The Need of Six-Ware Cyber Security Framework to Protect Critical Information System from Cyber Terrorism Threat

Rudy Agus Gemilang Gultom
Indonesia Defense University, Bogor, Indonesia

Abstract

In current era of Internet of Things (IoT), the terrorist groups have taken advantages the use of Internet access to support their activities, i.e, member recruitment, propaganda, fundraising, cyberattack actions against their targets, etc. This is one of the negative issues of internet utilization commonly used by radicalist or terrorist, so called cyber terrorism. They know the benefits of the online services that can be used to facilitate information control in their organizational command and control system. In order to tackle this cyber security issue, the internet users should get more understanding as well as protection from their government against the danger of cyber terrorism, cyber radicalism or cyber extremism activities over the Internet. Therefore, this paper tries to explain the need of a cybersecurity strategy to countering cyber terrorism activities via Internet by proposing the concept of SWCSF (Six Ware Cyber Security Framework). .

KEYWORDS–Internet, Internet of Things (IoT), Cyber Terrorism, Six Ware Cyber Security Framework security.

1. INTRODUCTION

Nowadays, the strength, sovereignty, and stability of a country are not only measured in terms of military or economic strength, but also depend on many aspects of cyber space and access to the Internet, use and empowerment. At present, many countries are largely dependent on cyberspace and Internet use, especially from the aspects of economics, business, academic, social, political, government, defense and security. Through constructive use of cyberspace, public relations can be directly regulated in a relatively short period of time, regardless of the deadline for peace, crisis or war. The phenomena of cyberspace show that reality in modern society is interrelated in cyberspace. From the point of view of cyber security, the purpose of using the Internet may also be to protect those who have malicious intentions for negative or destructive purposes by non-state actors and / or countries, including terrorist groups. How do we know that the various tools available on the Internet can be used to neutralize or damage infrastructure that will damage or threaten the national interest of the country, and even influence radical ideology or acts of terrorism. Different cyber threats or attacks at the moment of cybercrime (Internet) progression in information and communication technology are highly organized or acted as state actors or non-state actors for the national interest of another country to become a cyber-attack. Different cyberspace challenges such as web scams, cyber security, cyber radicalism, cyber terrorism, cyber warfare, child pornography, black propaganda, character assassination, hate speech, etc., in order to protect their national interests many countries build their own cybersecuriy institutions, such as: US Cyber Command, China PLA Blue Army, Korean KISA, Israel unit 8200 IDF or Indonesia BSSN (National Cyber Agency).In the US, it has a National Institute of Standards and Technology (NIST) which has been defined Cybersecurity terms as the ability to

protect or defend use of cyberspace from cyberattacks including Cyberterrorism action. In Indonesia, 19 May 2017, the President of Indonesia, Mr. Joko Widodo, has signed establishment of BSSN (the National Cyber and Encryption Agency) in charge of implementing national cyber security effectively and efficiently by utilizing, developing and consolidating all elements related to cyber security. BSSN is now a leading institution by the Presidential Decree No. 53 of 2017. Structurally, BSSN is directly under command of the president of the Republic of Indonesia.

