Syntax Idea: p–ISSN: 2684-6853 e-ISSN: 2684-883X
Vol. 3, No. 1, Januari 2021

INDONESIA'S CYBER DEFENSE STRATEGY IN MITIGATING THE RISK OF CYBER WARFARE THREATS

Agus Permana
Indonesia Defense University, Departement of Asymmetric Warfare
Email: agus.permana@idu.ac.id

Abstract

The purpose of this paper is to analyze and describe the strategy of the Indonesian government in mitigating the risk of dealing the threat of cyber warfare. This paper uses the qualitative method using 3 indicators of risk mitigation theory consisting of prevention, indentification and remedy to interpret the problem and explain it in more detail by collecting data from literature studies. Cyber defense threat mitigation refers to policies and processes put in place by an institution to help in preventing a potential security incident and data breaches as well as to limit the extent of damage when a security attack does happen. The results of the discussion of this study are the Indonesian government's strategy focusing on processes, technology and information, preparedness, response, and follow-up activities, all of which included in instruments for measuring risk mitigation of cyber warfare threats. The conclusion is that Cyber defense in the form of a strategic concept must be concrete if all infrastructure networks are held, then the cyber defense policy can be known. To build a reliable cyber defense system, the government and stakeholders must ensure that the cyberinfrastructure is secure. The Indonesian government must increase capacity and increase cooperation leading stakeholders and government is essential regarding cyber warfare. Having a good risk mitigation plan will help cyber defense policies in Indonesia as the basis for the preparation.

Keywords: *strategy; cyber defense; risk mitigation; cyber warfare*

Introduction

Nowadays, cyber-attacks on defense aim to attack the strategic sector of national security. These attackers mostly threaten the cyber defense system could be due to direct attacks from other countries or the impact of foreign countries at war. Meanwhile, cybercrime refers to every criminal violation in cyberspace. These actors do not target government objects or critical national infrastructure. They also cannot effectively endanger the country. They are usually considered a threat of cybercrime. This misleading identification has the potential to confuse which institutions must respond to the attack: the Ministry of Defense, and other stakeholders. The boundaries between the two must be clarified so that in the long run, there will be no overlap between government agencies in responding to these attacks.

Indonesia is the fourth most populous country in the world, and 64.8% of them are active internet users (CBNC Indonesia, 2019). In recent years, countries are no longer

defensive when it comes to facing a growing number of cyberattacks. The buildup of offensive cyberwar capabilities has become a cybersecurity policy trend among countries. The last thing Indonesia needs is an escalation of this trend into a global cyberwar. Indonesia could suffer unintended consequences, given that anonymous actors often use Indonesian territory as a launchpad for cyberattacks. In 2013, Indonesia even superseded China as the world's top source of cyberattack traffic, according to internet monitoring company Akamai. According to the Communications and Information Ministry, Indonesia was the target of more than 205 million attacks in 2017. In a cyberwar, Indonesia could face more concerted attacks that could cripple critical infrastructure, public services, and businesses. A cyberwar thus poses a serious threat to Indonesia's vision to become Southeast Asia's largest digital economy by 2020. To anticipate the global buildup of cyberwar capabilities, Indonesia must first officially publish a white paper on its international strategy in cyberspace. Such a document could explain Indonesia's position on offensive cyber capability and its impact on international security and stability (Aryadi, 2018).

In this paper, the focus of this research will be to identify and explain how Indonesia's strategy in the cyber defense system in which there are governments and stakeholders in mitigating the risk of cyber threats, this paper aims to provide analysis and description as literacy material for related parties in dealing with cyber threats. Moreover, prepare for cyberwar potential.

Methodology

This research uses qualitative research methods with a quasi-qualitative research design or in other words descriptive-qualitative. Qualitative research is a method for exploring and understanding individuals and organizations that are considered social or humanitarian problems (Creswell & Creswell, 2017). In this paper, the writer will will analyze the the Indonesian government strategy in dealing the threat of cyber warfare by using risk mitigation theory whose data is from the literature, especially the policies carried out by the Indonesian government and then described and discussed. The following is the theory used as an indicator of risk mitigation in this study. Cyber defense threat mitigation refers to policies and processes put in place by an institution to help in preventing a potential security incident and data breaches as well as to limit the extent of damage when a security attack does happen.

