Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security Framework

Rudy Agus Gemilang Gultom[1], Asep Adang Supriyadi[2] , Tatan Kustana[3]

Faculty of Defense Technology, Indonesia Defense University, Bogor, Indonesia[1,2]

Faculty of Management Technology, Indonesia Defense University, Bogor, Indonesia[3]

rudygultom@idu.ac.id[1] aadangsupriyadi@idu.ac.id[2] tatankustana@idu.ac.id[3]

Abstract

Nowadays, the extremism, radicalism and terrorism 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 issues of cyber security as a negative impact of internet utilization especially by the extremism, radicalism and terrorism groups. They know the benefits of the internet services and social media can be used to facilitate the control of information in their organizational command and control system. In order to tackle this cyber security issue, the internet users in Association of Southeast Asian Nations (ASEAN) member countries should get more understanding as well as protection from their government against the danger of cyber extremism, cyber radicalism or cyber terrorism activities over the Internet. Therefore, this paper tries to explain the need of an ASEAN Cyber Security Framework standard in order to countering cyber terrorism activities via Internet as well as introducing the initial concept of Six-Ware Cyber Security Framework (SWCSF).

Keywords: Asean Cooperation, Internet, Cyber Terrorism, Six-Ware Cyber Security Framework

Date of Publication: 2018-10-09

DOI: 10.24297/ijmit.v13i0.7624

ISSN: 2278-5612

Volume: 13 Issue: 1

Journal: INTENATIONAL JOURNAL OF MANAGEMENT AND INFORMATION TECHNOLOGY

Website: https://cirworld.com

This work is licensed under a Creative Commons Attribution 4.0 International License.

1. Introduction

In the current era of information globalization, the strength, sovereignty and resilience of a country is not only measured by the magnitude of military or economic power it has, but also depends on many aspects of mastery, use and empowerment of the Cyberspace and Internet access. Many countries nowadays, including ASEAN member countries, are highly dependent on the utilization of the Cyberspace and the Internet especially in economic, business, academic, social, political, governmental, defense and security aspects. Through the utilization of constructive cyberspace, nations social relations can be organized directly in a relatively short period of time without space and time constraints, whether in peacetime, crisis or war.

The cyberspace phenomenon illustrates the reality that activities in the modern society are interconnected throughout cyberspace. From the perspective of cybersecurity, the purpose of the use of internet might also be covering the misused for negative or destructive purposes by individuals with bad intention, non-state or/and state actors, including terrorist groups, in fact. As we may know, various facilities (tools) available on the Internet can be used to disrupt, damage, and paralyze critical infrastructure or to threaten the national interests of a country, even to influence radicalism ideology or extremism/ terrorism action, massively and continuously.

In the midst of advances in information and communication technology today the various cyber threats or attacks conducted throughout the cyberspace (Internet) is greatly organized by either a state actor or non-state actors to the national interest of one other country would have the potential to become a form of cyberattack is serious. From the perspective of Indonesian National Resilience ("Tannas"), threats or cyberattacks can reduce Tannas condition index as measured by Asta Gatra (8 Gatras) index parameters, namely: Ideology, Political, Economy, Social Cultural, Security, Geography, Demographic and Natural Resources.

Various cyber security challenges via cyberspace such as web defacing, cyber propaganda, cyber radicalism, cyber terrorism, cyber warfare, child pornography, black propaganda, character assasination, hate speech, hoax and so on cause many countries to then establish a National Cyber Agency with the single purpose to protect their national interests and resilience. Some of those institutions known are: US Cyber Command, China PLA Blue Army, Korea KISA, Israel Unit 8200 IDF or Indonesia BSSN (National Cyber Agency). In fact, the United States through the National Institute of Standards and Technology (NIST) has defined Cybersecurity as the ability to protect or defend the use of cyberspace from cyberattacks including Cyberterrorism action.

According to The National Conference of State Legislatures definition: "Cyberterrorism is the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, Denial-of-service attacks, or terroristic threats made via electronic communication." NATO defines cyberterrorism as: "a cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal."

