Jurnal Pertahanan
Media Informasi tentang Kajian dan Strategi Pertahanan
yang Mengedepankan Identity, Nasionalism & Integrity

ISSN : 2087-9415
Vol. 1 | No. 2

Evaluation of State Cryptographic Institutions

Adi Sulistyo[*], Yono Reksoprodjo[**]

[*]Universitas Pertahanan Indonesia
[**]Universitas Hang Tuah

Article Info

Keywords:
Cryptography,
Information,
Information Security,
Information Wafare,
State Cryptography Agency.

Abstract

State cryptographic institutions, coordinated by the State Cryptography Agency have contribute to protect the state classified information from potential threats and vulnerabilities posed by information warfare, using the methods of cryptography. State Cryptography Agency, so that need the anticipatory efforts to reduce the inhibiting factors. The research was conducted using the qualitative research methods with descriptive analysis techniques. Based on this research, it is known that the role of State Cryptography Agency in facing the information warfare is more widely available in the defense/defensive effort to protect state information, as well as there are still some factors that cannot be minimized.

Institusi persandian negara yang dikoordinir oleh Lembaga Sandi Negara (Lemsaneg) berperan untuk melakukan upaya perlindungan terhadap informasi negara yang berklasifikasi khusus dari potensi ancaman dan kerawanan yang ditimbulkan oleh perang informasi dengan menggunakan metode persandian. Penelitian dilakukan menggunakan metode penelitian kualitatif dengan teknik analisa deskriptif analitis. Berdasarkan hasil penelitian, diketahui bahwa peran Lemsaneg dalam menghadapi perang informasi adalah lebih banyak terdapat pada upaya pertahanan/defensif untuk melindungi informasi negara, serta masih adanya beberapa faktor penghambat yang belum dapat di minimalisir.

Corresponding Author:
YonoReksoprodjo@gmail.com

Jurnal Pertahanan
Volume 1 Nomor 2
May-August 2015
ISSN 2087-9415
pp. 143-164

Introduction

State Cryptography Agency (Indonesia: Lembaga Sandi Negara (Lemsaneg)) tasked with managing the security system of classified information belonging to the government and conduct signals intelligence activities. It makes Lemsaneg have a role and responsibility facing threats of information warfare, particularly in defense effort by guaranteeing a fixed confidentiality of any information accompanying threats.

Information is a resource that consists of two things, phenomenon (data) were observed, and the instruction (system) is needed to analyze and interpret data to have meaning or intent (Wilson, 2007). According to Waltz (1998) in the process of the country, the information is classified into four different categories, based on the identification of legal provisions, the analysis function units within the organization and job description, as well as risk analysis: open, restricted, secret, and top secret. Everyone in the organization has a different role to what information, where the main elements are the subject of the information is the owner, authorized officer (custodian), and user. Then each element also has responsibility for information security in accordance with the classification (Krutz and Vines, 2007).

Information security is an attempt to protect the information and important elements in it, either in the form of a system or hardware that is used to store and transmit information (Whitman and Mattord, 2011). Another definition said that information security is the effort made to protect the information that is valuable to individuals, organizations, and the value derived from the characteristic information (Ciampa, 2010).

Generally, information security can be defined as an effort to protect information and information systems from irresponsible parties that make access and unauthorized use, disclosure, disruption, modification, or destruction to maintain the integrity, confidentiality, and availability of information (Schaeffer, 2010), includes computer hardware, networking infrastructure, and organizational information (Crossler, *et.al* 2013).

Generally, the types of threats to information security that comes either through internal factors, external, intentional, or unintentional, among others: Human Error, infringement of intellectual property, Espionage, Blackmail, sabotage (destruction of information), theft (illegal extraction of the equipment and information), attack software (viruses, worms, Service Denial), natural disasters, Deviations services from CSPs, technical error hardware (damage to the equipment), software technical errors (bugs, error code programming), and the technology that is outdated or not up-to-date (Whitman, 2003).

Threats to information security is the activity of a person, organization, mechanisms, or events that could potentially lead to crime on the resources of an organization's proprietary information. Information security threats can come from internal or external factors, and intentional or unintentional (McLeod and Schell, 2004).

Cryptography is derived from the Greek, the Kryptos (hidden) and graphein (writing), which is scientifically defined as the art and science to protect or hide meaning or the information contained in a communication to the other parties do not want (Peltier, 2014). Lemsaneg function with its cryptography is to anticipate the threat of another party that seeks to capture the state by doing the tapping/intercept.

Where the intercept can be defined as an activity to listen, record, divert, alter, inhibit, or record the transmission of electronic information or electronic documents that are not public, using communication networks wired or wireless network, such as the emission of electromagnetic or radio frequency.

On the development of today's world, information has become a commodity that is dominant in society, so putting the information as one of the target goal for harassed and attacked, not just limited to the organization but also in the sphere of security and defense of a country. It reinforces the assertion that the most fundamental weapon once been targeted in information warfare is the information itself (Hutchinson and Warren, 2001).

Further explained that the main strategy in information warfare can be done through the denial of access to information, disrupt or destroy information, steal information, manipulate information, to change the context of interpretation of information, as well as changing people's perceptions of the information it receives.

