International Norms for Cybersecurity: The Challenging Issues as to Keep Stability and Security in Cyberspace

Giao Dinh

CYSE 495: Cyber War

Dr. Karahan

April 23, 2021

In research from Finnemore and Hollis (2016), they stated that the international cyberspace norm is not clear and become the focal point of serious conflicts. According to Carnegie Endowment for International Peace (n.d.), cybersecurity is one of the top-level rising issues with the "growing number of international accords focusing on rules of the road for cyberspace" (para. 1). As people invent and create more smart and lasting things increases, the number of demands for technology also increases. Besides, most of all work done also needs some help from technologies. People log into their accounts, searching for information, work through the Internet, and other activities like hacking, breaching, attacking in cyberspace. Even though there is international law on cybersecurity, the number of cyber threats or attacks is still increasing, staying continuing, and becoming a worldwide challenge as trying to keep stability and security in cyberspace (Ruhl et al., 2020).

The international norms of cybersecurity are also affecting the development of cyber norms in 2020 as the expanding opportunities for cybercrimes. The hitting of pandemic disease, in 2020, also has led to a trend of cyberattacks over the world. It also caused a huge impact on human life during the covid-19 crisis. The trending of cyberattacks could also speed up the process for a new age of international norms on cybersecurity or could slow down the process development of a nation. Therefore, the international norms of cybersecurity are very essential to maintain cyberspace stability and security. Besides, people also need to understand the international discussion of cybersecurity norms and the behavior of cyberspace. Furthermore, people also need to be understanding of the norm processing and the proposal of new cybersecurity norms.

Maintaining stability and security in cyberspace could not be done just by simple works or few sentences. The culture of cybersecurity is not the same as in another field. In research from Internet Governance Forum (2018), each individual's action on the Internet, cyberspace, should be

aware of the relevance of cyber risks. Besides, the article also stated every action made by an individual should make the Internet secure and safer. There is much more stress for participants from building trust and tackling cybercrime as they try to address issues made by cybercrimes. Meanwhile, there is much more effort and work that needs to be done such as on the introduction of security elements in the process of developing highlighted products and services of cybers. The article also mentioned the defining work on "organizational culture" of Sociologist Schwartz and Davis in 1981. It is about how the beliefs and expectations produced on norms that are shared by a group or members could influence and shape the behavior of individuals but also groups. Moreover, the governments' roles are very essential to the international norms from keeping cyberspace safe, especially for a healthy cyber ecosystem.

While mentioning how organizational culture impacts the norms and the efforts made by individuals and groups, the roles of governments' play in the international norm is very important, especially in cyberspace, so what roles do the governments play in cyberspace? According to the research from McKay et al. (2015), "the relationship of governments with the Internet is complex, making their efforts to develop cybersecurity norms even more of a challenge" (p. 4). They engage in activities of cyberspace and various roles. At the same time, they can be the users of information and communication technology (ICT) and data, the protectors of the Internet itself, the exploiters of ICT and data, and even the monitors (creators) of laws and policies in cyberspace. While struggling with these various roles, the governments also need to work together with the individual sectors (private sectors) and public sectors to solving the current problem and pursuing long-term participation in maintaining trust to the international security, for the national security, to the public safety and economies, and the trust in the global interconnected system (McKay et al., 2015).

There are some limits on state activities in cyberspace according to international norms. Due to the great opportunities of serious threats on both states and non-states, the behaviors are affected on "the use of information and communication technologies (ICTs)" has to be limited as a way to reduce or prevent any conflicts, which international peace and security can be in danger (Osula & Rõigas, 2016). Furthermore, innovation is also endangered as the rising of international insecurity and the increasing pressure on regulation. These concerns remain over and over; however, the primary discussion is focused on restraining state activities on the international cyber norms of behavior to regulate state activities in cyberspace. One is "carry a legally binding obligation" and the other is "act as points of reference for expected behavior but not subject to legal enforcement mechanisms" (Osula & Rõigas, 2016).

As mentioned about the limiting of state activities above, many states are stressing so much to maintaining and developing capabilities as to be able to defend and offend the adversary, enforce the criminal law, and reduce any other risks (Microsoft, 2013). According to the research from Microsoft (2013), the current themes in the norm discussion are the following as avoiding conflict; managing threats and vulnerabilities; building trust and transparency; sharing threat and vulnerability information and coordinating among nations; and the cybersecurity capacity-building. The article also stated five principles underlie international discussions on the cybersecurity norms: harmonization; risk reduction; transparency; collaboration; and proportionality.

