robust security measures in collaboration with the relevant sectors. Furthermore, the country has established a Cyber Crisis Center (C3) to manage and coordinate responses to cybersecurity incidents. The C3 works in close collaboration with various stakeholders, offering guidance on incident response and facilitating the sharing of threat intelligence.[58]

Indonesia recognizes the pivotal role of public-private partnerships in addressing cybersecurity challenges and proactively seeks collaboration and information sharing with the private sector. The government highlights the significance of cybersecurity education and workforce development in meeting the burgeoning demand for skilled professionals. Additionally, international cooperation is crucial for Indonesia, as it engages in bilateral and multilateral agreements and collaborates with other nations on cybersecurity issues. The Indonesian cybersecurity infrastructure is continually evolving to adapt to emerging threats and technological progress. The government and relevant stakeholders are dedicated to improving capabilities, protecting critical infrastructure, and ensuring overall resilience in the digital landscape.[59] Acknowledging that the Indonesian cybersecurity infrastructure

[56] Dana Indra Sensuse (et.al.), "Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology," *Information* 13, no. 12 (2022): 580, https://doi.org/10.3390/info13120580.

[57] Mulyadi and Dwi Rahayu, "Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency (BSSN)," *2018 6th International Conference on Cyber and IT Service Management (CITSM)* (2018): 3, https://doi.org/10.1109/CITSM.2018.8674265.

[58] Sarah Safira Aulianisa and Indirwan Indirwan, 41-42.

[59] Aleksander Kalisz (ed.), "Public-Private Partnerships on Cybersecurity and International Law: Finding Multilateral Solutions," in *Public and Private Governance of Cybersecurity: Challenges and Potential, Tomoko Ishikawa and Yarik Kryvoi* (Cambridge: Cambridge University Press, 2023): 4.

is constantly evolving, aiming to adapt to emerging threats and technological progress is crucial.

In collaboration with various stakeholders, the government is committed to enhancing cybersecurity capabilities, safeguarding critical infrastructure, and ensuring the comprehensive resilience of the nation's digital framework. Despite these efforts, Indonesia encounters specific challenges in effectively combating cyber espionage. These challenges encompass a scarcity of cybersecurity professionals, the imperative of continual adaptation to evolving threats, and concerns regarding privacy and surveillance measures. To surmount these challenges, ongoing initiatives are being implemented to bolster cybersecurity capabilities, invest in education and training in cybersecurity, and revise policies and regulations to remain aligned with the dynamic cyber environment.[60]

In conclusion, Indonesian policies and regulations on cyber espionage reflect the government's dedication to ensuring national security and guarding against cyber threats. By employing a multifaceted approach that includes legal frameworks, policy initiatives, and regulatory measures, Indonesia aims to strengthen its cybersecurity capabilities, increase awareness, and encourage international cooperation. To effectively counter cyber espionage, it is essential to persist in addressing the challenges and enhancing the efficacy of these policies and regulations.

## D. Germany Cyber Espionage Policies and Regulations

Germany has enacted policies and regulations to tackle cyber espionage and associated activities effectively, safeguard national security, protect critical infrastructure, and mitigate cyber threats.[61] These initiatives underscore Germany's commitment to cybersecurity.

A key element is the National Cyber Defense Policy, which delineates Germany's cybersecurity strategy, including measures for preventing and responding to cyber espionage. The policy highlights the importance of protecting critical infrastructure, boosting cyber resilience, and fortifying the country's capacity to identify and address cyber threats. [62]

Germany's legal framework to combat cyber espionage and other cyber-related offenses is embodied in the *Strafgesetzbuch* (German Criminal Code (StGB)). The German Criminal Code prescribes regulations for various cyberactivities, including

[60] Y Nugraha, "The Future of Cyber Security Capacity in Indonesia," *Oxford University Research Archive* (2016): 27-38.

[61] André Barrinha and Thomas Renard, "Cyber-Diplomacy: The Making of an International Society in the Digital Age," *Global Affairs* 3, no. 4–5 (2017): 356, https://doi.org/10.1080/23340460.2017.1414924.

