KnE Social Sciences

ICoSaPS Conference Proceedings
The 3rd International Conference on Social and Political Science
"The Impact of Information Technology on Social and Political Dynamics", (2016), Volume 2017

Knowledge E
Engaging minds

Conference Paper

The Rise of Cyber Diplomacy — ASEAN's Perspective in Cyber Security

Fauzia Gustarina Cempaka Timur

Doctoral Student of International Relations Study Program, Padjajaran University

Abstract

Recent decades have seenhow information technology have shaed global politics tothe extent that defense and security experts claim it to be the beginning of a new era in warfare. Many foreign countries have begun to include cyber threat as a defining factor in international security space, which also concludes the importance of cyber security in foreign policy. In the regional framework, ASEAN has promoted small but meaningful step to ensure cyber security. The paper focuses on the concept of cyber diplomacy in ASEAN and the development of cyber security in Southeast Asia to cope with the present security challenges.

Keywords: ASEAN, cyber diplomacy, cyber security, cyber space

Corresponding Author: Fauzia Gustarina Cempaka Timur; email: fgcempaka@gmail.com

Received: 09 April 2017
Accepted: 17 May 2017
Published: 12 June 2017

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the ICoSaPS Conference Committee.

OPEN ACCESS

1. Background

Vitality of information and communications technology (ICT) has been enhanced vastly by the diversity of entities which make use of it, such as governments, enterprises and individuals. For this reason, there is an urgency to foster international cooperation to ensure the safety of cyberspace as medium of ICT. Although the concept of cyberspace is plastic and argumentative, the United States Department of Defense (DoD) defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." [10]. The cyberspace usually characterized as borderless while the cyberspace infrastructure is under the state's sovereignty. Thus, cyber security is linked to national security and it has become an important element of social politics due to relevance to national security, public safety and foreign polycycle security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of information contained therein [3].

1.1. The Impact of Information and Communication Technology on Diplomacy

ICT is intimately embedded in national or international issues, international relations and diplomacy. Nowadays, ICT has also multiplied the human capability to cause damage or devastation in the social and political aspects of life. Thus, international relations and diplomacy has a challenge to find ways to preserve world peace. As sovereign states try to gain better position in the world compared to another nation, ICT has brought new tools for states to compete without open conflict. The new phase shows that diplomacy serves not only as the art to negotiate and protect one's interest or to promote the influence in international affairs. For every self-governing country, both diplomacy and ICT has grown to be fundamental instruments for managing international relations which projecting the essence of protecting national security and the national power it has.

'Newness' that occurred with diplomacy today has everything to do with the operation of new communication technologies to diplomacy. The changes that happened go right to the core of diplomacy including negotiation, representation function, and communication. The balance between new and old ways of communication is not similar and seems not to implicate that there are revolutionary changes with it. With the influence of governmental networks, in transnational multi-stakeholder environments, and in both friendly and antagonistic relations between states there is greatly significant shifting in the 'offline' side of diplomacy that interconnect with the emerging 'online' diplomacy side.

Despite the impact of ICT on international relations and diplomacy, it is still unclear whether the cyber-sphere perceived as borderless is notas borderless as commonly thought. The sphere itself is the combination of absent virtual borders with existing and distinct legal ones that have allowed cyber-offences to thrive [8]. The specific feature of cyber era is the multinational impactthat could be set by cyber-attacks. The impact it brings emphasizes the necessity for a public policy and common consensus by involving stronger international component. Due to the nature of the cyberspace itself and the asymmetric criteria, the cyber threat signifies a challenge for political leaders, which also obliges a diplomatic effort. Based on that context, it is important for countries to have coordination of legal frameworks on cyber security together with the implementation and operational consensus with another country. The frameworks itself may arise from regional bases.

1.2. Cyber Security in ASEAN: Challenges and Opportunities

At the international level, there is already acknowledgement that cyber threats are one of global security issue as many of the high-scale businesses and administrations are run on cyber space hence the cyber space is very fragile to be destructed by viruses created by hackers. Hand in hand with that argument, North Asia, Europe and North America have recognized the diplomatic opportunity to shape cyber policy elements of international security present through devoting hefty budgets and resources towards it. Cyber-security defined as a complex reality with many dimensions. Responding to the cyber challenge requires a good understanding of this complex issue. According to Joseph Nye, there are four different categories of cyber-attacks, which together make up the pillars of cyber-insecurity (2011). The first is cyber-crime as the most visible of all cyber-threats, and also the most widespread. The second is cyber-espionage which can be used for traditional or industrial espionage. The third is cyber-terrorism with the goal of radicalizing and recruiting new members to pursue the political objectives of terrorist group. Cyber-warfare occurs between states, despite a doubt about the actual form of cyber warfare. Nye also wrote that cyber security is also not an entirely new challenge. Rather, it developed new dimension to current challenges.