2. UNDERSTANDING CYBERSECURITY AND CHALLENGES

To understand the challenges of cyber security in the global context, it is necessary to understand the development of global strategic environment. A country should be able to have a complete picture of the cyber space as an infinite global space, less space and time-consuming challenges that bring new challenges to the globalization of information.The international concept that does not comply with the meaning of the Cyberspace territory and its regulatory governance will be maintained as obstacles, challenges, and resistance when a country tries to unilaterally claim that global cyber culture is part of the country's sovereignty. This contradicts the requirements of those countries that are governed by international treaties such as UNCLOS 1982 (UN Convention on the Law of the Sea) and in 1982, At UNCLOS it has been clearly and clearly defined that the state and the sovereign state are responsible for the use and management of the world's oceans where it has (ZEE / exclusive economic zone) and sets out guidelines for its business, environment and its natural resources management. Dominance in the territory of the Cyberspace is viewed as non-physical, dishonest, stateless and imprisoned for all.The terminology in the cyber space later described by the United States Government through the US DoD as "the global space in information encompasses an interconnected network of IT infrastructure and residency data, including the Internet, telecommunications networks, computer systems and embedded processors and controllers", where the Tallin manual refers to a more stringent definition of cyberspace operation, such as, "cyber-offense, offensive or defensive, which is supposedly intended to cause damage or damage or destruction of human death or property."Indonesia, as part of the international community, will hamper global challenges of international cyber security, global security and code coding, almost the same cyberspace. This challenge can lead to new forms of state security threats such as cybercrime, cybercrime, cyberattacking and cyberwarfare. Cybercrimes are most popular in Indonesia by international syndicate actors since the legal formulation of regulating cybercrime activities and the capacities of Indonesia law enforcement agencies are limited; in particular, the public will not be aware that Cybersecurity is generally understood. The peculiarities and attributes of infinite, useless and indefinable cyber security spaces make cybercrime as a mutual national crime or transnational crime. In some countries, the development of cyber terrorism and cyber propaganda by radical groups has become a cadaveric space as an effective media campaign. Some of their activities are carried out through a cyber space, that is, a hacker group of cybercrimes, such as collecting, monitoring and coordinating communication systems, collecting financial resources, including hiring cybercriminals and creating their own cyber security (see Fig. 1).

Figure 1: the ISIS's Cyber Caliphate Hacker Group

This condition makes the cyber security sphere a global domain, becoming a national priority, which must be properly identified, evaluated, expected to be comprehensive, complete, complete, effective and effective solution. Terrorist use social media and the Internet is well-documented to pursue ideological goals. This includes terrorist groups, such as Isis, who use the Internet and social media as a tool of propaganda, information exchange, data mining, fundraising, communication and recruitment through websites. Consequently, it is important to have a comprehensive understanding of the international community in terms of cyber security, which is directly aimed at increasingly complex and dynamic cyber security challenges to protect the integrity and sovereignty of the Republic of Indonesia.

3. CYBER SECURITY CASES

It cannot be denied that the digital technologies are great enablers, but they can be misused by actors to conduct criminal actions that may exploit nations, business and individuals. Critical infrastructures, such as government information systems, banking and financial markets, as well as military control and command center are targets of such cyber security challenges. Several examples of cyber security cases that have occurred in the world, such as.:

• The ISIS (2014), has been using videos posted on You Tube, oftenly, where the ISIS use social media calling to Muslims all over the world to join ISIS (see Fig. 2).

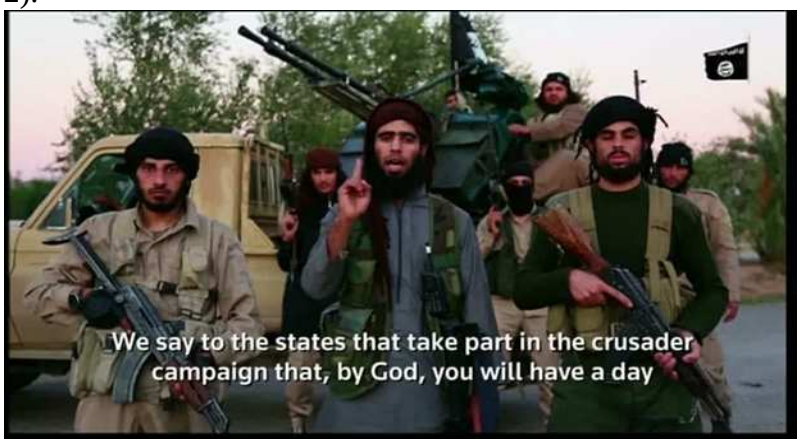

Figure 2: YouTube videos of the ISIS's social media campaign

ISIS has also application in social media, called “The Dawn of Glad Tidings” application (see Fig. 3) that can be downloaded on the google android system. This application shows us the ISIS group try to attract muslims al over the world to use this application in order to join or to support the ISIS group.