Threat mitigation in cyber defense can be broken down into three indicators, or layers of mitigation (Stroud, 2019).

a. Threat prevention: Best practices and policies that protect an institution applications and data from being threatened by threat actors.
b. Threat identification: Security tools and management to identify active security threats.
c. Threat remedy: Strategies and tools to reduce the impact of active security threats that have gotten past corporate security defenses and infiltrated the network by isolating or containing the threat.

Results and Discussion

1. The Emergence of Cyber Warfare Threats

Indonesia Honeynet Project (IHP) is a cybersecurity community and is part of the global Honeynet organization. The IHP was established on November 25, 2011, based on a petition by 15 members from academia, information security agreements, and the government proposing the establishment of the Honeynet-Indonesia Chapter Project supported by the Singapore Chapter. The Indonesia Chapter start to operate and responded by Honeynet Global on January 9, 2012 due to the ransomware malware attack that had crippled two hospitals in Indonesia. IHP initiated a system that could retaliate any cyberattacks by luring the attackers, by utilizing honeypot technique. This system is quite effective since unnoticed by the attacker as they has entered a trap (Badan Siber dan Sandi Negara., 2019).

In 2018, for the first time, BSSN and IHP launched the 2018 Honeynet project annual report. This report was to provide information to the public about the socialization and collaboration activities carried out by National Cyber and Crypto Agency (BSSN) and IHP with a collaboration among government institutions, private sectors, and academics. Following, there are also reports of cyber-attacks that occurs in Indonesia, results of data exchanges traffic checks and the detection of other cyber and malware attacks, including the analysis of the three most malware attacks in Indonesia and, the portal for introducing Honeynet as a public service including the discussion of the research and development of the Honeynet Project Indonesia. The Honeynet Project has five research fields for development, namely malware, fraud technology, data mining, cybercrime, and tools. While the five Honeynet Project research areas are equipped with DNS Traffic Analysis (analysis of dangerous traffic entering DNS), Crypto Currency (attacks on Cryptocurrency), Malware Detection (accurate detection of malware by extraction), Cyber Security Policy (Cyber Security Policy), and the Instruction Detection (detection of disturbances by various methods).

Following the project, BSSN and IHP developed research to draw a Threat Map that can be utilized by the government and business people. The research is conducted to create a Malicious Domain List for the public domain. In the National Cyber and Crypto Agency (BSSN) website (honeynet.bssn.go.id), a summary of the cyberattacks report from other countries to Indonesia is shown including the level of cyberattacks in each province, the type of malware that attacks Indonesia in real-time. Those cyberattacks on Indonesia are displayed in graphs based on the number cyberattacks per unit time (Badan Siber dan Sandi Negara., 2018). Cyber incidents or attacks are not always come from a country or from a single source. Although a suspected state may attack directly, when it comes to cyber, in order to remove traces of attack, utilising proxies is often a common choice of tactic. Countries may use proxies that may not necessarily know that they are being used as a launching attack platform and become an innocent proxy. In order to avoid this situation, a country must have the capacity and capability to secure all of their cyber components and

networks so that they may not be used as an attack launching platform for other countries or even an individual.

There are no common definitions for cyber terms they are understood to mean different things by different nations/organizations, despite prevalence in mainstream media and in national and international organizational statements (Torsten Corall, 2018). Nevertheless, no matter how good a country might be in building a cybersecurity ecosystem, in reality, it is almost impossible to maintain cybersecurity alone. Cyberspace is not built by one person, one company or one country but by many contributors and this will continue like it is today in the coming future (Reksoprodjo., 2015). In the 2018 Honeynet Project Annual Report, out of 21 honeypots that were installed it is recorded that the total number of attacks towards the 21 sensors installed is 12,895,554 attacks, with malware being the largest with 513,863 attacks. The 3 (three) largest source of attacks come from Russia (2,597,256), China (1,871,363), and the U.S.A. (1,428,256). The most attacked ports are smbd port (2,071,320), SipSession (1,298,691), and SipCall (1,187,560). The highest malware type attack is Win31/Conficker.worm.167765 (429,208 attacks). (Badan Siber dan Sandi Negara., 2019). The Honeynet Annual Report surely provide significant benefits for many companies in Indonesia especially for the governmental institutions because it give early warning of a potential cyberattacks coming origin and the location of the coming attack.