Attacks in the information warfare is generally directed to the national information infrastructure which is a computer system that collectively build the information system of military, government, education and commercial information systems state that became the target of attacks.

Some of the events included in the information warfare, among others, through the efforts to break into the information system through the Internet in Indonesia include: (1) On July 31, 2013, the official website of Criminal Investigation Police is addressed www.bareskrim.polri.go.id hacked, wherein the display that appears on the site just looks black with a setting in which Garuda emblem and flag background red and white.

Identity is known only from a hacker calling himself "pra5astea" listed in an article in the black background, accompanied by a provocative phrase, (2) On November 11, 2013, Site owned by the Ministry of Justice and Human Rights which is located at www.kemenkumham.go.id down. There are 502 bad gateway message, which indicates a server error of the shelter sites. In fact, the site was declared down 100 percent or 404 Not Found, and (3) On November 25, 2013, site of the National Narcotics Agency (BNN) is located at http://bnn.go.id completely inaccessible. BNN sites are having problems with the status of -1 means the server error. Not yet known exactly what causes the site server is down, but allegedly because of hacker attacks.

Based on a collection of Incident Monitoring Report (IMR) released by the Indonesian Computer Emergency Response Team (CERT-ID) related to misuse of the Internet and its handling during March-October in 2013, finds that there are as many as 68.465 cases with details and percentages (table 1). Incident Monitoring Network, which occurred March-October in 2013 can be described as follows in figure 1:

Table 1. IMR Data version of ID-CER Period March-October, 2013

Type	Number of Cases								Total
	Mar	Apr	Mei	Jun	Jul	Aug	Sep	Oct	
Spam	1,033	440	4,026	20,931	2,998	6,305	6,410	5,118	40,956
Network Incident	485	2,032	1,408	1,824	4,291	1,454	878	944	11,862
IPR	1,070	927	994	971	1,238	1,789	877	613	6,690
Malware	771	795	507	353	696	1,721	1,428	1,143	5,693
Spoofing	158	195	205	191	240	310	181	273	1,443
Spam Complaints	209	279	60	84	79	2,037	207	216	1,134
Response	86	122	263	125	91	122	0	0	687

Source: CERT ID Report, 2013

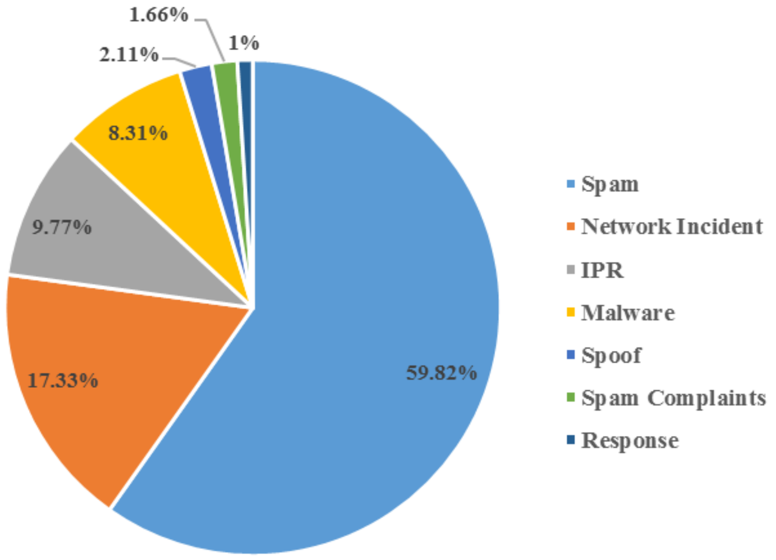


Figure 1. Incident Monitoring Network from March to October 2013

Several cases in the information warfare in Indonesia which has indirectly affect the assessment of the Lemsaneg role in securing information such as: an indication of leakage of information related to the investigation warrant (Sprindik) in Corruption Eradication Commission (Indonesia: Komisi Pemberantasan Korupsi (KPK)), the leaking of the National Exam questions in several regions in

Indonesia, as well as cases of wiretapping or intercept addressed to some government officials/state since the last few years.

Information warfare defined by Libicki (1996) which is a strategy, operations, and competition tactical across the spectrum of peace, crisis, crisis escalation, conflict, war, cessation of war, and recovery/restoration, which has erupted between rival or enemy use information to reach their purpose. Another opinion expressed by Haeni (1997) and Thornton (2011) that the information warfare is any action taken to achieve information superiority by affecting the information your opponent through a process of information-based, information systems, and network-based computers, which at the same time also maintain information possessed of the threat of similar action by the opponent. Information warfare use an Information weapon, information technology, means, and methods (Thomas, 2014).

Therefore, one of the defensive effort that can be done to counter the threat of information warfare is to build information security system that serves to protect the information and important elements of the other is in it, either in the form of system/software or hardware used to store and transmit high-value information (Whitman and Mattord, 2011), offensive or defensive purpose to immediately intrude, disrupt, or control the opponent's resources (Taddeo, 2012).