Figure 3: The ISIS social media application (illustration)

• In Panama (April 2016), There were "leakaged" through social media outlets of 11.5 million classified documents (2.6 terabytes) of sensitive data from 214,000 companies in Panama's famous service company, Mossack Fonseca. Important confidential documents are missed, such as, emails (4,804,618 files), images (1,117,026 files), PDF (2,154,264 files), database (3,047,306 files), text (320,166 files) and other formats (2,242 files). A suspicious "leakage" of 11.5 million secret documents is made by hackers or by deliberate drainage by people from the internal "Mossack Fonseca" company it self (see Fig. 4).

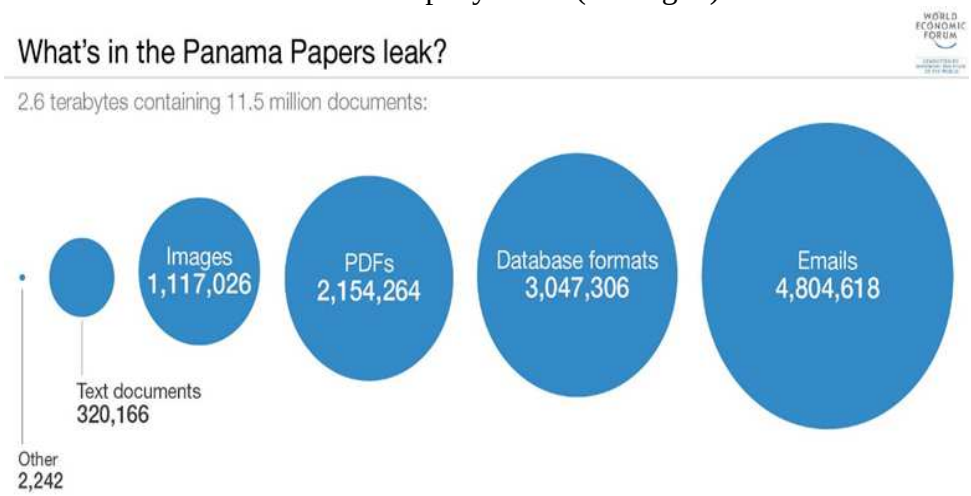

Figure 4: The Scale of Panama Papers Leak

• In USA (October 2016), The US government "accuses" Russia of political blockade and attacks on US President's election in 2016. According to the intelligence analysis of the CIA agency, the activity of Russian hackers influence to the party information system that directly related to the electronic voting in the United States, despite the fact that it was rejected by the Russian side. A valuable lesson from cyber security is the focus on cyber security, for the presidential election or the regional leader to conduct elections using the electronic system. The role of encoding (encryption) in this regard is extremely important to avoid.

• In England (2016), a British teenager who terrorised several FBI and CIA senior officials after tricking his way into their email and phone accounts has been sentenced to two years in youth detention.

• In May 2017, Ransomware Wannacry virus attacks 99 countries all over the world in the same day, it was a huge cyberattack by cryptoworm virus, that targeted computers running the Microsoft Windows OS. It encrypted targeted data and demand payments in Bitcoin transaction (see Fig. 5). Wannacry Ransomware also attack Indonesia in 13 May 2017, where two national hospitals which are located in Jakarta, RS. Harapan Kita and RS. Dharmais have been suffered from this devastating cyber attack, that paralyzed some health information systems in both hospitals. It shows that the impact of Ransomware cyberattacks is very harmful and dangerous. It can be imagined if this kind of virus infects our national critical infrastructure or the state defense system it can be sure that the impact will be much more greater and massive.

Figure 5: The Screenshot of a WannaCry ransomware attack on Windows 8.

4. NIST CYBER SECURITY FRAMEWORK: A CASE STUDY

In the US, the President declared an Executive Order (EO) 13636, in February 2013. This EO aimed to improve the cyber security of national engineering infrastructures. The FBI says: "US policy is to increase the security and stability of the critical infrastructure of the country and to maintain the cyber security environment that promotes productivity, innovation and economic prosperity, ensuring security, security, business credibility, confidentiality and civil liberties." The Presidential EO 13636 has ordered NIST to collaborate the related stakeholders to introduce standards, guidelines and practices to reduce the risk of national cyber infrastructure from cyber threats. NIST 2014 (Version 1.0) is based on standards, guidelines and experiences to help boost the most important infrastructure. It consists of five major cybersecurity activities:

- Identify, developing understanding of an organization to control its cyber risk management related to computer systems, company assets, data and information.
- Protect, developing the most suitable security in order ensuring services of critical information system infrastructure and implemented it.
- Detect, developing most proper actions in terms of identifying the occurrence of cybersecurity events and implemented it.
- Respond, developing the most proper actions for taking the events of cyber threats/attacks and implemnted it.