In Indonesia, 19 May 2017, the President of Indonesia, Mr. Joko Widodo, has signed establishment of the National Cyber and Encryption Agency (BSSN) in charge of implementing national cyber security effectively and efficiently by utilizing, developing and consolidating all elements related to cyber security. The BSSN become the leading sector of the national cyberspace affairs through the issuance of Presidential Decree No. 53 of 2017. Structurally, the BSSN organization is directly under the president and become the leading sector in the National Cybersecurity endeavour.

Indonesia is currently ranks 5 countries the largest Internet users in the world after China, India, the United States and Brazil with the number of Indonesian Internet users who reached 132.7 million users or about half of the population of Indonesia. Therefore, the utilization of internet access services by the people of Indonesia becomes an important and strategic issue.

2. Understanding the Challenges of Global Information Security

To understand the cybersecurity challenges in the context of the global domain requires an understanding of the development of the global strategic environment. One country must be able to comprehend holistically that cyberspace as a borderless global domain, space less and timeless that bring new challenges in the current era of globalization of information. The un-conformed international understanding of the meaning of cyberspace and how go govern it will remain as obstacles, challenges and resistance when one country try to make a unilateral claim that global cyberspace as part of their country's sovereignty.

This is in contrast to the claims of the conventional sovereignty of a country which governed by the international treaties, such as UNCLOS 1982 (United Nations Convention on Law of the Sea) whereas in UNCLOS 1982 it is clearly and assertively defined the right that a sovereign state and the responsibility of a sovereign state in the use and management of the oceans of the world in which it is entitled (ZEE/ Exclusive Economic Zone) and establishes guidelines for its business, environment and her natural reserves management. Sovereignty in cyberspace today are seen to be non-physical, border less, stateless and timeless to all.

The terminology of border in cyberspace then explained by the Government of the United States of America through The United States Department of Defense (DoD) as: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".

The US DoD then creates a definition derivative for cyberspace operations as: "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace".

When referring to the Tallin Manual document there is a more rigid definition of cyberspace operation: "a cyber-operation, whether offensive or defensive, that is reasonably expected cause injury or death to persons or damage or destruction to objects".

Indonesia, as part of the international community will also facing the global challenges of international cybersecurity affairs, cyber security and codes encryption through the almost the same cyberspace it is. This challenge may have the implications as new forms of threat to the state security such as cyberattack, cybercrime, cyber prostitution, cyber propaganda, cyber terrorism to cyber warfare.

Currently more and more emerging cybercrime action conducted by international syndicate actors through Indonesian territory because the legal formality governing cybercrime activities and the capacity of the law enforcement in Indonesia is very limited let alone the public are not too aware with the understanding of Cybersecurity in general.

The properties and characteristics of the borderless, space less and timeless cyber spaces make cybercrime as a form of trans national crime or transnational crime. The development of cyber terrorist and cyber propaganda actions by the radical groups in some countries has turned out to utilize cyber space as an effective "media of struggle".

Some of their actions are carried out through cyber space such as member recruitment, control and coordination communication systems, collection of financial resources management, including hiring hackers/ crackers to cyber troops and creating their own cyber weapons. This condition makes cyberspace as a global domain to become a national crucial issue that needs to be correctly identified, evaluated, anticipated in order to searched for a comprehensive, integral, holistic, effective and efficient solution.

Terrorist's use of social media and the Internet to pursue their ideological aims is well documented. This includes terrorist groups such as Isis who are using the Internet and social media sites, as a tool for propaganda via websites, sharing information, data mining, fundraising, communication, and recruitment. Therefore, a comprehensive understanding of the aspect of cyberspace as a global domain of the international community becomes important to be addressed correctly facing the increasingly complex and dynamic cybersecurity challenges to protect the integrity and sovereignty of the Republic of Indonesia and for one of them is in the framework of drafting the Integral and Holistic for ASEAN cyber cooperation in countering cyber extremism, terrorism and radicalism.

