The Role Of Cyber Security In Overcome Negative Contents To Realize National Information Resilience

Rustam

{rustampatia@yahoo.com}

Borobudur University

Abstract. The development of information/cyber technology has been used as a medium for the production and dissemination of negative content such as hoaxes, hate speech, fraud, SARA, and so on. In 2017, the Indonesian Ministry of Communication and Information recorded the number of negative content based on complaints reaching 51,456 content. This research uses qualitative methods with discussions using cyber security theory and role play theory approaches. The research results show that the implementation of cyber security carried out by the Indonesian Ministry of Communication and Information's Directorate General of Technology and other institutions such as the Ministry of Defense and the TNI Pusinfolahta has been able to become the basis for cyber security or information security but has not fully overcome the current negative cyber attacks. It is concluded that negative content is part of cyber attacks that threaten the instability of information security and national cyber security.

Keywords: Cybersecurity, Cybercrime, Attack, Content, Blocking.

1 Introduction

The technological revolution takes place with the rapid development of technology and information. This has had a major impact on various aspects of life such as socio-cultural, economic, political, security and defense aspects. Cyber technology or better known as ICT (Information and Communication Technology) brings great opportunities as a driving backbone in various strategic fields. The digital/cyber economy plays a role in replacing manual transactions known as ecommerce, internet marketing and internet banking.[1]

Technology and information become the backbone in the competition in modern human life. At present, humans are entering the era of information civilization. Information civilization also creates human behavior as an information person. Humanity rapidly receives, manages, stores, retrieves and distributes or disseminates information to fellow human beings. Not only is the slogan that "whoever controls information will rule the world", it has become a real law. The more adequate the availability of accurate information will determine the quality of a decision. Information has been considered as "power" which is interpreted as "power" and "power" which greatly determines human fate itself The rapid development of internet users also occurs in Indonesia.[2]

ICL-C 2023, November 11, Jakarta, Indonesia

DOI 10.4108/eai.11-11-2023.2351330

Referring to APJII (Indonesian Internet Service Providers Association) statistical data that internet users in Indonesia in 2011 consisted of 55 million people, 2012 consisted of 63 million people, 2013 consisted of 71.19 million people, 2014 consisted of 107 million people and in 2015 amounted to 139 million people. This shows that internet users in Indonesia are growing rapidly. Thus, information technology becomes an effective medium to influence the minds of the wider community in order to form positive / constructive opinions. On the other hand, information technology is also a threat to the instability of social life of the community, nation and state when the use of knowledge and information technology is used to spread news with negative or destructive content. The dissemination of negative content information through information technology (internet) media with various social media applications, online media and various other internet-based applications tends to be motivated by various interests such as personal / individual competition, business (economic motives) to politics.[3]

The spread of negative content such as fake news, blasphemy, propaganism and agitation has been used to disrupt the security, political and existence stability of the country both from within and outside the country. The spread of negative content with political motives falls into the realm of information war (information war / cyber war). So that this action is beyond the context of ordinary crime (cybercrime). The use of negative content information technology like this has basically become a medium for organizing asymmetric wars by carrying out proxy war attacks (wars that use third parties).

2 Method

This research uses qualitative methods to analyze the role of cyber security in overcoming negative content and realizing national information resilience. In the discussion, this research integrates cyber security theoretical approaches and role play theory. A cyber security theory approach is used to understand the mechanisms, strategies and policies that can be implemented to protect information infrastructure from negative content threats. This includes analysis of relevant threats, vulnerabilities and mitigation measures in a cyber context. Meanwhile, role play theory is used to explore the roles of various actors, such as the government, private sector and society, in facing and handling negative content. By understanding the roles and responsibilities of each actor, this research can identify effective collaborative strategies to increase national information resilience. Through a combination of these two approaches, the research seeks to provide deep insights into how to improve information security and reduce the negative impact of malicious cyber content.