Attempted theft of information by using tapping technique (intercept) carried out by other countries against Indonesia allegedly has long been the case, as the action of wiretaps conducted by the Australian Signals Directorate (ASD) against a number of communications Indonesian military officials during the crisis East Timor published by the newspaper Sydney Morning Herald, among others: (1) On February 9, 1999, Australia informed elite unit of Special Forces entry into East Timor by codenamed Task Force, Tribunal; (2) On 14 February 1999, Australia caught a conversation between Eurico Guiterres with the team, Tribunal, which in the communications team, Tribunal asks condition Eurico men who are victims of violence; (3) On May 5, 1999, Australia intercepted conversations Commander Military Command

(Korem)-164/Wiradharma (Colonel Tono Suratman) by Eurico Guterres, who asked the position of the forces of mass pro-integration that can be driven. From the conversation Eurico reported four hundred militia guard outside a hotel in Dili; (4) On August 9, 1999, one of the important info that bugged conversations senior Australian intelligence is the Strategic Intelligence Agency of Indonesian National Army (Indonesia: Badan Intelijen Strategis, Tentara Nasional Indonesia (BAIS-TNI)) (Brigadier Ariffudin). Revealed the military helped the pro-integration mass demonstrations against the United Nations Missions in East Timor (UNAMET) to provide anti-material demonstration mission of the United Nations (UN) in East Timor. There was also intercepts of conversations between Major General Zacky Anwar Makarim police officer associated with the referendum vote count; (5) On August 21, 1999, Australia intercepted conversations between the TNI and the politicians pro-Indonesia (Francisco Xavier Lopez da Cruz), where the core of the talks Kopassus formed a team of hunters “Goalkeeper-9”, which has a mission to hunt down leaders of pro-independence or pro-Indonesia who defected to the opponent; and (6) On 20 September 1999, Australian officials intercepted conversations between TNI (Zaky Anwar Makarim Major General, Lieutenant General and Lieutenant General Yunus Hendropriyono) are discussing the "transfer of population", as an effort to anticipate if the referendum won by the pro-independence movement.

Other news regarding the efforts intercepts that occurred in Indonesia is presented by The Australian newspaper, which wrote that the Australian government through the ASD allegedly tapped into Indonesia’s Palapa. Information about the satellite intercepts revealed by Des Ball, a professor in the field of Strategic and Defence Studies Centre of the Australian National University, which states that the Palapa as a key objective of the actions undertaken tapping Australia.

While, the Sydney Morning Herald newspaper on October 29, 2013 also reported the existence of tapping the US government against the Indonesian government. Here are some password interception operations of foreign parties who allegedly were also making Indonesia the target: Echelon and friendship (1990), Jupiter and Larkswood (1991-1999), Orion Satellite Spy (1999), and the Magic Lantern (2001).

The phenomenon of information warfare the most attention in recent general audience is Australian side wiretapping case against the Indonesian government. Where the case is raised in the meeting of the Joint Working between the Commission I of the House of Representatives with the Minister of Defense, Minister of Foreign Affairs, Chief of Indonesian National Police, Chief of the State Intelligence Agency, Head Lemsaneg, Minister's Secretariat, and the Minister of Communications and Information Technology on November 28, 2013.

The main topic of the meeting was about the action of tapping the Australian side against the Government of Indonesia, as well as the steps to be taken forward related to Information and Communication Systems Security State/Government Agencies.

One result of the decision of the meeting is the Commission I of DPR urges the Government of Indonesia to accelerate the use of a system of cipher in all state institutions and representative offices of Indonesia abroad, including in the security of communications for Very-Very Important Person (VVIP).

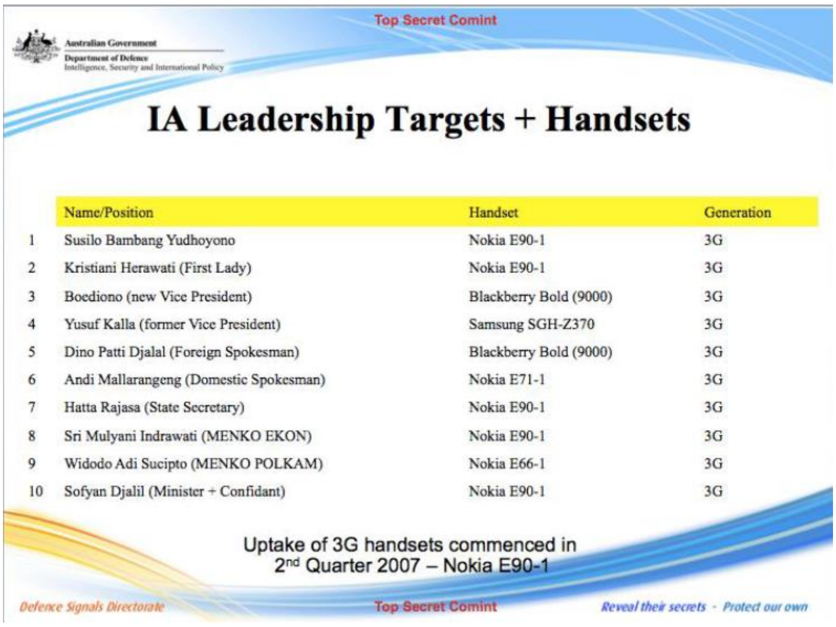
According to Krutz and Vines (2007) that the awareness of information security aims to guarantee the security of information systems within an organization, though

1. The owners, users and custodians of information understand their responsibilities towards the security of information and introduce how the means of securing the right to information, thereby helping to change their behavior to become more aware of the importance of the value of information within an organization.
2. Develop the skills and knowledge so that the owner, custodian and information users can do their jobs more secure; and
3. To develop an understanding of the knowledge required to design, implement, or operate the information security awareness training programs for

organizations.