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 operations, storage and delivery systems, banking and financial markets, as well as military control and command are targets of such cyber security challenges. In the context of cyber security issues there are several examples of cyber security cases that have occurred in the world, i.e. in 2014, The ISIS have been using both platforms as magnets that have attracted thousands of views, comments, forums and posts. For example, through the use of videos posted on YouTube, it began its' one billion campaign, which called upon Muslims to join ISIS. The videos attracted huge audiences and were accompanied with the words: "Proudly support the Muslim cause" (see Fig. 1).

Figure 1: YouTube videos of the ISIS's one billion campaign

Furthermore, ISIS had released a free to download application (app) which kept users updated with the latest news from the organisation. The application entitled: "The Dawn of Glad Tidings" (see Fig. 2) was promoted online and was available on the google android system, before it was detected and suspended. Most of the content was regulated by Isis's social media arm. This app shows us how the use of cyber-terrorism and social media have converged in this virtual space for terrorist groups such as ISIS.

Figure 2: The ISIS social media application

April 2016 in Panama, there is a "leakage" via social media of 11.5 million classified documents (2.6 terabytes files) containing sensitive data from companies around 214,000 companies in a Panama well-known service company, Mossack Fonseca. The “leaked” important secret documents are emails (4,804,618 files), database (3,047,306 files), PDF (2,154,264 files), images (1,117,026 files), texts (320,166 files) and other formats (2242 files). Suspected "leak" of 11.5 million secret documents are done through hacking by hackers or deliberately leaked / tapped by people in Mossack Fonseca itself.

October 2016 in USA, The United States government "accused" the Russian of political hacking and wiretapping attacks related to the election of the President of the United States in 2016. According to the CIA Agency intelligence analysis concluded that the activities of Russian hackers who managed to tap the information and information system of the parties directly related to the electronic votes in the United States, although this has been denied by the Russian side. A valuable lesson to be learned from this case is the requirement for special attention to cyber security for the implementation of Presidential election or Regional Head election using the electronic system votes. The role of the coding system (cryptography) is crucial in this aspect to avoid tapping.

In 2016, a British teenager who "terrorised" some of America’s most senior intelligence officials (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, Wannacry Ransomware attack was a worldwide cyberattack by the Wannacry ransomware crypto worm virus, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency (see Figure 3).

In Indonesia, two national level hospitals in Jakarta, RS. Harapan Kita and RS. Dharmais have been suffered from this fatal cyberattack that paralyzed some health information systems in both hospitals. It shows us that the impact of Ransomware cyberattacks is very harmful and dangerous. It can be imagined if such virus attacks our national critical infrastructure or the state defense system where the impact will be far greater and massive.

Figure 3: Screenshot of a WannaCry ransomware Attack on Windows 8

4. Case Study: The NIST Cyber Security Framework

In February 2013, the US President issued an Executive Order (EO) 13636, in order to improving national critical infrastructure cybersecurity. The EO states: "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cybersecurity environment that encourages efficiency, innovation and economic prosperity while promoting safety, security, business confidence, privacy and civil liberties".

The US President EO 13636 ordered NIST to work with stakeholders to develop a voluntary framework based upon existing standards, guidelines, and practices in order to reduce cyber risks to national critical infrastructure. The NIST 2014 framework (Version 1.0) consists of standards, guidelines, and practices to promote the protection of critical infrastructure. It is composed into five basic cybersecurity activities:

• **Identify,** to develop the organization's understanding to manage cybersecurity risk to systems, assets, data and capabilities.

• **Protect,** to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

• **Detect,** to develop and implement the appropriate activities to identify the occurrence of cybersecurity events.

• **Respond** (to develop and implement the appropriate activities to take action regarding a detected cybersecurity event).

• **Recover** (to develop and implement the appropriate activities to maintain the integrity of the security plan and maintain network resilience while restoring impaired ability or services because of cybersecurity attacks.