[62] A Tumkevič, "Uncertain Security Community: Building Western Cyber-Security Order," *Journal of Information Warfare* 17, no. 1 (2018): 79.

cyber espionage. The pertinent sections of the German Criminal Code addressing cyber espionage and related offenses are as follows.[63]

1) Section 202a – Unauthorized Access to Computer Systems: prohibits unauthorized access to computer systems or data. It targets activities such as hacking, unauthorized intrusion, and circumventing security measures to access data or disrupt system functionality.
2) Section 202b—Data Espionage focuses on the unauthorized acquisition, disclosure, or use of data that is not publicly accessible. This includes the unauthorized interception of data transmissions, the theft of trade secrets, or the accessing of confidential information without authorization.
3) Section 202c – Preparing for Data Espionage: criminalizes the preparation or planning of data espionage offenses, including developing or utilizing tools or software for unauthorized data acquisition.
4) Section 202d – Intercepting Non-Public Transmissions of Data: pertains to the unauthorized interception of non-public data transmissions. This section covers eavesdropping on private communications, intercepting emails, or capturing data during transmission without authorization.
5) Section 202e – Supplying Intrusion Software: outlaws the creation, distribution, or possession of software or tools intended for unauthorized intrusion into computer systems. It targets individuals or entities involved in producing and distributing malicious software, commonly called hacking tools or malware.

The sections of the German Criminal Code outlined above encompass a broad spectrum of cyber-related offenses, extending beyond cyber espionage to include unauthorized access, data theft, and the distribution of intrusion tools. In addition, the Cybersecurity Act of 2015, though not explicitly addressing espionage, establishes a robust legal framework for cybersecurity in Germany.

This act protects critical infrastructure and bolsters the nation's cybersecurity capabilities. It emphasizes the security and resilience of information technology systems and networks, rather than directly tackling espionage activities. The Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*-BSI), as designated by the Cybersecurity Act, serves as the central authority for cybersecurity matters.

The BSI's responsibilities include promoting cybersecurity measures, offering guidance to both public and private entities, and coordinating responses to cyber

[63] Filip Radoniewicz (ed.) “Cybercrime in Selected European Countries,” in *Cybersecurity in Poland*, Katarzyna Chałubińska-Jentkiewicz, Filip Radoniewicz, and Tadeusz Zieliński (Cham: Springer International Publishing, 2022), 425.

incidents. Thus, it plays a critical role in maintaining the security of Germany's digital infrastructure.[64]

The Cybersecurity Act delineates the critical infrastructure operators' responsibilities in safeguarding their systems, mandating the adoption of suitable technical and organizational measures to defend against cyber threats. Furthermore, the Act introduces frameworks for information sharing and collaboration between the Federal Office for Information Security (BSI) and operators of critical infrastructure, facilitating prompt communication of threat intelligence and coordination of incident responses. While the act is geared towards protecting critical infrastructure and enhancing cybersecurity measures, it does not expressly tackle espionage activities. Activities related to espionage are typically overseen by intelligence agencies, law enforcement authorities, and national security legislation rather than being directly governed by cybersecurity regulations.[65]

Germany has enacted regulations to safeguard sectors deemed critical infrastructure, including energy, water, telecommunications, transportation, and healthcare. Operators of these sectors are obliged to deploy appropriate cybersecurity measures to shield against cyber threats, encompassing espionage. The adoption of the Network and Information Security (NIS) Directive, an initiative of the European Union, augments Germany's cybersecurity stance. This directive requires that operators of essential services and digital service providers implement necessary security measures and notify authorities of significant cyber incidents. Consequently, this enhances the resilience of Germany's cybersecurity against espionage and various other cyber threats.[66]

Germany's intelligence agencies, especially the Federal Intelligence Service (BND), are deeply involved in foreign intelligence and counterintelligence operations. These agencies are instrumental in identifying and thwarting cyberespionage efforts by monitoring and analyzing cyber threats, conducting investigations, and protecting sensitive data.[67]