Harmonization of laws and standards could be understood in an easy way as the process or action of producing combinations of the laws and standards. This helps to create a more secure Internet. The governments are well able to "contribute technical expertise and political support for creating approaches to international cybersecurity"; however, not all national requirements are the

same and the default requirements are also opposite (Microsoft, 2013, p. 8). Meanwhile, the article stated the process of development of information and communications technology (ICT) will disrupt or slow down but also hinder innovation both domestically and internationally. The key role that plays in this principle is international standards (such as ISO 27034). For instance, "when governments choose to base their software assurance and supply chain policies on international standards" with the well-known best practices throughout the world and global, this could create more flexibility for vendors and suppliers but also increase the chance for more available solutions (p.8).

The next principle is the risk reduction on which and what the governments work on as trying to reduce the geopolitical risks. This principle is neither new nor a well-developing concept under both international law and public policy; however, the risks are still needed to manage on the global level when addressing the risk reduction in cyberspace. The governments and the ICT industry could improve the security on the Internet by "sharing information about threats and vulnerabilities, and by engaging in the active prevention of cybercrime" (Microsoft, 2013, p. 9).

The third principle is transparency which the governments work on their cybersecurity practices with greater transparency to "build trust and increase predictability and stability in cyberspace" (p. 9). However, this principle depends on several factors. For instance, Microsoft has released a paper on "promoting the development of a national cybersecurity strategy" which articulates the priorities, principles, but also ways to approach management in cyberspace to the level risk of national (p. 9).

The next principle is the collaboration in which the need of "given the shared ownership, management, and control of the Internet," and the main point of this principle is by itself to help to develop in any norm, making any law or any public policy, and executing any treaty (p. 10). Even

though working with others is not always an easy step for a long-term collaboration, the more efforts the governments and participants put on the more secure cyberspace can be.

The fifth principle was referring to an existing principle in international law which policies and responses have to be proportional concerning the need for self-defense in cyberspace. According to the research from Microsoft (2013), "nations should begin to develop interpretations of proportionality in cyberspace under customary international law" even though this principle has not yet stated clearly in cyberspace on how much proportionality will be interpreted (p. 10).

These five principles that could underline the international discussions on cyberspaces as mentioned above could be very necessary to keep in mind when governments discuss the rising level of cybersecurity issues from any activities made by the normative behaviors.

Moving back to the behavior in cyberspace, there are three specific types of norms that need to be evaluated. In the offensive norms, the actors are mainly national-states, primarily militaries, and intelligence agencies. The objectives of offensive norms are trying to reduce conflict between states, lower the risk of escalation from the offensive operation, and prevent consequences that are not acceptable. The action that takes in this norm is to exercise self-restraint in the conduct of the offensive operation. The governments use this norm to mitigate unacceptable influences of information and communications technology (ICT). In the defensive norms, the actors are the public and private sector (individual sector) in cyber-defense teams, whose objectives are to manage cybersecurity risk through the enhanced defense and incident response. The actions needed are the collaboration among defenders, which help to protect the government, infrastructures, enterprises, consumers, users of information and communication technology (ICT). The actors of industry norms are the international ICT companies, which try to deliver secure products and services. To do that, they need to be supporting defense and refraining from the

offense. The impacts of the industry norms are protecting the ICT but also enhancing trust in technology.

After evaluating the three specific types of norms as offensives, defensives, and industry norms, people also need to know exactly the background of norms development with the norm processing. In research from Ruhl et al. (2020), there were huge attacks and infects over hundreds of thousands of computer networks in many different countries in 2017, caused more damages up to billions of dollars, not able to access or control the confidential information, and continuing more than five thousand of a data breached in 2019, but these events are continuing and even worse. Based on the article, many stakeholders thought about and shared the idea of what expectations of behavior are appropriate in cyberspace, and this is how the idea of cyber norms begin or be born due to the rising of malicious activities in cyberspace. According to the research of Ruhl et al. (2020), the processing of cyber norm development and spreading those, "various state and nonstate stakeholders have promoted different processes," which including into four different contexts (multilateral, private, industry, and multistakeholder) as following: multilateral norm diplomacy, private norm processes, industry-focused norm processes, and multistakeholder norm processes (pp. 2-3).