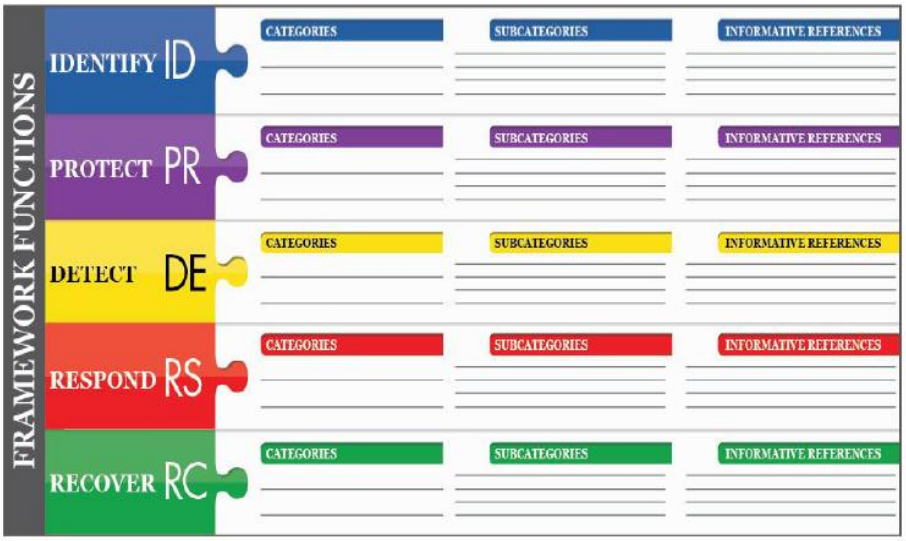
The five activities above are then divided into categories in order to determine a more specific security practices and capabilities, i.e. asset management, access control, etc. Categories are further divided into sub-categories to explain in more detail or technical controls needed to meet the goals of each category (see Table 1).

Table 1: The NIST Cyber Security Framework (Version 1.0)

Functions	Categories	Sub-categories	Information References
Identify	• Asset Management • Governance	• Invetory devices, systems and software, etc.	• NIST 800-53 CM-8, CA-2, etc.
Protect	• Access Control, etc.	• Review access periodically • Two-factor authentication	• ISO 27001 A6, A9, A11, A13, etc.
Detect	• Detect & Monitor for anomalies and events	• Review logs for suspicious activity, etc.	• NIST 800-53 AU-6, CA-7, etc.
Respond	• Mitigation of security events, etc.	• Report suspicious events, etc.	• ISO 27001 A6, A16, etc.
Recover	• Recovery planning, improve-ments and communication	• Recovery plan • Manage public relations • Repair reputation	• NIST 800-53 CP-10, IR-4, IR-8, etc. • ISO 27001 A16, etc.

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 II). 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 of the risk management for its national critical infrastructure especially from cyber security threats or cyberattacks that can be placing the Nation's security, economy and public safety and health risk.

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



The Framework Core elements work together as follows:

- **Functions** organize 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** 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 five Framework Core Functions are defined below:

- **Identify** - Develop 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** - Develop and implement 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** - Develop and implement appropriate activities to identify the occurences of a cybersecurity event, i.e., "Anomalies and Events", "Security Continuous Monitoring", and "Detection Processes".
- **Respond** - Develop and implement appropriate activities to take action regarding a detected cybersecurity incident, i.e., "Response Planning", "Communications", and "Improvements".
- **Recover** – Develop and implement 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".

5. The Six-Ware Cyber Security Framework Proposal

As mentioned above, this academic paper contributes an initial security framework proposal, so called, The Six-Ware Cyber Security Framework (The SWCSF) for ASEAN cyber cooperation. The SWCSF proposal is a comprehensive concept for cyber security solution to enhance an ASEAN countries network security resilience from various threats, attacks and vulnerabilities as well as in countering violent extremism activities over the cyberspace. This is an operational-level security strategy that enables to figure out the most efficient and effective actions that may lead to the success of cyber security operation.