Germany highly values international cooperation in addressing cyber espionage and other cyber threats. It works closely with other countries, international organizations, and law enforcement agencies to share information, exchange best practices, and coordinate efforts globally to combat cyber espionage effectively. Through implementing thorough policies, regulations, and collaborative initiatives,

[64] Andrew J. Grotto and Martin Schallbruch, "Cybersecurity and the Risk Governance Triangle: Cybersecurity Governance from a Comparative U.S.–German Perspective," *International Cybersecurity Law Review* 2, no. 1 (2021): 79, https://doi.org/10.1365/s43439-021-00016-9.

[65] Martin Schallbruch and Isabel Skierka, *The Organisation of Cybersecurity in Germany.* In *Cybersecurity in Germany* (Cham: Springer International Publishing, 2018), 32. https://doi.org/10.1007/978-3-319-90014-8.

[66] Ludwig Leinhos, "Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr," *Connections: The Quarterly Journal* 19, no. 1 (2020): 13, https://doi.org/10.11610/Connections.19.1.02.

[67] Martin Schallbruch and Isabel Skierka, 35.

Germany exhibits its dedication to cybersecurity and proactive approach against cyber espionage.[68]

## E. Conclusion

Indonesia showcases strengths in cybersecurity, characterized by an increasing awareness of cybersecurity issues, its leadership role within Southeast Asia in this domain, and its rapid digital transformation facilitating the adoption of advanced cybersecurity measures. Nevertheless, Indonesia grapples with challenges such as a shortage of skilled cybersecurity professionals, limited resources for implementing comprehensive cybersecurity strategies, and a regulatory and legal framework that requires ongoing refinement and adaptation.

Consequently, the establishment of specific regulations targeting cybersecurity is crucial for Indonesia. Conversely, Germany's robust legal framework acts as a bulwark against cyber threats. Coupled with its substantial technical expertise and innovative approaches to cybersecurity, Germany benefits from a transparent legal framework that ensures clarity and efficiency in handling cyber threats. Nonetheless, Germany also confronts weaknesses, such as reliance on external technologies and supply chains, the prevalence of sophisticated cyber threats, and the challenge of harmonizing cybersecurity practices across various sectors.

## References

### Books

Hore, Somosri and Kumarshankar Raychaudhuri (ed.) "Cyber Espionage—An Ethical Analysis." In Manoj Kumar Sharma (et.al.) *Innovations in Computational Intelligence and Computer Vision*. Singapore: Springer, 2021.

Hutabarat, Sumiaty Adelina (et.al.) *CYBER-LAW: Quo Vadis Regulasi UU ITE Dalam Revolusi Industri 4.0 Menuju Era Society 5.0*. Jambi: PT Sonpedia Publishing Indonesia, 2023.

Kalisz, Aleksander. "Public-Private Partnerships on Cybersecurity and International Law: Finding Multilateral Solutions." In Tomoko Ishikawa and Yarik Kryvoi (ed.) *Public and Private Governance of Cybersecurity: Challenges and Potential* Cambridge: Cambridge University Press, 2023.

Lambi, Manuel. *Sistem Informasi Manajemen Al (Artificial intelligence) as the Future Management Information System*. Ponorogo: Uwais Inspirasi Indonesia, 2023.

Maskun (et.al.) *Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional*. Makassar: CV Nas Media Pustaka, 2020.

[68] Olga Vakulyk (et.al.), "Cybersecurity as a Component of the National Security of the State," *Journal of Security and Sustainability Issues* 9, no. 3 (2020): 778. https://doi.org/10.9770/jssi.2020.9.3(4).

Nugraha, Leonardus K. and Dinita A Putri. *Mapping the Cyber Policy Landscape: Indonesia*. London: Global Partners Digital, 2016.

Nugroho, Catur. *Cyber Society: Teknologi, Media Baru, dan Disrupsi Informasi*. Jakarta: Prenada Media, 2020.

