BUILDING INDONESIAN NAVY CYBERSECURITY AWARENESS AS PART OF INDONESIA'S SEA DEFENCE STRATEGY

Syaeful Bakhri
siipul80@gmail.com
Sea Defense Strategy Faculty of Defense Strategy
Republic of Indonesia Defense University

ABSTRACT

The development of information technology advances in the cyber world today, making changes to human social life, which has positive and negative impacts. Cybercrime in the form of attacks through communication and data networks that cause disruption to the nation's security and defense systems. This attack can increase in escalation, so it requires special attention to overcome it. The Indonesian Navy as the main component in the Sea Defense Strategy is also not immune from this cyber threat. In order to realize the strategic objectives of sea defense, by building cyber security awareness of data and information in general so that it is protected from hackers, which starts from personal awareness, especially those who manage crucial data and information. The methodology used in this article is a literature study with a theoretical approach to communication and cyber defense with the literature of defense ministry regulations that provide guidelines for handling cyber defense, to find solutions to cyber threats and attacks by building cyber security awareness in Navy personnel. By studying the possibility of attacks and gaps in the system that can be a weakness used by hackers, it can be concluded that most attacks are from human errors that are less aware of the security of data and crucial information both personal and organizational. By taking examples of cyber attack cases during 2019.

Keywords: Indonesian Navy, Cyber awareness, Cyber defense, Cyber-attack, Information technology.

A. PREFACE

With the development of information and digital technology today, which has spread to all aspects of life, it is very helpful for human civilization and life. In terms of relationships and information exchange that no longer recognize the boundaries of space and time, this significantly improves the quality of life, both human life as an individual and humans in the social community of the state.

But in addition to these benefits, logically there must be a negative impact in the form of threats to the exchange of information which is currently very common and fast, with the emergence of hackers who penetrate and cause disruption to public service systems and theft of sensitive or confidential data.

Cyber threats that exist today occur due to many factors, one of which is human error that occurs due to lack of concern for data security, related to the use of information technology which has now become part of life.

By analyzing the development of work culture, and information on existing cyber threats and attacks, the possibility of human error must be minimized. In the military, especially the Indonesian Navy, there is also no escape from the problem of cyber threats and attacks, therefore it is necessary to build awareness of cyber security as part of Indonesia's sea defense strategy.

B. RESEARCH METHOD

In this article, the research method is conducted using qualitative research methods, with the collection and analysis of data (text, video, audio) to understand concepts, opinions, or experiences. It can be used to gather in-depth information about an issue or generate new concepts for research. Each research approach involves the use of one or more data collection methods. In this study, researchers used secondary research by collecting existing data in the form of text, images, videos. As well as literature studies from several BSSN books and articles, national and international cyber experts.

C. RESULTS AND DISCUSSION

The need for efforts to build cyber security awareness in the Navy, both human resources and infrastructure, is an urgent step, related to cyber from a communication perspective "the heralding of a second media age is almost exclusively based on the rise of interactive media, most especially the Internet" (David Holmes. 2005). Cyber is one of the interactive communication media via the internet, which has indeed been used as a domain in the technology and work activities of the Navy.

Therefore, the Indonesian Navy, which is the main force in the sea defense strategy, also has the risk of cyber threats and attacks that can cause disruption to communication and cyber infrastructure.

To start the discussion, this article includes the Regulation of the Minister of Defense of the Republic of Indonesia, Number 82 of 2014, concerning Cyber Defense Guidelines. Which contains guidelines and explanations of the general concept of Indonesia's cyber defense by state institutions and ministries. Further discussion will be discussed in the literature and comprehensive discussion in the following study.

Cyberspace

Cyberspace is a space where communities connect with each other using a network, namely the internet, to carry out various daily activities. Cyberspace is an area closely related to "the use of electronic devices and the electromagnetic spectrum to store, transform, or exchange information to a global scope, through networked information systems and the physical infrastructure that supports them" (Kuehl, D., & Pudas, T., 2010).