Countries in Southeast Asia appear to be unprepared to design cyber security cooperation as a new consequence of gaps in the development of ICT [5]. Therefore, Association of Southeast Asian Nations (ASEAN) should consider necessary action to synchronize the point of view of its members on the importance of such cooperation. Since each member countries are in different phase of their ICT development. Despite the challenges, ASEAN has already put ICT development as vital program of the ASEAN Connectivity. The development of ICT should not only address on strengthening of the network but also the prevention from threats or attacks on that network. The Master Plan on ASEAN Connectivity encompasses physical, institutional, and people-to-people connectivity with ICT as integral part of physical connectivity. The most recent ASEAN master plan released in 2011 is the ASEAN Master Plan which gives more detailed information on how ASEAN wants to develop its ICT sector. ASEAN's vision to build the ICT sector is to create a technologically advance and well-connected region. But ASEAN's development on ICT is lacking in incorporating the security aspect.

Nevertheless, during the development in ASEAN, it has to be realized that it is not the cyber space or the technology *per se* that is good or bad, rather its implementation. With dangerous intentions or irresponsible attitudes there will be no security, development, progress, cooperation and harmony. The future challenge therefore, will be to facilitate best use of technology for all mankind, to allow universal progress, peace and stability, while managing technology interactions and technology advances in a way to prevent its careless misuse or dangerous abuse.

2. Method

This research was conducted using qualitative method. Literature review was used to gain data and information from secondary resources such as books, articles, journals, research reports from prior relevant researches about cyber space, cyber security and diplomacy. Online research was also done to complement data analysis.

3. Finding and Discussion

The rise of cyber diplomacy has brought changes to the mode of foreign affairs in the traditional sense. It calls for a more rigorous mechanism on information collection, risk management as well as daily diplomatic management. In facing such challenges in cyberspace, ASEAN already developed a work plan through ASEAN Regional Forum (ARF). The work plan itself called the 'ARF Work Plan on Security of and in the Use of Information and Communications Technologies, often referred to by its pithier title 'the Work Plan'. The Work Plan was also built by Australian-led efforts by the Department of Foreign Affairs and Trade. As a Forum, the ARF is almost purpose built for negotiating cyber issues and through its practical meeting as emerged as the leading regional body that enables just that. The aim of the Work Plan is to 'promote a peaceful, secure, open and cooperative ICT environment and to prevent conflict and crises by developing trust and confidence between states. Beyond the tagline and jargon, the Work Plan is full of ideas to help prevent ICT-related squabbles from breaking out both for online or offline side of the world. It brings positive notion that the Work Plan also contains plans to quell tensions and re-build trust amongst ARF member states.

ASEAN is yet to have a formal agreement on cyber security beyond the ARF. Even though the necessity of having agreement on cyber security in ASEAN is important; agreeing on an understanding about security in this region is never an easy task. The problem of digital divide or networking advancement gap, among countries of ASEAN is causing different level of concern in each country [9]. From the Table 1 below, we can see that in ASEAN region alone, only Malaysia and Singapore are in the Top 20 Countries Best Prepared against Cyber Attack. The ranking was calculated from the country cyber security commitment and preparedness aspects.

The concept of cyber diplomacy summarizes a series of behaviors and attitudes of the international actors, among which we highlight the availability for dialogue with international partners, the identification of multilateral consultation mechanisms, the acceptance of compromises in order to overcome misunderstandings, the creation of a global culture regarding cyber security, the confidence building between states, the encouragement of transparency in communication, the identification of common advantages offered by cyberspace, the attention for internal vulnerabilities rather than

No.	Country	Percentage
1	United States	0.824
2	Canada	0.794
3	Australia	0.765
4	Malaysia	0.765
5	Oman	0.765
6	New Zealand	0.735
7	Norway	0.735
8	Brazil	0.706
9	Estonia	0.706
10	Germany	0.706
11	India	0.706
12	Japan	0.706
13	Republic of Korea	0.706
14	United Kingdom	0.706
15	Austria	0.676
16	Hungary	0.676
17	Israel	0.676
18	Netherlands	0.676
19	Singapore	0.676
20	Latvia	0.647

Table 1: Top 20 countries best prepared against cyber attack around the world. Source: ABI research, 2014.

external threats and the awareness of stakeholders about the cyber risks, threats and vulnerabilities [2]. Cyber diplomacy is also defined roughly as the effort to push governments around the world to work together to shape cyberspace policy. The goals should be to protect national interests and enhance the security of Internet users, thus there is need for continued cyber diplomacy between countries in ASEAN. Cyber Diplomacy has strong international implications that require each of ASEAN country's commitment and collaboration. Therefore, the diplomatic activity in the cyber domain has an important dimension of cooperation, of concluding diplomatic engagements and multi-level agreements, including with the private sector stakeholders.