Radoniewicz, Filip. "Cybercrime in Selected European Countries." In Katarzyna Chałubińska-Jentkiewicz, Filip Radoniewicz, and Tadeusz Zieliński. *Cybersecurity in Poland* (ed.) Cham: Springer International Publishing, 2022.

Rawat, Romil (et.al.) "Artificial Cyber Espionage Based Protection of Technological Enabled Automated Cities Infrastructure by Dark Web Cyber Offender." In Fadi Al-Turjman, Anand Nayyar, Ajantha Devi, and Piyush Kumar Shukla. *Intelligence of Things: AI-IoT Based Critical-Applications and Innovations*. Cham: Springer International Publishing, 2021.

Schallbruch, Martin and Isabel Skierka. *Cybersecurity in Germany*. Cham: Springer International Publishing, 2018.

Shipley, Todd G. and Art Bowker. *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*. Oxford: Syngress Publishing, 2013.

Wibowo, Sastya Hendri (et.al.) *Cyber Crime di Era Digital*. Padang: PT. Global Eksekutif Teknologi, 2022.

**Other Documents**

Anjani, Noor Halimah. "Cybersecurity Protection in Indonesia." *Policy Brief Center for Indonesian Policy Studies (CIPS) Jakarta*, no. 9 (2021): 1–12.

Adenansi, Retno and Lia Ayu Novarina. "Malware Dynamic." *JoEICT (Journal of Education and ICT)* 1, no. 1 (2017): 37–43. https://doi.org/10.29100/.v1i1.91.

Aulianisa, Sarah Safira and Indirwan Indirwan. "Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia." *Lex Scientia Law Review* 4, no. 1 (2020): 33–48. https://doi.org/10.15294/lesrev.v4i1.38197.

Barrinha, André and Thomas Renard. "Cyber-Diplomacy: The Making of an International Society in the Digital Age." *Global Affairs* 3, no. 4–5 (2017): 353–3 364. https://doi.org/10.1080/23340460.2017.1414924.

Bawono, Bambang Tri. "Reformation of Law Enforcement of Cyber Crime in Indonesia." *Jurnal Pembaharuan Hukum* 6, no. 3 (2019): 332–349. https://doi.org/10.26532/jph.v6i3.9633.

BBC News. "German Cyber Officials Defend Handling of Mass Data Attack." Accessed on January 5, 2019. https://www.bbc.com/news/world-europe-46768990.

Botua, Hafidz L., Chloryne Trie Isana Dewi, and R. Achmad Gusman Catur Siswandi. "Wiretapping on Submarine Communications Cable: Questioning Its Legality Amidst Long Standing Practice." *Padjadjaran Journal of International Law* 6, no. 1 (2022): 20–42. https://doi.org/10.23920/pjil.v6i1.772.

Caldwell, M. (et.al.) "AI-Enabled Future Crime." *Crime Science* 9, no. 1 (2020): 1-13. https://doi.org/10.1186/s40163-020-00123-8.

Chotimah, Hidayat Chusnul. “Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency].” *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 10, no. 2 (2019): 113–128. https://doi.org/10.22212/jp.v10i2.1447.

Cristani, Federica. “Economic Cyber-Espionage in the Visegrád Four Countries: A Hungarian Perspective.” *Politics in Central Europe* 17, no. 4 (2021): 697–721. https://doi.org/10.2478/pce-2021-0037.

Datta, Priyanka (et.al.) “A Technical Review Report on Cyber Crimes in India.” *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)* (2020): 269–275. https://doi.org/10.1109/ESCI48226.2020.9167567.

Dewi, Maharani Chandra. “Cyber Espionage in National and Global Perspective: How Indonesia Deal with This Issue?” *International Law Discourse in Southeast Asia* 1, no. 1 (2022): 1–22. https://doi.org/10.15294/ildisea.v1i1.56874.

Dilek, Esma, and Ozgur Talih. “Overview of Cyber Espionage Incidents and Analysis of Tackling Methods.” *2022 15th International Conference on Information Security and Cryptography (ISCTURKEY)* (2022): 55–60. https://doi.org/10.1109/ISCTURKEY56345.2022.9931893.