- Recover, developing the most proper actions to maintaining the integrity of the security plan while restoring impaired capability caused by cyber security threats/attacks and implemented it.

The five activities above divided within categories in terms of determining cyber security threats/attacks to management of assets, control of access, etc. Categories are further divided into sub-categories to explain in more detail to find the goals of each category (see Table 1). In 16 April 2018, NIST re-publishes the latest revision of its cyber security framework, Version 1.1, "Framework for Improving Critical Infrastructure Cybersecurity" (see Table 2). The newest version of NIST is the results of an ongoing collaborative effort involving industry, academia and government. This NIST version 1.1 was published to refine the previous NIST version 1.0 cybersecurity framework published in 2014. As we may know, the United States is very concern with the risk management of its national critical infrastructure

Functions	Categories	Sub-categories	Information References
Identify	• Asset Management • Governance	• Invetory devices, systems &software, etc.	• NIST , etc.
Protect	• Access Control, etc.	• Review access periodically • 2 factor authentication	• ISO 27001:2013 , etc.
Detect	• Detect/Monitor cyber threats/attacks events	• Review logs for suspicious activity, etc.	• NIST , etc.
Respond	• Mitigation of security events, etc.	• Report suspicious events, etc.	• ISO 27001 A6, A16, etc.
Recover	• Recovery planning,improve-ments &communi-cation	• Recovery plan • Manage public relations • Repair reputation	• NIST , etc. • ISO 27001, etc.

especially from cyber security threats or cyberattacks.

Table 1: The NIST Cyber Security Framework (Ver. 1.0)

NIST Framework Core elements are:

- **Functions** organizing basic cybersecurity activities at their highest level. These Functions are "Identify", "Protect", "Detect", "Respond" and "Recover".
- **Categories**, are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities, i.e. "Asset Management", "Identity Management and Access Control" and "Detection Processes".

- **Subcategories**, dividing category into specific outcomes of technical and/or management activities, i.e. “External information systems are catalogued”, “Data-at-rest is protected”, “Notifications from detection systems are investigated”.
- **Informative References (IR)** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory.

The NIST five Functions are:

- **Identify,**Developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities, i.e., “Asset Management”, “Business Environment”, “Governance”, “Risk Assessment”, and “Risk Management Strategy”.
- **Protect**, Developing and implementing appropriate safeguards to ensure delivery of critical services, i.e., “Identity Management and Access Control”, “Awareness and Training”, “Data Security”, Information Protection Processes and Procedures”, “Maintenance” and “Protective Technology”.
- **Detect,** Developing and implementing appropriate activities to identify the occurance of a cybersecurity event, i.e., “Anomalies and Events”, “Security Continuous Monitoring”, and “Detection Processes”.
- **Respond,** Developing and implementing appropriate activities to take action regarding a detected cybersecurity incident, i.e., “Response Planning”, “Communications”, and “Improvements”.
- Recover - Developing and implementing appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident, i.e., “Recovery”, “Planning”, “Improvements”, and “Communications”.