2. Stakeholders and Policies from the Government

Cyber defense is an effort aimed at overcoming cyber attacks that interfere with normal management. Cyber defenses are prepared to deal with such cyber attacks (Kementerian Pertahanan., 2014) Cyber defense is a computer network defense mechanism that includes a response to actions and critical infrastructure protection and information assurance for organizations, government entities, and other possible networks. Cyber defense focuses on preventing, detecting, and providing timely responses to attacks or threats so that no infrastructure or information is tampered with. With the growth in volume as well as the complexity of cyberattacks, cyber defense is essential for most entities in order to protect sensitive information as well as to safeguard assets. Cyber defense provides the much-needed assurance to run the processes and activities, free from worries about threats. It helps in enhancing the security strategy utilizations and resources most effectively. The cyber defense also helps in improving the effectiveness of the security resources and security expenses, especially in critical locations (Galinec, Možnik, & Guberina, 2017).

Cyber defense in the Ministry of Defense can be a real example of the government's efforts to build a cyber defense posture for the government environment. There are four frameworks developed in building a cyber defense namely; policy, institutional, technology, and human resources. Technology and human resources development are two technical aspects quite interesting to discuss further. Technology/infrastructure that needs to be built-in to support a cyber defense

must include; facility and infrastructure of building/location of the data centre, NOCs, laboratories, and other supporting facilities needed such as; data recovery centre, data network, cyber defense administration application, special technical applications for cyber defense and, exclusive technology (hardware and software supporting specific cyber defense activities).

Human resources will be considered as one of the main asset in cybersecurity that will play crucial roles. To develop a human resource, several things need to be considered such as; the recruitment process for the competencies needed must cover both mentally and scientifically (Kementerian Pertahanan., 2014) Cyber Resilience can be realized by strengthening all cyber defense, cybersecurity, and cyber sovereignty. In a situation of a cyber threat, the National Cyber and Crypto Agency has developed a strategy of three dimensions of defense called safeguard (protection against cybersecurity) (Badan Siber dan Sandi Negara., 2019)

Strategy is all these it is perspective, position, plan, and pattern. Strategy is the bridge between policy or high-order goals on the one hand and tactics or concrete actions on the other. Strategy and tactics together straddle the gap between ends and means. In short, strategy is a term that refers to a complex web of thoughts, ideas, insights, experiences, goals, expertise, memories, perceptions, and expectations that provides general guidance for specific actions in pursuit of particular ends. Strategy is at once the course we chart, the journey we imagine and, at the same time, it is the course we steer, the trip we actually make. Even when we are embarking on a voyage of discovery, with no particular destination in mind, the voyage has a purpose, an outcome, and an end to be kept in view (Nickols, 2016).

To build a strategy for secure cyber environment the user of internet must have the necessary understanding of the means of cybersecurity, social and cultural dynamics, the ethics of internet communication, and cyberspace management. On the other hand, the government must also build for themselves a security systems and good cyber governance by raising the security standards, so that may protect the governmental businesses as well as for the public to feel safe and comfortable in using the internet. Within the governmental services that are all affiliated with the internet, all governmental agencies must improve their information security postures especially institutions that directly affecting the goal of the national cyber defense and resilience.

BSSN took note that the must have technologies to build the information and internet security are as follows: (Badan Siber dan Sandi Negara., 2019)

1. Cryptography and data protection
2. Biometrics and critical public infrastructure
3. Secure programming
4. Wireless network security
5. Access controls and authentication
6. Web and virtual private network
7. Database and security software

8. Security resources and facilities
9. Internet of things
10. Cloud computing
11. Physical security
12. Third-party technology assurance

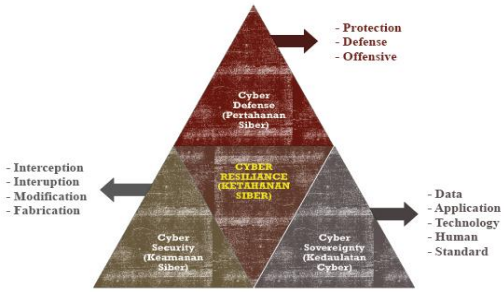

Fig. 1. Cyber Resilience (Badan Siber dan Sandi Negara., 2019)

