Deky Rosdiana

Ph.D. student

Bandung Islamic University, Indonesia

SPYWARE IN INTELLIGENCE ESPIONAGE OPERATIONS AS A THREAT TO THE STATE

Abstract

The development of globalization has changed the pattern of war from conventional military power with trained soldiers and sophisticated weaponry to non-military state power through cultural, economic, political, and technological aspects. Warfare now dominantly utilizes technological sophistication or cyber warfare, posing a threat to national security, sovereignty, and resilience in the virtual world. This article uses a qualitative approach that refers to the meaning, concept, definition, characteristics, metaphor, symbol, and description of a qualitative study, conducted through examining various social arrangements and groups or individuals in a social setting. The data collection technique used here is only a literature review or a descriptive review of previous research sources and other secondary data. In terms of Cyber Espionage issues, updating the law can be a step towards providing a legal basis for law enforcement against Cyber Espionage perpetrators as a legal breakthrough to ensnare the perpetrators. Cyber intelligence's role as a "new" form in the governance of national intelligence can become clearer and avoid potential issues. Attention to these issues should be accompanied by solutions in preparing competent human resources, infrastructure, funds, and technology to make cyber intelligence an asset for national and state security.

Key Words

Spyware, Intelligence espionage operations, Cyber attacks, Military

Introduction

The world's political landscape is constantly changing and affecting all aspects of global life. The dynamic world continues to experience changes that are sometimes marked by turbulence, affecting the relations between countries and global issues, thereby impacting national life. Every global development in the world will always affect the entire national life in each country, forcing each country to always observe and study every strategic environmental development, both at the global, regional, national, and local levels.

The dynamics of world politics are becoming increasingly complex and diverse, affecting the domestic political constellation of each country. Every country in the world is now increasing its vigilance against various threats such as conflicts between countries and intra-national domestic conflicts that endanger the national security of each country. In addition, globalization has driven the development of technology, resulting in various threats of conflict and warfare between militias and governments, as well as between major and small countries, making the infrastructure more complex. This is due to the use of information and communication technology, especially the virtual world, which then leads to the threat of cyber warfare.(Chotimah, 2019)

Countries in international relations are interested in explaining their natural resources and potential to other countries and nations for the advancement of cooperation and international development. Sensitivity to international developments is increasing due to the growing openness of the international system in the fields of technology and communication. On the one hand, this opens up opportunities for countries to collaborate to achieve their interests, and on the other hand, it triggers unhealthy competition. However, in this collaboration, global competition will arise in various sectors such as the economy, education, military, and politics. Global competition is a stage in the development of cultural phenomena that must be passed for the progress of civilization and life. The most important thing is to determine the attitude and prepare for the arrival of these phenomena.

Indonesia, as a country that is the highest organization or institution of a group of people consisting of a group of people in a certain area, who have aspirations to live together, and have a sovereign government system, must be able to realize it through the power it possesses, namely sovereignty, so that in the implementation of the government of a country can be carried out through a sovereign government. Therefore, through the power possessed by Indonesia in the form of sovereignty, it can be used as a form of self-protection from external attacks that can threaten national defense and security in facing global competition.(Ardiyanti, 1986)

One of the efforts to conquer a targeted country is through espionage or spying activities. The secret information and data obtained from espionage activities will be used to identify weaknesses, allowing them to easily plan and strengthen their attack strategies. In the past, gaining access to restricted areas of the target country was how secret information was obtained, but this conventional method is no longer relevant. Cyber espionage or spying through the internet has become more common and easier to carry out due to increasing opportunities for countries to spy on Indonesia through hacking and intercepting data. The government has struggled to regulate and address cyber espionage due to weakness in regulations and policies. Legal research has been conducted to support the government in legal matters related to cyber espionage, using primarily statute, conceptual, and comparative approaches. In 1998, Indonesia experienced its first cyber attack, allegedly carried out by hackers from China and Taiwan. Australia has also been accused of spying on the Indonesian government through its diplomatic representative office in Jakarta. (Rahmawati, 2017)