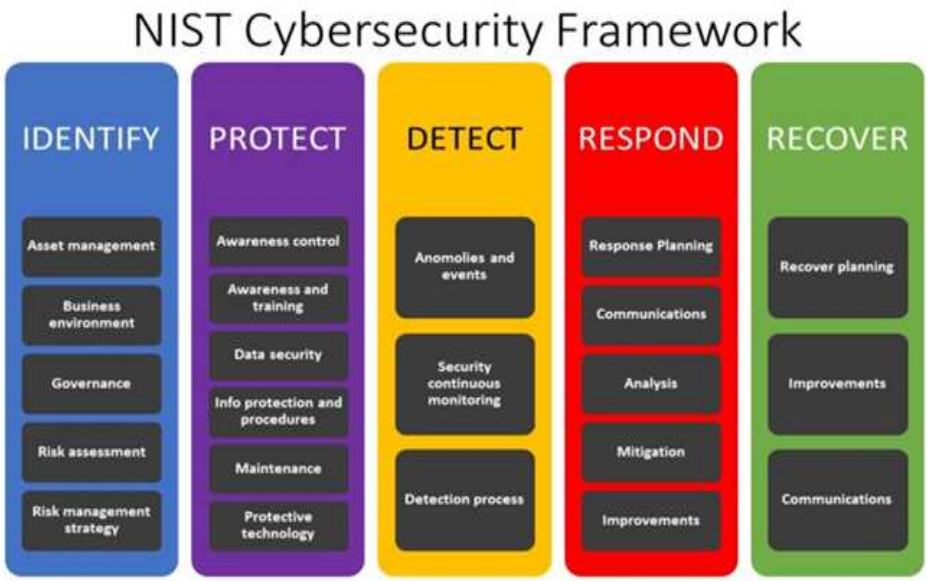

Table 2: The New NIST Cyber Security Framework (Ver. 1.1)

The NIST Framework Core elements are:

- **Functions,** organizing basic cybersecurity activities at their highest level. These Functions are “Identify”, “Protect”, “Detect”, “Respond” and “Recover”.

- **Categories**, are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities, i.e. “Asset Management”, “Identity Management and Access Control”, and “Detection Processes”.
- **Subcategories**,further divide a Category into specific outcomes of technical and/or management activities, i.e. “External information systems are catalogued”, “Data-at-rest is protected”, “Notifications from detection systems are investigated”.
- **Informative References (IR),**are specific sections of standards, guidelines, and ptactices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory.Framework

5. SIX WARE CYBER SECURITY FRAMEWORK (SWCSF)

This paper promotes the concept of cyber security, the so-called "Six Ware Cyber Security Framework" (SWCSF), as a cybersecurity strategy to combat cyber terrorism on the Internet. The SWCSF offers a comprehensive concept of cybersecurity strategy to tackle cyber threats, cyber attacks or vulnerabilities, as well as cyber-fighting against cyber-terrorism. This SWCSF is a practical level of cyber security concept. SWCSF inspired by NIST Cyber Security platform. The SWCSF concept tries to develop the NIST cyber security system Version 1.0. SWCSF concept contributes to the understanding of network security risks, management and expression of common thought, both internal and external. The SWCSF concept promotes the enhanced awareness of the security environment especially for Local Area Network (LAN) system within an organization.

6. SWCSF ENABLERS

SWCSF enablers provide a series of operations that consist of six main variables, subcategories, indices, and information reference links (for example, a link guide). SWCSF provides security integration aspects for managing cyber resources within an organization's computer network (see Table 3), they are:

- **Brainware or Human Factor,** the most important factor of the cyber security networks. The variable is the best listing variable in the SWCSF. From the point of view of the network security, it can not be denied that the user is the most weakest in the chain of cyber security systems. The human plays a dominant role, either to extend or vice versa, to undermine all the efforts of the organization's existing information security. Consequently, organizations should have a function or position with information security, for example, the Chief Information Security Officer (CISO). CISO is the important executive of the company responsible for the safety of users, strategic assets, data and physical and digital formats of information. Its position has increased in the era of cyberspace, where it is easier for the company to steal sensitive information. One of CISO's responsibilities is information security certification programs for all employees. The prerequisite is to produce "information security personnel" about their position and function.
- **Hardware,** is the important factor to tackle threats, attacks, and vulnerabilities of cyber attacks. CISO should teach all levels of staff in order to use and treat organizational hardware safely and wisely. This is because high-level hackers are not only relying on concrete techniques but also combining a conventional attack, such as a social engineering attack. Combination of internal

risk assessment and threat analysis is extremely necessary, for example, for individual access control of the organization's premises or objects, elimination of locking systems and removal of unnecessary CD-ROMs or USB disks, or monitoring and protecting the perimeter of the organization's structures.