Cyber defense must include three complementary categories: "proactive, "active," and "regenerative." "Proactive" activities will harden the cyber environment and maintain peak efficiency for cyber-infrastructure and mission functions. "Active" activities will stop or limit the damage of adversary cyber activities in cyber-relevant time. "Reactive" activities will restore effectiveness or efficiency after a successful cyberattack (Galinec et al., 2017). Cyberwarfare refers to the use of digital attacks like computer viruses and hacking by one country to disrupt the vital computer systems of another, intending to create damage, death, and destruction. Future wars will see hackers using computer code to attack an enemy's infrastructure, fighting alongside troops using conventional weapons like guns and missiles. A shadowy world that is still filled with spies, hackers, and top-secret digital weapons projects, cyberwarfare is an increasingly common and dangerous feature of international conflicts. The combination of an ongoing cyberwarfare arms race and a lack of clear rules governing online conflict today means there is a real risk that incidents could rapidly escalate out of control (Ranger, 2018). Most of the sources on cyber warfare that are publicly available do not address the problem of, for example, the cybercrime. The reasoning goes that war is a military problem, whereas a crime is a law enforcement problem; hence these two threats are dealt with by different agencies that rarely speak with one another. This typical approach is not only counterproductive, but it also creates serious information gaps in intelligence gathering and analysis. Besides, cybercrime is the laboratory where the malicious payloads and exploits used in cyber warfare are developed, tested, and refined. The reason why it is such a productive lab environment is that cracking a secure system, whether it is Heartland Payment Systems or the Global Information Grid, is valuable training, and it is happening every day inside the cyberspace underground (Carr, 2010).

3. Analyze Risk Mitigation

Risk mitigation is a strategy to prepare for and lessen the effects of threats faced by a data center. Comparable to risk reduction, risk mitigation takes steps to reduce the negative effects of threats and disasters on business continuity. Threats that might put a business at risk include cyberattacks, weather events, and other causes of physical or virtual damage to a data center. Risk mitigation focuses on the inevitability of some disasters and is used for those situations where a threat cannot be avoided entirely. Rather than planning to avoid risk, mitigation deals with the aftermath of a disaster and the steps that can be taken before the event occurring to reduce adversely, and potentially long-term, effects (Margaret Rouse., 2018). Therefore, the researcher describes the analysis that the researcher has done using 3 risk mitigation indicators.

4. Threat Prevention

In order to cope with incidents of cyber attacks on government bodies, the National Cyber and Crypto Agency (BSSN) compiled standard guidelines for each government agency in the defense sector that administers electronic systems, both at the central and regional levels. Based on the draft of the Indonesian National Cyber and Crypto Agency (BSSN) entiteled "*Instrumen Pengukuran Tingkat Maturitas Penanganan Insiden Keamanan Siber 2019*", the guideline requires each agency to develop the capability of handling cybersecurity by adopting a systematic and structured approach (Badan Siber dan Sandi Negara., 2018).

BSSN focuses on processes, technology and information, preparedness, response, and follow-up activities, all of which will be included in instruments for measuring the handling of cybersecurity incidents. The instrument itself will work as an assessment tool for the maturity of an organization that refers to CREST - CSIR (Cyber Security Incident Response) Guide Ver. 1.0, which includes several questions based on 15 steps in the three stages of the process of handling cybersecurity incidents, namely preparation, response, and follow-up. Through Gov-CSIRT, BSSN coordinates with constituents in dealing with cyber incidents, including looking for possible causes for incidents, provides recommendations for mitigation based on guidelines owned by Gov-CSIRT Indonesia to constituents, and coordinates with other parties concerned to enhance defense. In addition, the Gov-CSIRT service does a number of other things such as cyber incident resolution by conducting an investigation and analysis of the impact of an incident, technical recommendations for post-incident recovery, and providing technical recommendations to correct system weaknesses in an agency.