3 Results And Discussion

3.1 Cyber Security Implementation Overview Ministry of Communication and Information Technology of the Republic of Indonesia

The official website of Kominfo RI explained a brief history that the Ministry of Communication and Information Technology (previously named "Ministry of Information" (1945-1999), "State Ministry of Communication and Information" (2001-2005), and Department of Communication and Information Technology (2005-2009), abbreviated as Depkominfo) is a Department of Ministries in the Government of Indonesia in charge of communication and information affairs. The Ministry of Communication and Information is led by a Minister of Communication and Information Technology (Menkominfo) which since October 27, 2014 has been held by Rudiantara.[4]

a. Puskom Kemhan RI

   In accordance with the Regulation of the Minister of Defense of the Republic of Indonesia Number 58 of 2014, the Puskom Kemhan RI or Public Communication Center is a supporting element for the implementation of defense duties and functions under and responsible to the Minister.

b. Pusinfolahta Mabes TNI

   The official website of the TNI Information and Data Processing Center (Pusinfolahta) with http://pusinfolahtatni.mil.id/tugas-dan-fungsi/ URL explained that the TNI Information and Data Processing Center (Pusinfolahta TNI) is a rank that is under and directly responsible to the TNI Commander, as the Central Implementing Agency at the TNI Headquarters level based on the Decree of the TNI Commander Number Kep / 7 / XII / 2006 dated December 5, 2006.

c. National Cyber and Encryption Agency (BSSN)

   The National Cyber and Encryption Agency (BSSN) is a government agency in the field of Information Security and encryption by synergizing with stakeholders both government institutions and the private sector to participate in realizing national security led by the Head of the BSSN Agency who in carrying out his duties is directly under the President of the Republic of Indonesia.[5]

d. Data Analysis and Cyber Security Research Results

   Protection Against Cyber Attack / Cyber Crime The most basic understanding of cyber security is judging from the etymology. Cyber security comes from the English language cyber and security. Cyber means cyberspace or the world of the internet or information technology (IT). Security means security. So that the simplest understanding of cybersecurity is cyber security. Cyber security or cyber security functions or plays a role in overcoming, detecting, finding, counteracting or minimizing the level of risk of interference, threats (cyber threat) and cyber attacks (cyber attacks) as well as all cyber technology activities that threaten the security of all components of the cyber system itself which includes hardware, software, data / information and infrastructure. Referring to the Cybercrime Convention written in the book Cybercrime Legislation, it is explained that the

   target of cybercrime activities is the cyber security system. One of the cyber crime activities is related to negative content. offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; violations related to content or negative content (content-related offences); and 4) copyright-related offences.[6]

e. Key Components of Cyber Security
By understanding that cyber security is a system that plays a role in protecting system information from interference and cyber attacks or all cyber crime activities, cyber security has 3 (three) main components. The cyber security component is a model designed to guide information security policies in an organization as the target of cyber security implementation itself, namely: 1) Confidentiality; 2) Integrity; and 3) Availability.[7]

3.2 Securing Critical Information Infrastructure (Critical Information Infrastructure Security)

Critical information infrastructure is part of several strategic/vital infrastructures in a country. The general description of critical information infrastructure is an infrastructure that combines telecommunications networks and the internet used by the wider community. Security aspects Critical information infrastructure is very important. Disruption of critical infrastructure will have a fatal impact on disrupting and or paralyzing other strategic sectors (economy, defense and security, energy etc.). Information technology infrastructure becomes the backbone of the running of information in various political, economic, social, cultural, defense and security lines increasing the potential for threats / disruptions to internet technology systems National Critical Information Infrastructure Security is an absolute must to be held for the effectiveness of reliability, availability and integrity of information networks, at the national and international / global levels.[8]

Strategic Policy on Critical Infrastructure in Indonesia In the Cyber Defense Guidebook compiled by the Ministry of Defense of the Republic of Indonesia, 2014, it is stated that critical infrastructure is an asset, system, or network, in the form of physical and virtual which is very vital, where disruption to it has the potential to threaten security, national economic stability, safety and public health or a combination of them. Indonesia has defined the importance of critical infrastructure globally, but does not yet have provisions at the strategic national level or legislation that specifies areas that are calcified as objects of national critical infrastructure. Critical information infrastructure protection (CIIP) by developed countries such as the United States has been established as a national policy involving government institutions and self-reliance in a national coordination. CIIP implementation is formed in a professional and comprehensive system and organization / institution. CIIP is built with Four Model Pillars, namely: 1) Prevention and Early Warning, 2) Detection, 3) Reaction; and 4) Crisis Management. 2. National Critical Infrastructure America America as one of the developed countries, has established 16 critical infrastructure sectors that are vital to America's national interests. Sixteen critical infrastructures are: a) Chemical Sector, b) Communications Sector, c) Dams Sector, d) Emergency Services Sector, e) Financial Services Sector, f) Government Facilities Sector, g) Information Technology Sector, h) Transportation Systems Sector, i) Commercial Facilities Sector, j) Critical Manufacturing Sector, k) Defence Industrial Base Sector, l) Energy Sector, m) Food and