This area has a unique character because although it still requires technology, it no longer relies solely on physical space such as land and sea. Therefore, in cyberspace there are opportunities to exploit information, human interaction, and intercommunication. With these three important elements, cyberspace holds the potential as a source of cyberpower for users, be it individuals, organizations, or countries.

The term "cyberspace" is used in a book by Werner J Severin and James W Tankard Jr entitled Communication Theorie: Origins, Methods, & Uses in the Mass Media, and then cyberspace was popularized by science fiction writer William Gibson in his book entitled Neuromencer, so it became a term often used to refer to the metaphorical realm of electronic communication, where cyberspace is the place of interaction.

"A theory of communication must be developed in the realm of abstraction. Given that physics has taken this step in the theory of relativity and quantum mechanics, abstraction should not be in itself an objection" (D. Holmes, 2005). According to D. Holmes, cyberspace objects are not limited to physical space in the context of abstraction. So that all events in cyberspace are not limited by physical space and time, interaction and communication can be done quickly and instantly, by individuals or organizations effectively and practically cannot be implemented.

Gibson describes cyberspace as, A consensual hallucination experienced daily by millions of legitimate operators. A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the

nonspace of the mind, clusters and constellations of data. Like city lights, receding. (Gibson, 1984).

Cyber security

National cyber security is all efforts in order to maintain the confidentiality, integrity and availability of information and all supporting facilities at the national level, which are cross-sectoral in nature. Which is intended for protection against cyber attacks.

Law of the Republic of Indonesia Number 3 of 2002 concerning State Defense. It states that national defense aims to maintain and protect the sovereignty of the state, the territorial integrity of the Unitary State of the Republic of Indonesia (NKRI) and the safety of the entire nation from all forms of threats, both military and non-military threats.

Non-military threats, especially in cyberspace, have caused the state's ability in the field of soft and smart power defense to be improved through the strategy of deterrence, action and recovery of Cyberdefense in order to support the implementation of a national cyber security strategy led by the Ministry of Communication and Information Technology.

Furthermore, cyber security has become a horizontal multi-domain discipline that encompasses many fields and approaches. Indeed, due to the connection between various aspects of our digital and physical lives, the concept of cybersecurity involves knowledge coming from many different, and sometimes very distant, disciplines (European Commission and Directorate General for Research and Innovation, 2017).

Cyber Attack.

Cyber Attacks are all forms of actions, words, thoughts either intentionally or unintentionally carried out by any party, with any motive and purpose, carried out in any location, which are targeted at electronic systems or their content of information or equipment that is highly dependent on technology and networks on any scale, against vital and nonvital objects in the military and non-military spheres, which threaten state sovereignty, territorial integrity and national safety.

Some of the incidents related to cyber attacks include the Facebook data theft scandal for Donald Trump's election campaign. Indonesians and the world were also preoccupied with the issue of personal data misuse by FaceApp.

Cyber attacks targeting Indonesia during the period January to November 2020 reached 423 million times. This figure is based on data from the National Cyber and Crypto Agency (BSSN) in 2019. The number tripled compared to the same period last year. These statistics need to be a concern for internet users in Indonesia. Because cyber attacks are not only related to hardware or software.

Head of BSSN Hinsa Siburian stated that these attacks are divided into two characteristics, namely social and technical attacks. Social attacks are attempts to influence people in and through cyberspace and tend to be closely related to political warfare, information warfare, psychological warfare, and propaganda.