5. Threat Identification

The National Siber and Sandi Agency (BSSN) has installed Honeynet sensors that are evenly distributed in Indonesia to detect early cyber defense attacks in the future. Currently, Honeynet sensors are spread across six

provinces, with a total of 21 units. Therefore, BSSN will work with Honeynet to increase the number of Honeypot sensors to be evenly available in 34 provinces throughout Indonesia within the next three years. A honeynet is a system designed by Honeynet to trap attackers or hackers. Honeynet will record the attacker's interactions as a source of information to learn the techniques used.

The National Cyber and Crypto Agency Honeynet site uses a honeypot system to detect cyber attacks earlier in Indonesia. This is done in order to anticipate cyber-attacks that are dangerous to the defense. Honeypot (HP) is a system designed to lure attackers. This system has a function and provides the same interaction with the original system so that the attacker does not realize that he has entered a trap. The attacker's interaction with the cell phone will be recorded so that the information can be an essential source of information in learning the techniques used by the attacker. With this early detection system of cyber attacks, the possible losses can be avoided. The Indonesian government is now beginning to realize the protection against cyber attacks. This awareness led the Indonesian government to allocate more funds to ensure the early detection of cyberattacks, primarily to support the cyber defense.

6. Treat Remedy

In dealing with these cyber threats, there are several steps that need to be taken so that they are expected to be able to prevent and minimize the impact of any cyber threats and attacks. In this case, collaborative efforts, coordination, and synergy, as well as information sharing, are the right steps. One form of a collaborative effort, coordination, synergy, and information sharing is through BSSN's relationship as an institution that handles the Indonesian cybersecurity sector, with stakeholders.

According to Joko Setiadi as the Head of Indonesian National Cyber and Crpto Agency the number of cyberattacks in Indonesia in 2018 reached 232,447,974 attacks. Meanwhile, the number of cyber complaints to the BSSN Cyber Contact Center is 619 complaints. From 2018 to 3 May 2019, BSSN has detected as many as 27,700,668 cyber attacks and 514,202 malware attacks (Badan Siber dan Sandi Negara., 2019). Indonesia also did not escape the attacks of advanced persistent threat or apt and cyber threat intelligence or CTI. BSSN has detected several apt attacks on the government sector, the national critical information infrastructure sector, and the digital economy sector in Indonesia. These attacks need to be a concern in increasing national vigilance against cyber threats. This needs to be considered, given the impact that can be detrimental to Indonesia's defense.

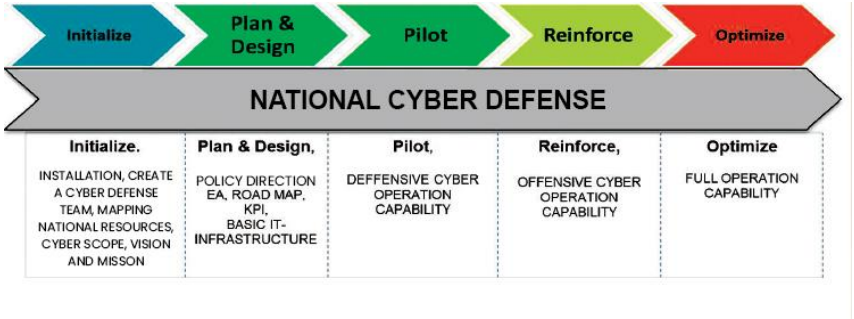

Fig. 2. National Cyber Defense Strategy (Soewardi, 2013)

Risk mitigation is one element of risk management and the organization will be different in its implementation. Risk management as a combination of personnel, policies, processes and technologies that enable an organization to achieve cost-effectively and maintain an acceptable level of loss exposure, a closer look at this definition reveals key take-aways from the responsibility of mature risk professional is not simply to help their organizations manage risk, but to manage it cost-effectively (Paul Proctor, 2019). Organizations compete at many levels, and if an organization is able to manage risk more cost-effectively than its competition, it will win at that level. Achieving an objective indicates that there is an objective. Maintaining a risk objective over time requires the ability to quantify and compare. The adoption of a risk assessment framework, predefined checklists and a set of standard practices is a form of implicit risk management action that will not allow us to achieve a defined acceptable level of risk. Explicit risk management requires the existence of one or more quantitative risk-based objectives.