Agriculture Sector n) Healthcare and Public Health Sector, o) Nuclear Reactors, Materials, and Waste Sector, p) Water and Wastewater Systems Sector.[9]

3.3 Negative Accounts Negative Content as a Cyber Attack (Cyber Attack)

The internet and its technology increasingly dominate the role in various lines of life both in the fields of government, business, science, social and other fields. Similarly, in the flow of information and communication traffic, the internet has become the backbone. The internet has connected almost all humans (netters) and devices in all corners of the world. According to eMarketer records, in 2017 eMarketer estimates that Indonesian internet users (netters) will reach 112 million people, while the number of internet users worldwide is projected to reach 3 billion people in 2015 and 2018, estimated to reach 3.6 billion people. The data illustrates the internet as an opportunity for various positive things for humans. But besides the use of the internet as an opportunity also contains negative potential for the international, regional and national communities. The use of internet technology to spread negative content such as fake news (hoax), hate speech (hate speec), fraud, racial issues,, terror and so on, has a high potential to be done massively and easily by netters.[10]

Understanding of negative content is generally understood as a content of news or information or distribution in the form of images, videos, sounds and texts that can be considered negative in terms of ethical, social, religious and legal aspects. According to M. Salahuddien (Information Technology practitioner and consultant), currently serves as Vice Chairman of ID-SIRTII (Indonesia Security Incident Response Team On Internet Infrastructure) in the article Concept of Filtering Porn Content on the Internet (https://inet.detik.com) that in Indonesia what is meant by negative content on the internet is that which contains acts prohibited in Law Number 11 of 2008 concerning Electronic Information and Transactions

3.4 Types of Negative Content

In accordance with the Cybercrime Convention written in the book Cybercrime
Legislation and Law of the Republic of Indonesia number 11/2008 concerning ITE formulated universally negative content covering all activities of attacks and cybercrimes, as follows: 1) Pornography, 2) SARA, 3) Slander or hatespeech, 4) Gambling, 5) Fraud Action, 6) Disputing Society, 7) Terrorism / Radicalism, 8) Trade Products with Special Rules, 9) Fraud Trade Products, 10) Children Violence Information Security Threat; and 11) Attack activity or other cybercrime.[11]

3.5 Perpetrators of Negative Content

Negative content can be created or disseminated by any internet user (user generated). Negative content can be done by utilizing social media platforms or applications
such as Bigo Live, Twitter, Instagram, Facebook and others. While the perpetrators of negative content itself consist of the level of individuals / individuals, groups and even larger organizations, carried out by bringing up real identities, fake account identities (fake accounts) and / or without

identity (anonymous). The spread of negative content is massive, more likely to be done by buzzers or robot systems (boot accounts) where accounts are designed to work machine or automatically.[12]

3.6 The Role of Cyber Security in Overcoming Negative Content

The results of research conducted on the role of cyber security in overcoming negative cyber content or cyber in Indonesia show that cyber security is a backbone (backbound) which has a broad role that is manifested in a defense system and as the main tool to deal with negative content attacks on the internet. Based on the approach to role theory that the role dimension can be a role as a policy, tool, dispute resolution or shock therapy role.[13]

1) Cyber Security as policy. In handling negative cyber content in Indonesia, the government is present through the Director General of Aptika Kominfo RI with a policy, namely upstream and downstream handling.
2) Cyber Security as an instrument or tool of Cyber Security as a way to overcome negative content cyber attacks is implemented by empowering Newsletter application technology and crowling system.
3) Cyber Securiti as Shock Terapy. The act of distorting and filtering the content also gives the effect of shock terpy
4) Cyber Security as Dispute Resolution

3.7 Negative Content, Indonesia's Biggest Internet Threat Today and in the Future

According to the results of the study, some of the main factors that drive the development of negative internet content in Indonesia include:[14]

1. The rapid development of internet users (netter) in Indonesia
2. IT infrastructure development
3. Lack of digital literacy

At the coordination meeting of the Ministry of Communication and Information of the Republic of Indonesia with Commission I of the House of Representatives on November 28, 2017, it was conveyed that in the period January - October 2017, there were 51,456 negative content on the internet based on public complaints.18 The results showed that in 2016, the number of complaints processed and submitted by the Indonesian Ministry of Communication and Information for take down action on new content was carried out by 50%, while in 2017 it increased to 55%. This shows that the handling of negative content has not reached the optimal point. Moreover, the amount of complaint content that
has not been acted upon will be a contributor to the following year's threat.

