JOURNAL OF SOCIAL SCIENCE
jsss.co.id
ISSN : P 2720-9938 E 2721-5202

DEVELOPMENT OF CYBER WEAPONS TO IMPROVE INDONESIA'S CYBER SECURITY

Achmad Wardana[1], Gunaryo[1,2], Y.H. Yogaswara[1,3]
Faculty of Defense Technology, Indonesia Defense University, Indonesia[1]
Defense Research and Development Agency, Ministry of Defense, Indonesia[2]
Research and Development Service, Indonesia Air Force, Indonesia[3]
Email: achmad.wardana@tp.idu.ac.id, gunaryo@idu.ac.id, yh.yogaswara@idu.ac.id

ARTICLE INFO

Received : 21 April 2022
Revision : 01 May 2022
Received : 17 May 2022

Keywords:
Cyber weapons; cyber security; technological developments

ABSTRACT

It is indisputable that technical advancements have an impact on a country's military capability and security. This is inextricably linked to the deployment of numerous technologies and new discoveries aimed at boosting the military's defense system. As a result of this predicament, all governments are attempting to modernize their defense systems in order to deal with dangers posed by technological advancements. This is both a challenge and an opportunity for Indonesia's existing defense system. The goal of this study is to look into the development of cyber weapons and how they may help Indonesia improve its cyber security. The purpose of this study is to utilize a descriptive qualitative technique to investigate or explain the concerns surrounding the importance of cyber weapons in strengthening cyber security in Indonesia. The conclusions of this study show that as the number of Internet users grows, so does the global trend of cyber attacks. It's difficult to compare precision cyberweapons systems to existing kinetic weapons because of their new nature. Additionally, the development and use of cyber weapons can yield economic rewards. Human resources, as well as support and cooperation from Indonesian cyber defense groups with professionals in the field of hacking, are all crucial variables to consider while designing cyber weapons.

Introduction

Military history provides a rich literature on war and technology, but the focus tends to be on the importance of technology in helping the military win the war. It is undeniable that technological developments have an effect on military power and defense of a country (Chin, 2019). This is closely related to the deployment of various new technologies and inventions aimed at improving the military defense system. As a result of these difficulties, all governments are trying to modernize their defense systems to deal with the dangers posed by technological advances. For Indonesia's current defense system, this is both a challenge and an opportunity (Rachmat, 2014).

To produce the latest technical instruments, after increasing human resources, the next most important step is mastering technology. Technology mastery cannot be carried out by one institution or agency. For instance, Internet of Things, cloud computing, and other developing technologies are broadening cyberspace's meaning (Zheng, Li, Xu, & Zhao, 2021). On the other hand, mastery of technology requires close collaboration between several institutions, such as educational institutions that produce reliable human resources, especially those directly involved in defense work, R&D institutions to increase

How To Cite: Wardana, A., Gunaryo, & Yogaswara, Y. H. (2022). Development of Cyber Weapons to Improve Indonesia's Cyber Security. *Journal of Social Science. 3*(3). https://doi.org/10.46799/jss.v3i3.334
E-Issn: 2721-5202
Published By: Ridwan Institut

technological mastery, and national industries that produce equipment needed en masse (Hutahuruk, Bura, & Wibowo, 2020).

Cyberspace as it is known in Indonesia, is an operational area that creates, stores, transforms, and exchanges information using electricity or electromagnetism. Previously, regional control was the main focus; However, in this era of increasingly advanced technology, the control is more virtual, namely the control and management of cyberspace stored in big data. Cyberspace weapon arsenals are constructed by exploiting target defense flaws (Sokri, 2018). In contrast to traditional national sovereignty with physical boundaries, cyber sovereignty does not have clear de jure boundaries, but must be ensured to provide security for the country's strategic activities. The power of the network appeals to all participants because of its low cost and high impact potential (Hidayati & Gultom, 2019).

Since 2003, crimes using information technology have increased, such ascredit card fraud, ATM/EDC looting (early 2010), hacking, cracking , phishing (online banking fraud), malware (virus/ worm/ trojan), robots), cybersquatting, pornography, online gambling, transnational crime (drug trafficking, mafia, terrorism, money laundering, human trafficking, underground economy) (ID SIRTII /CC (Islami, 2018). In addition, the proliferation of hoaxes is made possible through cyberspace with the widespread adoption of Facebook, Twitter, WhatsApp, Line, Google+, and other new media platforms, which enable the rapid dissemination of information through high levels of interactivity and interconnectivity.Hoax has spread uncontrollably through cyberspace, and some have serious social implications. In response to hoaxes, people are killed and national stability and security are threatened.hoaxes involve fake news about sensitive issues of ethnicity, religion, and race as well as hate speech directed at those in power (Gunawan & Ratmono, 2020).