Drouin, Michelle, Brandon T. McDaniel, Jessica Pater, and Tammy Toscos. “How Parents and Their Children Used Social Media and Technology at the Beginning of the COVID-19 Pandemic and Associations with Anxiety.” *Cyberpsychology, Behavior and Social Networking* 23, no. 11 (2020): 727–736. https://doi.org/10.1089/cyber.2020.0284.

Dwi Hastri, Evi. “Cyber Espionage Sebagai Ancaman Terhadap Pertahanan dan Keamanan Negara Indonesia.” *Law & Justice Review Journal* 1, no. 1 (2021): 12–25. https://doi.org/10.11594/lrjj.01.01.03.

Fransiska, Futri Bela and Fredy BL Tobing. “Securing Indonesia Cyber Space: Strategies for Cyber Security in the Digital Era.” *Jurnal Studi Sosial dan Politik* 7, no. 1 (2023): 50–62. https://doi.org/10.19109/jssp.v7i1.15925.

Grotto, Andrew J. and Martin Schallbruch. “Cybersecurity and the Risk Governance Triangle: Cybersecurity Governance from a Comparative U.S.–German Perspective.” *International Cybersecurity Law Review* 2, no. 1 (2021): 77–92. https://doi.org/10.1365/s43439-021-00016-9.

Hamdan Mustameer. “Penegakan Hukum Nasional Dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0.” *Jurnal Yustika: Media Hukum Dan Keadilan* 25, no. 1 (2022): 40–53. https://doi.org/10.24123/yustika.v25i01.5090.

Iqbal, Muhammad and Nyoman Serikat Putra Jaya. “Development of Cyber Crime and Its Regulations in Indonesia.” *International Journal of Social Science and Human Research* 4, no. 2 (2021): 141–147. https://doi.org/10.47191/ijsshr/v4-i2-04.

Javaheri, Danial, Mehdi Hosseinzadeh, and Amir Masoud Rahmani. “Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines.” *IEEE Access* 6 (2018): 78321–78232. https://doi.org/10.1109/ACCESS.2018.2884964.

Kara, Ilker. “Cyber-Espionage Malware Attacks Detection and Analysis: A Case Study.” *Journal of Computer Information Systems* 62, no. 6 (2022): 1253–1270. https://doi.org/10.1080/08874417.2021.2004566.

Khan, W.Z. (et.al.) “Industrial Internet of Things: Recent Advances, Enabling Technologies and Open Challenges.” *Computers & Electrical Engineering* 81 (2020): 106522. https://doi.org/10.1016/j.compeleceng.2019.106522.

Lallie, Harjinder Singh (et.al.) “Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic.” *Computers & Security* 105 (2021): 1-20. https://doi.org/10.1016/j.cose.2021.102248.

Leinhos, Ludwig. “Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr.” *Connections: The Quarterly Journal* 19, no. 1 (2020): 9–19. https://doi.org/10.11610/Connections.19.1.02.

Lestari, Elva Azzahra Puji. “Complex Interdependence Between Indonesia-Australia Through Cybersecurity Cooperation Post Indonesia Australia Cyber War in 2013.” *Jurnal Hubungan Internasional UMY* 9, no. 2 (2021): 178–188. https://doi.org/10.18196/hi.v9i21.10522.

Lin, Danping, C.K.M. Lee, Henry Lau, and Yang Yang. “Strategic Response to Industry 4.0: An Empirical Investigation on the Chinese Automotive Industry.” *Industrial Management & Data Systems* 118, no. 3 (2018): 589–605. https://doi.org/10.1108/IMDS-09-2017-0403.

Marune, Abraham Ethan Martupa Sahat, and Brandon Hartanto. “Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective.” *International Journal of Business, Economics, and Social Development* 2, no. 4 (2021): 143–152. https://doi.org/10.46336/ijbesd.v2i4.170.

Mulyadi, and Dwi Rahayu. “Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency (BSSN).” *2018 6th International Conference on Cyber and IT Service Management (CITSM)* Parapat, Indonesia (2018): 1–6. https://doi.org/10.1109/CITSM.2018.8674265.