The idea behind this new concept was inspired by NIST cyber security platform version 1.0., dated 12 February 2014. The SWCSF concept tries to elaborate NIST cyber security framework to be more practical for the operational level. The security framework discussion can be found also in mashup web data extraction system. The SWCSF concept contributes a common thought to understanding, managing, and expressing network security risks, both internally and externally.

The SWCSF concept contributes increased security awareness environment within an organization where it requires internal/external risk assessment and also threat analysis policies. All levels employees in the organization, ranging from highest level to lowest level must be actively involved in the SWF concept implementation. Otherwise, they cannot obtain better understanding of how threats or attacks can be carried out successfully across the entire organization.

5.1. The SWCSF Enablers

The SWCSF enablers provide a set of activities, which consists of six main variables, sub-variables, indicators and information references (e.g., reference guidance). The SWCSF enablers are not only a set of checklist of actions to perform, but it presents key network security solutions to manage security risk and analysis in an organization computer network. The SWCSF enablers comprises six main aspects, e.g., Brainware, Hardware, Software, Infrastructureware, Firmware, Budgetware (see Table III).

• **Brainware** or **Human Factor,** is the main aspect in network security environment. This variable becomes top list variable within the SWF concept. From network security perspective, it commonly known that human is the weakest link in information security environment. Human factor plays dominant role to enhance or on the contrary, to disrupt all efforts of existing information security within an organization. Therefore, organizations must have function or position related to information security, e.g., Chief Information Security Officer (CISO). The CISO is a company's top executive who is responsible for security of personnel, physical assets, data and information in both physical and digital form. The CISO position has increased in the era of cyberspace where it becomes easier to steal sensitive company information. One of CISO's responsibilities is to conduct information security certification programs to all level employees. The intention is to produce "information security awareness employees" related to their position and function.

• **Hardware,** plays dominant role in handling threats, attacks and vulnerabilities. CISO has to teach all level employees how to use and treat organization's hardware devices safely and wisely. It is because a high-level hacker is not just relying on a specific technique, but still combined with the conventional attack, e.g., social engineering attack. Combination of internal risk assessment and threat analysis are extremely needed, e.g., controlling individual access into the organization's premises or facilities, locking systems and removing unnecessary CD-ROM or USB thumb drives, or monitoring and protecting the security perimeter of organization's facilities, etc.

• **Software,** relates to utilization of software applications security which are used daily in the office, e.g., email, website, social media and other applications. High security awareness is really required because a high profile attacker will always kept on trying to infect or inject malicious emails and its attachments or invite to visit malware-infected websites. The attackers are also constantly introducing new threats although various cyber security application tools are available in the market.

• **Infrastructureware,** has an important role in facilitating secure organization network infrastructure, e.g., monitoring network from various threats, attacks and vulnerabilities. Nowadays, most of organizations have been highly dependent on Internet access. On the other hand, not all of employees have a good level understanding about security risks they might face in the office, where this condition is making the organization's network infrastructure more vulnerable.

• **Firmware,** includes documentation of an organization security strategy and policy, standard operating procedures (SOPs), business continuity plans (BCPs), network security frameworks or International Organization for Standardization (ISO), i.e. ISO 27001:2013, etc., NIST cyber security framework version 1.0, government security policy & strategy, etc.

• **Budgetware,** plays important and strategic role in facilitating implementation of the five-ware variables above. It is because an organization is urged to provide big enough money or sufficient budget to purchase e.g., network security application tools, patching systems, software licenses, training and education, certification programs, etc. It is highly recommended top level management must put this matter as a high level priority in order to build information security awareness. Allocating sufficient information security budget could protect the entire network system. Otherwise, they will face organization's significant financial losses, etc.

Table 3: The SWCSF Concept (Enablers and Components)

Aspects	Variables	Sub-variables	Indicators	Information Security References
Brainware	• CISO, etc.	• Security training, etc.	• Security Awareness	• CISSP, CISA, etc.
Hardware	• Server Farms	• USB, etc.	• No compromises	• Bench marking, etc.
Software	• Application	• MSOffice , etc.	• No pirated Application, etc.	• Regular updates, etc
Infrastruc-tureware	• Network Infrastructure	• Firewalls. • IDS. • DMZ, etc.	• No network 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.	• Licences always updated, etc.	• Allocated budget policy, etc.