Cyber crime and cyber war not only jeopardizes personal security through the acquisition of personal assets. Notable incidents include: identity and data theft (source of information) and account hijacking, cases of transmission of viruses embedded in files and websites and important code, defamation, blasphemy, or defamation (Soewardi, 2013). Likewise, industrial espionage and piracy of important information resources are rampant today. All of this has created turmoil in society due to loss of privacy and threats of loss of assets and assets. The online world can also be used as a political tool to spread fake news for political provocation and economic engineering.

Indonesia is still in the stage of development and strengthening, not yet leading to the development of cyber weapons (cyber-weapons) capable of counterattacking during cyber wars (Hidyati & Gultom, 2019). Research data shows that the trend of global cyber attacks is increasing along with the increasing number of internet users. To strengthen cyber defense, Indonesia needs to consider the development of cyber weapons. Therefore, this study aims to examine the development of cyber weapons in strengthening cyber security in Indonesia.

Method

This study uses a descriptive qualitative approach by exploring or explaining more broadly the issues related to the importance of cyber weapons in strengthening cyber security in Indonesia. The research focuses on cyber attack trends in Indonesia and the development of cyber weapons. Data collection was carried out through a literature review from reputable national and international journals, ebooks, and online media

Results And Discussion

A. Cyber Security trend in Indonesia

Cyber security can be defined as a series of activities and actions aimed at preventing attacks, intrusions or other threats through elements of cyberspace (hardware, software, computer networks) (Islami, 2018). In Indonesia, the emergence of new media has revived the civil society movement and empowerment, especially after the fall of the New Order regime. Cyberspace seems to promise freedom of expression and active participation of citizens in the political process. At the same time, elections, a common manifestation of the democratization process, faced strong public distrust. Few citizens trust political

parties or the commitment and performance of politicians. There was considerable public disillusionment and resistance to the political process. In cyberspace, people have a greater opportunity to voice criticism and fight those in power, something that is impossible under an authoritarian regime. However, the resulting excesses become the basis for false news and hate speech in Indonesia (Gunawan & Ratmono, 2020).