Nugraha, Y. “The Future of Cyber Security Capacity in Indonesia.” *Oxford University Research Archive* (2016): 23-78.

Poli, Sara, and Emanuele Sommario. “The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions.”

*German Law Journal* 24, no. 3 (2023): 522–536. https://doi.org/10.1017/glj.2023.25.

Raharjo, Agus (et.al.) "The Legal Policy of Criminal Justice Bureaucracy Cybercrime." *BESTUUR 10*, no. 2 (2022): 105-122. https://doi.org/10.20961/bestuur.v10i2.64498.

Ray, Vicky and Kaoru Hayashi. "Tracking Ocean Lotus' New Downloader, KerrDown." Accessed on February 1, 2019. https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/.

Rijal, Muhammad, Amil Ahmad Ilham, and Ady Wahyudi Paundu. "Evaluasi Algoritma Klasifikasi Dengan Berbagai Metode Seleksi Fitur Untuk Mendeteksi Aktivitas Trojan." *Jurnal Pekommas* 7, no. 2 (2022): 85–97.

Satria Unggul, Wicaksana Prakasa, and P.E. Noviandy. "Analysist of Cyber Espionage in International Law and Indonesian Law." *Humanities & Social Sciences Reviews* 7, no. 3 (2019): 38–44.

Sensuse, Dana Indra (et.al.) "Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology." *Information* 13, no. 12 (2022): 1-10. https://doi.org/10.3390/info13120580.

Setiyawan, Anang. "National Cybersecurity Policy in the US and Indonesia." *UNTAG Law Review* 3, no. 1 (2019): 71–87. http://dx.doi.org/10.56444/ulrev.v3i1.1071.

Siahaan, Andysah Putera Utama. "Pelanggaran Cybercrime dan Kekuatan Yurisdiksi di Indonesia." *Jurnal Teknik Dan Informatika* 5, no. 1 (2018): 6–9.

Solomon, Edna Maeyen, and Aaron Van Klyton. "The Impact of Digital Technology Usage on Economic Growth in Africa." *Utilities Policy* 67 (2020): 1-12. https://doi.org/10.1016/j.jup.2020.101104.

Sudarmadi, Damar Apri and Arthur Josias Simon Runturambi. "Strategi Badan Siber Dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia." *Jurnal Kajian Stratejik Ketahanan Nasional* 2, no. 2 (2019): 157–78.

Sviatun, Olena V. (et.al.) "Combating Cybercrime: Economic and Legal Aspects." *WSEAS Transactions on Business and Economics* 18 (2021): 751–762. https://doi.org/10.37394/23207.2021.18.72.

Tumkevič, A. "Uncertain Security Community: Building Western Cyber-Security Order." *Journal of Information Warfare* 17, no. 1 (2018): 74–86.

Vakulyk, Olga (et.al.) "Cybersecurity as a Component of the National Security of the State." *Journal of Security and Sustainability Issues* 9, no. 3 (2020): 775–784. https://doi.org/10.9770/jssi.2020.9.3(4).

Yeboah-Ofori, Abel, J Abdulai, and Ferdinand Katsriku. "Cybercrime and Risks for Cyber Physical Systems." *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* 8, no. 1 (2019): 43–57. https://doi.org/10.17781/P002556.

Yerjanov, Timur Keldeshevich (et.al.) “Legal Issues Related to Combating Cybercrime: Experience of the Republic of Kazakhstan.” *Journal of Advanced Research in Law and Economics* 8, no. 7 (2017): 2286–2301. https://doi.org/10.14505/jarle.v8.7(29).29.

Yulianto, Anggoro. “Cybersecurity Policy and Its Implementation in Indonesia.” *Law Research Review Quarterly* 7, no. 1 (2021): 69–82. https://doi.org/10.15294/lrrq.v7i1.43191.

**Legal Document**

Law Number 1 of 2023 on Indonesian Criminal Code [*Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*].