The negative impact of cybercrime in Indonesia, as reported by the CIA, has reached 1.20% when compared to global losses. The loss is caused by cybercrime, with estimated losses of USD 895 billion in Indonesia, which is 1.20% of the total estimated global losses of USD 71,620 billion. The globalization development has changed the conventional pattern of war, where military forces with advanced weaponry were used to compete, to non-military state competition in aspects of culture, economy, politics, and technology. Cyberwarfare is now dominant, with various subjects involved, such as state intelligence operations, hacker individuals or groups, non- government organizations (NGOs), terrorism, organized criminal groups, and private sectors (internet companies and carriers, security companies). Cyber threats to national security are no longer limited to virtual sovereignty and resilience, but also to environmental threats. With the limitless virtual world, countries must build cooperation to overcome similar threats faced by other countries. Cybercrime is an actual threat that has evolved and diversified to different types, such as hacking, cyber sabotage, cyber espionage, guarding cyber attack, vandalism, spyware, and power grid attacks. Hackingis one of the most dangerous types of cybercrime.(Putri et al., 2022)

Research Methodology

This article uses a qualitative approach that focuses on meaning, concepts, definitions, characteristics, metaphors, symbols, and descriptions of a qualitative research. The research is conducted by seeking an answer by examining various social arrangements and groups or individuals in a social setting. In data collection technique, the writer only uses literature review or desk study with a descriptive method from previous research sources and other secondary data. These sources come from annual reports or studies conducted by government and non-government agencies, international agreement documents, government magazines, as well as online news that are still relevant to cyber security and cyber diplomacy issues, as well as the role of BSSN as a cyber institution in Indonesia.

The Framework of Thought The Theory of Development Law uses a reference framework based on the way of life of Indonesian society and nation, according to the principles of Pancasila, which are characterized by a sense of familyhood. Therefore, the norms, principles, institutions, and rules contained in the Theory of Development Law are relatively dimensions that cover structure, culture, and substance, as stated by Lawrence W. Friedman. Secondly, basically the Theory of Development Law provides the basis for the legal function as a "means of renewing society" (law as a tool for social engineering), and law as a system is needed for Indonesia as a developing country. (Mulyadi 2009)

In the issue of Cyber Espionage, renewing the law in the field of legal substance can be a step to establish a legal basis for law enforcement against perpetrators of Cyber Espionage as a legal breakthrough to catch the perpetrators."

Framework

Development Law Theory uses a frame of reference on the way of life of the Indonesian people and nation based on the Pancasila principle which is familial in nature, so that the norms, principles, institutions and rules contained in the Development Law Theory are relatively a dimension that includes structure, culture (culture) and substance (substance) as said by Lawrence W. Friedman. Third, basically Development Law Theory provides the basic function of law as a "means of community renewal" (law as a social engineering tool) and law as a system is indispensable for the Indonesian nation as a developing country. (Mulyadi 2009)

In the case of Cyber Espionage, law reform in the field of legal substance can be used as a step to be used as a legal basis in enforcing the law against perpetrators who carry out Cyber Espionage as a legal breakthrough to ensnare the perpetrators.

Discussion

Indonesian Laws in Accommodating Cyber Espionage Attacks.

The rapid development of information technology has transformed and evolved all aspects of life. What was once done conventionally can now be easily accomplished through digital means, from social interactions to all forms of transactions. However, this phenomenon has also led to the emergence of various criminal activities, indicating the need for national and international legal systems to be prepared on a global scale. Cyber espionage is one such unconventional crime that poses a risk to national security.

While traditional spying during war is regulated by international law, cyber espionage lacks specific regulations during times of peace. The interception of confidential information through technology is a prevalent method used in cyber espionage, and it is regulated in Indonesia by various laws, including Pasal 31 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE). There are different definitions and objectives for interception among these laws, which can lead to legal loopholes and pose a threat to individual privacy and national security. Cyber espionage combines interception, cybercrime, and spying in one cycle, and it poses a significant risk to national defense and security. The legality of espionage during wartime is regulated by the Geneva Convention and the Hague Convention.(Anggoro Yulianto, 2021)

The world of cyber is threatened by attacks that come from various directions, such as viruses, hacking from individuals or groups who are not responsible, because it is so difficult to identify the cyber attacker. Cyber attacks happen because of the complexity of the cyber world, making it difficult to contain its development. Infrastructure development can also be disrupted by cyber attacks, as all activities are now connected to a network to facilitate work that previously used conventional methods.