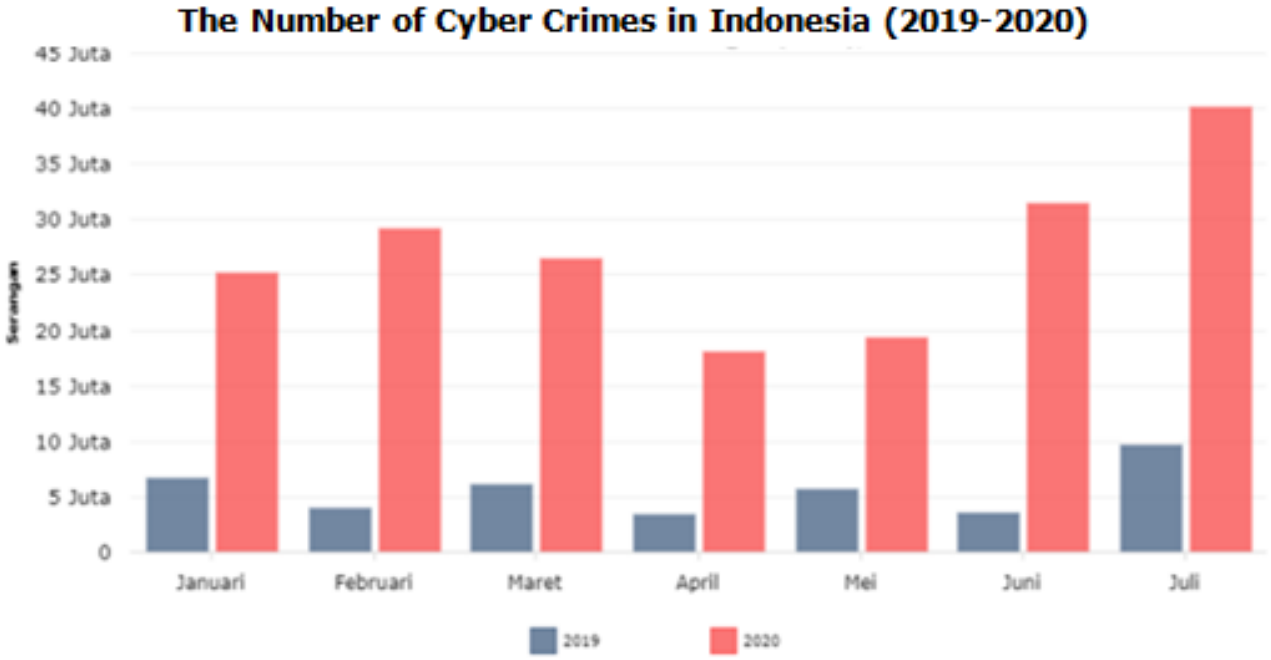

Figure 1. Number of Cyber Crimes in Indonesia (2019-2020)
Source: (Databoks, 2020b)

From January to July 2019, Indonesia experienced at least 39.3 million cyber attacks. In the year since, that number has almost tripled. BSSN reported that as of last July, 189.9 million had been discovered, with the most common types being internet site attacks, data collection, and Trojans being examples of cybercrimes. Trojans are virus attacks that can silently install and steal user's sensitive data.

Based on the Interpol 2020 report titled "Cybercrime: The Impact of Covid-19" it shows that there are 4 types of internet cyber attacks related to Covid-19, the majority of which occur during the pandemic. Phishing/scam crimes are the most common, accounting for 59% of all crimes. Notably, nearly two-thirds of the surveyed member countries reported the use of Covid-19 topics related to phishing scams and cybercrimes since the virus epidemic. This was accompanied by malware/ransomware attacks (36%), suspicious domains (22%), and fake news (22%). (14 percent) (Databoks, 2020a).

There is a lot of literature related to the detection of cyberattacks including research conducted by (Zhou, Han, Liu, He, & Wang, 2018), in his journal it is explained that with the accelerated growth of internet of things (IoT) applications in recent years Lastly, cities are becoming smarter to optimize resources and improve people's quality of life. On the other hand, IoT faces severe security issues such as confidentiality, integrity, privacy and availability. To prevent irreversible damage from cyber attacks, researchers propose a framework, called DFEL, to detect internet intrusions in IoT environments. Through the experimental results, the researchers found that DFEL not only improves the accuracy of the classifier for predicting cyberattacks, but

also significantly reduces the detection time.

B. Development of Cyber Weapons

In the decades following the creation of the Internet, cyberspace has become an area of conflict as countries enhance their cyber capabilities by creating sophisticated arsenals of cyber weapons; adding specialized personnel and force structures, and engaging in and seeking cutting-edge research and development resources of offensive and defensive capabilities. It is estimated that about 140 countries have developed, or are developing, the capacity to foment cyber armed conflict. In fact, in 2016 at the Warsaw Summit, NATO announced that cyberspace is now considered a domain of operations in which it must defend itself as effectively as it does in the air, on land and at sea. This declaration is widely believed to be an acknowledgment that cyber threats are becoming more common, complex, and potentially destructive. At the heart of this trend is the development and use of cyber weapons. To date, relatively few examples of cyberweapons are publicly recognized. The most well-known and controversial cyber weapon is the so-called Stuxnet worm (Wallace, 2018).

From the definition of a weapon (weapon), namely a device that threatens or causes physical, functional, or mental damage to structures, systems, or organisms As a result, networks can be defined as an internet weapon if the computer model is aimed at destroying the integrity or accessibility of data in an adversary's IT The system is primarily used for defense equipment. Thus, cyber weapons are computer code or physical tampering, operation or damage to critical infrastructure structures or systems used or designed for threatening purposes, military email services, refinery and pipeline explosions, flight control system failures, freight trains and subway derailments. , power plant failures, and even satellites can all get out of contro (Hidayati & Gultom, 2019).

Referring to the journal article written by (Nguyen, Ngo, Duong, Tuan, & Da Costa, 2017) To improve the performance of confidentiality protection scenarios, understanding the unauthorized side is very important. In this paper, from an illegitimate point of view, security attacks from full-duplex cyber weapons equipped with massive antenna arrays are considered. In order to evaluate the behavior of the proposed cyberweapon, the researcher developed a closed form, strict approach, and asymptotic expression of the level of ergodic secrecy that can be achieved by considering imperfect channel estimation in cyberweapons. The results show that even under some adverse conditions, namely, imperfect channel estimation and self-interference, full-duplex can disable traditional physical layer protection schemes, i.e., increase the transmit power and number of antennas in the legitimate transmitter. In addition, when the transmission power optimization scheme to maximize the difference between the eavesdropping rate and the legitimate rate is applied to full-duplex cyberweapons, malicious attacks are even more dangerous. The results also reveal that when legitimate parties face adversaries in advance, it is important to prevent critical information in the training phase from being exposed to unauthorized parties.