As reported in several national and international media, Australian spy agencies have tried to tap the phones of President Susilo Bambang Yudhoyono and his wife, along with several ministers.

Documents leaked by whistleblower from the US, Edward Snowden (in the form of a slide presentation classified as highly confidential ASD) is in the hands of the Australian Broadcasting Corporation (ABC) and the British daily The Guardian, said that the President and nine (9) people in his inner circle as a target of wiretapping Australian side can be seen in below:



Top Secret Comint

Australian Government
Department of Defence
Intelligence, Security and International Policy

IA Leadership Targets + Handsets

	Name/Position	Handset	Generation
1	Susilo Bambang Yudhoyono	Nokia E90-1	3G
2	Kristiani Herawati (First Lady)	Nokia E90-1	3G
3	Boediono (new Vice President)	Blackberry Bold (9000)	3G
4	Yusuf Kalla (former Vice President)	Samsung SGH-Z370	3G
5	Dino Patti Djalal (Foreign Spokesman)	Blackberry Bold (9000)	3G
6	Andi Mallarangeng (Domestic Spokesman)	Nokia E71-1	3G
7	Hatta Rajasa (State Secretary)	Nokia E90-1	3G
8	Sri Mulyani Indrawati (MENKO EKON)	Nokia E90-1	3G
9	Widodo Adi Sucipto (MENKO POLKAM)	Nokia E66-1	3G
10	Sofyan Djalil (Minister + Confidant)	Nokia E90-1	3G

Uptake of 3G handsets commenced in 2nd Quarter 2007 – Nokia E90-1

Defence Signals Directorate

Top Secret Comint

Reveal their secrets - Protect our own

Figure 2. Leadership Target

The document shows that the Australian electronic intelligence agency or ASD, had engaged in tracking cell phone communications of the president for 15 (fifteen) days in August 2009, when Kevin Rudd of the Labor Party Prime Minister of Australia. Target list intercepts in addition to the Chief and the First Lady, also includes Vice President (Boediono), former Vice President (Jusuf Kalla), Presidential Spokesman for Foreign Affairs (Dino Patti Djalal), Presidential Spokesman for Home Affairs (Andi Mallarangeng), State Secretary (Hatta Rajasa), Coordinating Minister for Economic Affairs (Sri Mulyani Indrawati), the Coordinating Minister for Politics (Widodo AS), and the Minister of

State Enterprises (Sofyan Djalil).

The incidence of wiretapping disruption to the bilateral relationship between Indonesia and Australia, following the violent protests carried out by the Indonesian government by calling home while Ambassador (Ambassador) of Indonesia to Australia (Najib Riphat Kesoema) and reviewed the cooperation relations between countries that have been previously established, as (1) Discontinue military cooperation between Indonesia and Australia, (2) Discontinue cooperation on exchange of information and intelligence exchange between the two countries; and (3) Discontinue Indonesia-Australia co-operation related to the handling of illegal asylum seekers (people smuggling).

Indonesian crypto coordinated by Lemsaneg includes two domains, which cryptology on aspects of science, intelligence and communication aspects of the operations.

Cryptology is the science of the method of concealment/ concealment of information, while the communications intelligence is activities that utilize the results of cryptology in every movement (Lembaga Sandi Negara, 2007).

The role of cryptography Indonesia, especially Lemsaneg is to regulate and organize cryptography system national in order to safeguard a state secret message sent through the means of communication between the state apparatus, at the central, local, foreign, state-owned enterprises, as well as in the military and police.

Research Methods

This research used a qualitative approach with descriptive methods of analysis. Research subjects are something, people, objects or institutions, which due to the nature and circumstances then it ought to be investigated (Creswell, 2014).

Therefore, the subject of this research includes government agencies that have a unit or division cryptology, i.e. Lemsaneg, Ministry of Foreign Affairs, the Coordinating Ministry for Political, Legal and Security, and the Ministry of Defense, while the object of research include the role and function of cryptology state institutions (especially Lemsaneg) in the face of the information war.

Data collection techniques including observation, interviews, documents, and audio and visual materials (Creswell, 2014). Implementation research began from October 2014 until February 2015 with an informant as much as six divisions, Principal Secretary Lemsaneg, Deputy of Development and Control Cryptology of Lemsaneg, Deputy Security Cryptology of Lemsaneg, Deputy Assessment Cryptology, expert staff/functional cryptology competent and related the focus of research; as well as official government agency that oversees the cryptology and telecommunications unit that uses a cryptology system Lemsaneg.

Results and Discussion

Lemsaneg role in the War Information

Lemsaneg prevention efforts against the threat of war by organizing the dissemination of information cryptology, equipment demo password, counter-sensing activities, sterilization, and IT-Security Assesment of all government institutions. Where it is done routinely by Deputy II Lemsaneg, as well as on specific request from the relevant authorities.