5.2. The SWCSF Components

The SWCSF components work together as follows:

• **Variables,** organize network security fundamental aspects as enablers, e.g., brainware, hardware, software, infrastructureware, firmware and budgetware) at highest level. These variables help an organization in managing its security risk and analysis by organizing or clustering data or information, threats and attacks activity. Variables align with security and policy framework to reduced impact to organization quality of services (QoS) e.g., investments in human resources, planning and budgeting exercises or recovery actions, etc.

• **Sub-variables,** are sub-divisions of a variable closely tied to a particular (for example, brainware variable) security awareness activities e.g., "security awareness", "socialization and training", "cyber security certification program", etc.

• **Indicators,** are sub-divisions of a sub-variable, divided into technical outcomes. Indicators provide a set of results to achieve outcomes for each sub-variable. Indicators example (like security awareness sub-variable) e.g., "conducting security awareness training program"; "socializing and implementing security awareness culture in the company"; or "notifications from any social engineering attacks or security breaches that are being investigated", etc.

• **Information References (IR),** consists of network security standards, guidelines, methods and practices to achieve solutions or outcomes associated with each indicator. IR which presented in the SWF concept are illustrative and not complete. Examples of IR (like conducting security awareness training program indicator) e.g., "certified ethical hacking (CEH) course from EC-council"; "DoD information assurance awareness training"; and "Achieving ISO 27001 Certification"; etc.

The SWCSF component provides a set of activities to achieve specific network security outcomes, and references examples of guidance to achieve those outcomes. The SWCSF component is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by organization as helpful in managing the risk within organization network security environment.

6. Strategic Recommendations

This academic paper recommends several strategic recommendations, they are:

• **To build the ASEAN Cyber Security Strategy and Policy,** the ASEAN countries needs an ASEAN Cyber Security Strategy and Policy as the frame of reference of a comprehensive model based on the involvement, coordination and harmonisation of all the ASEAN countries and on public-private collaboration and citizen participation in countering violent extremism activities over Internet. To achieve this objective, the ASEAN Cyber Security Strategy and Policy creates single ASEAN cyber security organisational structure that is integrated into the ASEAN cyber security framework (the SWCSF - Six Ware Cyber Security Framework proposal).

• **To build the ASEAN Cyber Security Master Plan,** the ASEAN needs an integrated and strategic cyber security approach in order to build cyber security master plan in related to achieve ASEAN cyber security cooperation outcomes. The ASEAN cyber security master plan will provide a clear plan of action in combating violent extremism activities over Internet to ensure ASEAN member countries may implement the Six Ware Cyber Security Framework (SWCSF) proposal. This ASEAN cyber security master plan will have the ASEAN Cooperation Grand Strategy, Roadmap and the SOPs.

• **To define a common ASEAN Cyber Critical Information Infrastructures and protect it against Cyber Terrorism activities,** it is essential for ASEAN governments to define a common ASEAN Critical Infrastructures. The ASEAN governments need to work closely with the private sector, often in Public-Private Partnerships (PPPs) to help manage the threats to ASEAN Cyber Critical Information Infrastructures, because

the private sector is often the first to detect these threats or attacks, therefore the government plays a vital role in coordinating the response, where the Six Ware Cyber Security Framework (SWCSF) proposal could be implemented.

• **To unify vision of the ASEAN countries in countering Cyber Terrorism activities over the Internet,** for the issue of cyber terrorism activities over the Internet or Counter-Cyber Terrorism, it considered necessary to unify the vision of the ASEAN policy and action toward the terrorism threat such as actors, organizations and models of the terror as the current trend. In addition, to best practice from several countries which have successfully eradicated of terrorism also important to socialize of terror prevention system through the mechanism of de-radicalization approach besides the military or police operation.