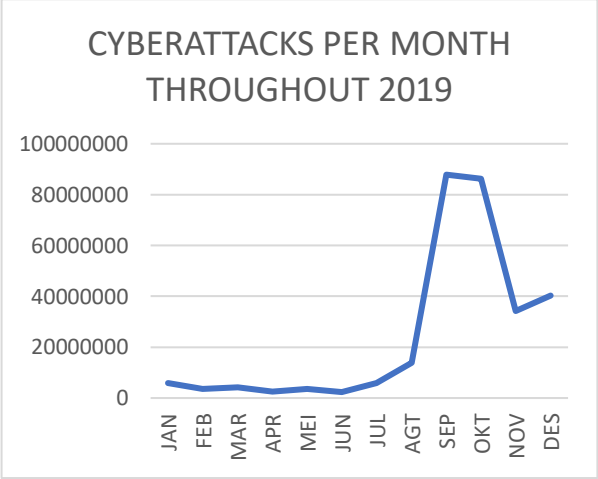

Figure 1. 2019 cyber attacks
Source: Mata Garuda - IDSIRTII, 2019

Threat Types

Threat Types According to Michael D. Mcdonnell and Terry L. Sayers, cyber threat types are categorized into:

1. Hardware threats, which are threats caused by the installation of certain equipment that functions to carry out certain activities in a system, so that the equipment is a disruption to the Network system and other Hardware, for example: Jamming and Network Intrusion.

2. Software threat, which is a threat caused by the entry of certain software that functions to carry out activities such as: Information Theft, Information/System Destruction, Information Manipulation (Information Corruption) and so on, into a system.

3. Data/Information threat, is a threat caused by the dissemination of certain data/information aimed at certain interests, such as those carried out in information warfare including propaganda activities.

Forms of Threat

Based on Minister of Defense Regulation No. 82 of 2014 concerning Cyber Defense Guidelines, the forms of cyber threats that often occur today can be in the form of the following:

1. Advanced Persistent Threats (APT), Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, usually carried out by overloading system capacity and preventing legitimate users from accessing and using targeted systems or resources. These attacks aim to disrupt system operations, by exposing the system to far more access requests and processes than it can handle. As a result, the system becomes overly busy and crashes, becoming unserviceable or inoperable. This problem is a dangerous threat to organizations that rely almost entirely on the capabilities of the internet to run their activities.

2. Defacement attack, carried out by replacing or modifying the victim's web page so that the content of the victim's web page changes according to the attacker's motives.

3. Phishing attack, carried out by providing a fake website address that looks exactly the same as the original website. The purpose of this phishing attack is to obtain important and sensitive information such as usernames, passwords and others.

4. Malware Attack, which is a program or malicious code that can be used to disrupt the normal operation of a computer system. Usually, malware programs have been designed to gain financial or other planned benefits. The number of malware attacks continues to grow, so that today it has become a very real pandemic. Malware has become ubiquitous and affects everyone involved in every sector of activity. The term generic virus is used to refer to any malicious computer program capable of reproducing and spreading itself.

5. Cyber intrusions, which can attack systems through the identification of authorized users and connection parameters such as passwords, through the exploitation of vulnerabilities present in the system. The main methods used to gain access to the system are:

    a. Guessing. Obvious passwords, such as a user's name, spouse or child's name, date of birth or important personal and family details, are easy to guess and crack.

Unprotected accounts. Users can also make mistakes, by not setting a password or easily giving the password to someone else.

b. Fraud and Social Engineering, e.g., the perpetrator may claim to be and act as an administrator and ask for the password under some technical pretext. In a large number of cases, users will reveal their data. The perpetrator may deceive by phone or electronic message. Some perpetrators are not computer literate, but it turns out that the perpetrators can obtain keys according to the system they want to penetrate.

c. Listening to data communication traffic. Eavesdroppers will listen to unencrypted data transmitted over the network via communication protocols. They operate using PCs by sniffing and analyzing data in transit on the network, then extracting encrypted passwords transmitted by users during the connection. If the perpetrators cannot rely on involvement from within the organization in obtaining passwords directly, then with the help of electronic devices they can intercept them from communication protocols or access files containing all passwords.