From interviews with the Deputy First, the strategy adopted by Lemsaneg in the face of threats of information warfare is:

(1) Carrying out socialization cryptology as qualified information security efforts intensively within the government and the public;

(2) Provide technical support and non-technical in terms of security and information management qualified, in accordance with the development of information and communication technology;

(3) Carry out periodic supervision improvement in the operations of cryptology;

(4) Supporting the operational security of information to government agencies on aspects of human resources, equipment password, and the password system;

(5) Increase in terms of information security services to support the

operations of the national cryptology;

(6) Empower password education and training center by building a network of cooperation with third parties;

(7) Promoting virtue competitive profession password; and

(8) Carrying out technical guidance cryptology, both within and outside the country.

Generally, the strategy undertaken in order Lemsaneg able to participate in the information war is by upgrading or development of human resources, as well as mastery of information and communication technologies that lead to the independence of the cryptology. This is in accordance with the interview obtained from various informants about Lemsaneg role in the face of a information warfare, namely.

Table 2. The Role of Lemsaneg

No	Informants / Sources	Lemsaneg role in the face of information war
1	Settama Lemsaneg	• Information security obviously has associated with information warfare, where one threat is an attempt intercepts the traffic lane information transmitted via electromagnetic waves. • Role Lemsaneg make efforts in securing information transmitted over the path.
2	Deputi I Lemsaneg dan Team	• Provide technical support and non-technical in terms of security and management of qualified information. • Operational support information security at government agencies on aspects of human resources, equipment password, or a password system
3	Deputi II Lemsaneg	• Prevention efforts by providing socialization cryptology, equipment operational demo password, counter-sensing activities, sterilization, and IT-Security Assesment of all government institutions. • Prevention activities carried out regularly by Lemsaneg, or based on specific requests submitted by relevant agencies
4	Kapuskaji Kriptografi Deputi III Lemsaneg	• Indonesia is currently in a state of war information. • Lemsaneg protecting information transmitted via digital and analog lines.
5	Kapuskaji Komsan Deputi III Lemsaneg	• Lemsaneg role in the war was to develop a network of information and material that is private. • Make a design of equipment in the framework of information security
6	Kapuskom Kemlu	• Cryptology instrumental in securing traffic information and strategic information between the Ministry of Foreign Affairs with representatives of Indonesia and other relevant government agencies. • Security information can be regarded as the life of a policy, which during the policy formulation process of cryptology needed to secure the flow of information that can be used in formulating policy
7	Kasubbid Opsan Pusadatin Kemhan`	• Cryptology has a very important role, because it is one part of the country's defense. • There is some state information that must be protected in order not to be public or known by third parties / opponent.
8	Kasubbag Persandian Kemenkopolhukam	• Cryptology has a very important role as a defensive effort in the information war. • Should be a leading sector

Source: Results of Interview with informants/resource research

Factors Influencing Threat of War Information

Success Lemsaneg carry out its role in the face of threats of information warfare is determined by factors that can affect. Based on the research, found some internal and external factors that can influence, which in addition to being a factor supporting role Lemsaneg, also can be a factor inhibiting Lemsaneg role in facing the threat of information warfare. Primary data related to factors affecting Lemsaneg role in the war information obtained through the interviews with informants/sources are:

Table 2. Factors Influencing

No	Informants / Sources	Factors Influencing Threat of War Information
1	Settama Lemsaneg	• Legislation that became the basis for Lemsaneg to carry out their duties. • Human Resources (HR) • The need for cryptology by government agencies. • *Information Security Awareness*.
2	Deputi I Lemsaneg dan Tim	• President of the existence of the policy Lemsaneg. • Lemsaneg authority which is still contained in the Presidential Decree. • Commitment Head Lemsaneg. • Head Lemsaneg support to policy. • The organizational structure and HR password. • Officials' understanding of the information security and cryptology. • Public acceptance of cryptology.
3	Deputi II Lemsaneg	• HR with competencies in accordance with the field work. • Password and supporting equipment that suits your needs. • Communications infrastructure. • There is no strong legal protection for Lemsaneg to support the operation. • Information security awareness. • utilization cryptology
4	Kapuskaji Kriptografi Deputi III Lemsaneg	• HR passwords are limited and unevenly spread. • Software and hardware. Communications infrastructure. • *Information Security Awareness*
5	Kapuskaji Komsan Deputi III Lemsaneg	• HR. *Software & Hardware*. • Cryptology system of the country. • Communication network. • Independence cryptology. • *Information Security Awareness*.
6	Kapuskom Kemlu	• HR factor is the most vulnerable point in the information leakage factors other than equipment and communication lines. • Budget implementation of cryptology. • Cryptology system of the country. • Coordination among agencies
7	Kasubbid Opsan Pusadatin Kemhan`	• Socialization cryptology of Lemsaneg still lacking. • An understanding of public officials and to information security and cryptology. • Net communications password. HR password.
8	Kasubbag Persandian Kemenkopolhukam	• Officials' understanding of the cryptology and information security. • Limited communication nets