• **To share Information regarding countering Cyber Terrorism activities over the Internet,** regarding the issues of Cyber Security and Countering cyber terrorism activities over the Internet lots of experiences from ASEAN member countries of dealing with these issues can be a valuable asset to the other ASEAN countries through share information mechanism. The ASEAN countries need to create a Cyber Security Forum for information sharing activities.

• **To create ASEAN Cyber Security Cooperation Handbook,** the ASEAN cyber security cooperation handbook will offer a simplified and practical reference template as a standard to implement the Six Ware Cyber Security Framework (SWCSF) proposal for the ASEAN governments.

• **To create ASEAN Cyber Command and Control Center,** the ASEAN countries need to build an ASEAN Cyber Command and Control Center (ACCCC or AC4), as well as, to create ASEAN cyber security framework standard such as the Six Ware Cyber Security Framework (SWCSF) concept.

7. Conclusion and Further Work

ASEAN 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 cyberspace defense. The SWCSF is just an initial concept to enhance ASEAN countries cyber security environment. In the future, the SWCSF concept needs to be developed and implemented more in-depth through further research on specific areas especially in the six main aspects of SWCSF enablers: Brainware, Hardware, Software, Infrastructureware, Firmware, Budgetware.

Acknowledgement

The authors would like to thank and also to give high appreciation to the Rector of the Indonesia Defense University (IDU) and the Network of ASEAN Defence and Security Institutions (NADI) Track II for giving a valuable chance to attend and present this academic paper at the Workshop on "ASEAN Cooperation in Cyber Capacity Building" 7 -11 May 2018, Ayutthaya, Thailand.

References

1. Establishing BSSN - National Cyber Agency, https://id.wikipedia.org/wiki/Badan_Siber_dan_Sandi _Negara, accessed august 19th, 2018.

2. Chen, J., 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, accessed August 24th, 2018.

3. Colonel Dr. Rudy Agus Gemilang Gultom,"Cyberspace as Global Domain", Materials of Cyber Security For Information Leaders Course, The National Defense University (NDU),Washington,DC. USA, March 2015.

4. Colonel Dr. Rudy Agus Gemilang Gultom, "Cyber Intelligence Overview", Materials of Cyber Security Policy & Practice Course, The Naval Postgraduate School (NPS), Monterey, California, USA, May 2015.

5. Dr. Conway, M., "What is cyberterrorism? The story so far", Journal of Information Warfare, 2(2), pp. 33–42., 2003.

6. Internet sources, "Cyber Attacks: Technique, Tools, Motivation & Impact", accessed August 18th, 2018.

7. Internet, "The Famous Cyber Attacks/ Cyber Warfare in the World", accessed August 16th, 2018.

8. 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, accessed August 2nd, 2018.

9. Sueddeutsche, "Panama Papers (the Secrets of Dirty Money)", http://panamapapers.sueddeutsche.de/articles/56febff0a1bb8d3c3495adf4/, accessed July 29th, 2018.

10. 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, accessed July 27th, 2018.

11. Independent, "British teenager who 'cyber-terrorised' 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, accessed July 29th, 2018.

12. 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, accessed August 14th, 2018.

13. The NIST, Version 1.1, "Framework for Improving Critical Infrastructure Cybersecurity", https://www.nist.gov/sites/default/files/ documents/2017/12/05 /draft-2_framework-v1-1_without-markup.pdf, accessed July 19th, 2018.

14. Wikipedia, The National Conference of State Legislatures, "Cyberterrorism", https://en.wikipedia.org/wiki/Cyberterrorism, accessed July 19th, 2018.

15. Wikipedia, NATO, "Cyberterrorism", https://en.wikipedia.org/wiki/ Cyberterrorism, accessed July 19th, 2018.

16. NIST (National Institute of Standard and Technology), http://www.nist.gov/, accessed August 22nd, 2018.

17. Plan To Establish National Cyber Agency (BSSN), http://nasional.kompas.com/read/2015/01/06/ 12550571/Presiden.Bahas. Pembentukan.Badan.Cyber.Nasional, accessed July 23rd, 2018.