In this rapidly developing age of Cyber Warfare, it is not only carried out by a country's military forces but can also be done by individuals, organizations, or other groups claiming to be nationalists of a nation. In such attacks, various types of malware are usually used, with the most commonly used ones to attack or hack individuals, state institutions, or companies being Worms, Trojans, and Spyware. Worms are a type of malware similar to computer viruses that can damage parts of a computer and are self-contained. Trojans can eat up data stored by the infected computer, which can be hidden in unexpected places like email and other unpredictable locations. Spyware is malware that collects browsing history information secretly over the internet and directly transmits it to a third party without the knowledge of the company, institution, or country. This type of malware can attack the identity of third parties through email and other means. Spyware is used for the interests of a party in conducting espionage, which causes damage to a country that is attacked by malware.

The risks faced in dealing with cybercrime are no less than conventional warfare. The use of cyber technology has a wide impact as it can cover various aspects of social and state life, including ideology, politics, economics, socio-culture, and security. Cybercrime is increasing, and certain parties, either individual or group or country, take advantage of it for specific purposes to weaken their opponents. This condition needs to be anticipated because there is a possibility that a country can be disabled and destroyed through technology warfare or through cyberspace.

In terms of Cyber Warfare, most attacks are carried out by a community group calling themselves Anonymous. In its classification, Cyber Espionage can be considered as a form of Cyber Warfare. This is because Cyber Espionage is a type of spying crime to obtain secret information that utilizes the internet network through malware with various types and levels of danger, which in classifying such actions against actions that can threaten the defense and security of a country, namely the stability of the Unitary State of the Republic of Indonesia according to Article 10 of Law Number 3 of 2002 concerning State Defense.(Atmadja, 2017)

The characterization of a legal action that can have legal consequences is not only based on the context that can be generated but also on the universal spectrum in relation to the elements of the act and mistake. The interception elements in Article 31 paragraph (1) of Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE) consist of intentional individuals without rights, electronic documents belonging to others. Meanwhile, paragraph (2) of the same article involves intentional individuals without rights, electronic documents that are not public, causing changes, removals, and/or termination of electronic information being transmitted. The regulation on cyber espionage is urgent to protect against potential threats that can harm society. The law is not only a tool to regulate and maintain values but also a means of renewal in society that can lead to peace and justice. The application of the theory of legal development is necessary for the reconstruction of the law and should be dynamic to bring peace and justice in society.(Muhamad Helmi Kaffah Nur Iman Andrea Abdul Rahman Azzqy, 2017)

Legal interpretation can be carried out by taking into account the theory of Lawrence M. Friedman who argues that the effectiveness and success of law enforcement depend on three elements of the legal system, namely the structure of law, the substance of law, and the legal culture. The structure of law concerns law enforcement agencies, the substance of law includes legislative devices, and legal culture is the living law adopted in a society. Thus, the legal system theory of Lawrence M. Friedman is in harmony with the theory of Mochtar Kusumaatmadja's development law, as discussed earlier, that good law is one that grows and develops in society (the living law) and is in line with the values of community life. Any developing society is always identified with change, where law in this context has the function of guaranteeing such a change by not positioning itself as an instrument but as a means of change while still paying attention to the reflection of the values of community life in the process of change. The theory of Mochtar Kusumaatmadja's development law also uses a reference framework for the view of the life of Indonesian society and nation, which includes structure, culture, and substance, as stated by Lawrence F. Friedman. Essentially, this provides the basis for the function of the law as a means of renewing society and as a system that is essential for Indonesia as a developing country. The underlying principles of this concept are that order and organization in development and renewal efforts are not only desired but also essential, and that the law, in the sense of norms, is expected to direct human activities towards the desired direction of development and renewal.(Rahmawati, 2017)

Efforts by the Indonesian government to maintain the stability of defense and security against cyber espionage attacks."