4 Conclusion

Cybersecurity plays an important role in protecting information security and national stability from the threat of negative content spread digitally. Negative content, such as disinformation, hate speech, and propaganda, can be part of cyberattacks designed to cause social, economic, and political instability. By implementing effective cybersecurity strategies, including monitoring, early detection, and rapid response to these threats, a country can improve national information resilience. In addition, public education about digital literacy and cooperation between government, the private sector and society are key to creating a safe and trustworthy information environment. This joint effort will help minimize the impact of negative content and strengthen overall cybersecurity.

References

[1] F. D. Silalahi, *Cyber Security*. Semarang: Penerbit Yayasan Prima Agus Teknik, 2022.

[2] H. Ardiyanti, "Cyber-security and its development challenges in Indonesia," *J. Polit. Dyn. Domest. Polit. Issues Int. Relations*, vol. 5, no. 1, 2016.

[3] I. Ramadhan, "Cyber Security Strategy in Southeast Asia Region," *J. Asia Pacific Stud.*, vol. 3, no. 2, pp. 181–192, 2019.

[4] Ruswanto.R, "DESIGNING ANDROID-BASED GUEST DATA COLLECTION APPLICATION (CASE STUDY: PUSINFOLAHTA TNI)," *(Doctoral Diss. Univ. Mercu Buana Bekasi)*, 2022.

[5] D. A. Sudarmadi, U. Indonesia, A. Josias, and S. Runturambi, "Jurnal Kajian Stratejik Ketahanan Nasional Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia," *J. Kaji. Strat. Ketahanan Nas.*, vol. 2, no. 2, pp. 157–178, 2019, doi: 10.7454/jkskn.v2i2.10028.

[6] I. Koto, "Cyber Crime According to the ITE Law," *Int. J. Reglem. Soc. (IJRS*, no. August, pp. 103–110, 2021, doi: 10.55357/ijrs.v2i2.124.

[7] A. D. Rahman, A. F., Anwar, S., & Sumari, "Analysis of the minimum essential force (MEF) in the framework of cyber-defense development," *J. Def. State Def.*, vol. 5, no. 3, pp. 63–86, 2018.

[8] D. A. S. Ilhami, "Data Privacy and Cybersecurity in Smart-City: A Literature Review," *J. Sci. Reason. Inf. Technol. Appl.*, vol. 2, no. 1, 2022.

[9] R. A. Prastyanti and R. Sharma, "Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India," *J. Hum. Rights, Cult. Leg. Syst.*, vol. 4, no. 2, pp. 354–390, 2024, doi: 10.53955/jhcls.v4i2.200.

[10] K. Shu, A. Sliva, J. Sampson, and H. Liu, "Understanding cyber attack behaviors with sentiment information on social media," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10899 LNCS, no. June, pp. 377–388, 2018, doi: 10.1007/978-3-319-93372-6_41.

[11] C. Wulandari, "Kebijakan Kriminal Non Penal Dengan Techno Prevention (Analisis Pencegahan Konten Negatif Melalui Internet)," *Pandecta*, vol. 15, no. 2, pp. 228–241, 2020.

[12] I. P. S. Siregar, G. T., & Sihite, "Criminal Law Enforcement for Perpetrators of Disseminating Pornographic Content on Social Media is reviewed from the Electronic Information and Transaction Law," *RECTUM J. Juridical Rev. Crim. Handl.*, vol. 3, no. 2, pp. 1–11, 2020.

[13] H. C. 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]," *J. Polit. Din. Masal. Polit. Dalam Negeri dan Hub. Int.*, vol. 10, no. 2, pp. 113–128, 2019, doi: 10.22212/jp.v10i2.1447.

[14] D. R. S. Astarini and M. S. Rofii, "Siber Intelijen Untuk Keamanan Nasional," *J. Renaiss.*, vol. 6,

no. 1, p. 703, 2021, doi: 10.53878/jr.v6i1.143.