18. President Obama's 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, accessed July 22nd, 2018.

19. Prof. Kevin P. Newmeyer, "Who Should Lead U.S.Cybersecurity Efforts?", PRISM Magazine vol. 3, no. 2, The National Defense University (NDU), Washington, DC., USA, March 2015.

20. Reasons for the Government to form BSSN, http://nasional. kompas.com/read/2015/01/06/15464401/Ini.Alasan.Pemerintah.Ingin.Bentuk.Badan.Cyber.Nasional, accessed August 19th, 2018.

21. Rudy Agus Gemilang Gultom, "Proposing the new Algorithm and Technique Development for Integrating Web Table Extraction and Building a Mashup," Journal of Computer science, Science Publication, NY, USA,

DOI: 10.3844/jcssp.2011.129.142, http://www.thescipub.com/ issue-jcs/7/2, 25 February 2011. Download PDF version, http://thescipub.com/PDF/jcssp.2011.129.142.pdf, accessed August 19th,2018.

22. The Government of Indonesia has accelerated the formation of the National Cyber Agency in the year2017), http://nasional.kompas.com/read/2017/01/03/18063511/pemerintah.percepat. pemben-tukan.badan.siber.nasional.pada.2017, accessed July 23rd, 2018.

23. The United Nations Convention on the Law of the Sea (UNCLOS) in 1982, accessed July 29th, 2018.

24. The US DoD, "Department of Defense Strategy for Operating in Cyberspace", http://www.defense. gov/news/d20110714cyber.pdf, accessed August 2nd, 2018.

25. The Tallinn Manual, "Tallinn Manual on the International Law Applicable to Cyber Warfare", https://ccdcoe.org/tallinn-manual.html, accessed July 22nd, 2018.

26. Youtube, "YouTube videos of the ISIS's one billion campaign", https://www.youtube.com/results?search_query=YouTube+videos+of+the+ISIS%E2%80%99s+one+billio n+campaign, accessed July 26th, 2018.

Authors

Rudy Agus Gemilang Gultom as the author is a researcher and also a senior lecturer at Faculty of Defense Technology, the Indonesia Defense University (IDU), Bogor, Indonesia. He finished his Under Graduate from Gunadarma University, Indonesia in 1991. He finished his Master degree (M.Sc.) in Telematics from the Department of Computer Science, University of Sheffield, United Kingdom in 1999 with scholarship from the British Chevening Award. In 2012, He finished his Doctoral degree (Dr.) in Information Technology from the University of Indonesia, Indonesia with scholarship from Indonesian Government. He can be contacted at (+62)81380695525 or office: (62)(21) 87951555 ext.7257; fax: (62)(21)29618766; e-mail: rudygultom@idu.ac.id.

Asep Adang Supriyadi as the co-author is also a researcher and also a senior lecturer at Faculty of Defense Technology, the Indonesia Defense University (IDU), Bogor, Indonesia. He finished his Master degree from Air Marshal Suryadarma University, Jakarta, Indonesia, in 2014. He finished his Doctoral degree (Dr.) from Brawijaya University, Malang, Indonesia in 2017. He can be contacted by mobile phone: (+62) 81219588063 or at office: (62)(21) 87951555 ext.7257; fax: 62-21-29618766; e-mail: aadangsupriyadi@idu.ac.id.

Tatan Kustana as the co-author is also a researcher and also a senior lecturer at Faculty of Defense Management, the Indonesia Defense University (IDU), Bogor, Indonesia. He finished his Master Degree (M.Bus) from RMIT University of Melbourne, Australia in 1997. He also finished another Master Degree (M.A) from Deakin University, Melbourne, Australia in 2010. He finished his PhD study from National University of Jakarta, Indonesia in 2017. He can be contacted by mobile phone: (+62) 81294340609 or at office: (62)(21) 87951555 ext.7108; fax: (62)(21)29618766; e-mail: tatankustana@idu.ac.id.