The implementation of cyber diplomacy also should recognize the role of social political aspects together with its technical aspects. Some of the social political aspects that need to be recognized are the existence of diverse entities and values in cyberspace, and what should be implemented to maximize its benefit [4]. Common global understanding needs to be fostered while appreciating diversity. Issues pertaining to cyber diplomacy vary widely across a broad spectrum, from socio-economic to national security, and from the easily resolved to the more difficult. There is also an infinite variety of entities that can take part and degrees to which a common

understanding can be fostered. Therefore, a common understanding needs to be fostered incrementally, wherever feasible, while appreciating the diverse values. Through the use of cyber diplomacy, all platforms will be utilized in promoting this approach, including bilateral, multilateral and regional frameworks such as ASEAN.

4. Conclusion

Diplomacy as a major instrument between states in the world is facing a new phase. The new phase shows that diplomacy is not only the art to negotiate and protect one's interest or to promote the influence in international affairs. Cyber diplomacy has strong international implications that require international commitment and collaboration and along with appropriate defense capabilities, cyber diplomacy development and diplomatic strategies designed to outline the present security environment. Cyber diplomacy is also fundamental for confidence building measures between countries in a region.

In a region like Southeast Asia, ASEAN as a regional organization must serve as a platform that enable the member countries to be prepared for any security threats that challenge the region as the security issues evolve from time to time. To complete strategies to face the conventional security threat like border dispute should still be the headline. Even though ASEAN readiness to face contemporary security issue is still questionable, ASEAN still manage to have blueprints and master plans for the realization of ASEAN Community to ensure its path in the beyond 2015. These programs will embrace the needs of future generation. In the case of cyber security, unfortunately the designed documents that supposed to be related to issue like ASEAN Political Security Blueprint, Master Plan on ASEAN Connectivity and ASEAN ICT Master Plan 2015 have not point out significant idea on how ASEAN cyber security will be defined and maintained.

It can be concluded that the development of cyber diplomacy in ASEAN is going very slow. In previous documents of ARF, ASEAN has noted the significance of cyberspace issue. That can be found in ARF discussion since 2004 when ARF Seminar on Cyber Terrorism was held in South Korea. During the years and not until the meeting in 2006 13th ARF Meeting, it released the Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space. Although the statement is not as comprehensive as the Council of Europe's Convention on Cybercrime, the statement already sent a strong message about the agreement among ARF's member states to combat the terrorism including types of terrorism using cyber space as its way for committing their act.

Finally, there are three points worth to be taken from ASEAN cyber diplomacy today. Firstly, ASEAN must stand on the same basic understanding on outlining and treating

the issue of cyber security and cyber threats in Southeast Asia. Secondly, ASEAN member countries must be willing to put the issue of cyber security as their priority area, and by doing so, the policy made in the regional level will be easier to implement in national level. Thirdly, cooperation in technical level must be taken seriously because networking security will need to run smoothly if every party has the same technical capability.

References

[1] Allied Business Intelligence (ABI) Research. 2015. Global Cybersecurity Index. https://www.abiresearch.com/whitepapers/Global-Cybersecurity-Index/. Retrieved October 30, 2016.

[2] Danca, Dana. 2015. Cyber Diplomacy — A New Component of Foreign Policy. Journal of Law and Administrative Sciences, Issue 3, July 2013, pp. 93–97.

[3] Heinl, Caitríona H., 2013. Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime. Singapore: S. Rajaratnam School of International Studies Working Paper, No. 263.

[4] Japan Information Security Policy Council. 2013. International Strategy on Cyber security Cooperation: Japan Initiative for Cyber security.

[5] Khanisa. 2013. A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. Journal of ASEAN Studies, Vol. 1, Issue 1, July 2013, pp. 41-53.

[6] Mallik, Amitav. 2016. Role of Technology in International Affairs. New Delhi: Pentagon Press.

[7] Nye, Joseph. 2011. The Future of Power. New York: Public Affairs.

[8] Renard, Thomas. 2014. The Rise of Cyber Diplomacy: The EU, its strategic partners and cybersecurity. European Strategic Partnership Observatory Working Paper, Issue 7, June 2014, pp. 7-25.

[9] Setyawan, David P. 2016. Indonesia Defense Diplomacy in Achieving Cybersecurity Through ASEAN Regional Forum on Cyber Security Initiatives. Jurnal Penelitian Politik. Vol. 13. No. 1. June 2016. pp. 1–20.

[10] United States Joint Doctrine Division Joint Publication 1-02, DoD Dictionary of Military Terms, Washington D.C.: Joint Staff, J-7, October 17, 2008.