Cybersecurity development in Indonesia was initiated in 2007. The development of cybersecurity capacity was realized through a policy that provided legal certainty. The policy was the issuance of the Minister of Communication and Information Regulation No. 26 / PER / M.Kominfo / 5/2007/21 on Security for the Utilization of Internet Protocol-Based Telecommunication Networks. The regulation underwent several revision processes, which finally resulted in the establishment of Minister of Communication and Information Regulation No. 29 / PER / M.KOMINFO / 12/2010. In this regulation, it is also regulated regarding the formation of the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII), which is a team responsible for helping to monitor the security of internet protocol-based telecommunication networks.(Ramadhan, 2017)

In strengthening national security through effective cyber security, Indonesia collaborates both bilaterally and multilaterally. In bilateral terms, Indonesia collaborates with the Netherlands Ministry of Foreign Affairs and the United Kingdom in 2018 which includes information sharing in the field of law, legislation, national policy, and policy management strategies in the cyber realm, capacity building and institutional assistance, and technology development in the field of cyber security through networking and training and education programs, as well as joint efforts to build resilience against cyber attacks and protection of vital assets in the cyber realm and technical aspects that support cooperation. In the same year, Indonesia also collaborated in a wider cyber and digital concept with Australia, which covered digital economics, as well as with the United States. These collaborations aim to advance cooperation and capacity building in the cyber space in areas such as discussion on the development of national cyber strategies, national incident management capabilities, capacity and cooperation in countering cybercrime.

In multilateral terms, Indonesia, together with ASEAN through the ASEAN Regional Forum (ARF) and the ASEAN Political-Security Community (APSC), has an agreement to enhance cooperation in non-traditional threats, specifically focusing on transnational and cross-border crime issues. Then, in 2006, ARF formed ARF on cybersecurity initiatives related to the discussion of cybercrime in ASEAN, which was embodied in ASEAN's Cooperation on Cybersecurity and against Cybercrime. Indonesia's participation in the ARF can provide benefits in the form of point of contact with non-member countries that cooperate through the ARF framework. This can ultimately facilitate Indonesia's cyber diplomacy process, including in handling cyber incidents.(Muhamad Helmi Kaffah Nur Iman Andrea Abdul Rahman Azzqy, 2017)

Indonesia's collaboration in cyber security, both bilaterally and multilaterally, can be categorized as a form of cooperative security. This is because the parties involved in the collaboration are not under coercion and form cooperation based on the same goal of realizing their national security. In addition, there is a shared perception among the parties involved in the collaboration, and there are no zero-sum conditions as in game theory, where if one party gains, the other party does not gain (zero). This is because all parties involved in cooperative security in the field of cyber security benefit from information, equipment assistance, and other benefits in efforts to address threats to national security that they all face together, namely cybercrime.(Adrian, 2022)

Indonesia's strategic position among major powers in the cyber field makes it necessary to establish a cyber institution that deals with both cyber security and cyber diplomacy. Therefore, Indonesia formed the National Cyber and Encryption Agency (BSSN), which plays a role in coordinating and collaborating between institutions and stakeholders in the cyber field, both nationally and internationally. In this context, BSSN has collaborated bilaterally with countries such as Australia, the United Kingdom, the Netherlands, and the United States. At the regional level, Indonesia is also involved in the ASEAN's Cooperation on Cybersecurity and against Cybercrime and the ASEAN Cyber Capacity Program (ACCP). These diplomatic efforts are aimed at maintaining Indonesia's cyber security and sovereignty, with BSSN as the national cyber institution .(Putri et al., 2022)

The military readiness of Indonesia in defending the country's sovereignty and security is still very minimal. This is evident in Article 7 paragraph (2) about the main duties of the Indonesian National Armed Forces (TNI) to uphold the sovereignty of the state and maintain the integrity of the Unitary State of the Republic of Indonesia, which only covers military operations other than war. In military operations other than war, there are 14 tasks assigned, but none of them address the cyber aspect. This aspect, along with convergence, also determines the operation of the military outside of war. Military equipment is not only limited to firearms but also involves the use of information technology because the virtual world cannot be separated from every aspect of life, including the military .