Moreover, the research entitled Cyber Weapon Model for the National Cybersecurity written by (Bae, 2019). In this paper, the researcher analyzes the cyber kill operations, and military operations as initial information on cyber operations for national cyber security. Through this, cyber attack operating procedures for cyber security are established, and cyber weapon configuration and function modeling is carried out. The cyber battlefield environment is still evolving, and continuous research is needed for the nation's cyber security. In addition, this paper has improved the efficiency of cyber operations through the composition of target management and cyber weapons operational management.

In the military world, the existence of cyber soldiers has become inevitable, as the United States, North Korea, China, Singapore, Australia, etc. already have cyber soldiers. on October 2017, TNI

formed a network unit (satsiber) with the aim of protecting information resources within the TNI from interference and misuse or exploitation by other parties. (Hidayati & Gultom, 2019) If the leadership of a country has determined that billions of dollars must be spent on capabilities kinetic weapons to provide national security, the high cost of kinetic weapons alone would suggest that careful consideration should be given to the development of precision cyberweapons systems that can achieve a similar, or free, effect for many kinetic weapons. In some cases, the investment required to develop and deploy cyber capabilities may be less than kinetic capabilities. If the effects of the cyber weapons system benefit the military in any way, the return on investment could be much higher than the other options. (Hare, 2019) below is a comparison of the costs of kinetic weapons with cyber weapons.

Table 1
Cost comparison between conventional and cyber weapon systems.

Cost Compenents	Kinetic Weapon	Cyber Weapon
Delivery platform development	Each new weapon system requires extensive configuration and, in many cases, competition among construction companies to ensure that it meets the specific needs of the domain (air, land and sea).	Limited requirements for platforms to undergo testing in extreme environments
Platform Construction	Aircraft, naval vessels, and tanks must be built to operate in extreme conditions and withstand kinetic attacks	Some capabilities can be used, but must be strengthened, and many of them can be used to target "soft" infrastructure.
Development, testing, and evaluation ammunition effects	Military email systems, oil refinery and pipeline explosions, air traffic control system failures, freight and subway accidents, power plant failures, and even geosynchronous orbits can all spiral out of control.	Cyberweapons systems should also be inspected remotely to evaluate their impact and find unintended consequences or further damage. Since most tests do not cause physical damage, the ringer can be widely used.
Intelligence preparation.	Kinetic weapons are usually designed to be effective destroying a target with sufficient intelligence to hit the closest attack. Nonetheless, their work does require sufficient intelligence to identify and locate potential targets. The more precise the operation, the more intelligence required	To be effective, a cyber weapon usually requires very high precision. If one IP address number is wrong, the weapon will have no effect at all. The intelligence required is often "layered" so that multiple intelligence gathering operations must be carried out before cyber operations can even be considered an option.
Construction, maintenance, and dispensing of ammunition.	Precision weapons require the storage of complex and expensive components in separate, high-security locations after deployment. When ammunition is used, it must be destroyed.	All components of the weapon system can be stored in locations at low cost. Each software payload can be reused until the enemy develops an effective counter. Then it may only need to be modified slightly to remain effective, or it may need to be completely re-engineered
Training personnel	All individuals in charge of weapons systems must be undergo realistic	operators cyberspace requiring several years of training to

	training for combat operations. Before becoming combat ready, fighter pilots must complete several years of training. It is also necessary to consider the cost of their training aircraft.	eligible, but training can take place in a classroom on a software-updated platform for several years before the training system becomes obsolete.
path. access.	Kinetic weapons depend on the existing domain in which they operate (air/ground/sea).	Parts of the access point may need to be engineered by cyber operators and enablers to ensure that the payload reaches the target.
Reconstruction. destroyed targets	when .kinetic weapons destroy. bridges, cell towers, or power plants, the system must be rebuilt.	Most targets take minimal or no physical damage. The effect is reversible.