d. Trojan Horse. A specific and very dangerous spy program (spyware) can secretly record the parameters used to connect it to the remote system. A Trojan is a small program that generally substitutes itself for a login code that asks the user to capture or provide identification and passwords, in the belief that it is in a normal operating environment, whereupon the passwords are immediately transmitted to the server as an anonymous message from the perpetrator.

e. Authentification System. All user passwords should be stored on a server. The perpetrator will access a file that stores all encrypted user passwords, which is then unlocked with a utility available on the network.

f. Cracking Encrypted Passwords. If the perpetrator or cracker knows the cypher algorithm, he can test all possible permutations, which can be the key to cracking the password. This attack is known as brute force. Another alternative is to use a dictionary to find the encrypted password, which is called a dictionary attack. By successive comparison, the coded form of the password contained in the criminal dictionary can be used to guess the encrypted password being used.

h. Spying. This is done by recording their connection parameters using software, spyware or multimedia devices, such as video cameras and microphones, to capture confidential information, such as passwords to access protected systems.

6. Spam, is the sending of unsolicited bulk Email, with the purpose of:

   a. Commercial or publicity.

   b. Introducing malicious software, such as malware and crimeware into the system.

   c. In the worst situations, spam resembles an Email bomb attack, with the result that mail servers are overloaded, user mailboxes are full and management inconveniences. Earlier spam was only considered as a nuisance, but nowadays Email spam is a real threat. It has become a privileged vector for the spread of viruses, worms, trojans, spyware and phishing attempts.

7. Communication Protocol Misuse. A Transmission Control Protocol (TCP) spoofing attack relies on the fact that the TCP protocol establishes a logical connection between two end systems to support data exchange. Logical identifiers (port numbers) are used to establish a TCP connection. A TCP attack would involve predicting the next port number to be allocated for data exchange in order to use the numbers of a non-authorized user.

Impact of Cyber Attacks

Based on Minister of Defense Regulation No. 82 of 2014 on Cyber Defense Guidelines, the possible impacts of a cyber attack can take the form of:

a. Functional disruption.

b. Remote system control.

c. Misuse of information.

d. Unrest, fear, violence, chaos, conflict.

e. As well as other conditions that are very detrimental, making it possible to cause destruction. (Indonesian Defense Minister, 2014).

Meanwhile, technical attacks are more aimed at attacking logical networks through various methods to gain illegal access, steal information, or insert malware that can damage physical and personal cyber networks. Cyberattacks can be both technical and social depending on the context of how the attack is intended. Head of BSSN Hinsa talked about the #SiberCorner online talk show titled Indonesian Cyberspace Ecosystem, saying "Cyber attacks can be categorized into ordinary crimes, extraordinary crimes and cyber wars depending on the purpose and intensity of the attack without being limited to the division of

the time spectrum in times of peace, crisis or in a state of war" recently. This event was initiated by BSSN together with Siberthreat.id.

Policy Implementation

The government through Presidential Regulation No. 53/2017 on the State Cyber and Crypto Agency (BSSN) and its amendment regulation Presidential Regulation No. 133/2017 established BSSN which is tasked with implementing cyber security effectively and efficiently by utilizing, developing and consolidating all elements related to national cyber security.

And Regulation of the Minister of Defense of the Republic of Indonesia, Number 82 of 2014, concerning Cyber Defense Guidelines. In point 2.4 Cyber Defense Needs the Ministry of Defense and the Indonesian National Army have two interests in cyber defense. First, to secure all electronic systems and information networks in their environment. Second, to support cyber security coordination in other sectors as needed. Which is realized by the establishment of Pushan Siber, Satsiber TNI, Labpamsisjar TNI AL, is the implementation of the current cyber defense strategy.