However, the articles also talked about some interconnected challenges that participants detected when facing these cyber norms processes above. The first interconnected challenge is the inherent characteristics of the cyber domain, which are affected or disrupted by somehow the development of effective norms because the cyber domains change constantly by themselves. Another challenge is the lacking transparency about the state behavior as to how dealing with which "cyber norm proposals actually constitute existing cyber norms" to some kind of secrecy cyber activities of states (Ruhl et al., 2020, p. 16). The next interconnected challenges are the

absence of great power cooperation on the differentiate how power split up based on the different positions on specific norms. The last challenge is about the lack of incentives to the internalizing norms, which states need to "perceive the prospective benefits of adherence as outweighing the prospective benefits of remaining outside of normative constraints" (p. 16).

The new cybersecurity norms as mentioned in the second paragraph above are about the four centrals of cybersecurity norms pervading through the public and individual sectors (Usi, 2020). These four central cybersecurity norms are responsibility, restraint, requirement to act, and respect to human rights which has been concluded by the Global Commission on the Stability of Cyberspace (GCSC) are critical to ensure stability in cyberspace. For the first central, everyone must be responsible for maintaining stability in cyberspace. For the second central, there is neither state nor non-state actors should take any actions to impair stability in cyberspace. For the third central, every step the state or non-state actors take must be reasonable and appropriate for keeping cyberspace stability. For the fourth central, all the efforts to maintain stability in cyberspace need to respect human rights but also to the rule of law.

As the title of this paper is about the international norms for cybersecurity on how hard and challenging it is as dealing with cybersecurity issues to the needs of maintaining stability and security in cyberspace. While trying to explain what made cybersecurity seem difficult, the paper also needs to give some explanations from the current issues to the process issues had been working on, to the international discussion of cybersecurity norms but also not forgetting to introduce the new cybersecurity norms with a reminder of retelling the background of norms development.

Understanding how difficult it is to keep cyberspace stable and secure, the governments and participants need to put in a lot of hard work and effort to achieve that. The governments take responsibility and engage in many different roles in cyberspace activities. Besides, there are some

strictly limiting on the state activities that make more stress to ensure the capabilities to be able to defend and offend. Meanwhile, the five principles that influence international discussions of cybersecurity norms can be helpful as trying to help governments on how to be dealing with the increasing level of cybersecurity issues to the malicious behaviors in cyberspace. By evaluating each behavior, people can understand how each different type of norm works. While trying to know how hard it is to keep cyberspace, people can get to know about the idea of "cyber norms" beginning or being born. Furthermore, the background of cyber norms can help to explain how the development of the norms has been spread with some challenges that occur during the norm processing.

As introducing the new age with new types of cybersecurity norms, these four central cybersecurity norms are much different from other cybersecurity norms mentioned before because these four centrals of cybersecurity norms also focus on human responsibility and human rights with the rule of law. This new age of cybersecurity norms could contribute to the change of cyberspace in positive ways as ensuring security for all participants but also keep cyberspace stability.

References

Carnegie Endowment for International Peace. (n.d.). *Comparing Cybersecurity Norms*. https://carnegieendowment.org/publications/interactive/cybernorms#timeline-section

Finnemore, M., & Hollis, D. B. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, *110*(3), 425–479. http://www.jstor.org/stable/10.5305/amerjintelaw.110.3.0425

Internet Governance Forum. (2018). *Cybersecurity Culture, Norms and Values*. https://www.intgovforum.org/multilingual/es/system/files/filedepot/13/igf_2018_-_bpf_on_cybersecurity_background_paper_-_culture_norms_and_values_0.pdf

McKay, A., Neutze, J., Nicholas, P., & Sullivan, K. (2015, January 23). *International Cybersecurity Norms: Reducing Conflict in Internet-Dependent World*. Microsoft. https://www.microsoft.com/en-us/download/details.aspx?id=45031

Microsoft. (2013). *5 Principles for Shaping Cybersecurity Norms*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc9

Osula, A., & Rõigas, H. (2016). *International Cyber Norms: Legal, Policy & Industry Perspectives* [E-book]. NATO CCD COE. https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf

Ruhl, C., Hollis, D., Hoffman, W., & Maurer, T. (2020, February 26). *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*. Carnegie Endowment for International Peace.

https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110

Usi, G. (2020, October 7). *Understanding the New Cybersecurity Norms & Why They Matter*. Omnistruct Inc. https://omnistruct.com/understanding-the-new-cybersecurity-norms-why-they-matter/