Source: (Hare, 2019)

To ensure that the potential benefits of precision cyberweapons systems are realized and the problems raised by detractors are minimized, several steps must be taken to create an effective capability. First, the professional military will form a special corps of cyber operators. These operators cannot be "double hat" that is, they should not have technologically related but potentially conflicting responsibilities in intelligence or communications. Personnel must be dedicated to cyber operations missions and receive appropriate training in conducting combat operations to ensure effective integration with conventional military weapons systems. Cyber operators should be trained in armed conflict laws to reduce the likelihood of carrying out operations that violate those laws, as operators will be held accountable for their actions in the same way as infantry pilots or bomber pilots.

Conclusion

Based on the results of the analysis, conclusions can be drawn in this study as follows. The global trend of cyber attacks is increasing along with the number of Internet users. in cyberspace disruption and the possible legal, moral, and other implications of such strategic incidents. Many writers and popular media have warned of the dangers that will confront us as a result of the massive blaze of cyberspace. There are strong arguments for using precision cyberweapons systems in combat to reduce the risk of harm to cyber operators using the capability, the risk to enemy combatants, and the risk to civilians. Additionally, when military commanders have access to the right cyberweapon options, their troops can conduct effects-based operations more effectively. Finally, while the new nature of precision cyberweapons systems makes it difficult to directly compare them with current kinetic weapons, there are economic benefits that can be realized through their development and use. Wrong. one. An important factor that needs to be considered in developing cyber weapons is the reliable Indonesian Human Resources (HR) factor, especially in the IT field. Therefore, support and cooperation from Indonesian cyber defense organizations are needed which have experts in hacking field.

References

Bae, S.-H. D.-W. (2019). Cyber Weapon Model for the National Cybersecurity. *Journal of the Korea Institute of Information and Communication Engineering*, *23*(2), 223–228. Google Scholar

Chin, W. (2019). Technology, war and the state: Past, present and future. *International Affairs*, *95*(4), 765–783. Google Scholar

Databoks. (2020a). Phising dan Malware, Serangan Siber Paling Banyak Selama Pandemi.

Databoks. (2020b). Tren Serangan Siber Meningkat Selama Pandemi Covid-19.

Gunawan, B., & Ratmono, B. M. (2020). Social Media, Cyberhoaxes and National Security: Threats and Protection in

Indonesian Cyberspace. *International Journal of Network Security*, *22*(1), 24–35. Google Scholar

Hare, F. B. (2019). Precision cyber weapon systems: An important component of a responsible national security strategy? *Contemporary Security Policy*, *40*(2), 193–213. Google Scholar

Hidayati, S., & Gultom, R. A. G. (2019). Analisis Kebutuhan Senjata Siber dalam Menigkatkan Pertahanan Indonesia di Era Peperangan Siber. *Jurnal Teknologi Persenjataan*, *1*(1), 79–96. Google Scholar

Hutahuruk, J., Bura, R. O., & Wibowo, H. B. (2020). Analisis Karakteristik Material Padat (Ammonium Perchlorate) Propelan Komposit Terhadap Kinerja Propelan Lembaga Penerbangan Dan Antariksa Nasional (Lapan) Dalam Rangka Penguasaan Teknologi Propelan. *Jurnal Teknologi Persenjataan*, *2*(1), 51–64. Google Scholar

Islami, M. J. (2018). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *8*(2), 137. Google Scholar

Nguyen, N. P., Ngo, H. Q., Duong, T. Q., Tuan, H. D., & Da Costa, D. B. (2017). Full-duplex cyber-weapon with massive arrays. *IEEE Transactions on Communications*,*65* (12), Google Scholar

Rachmat, A. N. (2014). Tantangan dan Peluang Perkembangan Teknologi Pertahanan Global Bagi Pembangunan Kekuatan Pertahanan Indonesia. *Jurnal Transformasi Global*, *1*(2), 199–212. Google Scholar

Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. *Media Informasi Ditjen Pothan Kemhan*. Google Scholar

Sokri, A. (2018). Optimal resource allocation in cyber-security: A game theoretic approach. *Procedia Computer Science*, *134*, 283–288. Scopus

Wallace, C. D. (2018). Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis. *Tallinn Paper*, (11), 11. Google Scholar

Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2021). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*. Scopus

Zhou, Y., Han, M., Liu, L., He, J. S., & Wang, Y. (2018). Deep learning approach for cyberattack detection. *INFOCOM 2018 - IEEE Conference on Computer Communications Workshops*, (November), 262–267. Google Scholar