Source: Results of Interview with informants/resource research

Cryptology function on Government Agencies

The implementation of cryptology functions on each of the objectives Lemsaneg government agencies to minimize the risk of information leaks that have the potential to occur at the institution. Until now, this research was conducted, the cryptology function has been run/owned in several government agencies both at home and abroad. During the research data showed the distribution of Cryptology Technical Unit (Indonesia: Unit Teknis Persandian (UTP)) contained in government agencies both at home and abroad with the following details: (1) UTP Center; consists of 17 who are in the central government agencies, (2) Regional UTP; All provinces in Indonesia have had UTP spread from the Provincial Government level (33 provinces), the District, and the City (66th District / City) that coordinate directly with UTP center owned by Kemdagri, (3) Representative of the Republic of Indonesia; Abroad (132 representatives), which consists of 95 Indonesian Embassy, 3 Permanent Representative of Indonesia, the Indonesian Consulate General, and 3 Consulate Affairs, as well as 112 representatives of Indonesia has had a UTP performing cryptology under the coordination of Ministry of Foreign Communication Center.

HR National Cryptology

Data distribution of HR cryptology with qualifications obtained during research interviews with the Deputy Minister Cryptology (Deputy I) of Lemsaneg (table 4).

Table 4. Data Distribution of HR Cryptology

No	UTP	AS-III	AS-II	AS-I	PAS	Total
1	Ministry of Home Affairs	5	102	187	1553	1847
2	Ministry of Foreign Affairs	75	76	131	46	328
3	Indonesian National Police	2	8	188	521	719
4	Strategic Intelligence Agency of Indonesian National Army	2	10	28	23	63
5	Indonesian Army	4	114	262	146	526
6	Indonesian Air Force	4	25	226	126	381
7	Indonesian Navy	2	25	338	458	823
8	Attorney General	23	19	79	46	167
9	Presidential Work Unit for Development Supervision and Control	10	0	0	0	10
10	Maritime Security Agency	0	0	3	10	13
11	Geospatial Information Agency	0	1	0	5	6

No	UTP	AS-III	AS-II	AS-I	PAS	Total
12	Ministry of Maritime and Fisheries Affairs	0	3	25	10	38
13	National Intelligence Agency	0	3	5	0	8
14	Coordinating Minister for Political, Legal & Security	10	2	0	0	12
15	Ministry of Defense	1	1	4	14	20
16	Pertamina Companies	1	2	5	3	11
	Total	**139**	**391**	**1481**	**2961**	**4972**

Source: Sub-Directorate of Human Resources Management, Deputy I Lemsaneg, Recapitulation Lemsaneg HRM, 2014

Based on the above table, until the end of 2014 Lemsaneg has scored a total of 4972 active HR function cryptology on UTP government agencies that work with Lemsaneg.

Information Security Awareness

Improving information security awareness is to organize socialization at central and local government agencies, which was attended by all echelon 1, 2, 3, and 4. Other efforts made by Lemsaneg is to organize technical assistance (bimtek), among others, such (1) Bimtek and workshops related to the improvement of information security awareness echelon 3 and 4 in charge of field/cryptography unit; (2) Bimtek cryptography on the executive staff of Administration (TU) in government agencies; and (3) Bimtek to the aide of state officials or VIPs.

Lemsaneg Socialization is done by raising awareness of state officials to the vulnerability and threats to information, where the realization is expected after the socialization is the use cryptography by the officials concerned. Socialization activities last at the time the study was conducted was in mid-October 2014 Lemsaneg Seminar on Security Awareness Information (SKKI) held in Bali, Batam and Makassar devoted to official policy makers at all government agencies that exist in the western part of Indonesia, middle and east.

Moreover, according to Principal Secretary Lemsaneg, the result of the dissemination activities undertaken by Lemsaneg is the signing of the MoU between Lemsaneg the Investment Coordinating Board (BKPM) on securing information systems in order to support the tasks and functions of BKPM on Implementation Services One Stop (OSS) Center in Regional and PTSP BKPM dated February 9, 2015.

National Cryptology System

The conception of the state of information security implementation, which, according to Principal Secretary Lemsaneg, for now State Coding System (Indonesia: Sistem Persandian Negara (SISDINA)) has been the need for a shift in paradigm, but for the purpose is still valid / relevant.

According to Deputy Security Cryptology (Deputy II) Lemsaneg stated that until now SISDINA still the focus of Lemsaneg, where the relevance of aspects manware, software, hardware strengthened continuously strived to always keep up with technology.

SISDINA currently implemented into the national communication network cryptology using publicly owned communications infrastructure with a plus tunneling (closed communication system), as well as regulations regarding SISDINA also listed in the Bill Cryptology, which is now at the level of an academic text.

State Secrecy Bill and draft law Cryptology

Principal Secretary Lemsaneg stated that the Act become one of the handles/legal basis for government agencies in carrying out its duties and functions, which the law can also strengthen the position/presence of government agencies. Currently Lemsaneg has submitted two draft law, which is State Secrecy Bill and draft law cryptology, which it is expected that the bill be approved and enacted as a law.

Ratification of the State Secrecy Bill and draft law into Law Cryptology can also be a motivating factor or "force" the government agencies to immediately organize cryptography to protect classified information held. Thus, officials at the agencies also have responsibility for strategic or state secret information assigned to.