BSSN Cybersecurity Report 2019

Indonesia's cyber world in 2019 was enlivened by two major events. The first event was related to cyber incidents that continue to hit the national cyber security system and the second event was related to the government's efforts to strengthen national cyber security itself. Because attacks can come from anywhere, not just Indonesia. Cyberattacks are also not necessarily carried out from the recorded source of the attack but may be from other countries that use the source country as a foothold or platform. BSSN's national monitoring system, for example, recorded as many as 290.3 million cyber attacks that entered Indonesia throughout 2019. The biggest attack came from IP addresses located in the United States, shifting from the previous year's conditions which recorded more from IP addresses in Indonesia itself (BSSN, 2019).

The method of cyber attack using malware is recorded to be the most widely used in the global cyber world, hackmagedon noted 39% of the world's top distribution of cyber attacks are attacks using malware. Malware attacks are still ranked first in cyber attacks globally. The same trend is also shown in Indonesia, where malware ranked as the first frequently used attack method in nine months out of twelve months throughout 2019. 36.2% of the top distribution of cyberattacks to Indonesia were recorded as malware attacks.

Some other important cyber incidents besides malware are data leakage incidents and electricity blackouts. Data leakage incidents include a passenger data leak incident that occurred at Malindo Air, a subsidiary of Lion Air, and a data leak of 13 million Bukalapak accounts that were traded on the dark web. The electricity blackout incident occurred on August 4, 2019 for 9 hours, causing a major impact on the internet network and digital businesses that run on it.

INDONESIA'S 2019 CYBERSECURITY MILESTONES	
DATE	SECURITY INCIDENT
18 Mar 2019	Data leaks of 13 million Bukalapak users
24 May 2019	Whatsapp social media restrictions by the Ministry of Communication and Information
18 Sept 2019	Leak of 7.8 million Malindo Air passengers' personal data
22 Sept 2019	Home Affairs Ministry website hacked
24 Sept 2019	DPR's website is not accessible
25 Sept 2019	KPAI's website hacked
15 Oct 2019	BMKG's website hacked
19 Des 2019	Central Jakarta District Court website hacked
28 Des 2019	Bareskrim Polri website hacked
30 Des 2019	Central Jakarta Bawaslu's website hacked

Table 1. 2019 cybersecurity events
Source: BSSN, 2019

Cyber threats will continue to exist and become more sophisticated. Not only in Indonesia, but the United States is also having trouble dealing with this threat. According to the FBI, cybercrime in America throughout 2019 has resulted in losses of 3.5 billion dollars or around 47.9 trillion rupiah. Donna Gregory, head of the FBI's Internet Crime Complaint Center, said: Criminals are becoming more sophisticated, making it more difficult for victims to determine what is real and what is fake.

Loopholes for cyberattack

Recently, a study was conducted by the Kaspersky organization to find out how many organizations fear cyberattacks stemming from the mistakes of their personnel. More than half of the organizations surveyed believe a lack of knowledge, carelessness or malice on the part of personnel can lead to a cyberattack. Additional research shows 84% of cyberattack

victims are attributed to the aforementioned causes, some of which are human error, according to KomputerWeekly.com (Kaspersky, 2019). What kind of personnel errors leave your organization open to cyberattacks. Here is a list of the seven most common personnel errors.

Opening Emails from Unknown People. Email is the preferred form of business communication. The average person receives 235 Emails every day, according to Radicati Group. With that many Emails, it stands to reason that some are scams. Opening unknown Emails, or attachments within Emails, can release viruses that give hackers a backdoor into your organization's digital space.

Have Weak Login Credentials. Mashable reports that 81% of adults use the same password for everything. Repeated passwords that use personal information, such as nicknames or street addresses, are problematic. The cybercriminals have a program that mines public profiles for potential password combinations and pairs that can match up to one hit. They also use dictionary attacks that automatically try different words until they find a match.

Leaving Passwords on Sticky Notes paper. Have you ever walked through the office and seen a Post-it note on display with your password written on it, it happens more often than you think. Leaving passwords visible is too risky.