- **Software,** refers to the use of software used daily in the organization office, such as websiteor portal, e-mail, social media, and others. Therefore, highly security awareness regarding software application is required because the hacker will always keep pinging on or unsuitable for email attachments or invites you to visit malicious infected websites. Hackers also have new threats, although cyber security tools are available on the market.
- **Infrastructureware.** it plays dominant factor in building a secure organizational network infrastructure related to threats, attacks and vulnerabilities. Today, lots of organizations are heavily dependent on the possibility of using the Internet. In the mean time, not all users (employees) have a good understanding of the security risks that may be encountered in the office where the condition makes the firm's computer network more critical.
- **Firmware** is the factor that includes organizational security strategy and policy documents, standard operating procedures (SOPs), business continuity plans, network security frameworks or ISO standards, ISO 27001. 2013 and more. NIST cyber security framework version 1.0, government security policy and strategy, and more.
- **Budgetware** is the factor that plays an critical role in the introduction of 5 factor variables mentioned before. This is because the organization calls for a fair amount of money or sufficient budget, such as network security enforcement, picking systems, software licenses, training and education, certification programs, and more. High level of security management should address this issue at a high level of priority for informational security awareness also providing sufficient information security budget to protect the entire network system from cyber threats or cyber attacks. Otherwise, the organization will be facing significant financial losses.

7. SWCSF COMPONENTS

SWCSF components work together as an integrated system:

- **Variables,** this component organizing network security aspects as the enablers, for example, brain software, hardware, software, infrastructure software, crystal and cell phones) in top level to manage and analyse data, information by organizing or consolidating. Variables are in line with the security and policy framework to minimize the impact of enterprise quality, such as human resource investments, budgeting planning or restoration activities, and so on.
- **Sub-variables,** this component are the sub-divisions of variables consist of security activities, such as "Security awareness", "socialization and retraining", "cyber security certification scheme", and so on and closely related to certain certified subdivisions.
- **Indicators,** consist of sub-divisions of sub-variables that breakdown into results. Numbers of indicators, for example, a variable of the security awareness sub-system), for example, "Implementation of a Security Awareness Training Program", etc.

- **Information** References (IR) are information for computer security standardization, SOP, etc. related to every indicator above, for example, an indicator of the safety awareness course, "CE-certified EHC course", etc.

SWCSF aspects have a range of actions that are targeted at achieving certain network security results and linking them to those results. SWCSF component is not an action checklist. It represents the key cyber security results found by the organization in risk management in the organization's network security environment.

Aspects	Variables	Sub-variables	Indicators	Information Security References
Brainware	• CISO, etc.	• Security training, etc.	• Secu rity Awareness	• CISSP, CISA, etc.
Hardware	• Server Farms	• USB, etc.	• No comp romi ses	• Bench marking, etc.
Software	• Application	• MS Office, etc.	• No pirated Appli cation, etc.	• Regular updates,etc
Infrastructu re-ware	• Network Infrastructu re	• Firewalls • IDS. • DMZ, etc.	• No net work security breaches, etc.	• Self penetration testing, etc.
Firmware	• Security handbook	• Bussiness Continuity Plan (BCP)	• Good Bussiness processes	• NIST. • ISO 27001, etc.
Budgetware	• Sufficient budget	• Buy software licenses, etc.	• Licen ces always upda ted, etc.	• Alloca ted budget policy, etc.

Table 3: The SWCSF Concept (Enablers and Components)

8. CONCLUSION

The Internet users in all countries must aware and prepare of the cyber security issues in Internet especially utilized by terrorism or radicalist groups, because they know the benefits of the internet services that can be utilized for facilitating the control of information in their organizational command and control system. To countering cyber extremism activities via internet within the region, countries need to cooperate in the use of cyber space. Countries should establish efforts to increase security measures with collaborative efforts in cyber security by including collaborative usage of critical information infrastructure, conduct of cyber security exercises, collaborative usage of information resource, control of information network infrastructure, control of information flow and conduct of collaborative cyber space defense. The Internet users in all countries need to have a national cyber security framework standard such as SWCSF. At the moment, SWCSF is simply a preliminary offer or concept designed to improve the cyber security environment. Later, SWCSF

should be developed and further implemented by further research in order to achieve a proper and suitable cyber security framework for the Internet users.