Services and Cooperation Lemsaneg with User Agencies

Lemsaneg services to user institutions embodied in the form of cooperation in cryptography in the institution. The forms of cooperation between Lemsaneg with other government agencies carried out in the form of a Memorandum of Understanding / MoU actualized through several technical cooperation agreements as technical cooperation in the field of HR and technical cooperation information system security protection field.

Other cooperation is also often done by Lemsaneg is direct coordination with relevant agencies in organizing cryptography. To maintain the consistency of cryptography implementation in government agencies, Lemsaneg guidance and control HR cryptography periodically.

User Response on Lemsaneg Agencies

Efforts to safeguard classified information belonging to the state is not only done by Lemsaneg, but should also be implemented by other government agencies through UTP they have. To view Lemsaneg role in facing the threats of information warfare, the authors also conducted the interviews with the government office formed a partnership with Lemsaneg to see the extent of guidance functions and the services provided by Lemsaneg on UTP contained in these institutions:

(1) Kemenkopolhukam; Lemsaneg send cryptology HRM held for support in organizing cryptography at Kemenkopolhukam,

(2) Kemhan; Lemsaneg expect can make the machine cryptography hundred percent homemade,

(3) Kemlu; Lemsaneg give direction to the Ministry of Foreign-related matters related to information security, such as providing technical policy that can be used by the Ministry of Foreign Affairs, as well as the sending system change cryptography regularly every year, both the Computer Center and the UTP-UTP others scattered throughout the Indonesian representatives abroad.

The Role of Lemsaneg in Information Warfare

Based on the research and analysis of data, it is known that the role Lemsaneg through cryptography in the face of a information warfare is more widely available in the defense/defensive to protect state information, to ensure the fulfillment of the aspects in information security such as:

(1) Stay confidentiality content/

information content of the readings efforts undertaken by third parties;

(2) Certainty of the authenticity of the identity of senders and recipients of information;

(3) No change of the whole or part of the content of information during the process of sending or receiving (integrity); and

(4) Make sure there is no denial of the news or information that has been sent to the user of the sender (non-repudiation).

Factors Affecting Lemsaneg Role in Confronting War Information

Factors that may affect Lemsaneg role in the face of war information obtained based on the results of research and data analysis are as follows:

(1) HR; HR factors becomes the most decisive factor for cryptography (Lemsaneg in particular) in the face of the information war. HR can be a supporting factor is human resources that have a high information security awareness, dedication, and intellectual level that can adapt to the latest technological developments,

(2) Software and hardware; Currently Lemsaneg are working to create their own cryptography devices are not limited to any algorithm,

(3) Lines of communication; State Coding System (SISDINA) held by Lemsaneg have a communication network called the National Communication Network Cryptography (JKSN) connecting with UTP Lemsaneg contained in government agencies.

Besides the three main factors above, there are also other external factors that may affect Lemsaneg role in the facing information warfare, among others:

(1) The absence of legal protection remains that may be invoked / handle for Lemsaneg to act,

(2) Partial understanding of government officials towards cryptography and information security is still lacking,

(3) The attitude of resistance from the public on matters that are confidential because they are opposed to the era of information, and

(4) Budget implementation of cryptography.

Anticipate Obstacles Lemsaneg Role in Confronting War Information

Lemsaneg efforts in the face of factors that can lead to insecurity and threats in the process of cryptography in the facing information warfare:

Tabel 5. Anticipate Obstacle Factors

No	Informants/Sources	Factors Influencing Threat of War Information
1	Settama Lemsaneg	• Improvement / development of human resources through formal education and courses / seminars. • Mastery of technology that led to the independence of cryptography. • Socialization at raising awareness of state officials to the vulnerability and threats to information. • Issuing the laws and regulations that can be "forced" to perform the functions of government agencies cryptography
2	Deputi I Lemsaneg and Team	• Seminar/workshop on information security and cryptography on a national scale. • Dissemination to all ministries. Develop and apply for state secrecy bill and the bill cryptography that can be set into law. • The introduction of cryptography and its use to the public. • Sharpening function at several units.
3	Deputi II Lemsaneg	• Increased HR competencies. • Procurement of equipment that fit the needs of cryptography. • Build webs signal analysis that aims to code breaking. • Socialization concerning utilization of cryptography and Information security awareness to government officials.
4	Kapuskaji Kriptografi Deputi III Lemsaneg	• Modification of cryptography algorithms. • Improving the quality of human resources-related cryptography technology.
5	Kapuskaji Komsan Deputi III Lemsaneg	• Developing the network and cryptography is private material. • Customization of cryptography encryption algorithms against foreign machine. Cooperation with experts and academic institutions related to cryptography. • Increased HR competencies. • Consistency led to policies that have been issued.
6	Kapuskom Kemlu	• Strengthening the element of human resources through training, seminars and comparative study. • Increased budget for the organization cryptography • Establishment of communication network cryptography that is separate from the public.
7	Kasubbid Opsan Pusadatin Kemhan`	• Socialization cryptography of Lemsaneg still lacking. • Lemsaneg cryptography can create equipment that is 100% homemade
8	Kasubbag Persandian Kemenkopolhukam	• Fulfilling the needs of information security required by government agencies that have a cryptography unit

Source: Results of Interview with informants/resource research

Efforts must be made by Lemsaneg to reduce inhibiting factors include: *first* Strengthen the capacities of human resources by providing training, study tours, seminars, and provide duty/responsibility to raise awareness of information security. Cooperation with academic institutions and information security experts is also important to be done on an ongoing basis to be able to follow the latest technological developments,

Second, fully apply the national algorithm (national cryptography algorithms) on any equipment purchased from the password outside parties can also reduce vulnerability contained in the software and hardware elements.