1. Have access to everything. In some cases, organizations do not organize data. In other words, everyone can access the same organizational files. Giving everyone the same access to data increases the number of people who can leak, lose or mishandle information.

2. Lack of effective personnel training. Research shows the majority of organizations do offer sibersecurity training. However, only 25% believe the results of this training are effective.

3. Not updating antivirus software. Your organization should use antivirus software as a protective measure, but it should not be up to personnel to update it. In some organizations, personnel are required to update and can decide whether or not the update takes place. Personnel may say no to updates when they are in the middle of a project, as many updates force them to close the program or restart the computer. Antivirus updates are important, should be handled immediately and should not be left to personnel.

4. Using unsecured mobile devices. Many of your personnel have cell phones, tablets or laptops? If so, do you have protocols in place to keep these devices secure? Many

organizations have a lax attitude towards mobile devices, but they still present an easy target for cybercriminals.Personel adalah manusia, dan kecelakaan digital bisa terjadi. Namun jika Anda mengambil langkah-langkah tertentu untuk melindungi perangkat dan melatih personel, Anda dapat mencegah ancaman siber. Tentu saja, mengelola keamanan siber organisasi Anda melampaui pendidikan personel. Melindungi jejak digital organisasi dan mengelola ancaman membutuhkan bantuan dari organisasi keamanan siber yang profesional.

D. CONCLUSION

Cyber security has become a priority issue for all countries in the world since information and communication technology is used in various aspects of life, especially in government, security, and defense. Directly proportional to the high level of utilization of information and communication technology, the level of risk and threat of misuse of information and communication technology is also getting higher and more complex.

To address this phenomenon, the Indonesian Navy, as the main component in the sea defense strategy, must be able to build cyber vigilance by creating a strategic cyber environment and organizing a safe, reliable and trusted electronic system. And also build awareness and sensitivity to resilience and security in cyberspace to TNI AL personnel, in order to minimize human error as a cause of data and information leakage. Through making rules or regulations with measurable sanctions, then compiling a cyber security management system both in the form of software and hardware to protect critical data infrastructure. In order to realize the objectives of the sea defense strategy.

E. REFERENCE

BSSN. (2019). Laporan Tahunan 2019 Pusopskamsinas, BSSN. https://cloud. bssn.go.id/s/nM3mDzCkgycRx4S#pdfviewer.

Kaspersky. (2019). Cyber Security Awareness: 7 Ways Your Employees Make Your Business Vulnerable to Cyber Attacks. https://www.kaspersky.com/resource-center/preemptive-safety/7-ways-to-cyberattack-vulnerability.

Holmes, D. (2005). Communication theory: Media, technology and society. Sage.

Kuehl, D., & Pudas, T. (2010). Perspectives on building a cyber force structure. In Proc. Conf. on Cyber Conflict (pp. 163-181).

McDonnell, M. D., & Sayers, T. L. (2002). Information Systems Survivability in Nontraditional

Warfare Operations. Nontraditional Warfare: Twenty-First Century Threats and Responses.

Gibson, W. (2019). Neuromancer (1984). In Crime and Media (pp. 86-94). Routledge.

Presiden RI. (2002). Undang-Undang RI Nomor 3 Tahun tentang Pertahanan Negara.

Presiden RI. (2017). Perpres No. 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN).

Menhan RI. (2014). Permenhan No. 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

Komisi Eropa dan Direktorat Jenderal Untuk Penelitian dan Inovasi. (2020). Cybersecurity Jangkar Digital Kami Perspektif Eropa (pp. 15).

AUTHOR'S BIOGRAPHY

Syaeful Bakhri

The author of these article is Syaeful Bakhri. Born in Jakarta, August 9, 1980. The author is an Indonesian national. The author's history of military education is that he graduated from the Naval Academy in 2004. In 2012 he carried out further education for officers in the Indonesian Naval Education Command. In 2015 carried out in Yapan University Surabaya. He completed his masters in Defense University in 2023.