Conclusion

Current information technology can help to perfect strategy in mitigating cyber defense risk by increasing the ability to identify, evaluate, and monitor risks. It may also strengthening defense in the field of cyberspace by estimating threats with greater accuracy so that stakeholders and the government can determine the best cyber defense policies appropriately and directed in the interests of achieving the national goals.

Indonesia has become one of the targets of cyber-attacks on individuals as well as agencies or companies. Therefore, in addition to creating a safe and comfortable environment for internet users, the government must also build a suitable defense mechanism against a variety of attacks in cyberspace (defense) and the ability to paralyze the technological systems that are actively conducting attacks (offense). Cyber defense systems must be built based on several things such as; the internet network defense, firewalls management, attack analysis, computer and digital forensics, the capability to respond to danger and emergencies, cyber retaliation and deception, cyber law enforcement, and security monitoring and operations.

Cyber defense in the form of a strategic concept must be concrete if all infrastructure networks are held, then the cyber defense policy can be known. To build a reliable cyber defense system, the government and stakeholders must ensure that the cyberinfrastructure is secure. To realize a strong cyber defense, a defense system development strategy is needed that can be started from updating cybersecurity technology to accommodate new cyber threats and mitigating risk holistically to ensure national security.

BIBLIOGRAFI

Aryadi, T. (2018). *Retrieved January 9, 2020, from The Jakarta Post:* Retrieved from https://www.thejakartapost.com/academia/2018/07/13/indonesias-survival-in-age-of-cyber-warfare.html

Badan Siber dan Sandi Negara. (2018). *Retrieved December 27, 2019, from bssn.go.id: https://bssn.go.id/laporan-tahunan-honeynet-project-bssn-ihp-2018/*. Retrieved from //bssn.go.id/laporan-tahunan-honeynet-project-bssn-ihp-2018/

Badan Siber dan Sandi Negara. (2019). *Kewaspadaan Nasional Dalam Menghadapi Ancaman Siber*. Retrieved from https://bssn.go.id/kewaspadaan-nasional-dalam-menghadapi-ancaman-siber/

Carr, J. (2010). *In M. Loukides (Ed.), Inside Cyber Warfare (p. 5). CA: O'Reilly Media.*

CBNC Indonesia. (2019). https://www.cnbcindonesia.com/tech/20190516191935-37-73041/survei-pengguna-internet-di-ri-tembus-17117-juta-jiwa. CBNCIndonesia.*com.* Retrieved from ttps://www.cnbcindonesia.com/tech/20190516191935-37-73041/survei-pengguna-internet-di-ri-tembus-17117-juta-jiwa

Creswell, John W., & Creswell, J. David. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Galinec, Darko, Možnik, Darko, & Guberina, Boris. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika: Časopis Za Automatiku, Mjerenje, Elektroniku, Računarstvo i Komunikacije*, *58*(3), 273–286.

Kementerian Pertahanan. (2014). *(2014, October 17). Kementerian Pertahanan. - Tahun-2014-tentang-Pertahanan-Siber.pdf*. Retrieved from //www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf

Margaret Rouse. (2018). *Retrieved from TechTarget: https://searchdisasterrecovery.techtarget.com/definition/risk-mitigation*. Retrieved from//searchdisasterrecovery

.techtarget.com/definition/risk-mitigation

Nickols, F. (2016). *Strategy: Definitions & Meanings. Stategic Studies, 7.*

Paul Proctor, J. J. (2019). *Risklens. Retrieved January 7, 2020, from https://www.risklens.com/cyber-risk-management*. Retrieved from//www.risklens .com/cyber-risk-management

Ranger, S. (2018). *Cyberwar a guide to the frightening future of online conflict*. Retrieved from //www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

Reksoprodjo. (2015). *Cybersecurity: Emerging Issues, Trends, Technologies and Threats in 2015 and Beyond. RSIS (p. 35).* Singapore: NSCS.

Soewardi, Bagus. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. *Media Informasi Ditjen Pothan Menhan*.

Stroud, F. (2019). *Webopedia*. Retrieved from //www.webopedia.com/TERM/C/cyber-security-threat-mitigation.html

Torsten Corall, K. H. (2018). *The NATO Cooperative Cyber Defence Centre of Excellence*. Retrieved from //ccdcoe.org/uploads/2018/10/NCSS-International-Cooperation.pdf