The accountability of a country in international law depends on the type of activity carried out, namely activities that conflict with the international obligations of the country. If the activity is within its jurisdiction, whether it is national or private civil jurisdiction, the country is also responsible. Therefore, there must be a check and balances system for all forms of activity within a country's jurisdiction .

Conclusion

Based on the research and analysis conducted, it can be concluded that cyber media has vulnerabilities that can be manipulated to threaten national security. Therefore, the government needs to take appropriate steps to prevent cyberspace from becoming a threat to national security. By considering these issues, the role of cyber intelligence as a "new" form of national intelligence governance can become clearer and avoid potential problems. In this regard, attention to these issues must be accompanied by solutions in preparing competent human resources, infrastructure, funding, and technology to make cyber intelligence an asset for national and state security interests.

Indonesia's law in dealing with Cyber Espionage as a form of Cyber Warfare that can threaten the stability of defense and security of the Republic of Indonesia is still not able to accommodate it because Indonesian law on Cyber Espionage does not explicitly regulate it, only partially explaining the act of spying, even when done conventionally. Therefore, in its implementation, Indonesian law on Cyber Espionage has vague norms and requires extensive interpretation. Moreover, systematic interpretation is also needed to support the interpretation of articles that are considered relevant to Cyber Espionage. Indonesia's efforts to address the threat of Cyber Espionage include preventive measures through Cyber Defense and Cyber Security, optimizing state tools such as the Indonesian National Army (TNI) as a guardian of national security, and the National Intelligence Agency (BIN) as a platform for early detection of external attacks. In addition, the police force (POLRI) is also placed as a national legal source as a supporting component in the country's defense efforts. Furthermore, the handling of legal efforts in positive Indonesian law with the concept of state accountability is necessary.

Bibliography

Adrian, W. (2022). POTENSI SPIONASE TERHADAP PENGGUNAAN WHATSAPP DALAM BIDANG PERTAHANAN INDONESIA. *Peperangan Asimetris (PA)*, *8*(2), 44. https://doi.org/10.33172/pa.v8i2.1454

Anggoro Yulianto. (2021). Cybersecurity Policy and Its Implementation in Indonesia. *LAW RESEARCH REVIEW QUARTERLY*, *7*(1), 69–82. https://doi.org/https://doi.org/10.15294/lrrq.v7i1.43191

Ardiyanti, H. (1986). *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*. 95–110.

Atmadja, N. P. (2017). Dukungan Indonesia Terhadap Resolusi Anti Spionase Perserikatan Bangsa-Bangsa. *EJournal Ilmu Hubungan Internasional*, *5*(3), 933–948. https://suntzusaid.com

Chotimah, H. C. (2019). 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*(2), 113–128. https://doi.org/10.22212/jp.v10i2.1447

Muhamad Helmi Kaffah Nur Iman Andrea Abdul Rahman Azzqy. (2017). *Aktifitas Spionase Republik Rakyat Tiongkok ke Amerika Serikat (Cyber Spionase*.

Putri, A. W. O. K., Aditya, A. R. M., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*(1), 35–46. https://doi.org/10.34010/gpsjournal.v6i1.6698

Rahmawati, I. (2017). the Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense. *Jurnal Pertahanan & Bela Negara*, *7*(2), 51–66. https://doi.org/10.33172/jpbh.v7i2.193

Ramadhan, I. (2017). Peran Institusi Internasional Dalam. *Populis*, *2*(4), 495–508.

Декі Росдіана

Докторант, факультет права, Ісламський Університет Бандунг

ПРОГРАМИ ДЛЯ СТЕЖЕННЯ В МЕЖАХ АКТІВ ШПІОНАЖУ ЯК ЗАГРОЗА ДЕРЖАВІ

Статтю присвячено дослідженню питання застосування програм для стеження у межах актів шпіонажу. Детально оцінюється їх вплив у різних сферах життя держави, описуються нетипові аспекти та надаються пропозиції щодо захисту від таких програм.

Ключові слова:

Програми для стеження, акти шпіонажу, загроза, збройні сили