References

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. The qualitative report, 13(4), Pp. 544-559.

Cyber Attacks: Technique, Tools, Motivation & Impact, last accessed on 23 May 2019.

Dr. Conway, M., "What is cyberterrorism? The story so far", Journal of Information Warfare, 2(2), 33–42., 2003, last accessed on 1 June 2019.

[Establishing BSSN – Indonesia National Cyber Agency, https://id.wikipedia.org/wiki/Badan_Siber_dan_Sandi _Negara, last accessed on 19 May 2019.

Gultom, RAG, "Development of the NIST Cybersecurity Framework", Materials of Cyber Security Policy & Practice Course, The Naval Postgraduate School (NPS), Monterey, California, USA, May 2015.

Gultom, RAG, "Cyber Conflict & Cyber Warfare," Materials of Cyber Security Policy & Practice Course, The Naval Postgraduate School (NPS), Monterey, California, USA, May 2015.

Gultom, RAG, "Cyber Intelligence Overview", Materials of Cyber Security Policy & Practice Course, The Naval Postgraduate School (NPS), Monterey, California, USA, May 2015.

Sueddeutsche, "Panama Papers (the Secrets of Dirty Money)",http://panamapapers.sueddeutsche.de/articles/ 56febff0a1bb8d3c3495adf4/, last accessed on 19 May 2019.

Independent, "Vladimir Putin says Russians accused of hacking US election 'do not represent' the country)", https://www.independent.co.uk/news/world/americas/us-politics/ vladimir-putin-internetresearch-agency-troll-farm-robert-mueller-indictment-13-russians-a8239386.html, last accessed on 2 June 2019.

Independent, "British teenager who 'cyber-terrorized' US intelligence officials gets two years detention",https://www.independent.co.uk/news/uk/british-teen-hacker-kane-gamble-us-intelligence- officials-jailed-cia-fbi-a8315126.html, last accessed on May 1 June 2019.

Irshaid, F., "How ISIS is spreading its message online", BBC news, Available at: http://www.bbc.co.uk/news/world-middle-east-27912569", Journal of Information Warfare, 2(2), 33–42., 2003, last accessed on 2 June 2019.

ISIS Cyber Attack, "Islamic State sympathisers launch cyberattack on US, hack Central Command's Twitter, YouTube accounts", https://zeenews.india.com/news/world/islamic-state-sympathisers-launch-cyber-attack-on-us-hack-central-commands-twitter-youtube-accounts_1529074.html, last accessed on 19 May 2019.

Jim Chen and Duvall, G., "On Operational-Level Cybersecurity Strategy Formation," Journal of Information Warfare: 13.3: 79-87. SSN 1445-3312 print/ISSN 1445-3347 online, 2014.

Obama's US International Strategy for Cyberspace, "Prosperity, Security, and Openness in a Networked World", May 2011, https://www.whitehouse.gov/sites/default/files/

rss_viewer/international_strategy_for_cyberspace.pdf, last accessed on 2 June 2019.

The US White House, Executive Order, "Improving Critical Infrastructure Cybersecurity", 12 February 2013, https://www.whitehouse.gov/the-press-office/ 2013/02/12/ executive-order-improving-critical-infrastructure-cybersecurity, last accessed on 1 June 2019.

The NIST, Version 1.1, "Framework for Improving Critical Infrastructure Cybersecurity"", 16 April 2018, https://www.nist.gov/sites/default/files/ documents/2017/12/05 /draft-2_framework-v1-1_without-markup.pdf, last accessed on 20 May 2019.

Wikipedia, The National Conference of State Legislatures, "Cyberterrorism", https://en.wikipedia.org/wiki/Cyberterrorism, last accessed on 1 June 2019.

Wikipedia, NATO, "Cyberterrorism", https://en.wikipedia.org/wiki/Cyberterrorism, last accessed on 29 May 2019.