Third, the use of separate special communication line with the communication lines are in use by the public may be one factor that can strengthen JKSN. *Fourth,* the highest legal protection hitherto owned by Lemsaneg is merely a Presidential Decree and Law No.23 of 2014 on Regional Government stating coding as one part of the obligatory functions not related to basic services,

Fifth, Lemsaneg provide insight to the state officials with information dissemination, seminars, and workshops conducted by Lemsaneg continuous targeting both official policy makers and to the general public. *Sixth*, providing basic introduction to the public on what was cryptography and utilization, as well as published through the mass media, both print and electronic; and *Seventh,* provide insight related to information security awareness echelon I and II at each government agency.

Conclusions

Based on the analysis of data and discussion that has been carried out, the conclusions that can be drawn in this study are as follows: *First*, the role of the state on cryptography information warfare threats are more numerous in the defense/defensive to protect information classified as confidential or highly confidential by the state, by ensuring confidentiality aspects, authentication, integrity and non-repudiation.

Second, factors affecting Lemsaneg role in facing the threats of information warfare is the Human Resources (HR), software and hardware cryptography, as well as the lines of communication as a major factor. While other factors also influenced the legal protection/legislation, understanding of state officials, public acceptance, as well as the budget allocation cryptography.

Third, Anticipating that can be done by Lemsaneg to eliminate the factors that constrain their role in facing the threats of information warfare is as follows: (a) Doing guidance and control; (b) Accelerate the realization of independence cryptography, by creating a hardware cryptography that is 100% homemade; (c) Using separate dedicated communication lines of public communication path in the process of cryptography; (d) Increasing the power of legal protection by proposing a state secrecy bill and the bill cryptography in order to set into law; and (e) Dissemination, seminars, and workshops related to information security awareness and cryptography continuously devoted to official policy makers and to the general public.

Recommendation

Further research is could examine the coding state function in the information warfare, particularly by conducting further research and specific efforts to minimize (anticipate) the inhibiting factors in the encryption process, such as human resource factors, technological factors coding, factor pathway communication, regulatory factors or legislation, efforts to increase security awareness, and other factors are have not been discussed in this study.

Reference

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *computers & security*. Vol. *32*. pp. 90-101. DOI: http://dx.doi.org/10.1016/j.cose.2012.09.010

CERT ID. (2013). *Report of the bi-month.* Retrieved from *http://www.cert.or.id.*

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. California: SAGE Publications, Inc.

Ciampa, M. (2010). *Security awareness: Applying practical security in your world.* Boston: Cengage Learning.

Haeni, R. E. (1997). *Information warfare: An introduction.* Washington: Cyberspace Policy Institute, The George Washington University.

Hutchinson, B., and Warren, M. (2001). *Information warfare: Corporate attack and defence in a digital world*. Oxford: Butterworth Heinemann.

Krutz, R. L., and Vines, R. D. (2007). *The CISSP® and CAP^{CM} prep guide: Platinum edition*, Indianapolis: Wiley Publishing, Inc.

Lembaga Sandi Negara. (2007). *Jelajah Kriptologi.* Jakarta: Lembaga Sandi Negara.

Libicki, M. C. (1996). *What is information warfare?*

Washington: National Defense University.

McLeod, R., and Schell, G. P. (2004). *Management information systems*. New Jersey: Prentice Hall.

Peltier, T. R. (2014). *Information security fundamentals.* Boca Raton: CRC Press.

Schaeffer, R. C. (2010). *CNSS instruction No. 4009: National Information Assurance (NIA) Glossary*. Maryland: Committee on National Security Systems.

Thornton, R. (2011). *Asymmetric warfare: Threat and response in the twenty-first century.* Cambridge: Polity Press.

Thomas, T. (2014). Russia’s Information Warfare Strategy: Can the Nation Cope in Future Conflicts?. *The Journal of Slavic Military Studies*. Vol. *27* No. 1. pp. 101-130. DOI: 10.1080/13518046.2014.874845

Taddeo, M. (2012). Information warfare: A philosophical perspective. *Philosophy & Technology*. Vol. *25* No. 1. pp. 105-120.

Whitman, M. E. (2003). *Communication of the ACM/Vol.46 No.8: Enemy at the Gate – Threats to Information Security.* New York: Association for Computing Machinery.

Whitman, M. E., and Mattord, H. J. (2011). *Principles of information security.* Atlanta: Cengage Learning.

Wilson, C. (2007). *Information operations, electronic warfare, and cyberwar: Capabilities and related policy issues*. Washington: CRS.