

CHAPTER II

GLOBALIZATION AND THE DEVELOPMENT OF CYBERSECURITY ISSUES

It is admitted that International relations is traditionally recognized as a field of study that focuses in analyzing the interactions and behavior of many actors which is usually represented by State as well as MNCs, NGOs and even people in general. These actors are examined by their interactions between one another in particular issues either in term of good engagement such as cooperation or even in conflictual relations.

The issues arising in International relations studies are very wide in range which become the consequences of world's dynamic development in terms of economics, politics, environmental and even technology. The tendency of International relations scholars has been shifting not only focusing on analyzing traditional issues such as conventional border security issues, war and peace, and state politics in general but also contemporary issues like gender, environment and even globalization.

Globalization in specific is often linked as an overlapping phenomenon whose effects are significantly influencing the way world runs today in many aspects of statehood lives including politics, economy and social-cultural. Hence, based on the overview that writer has given above, the following discussion within this chapter will be focusing on explaining globalization in deep as well as any aspects relevant to the topic of this undergraduate thesis including globalization in term of its reciprocal influence in technology advancement such

as internet and cyberspace. Furthermore, the writer will also provide the other variable of this chapter that relates to the issue of cybersecurity especially its importance and significance in term of its development as well as its ability to influence state in creating policies to respond at the relatable cybersecurity phenomenon at the moment..

A. Understanding Globalization: Past and Present

Globalization as a phenomenon is recognized as one of the most complex contemporary issues that provide new perspective in analyzing international relations study. Globalization itself has many definitions following the fact that it embraces concept and theories not only within the study of political science but also sociology, anthropology and even economy (Wild and Wild, 2016).

In general, globalization can be defined as a trend toward greater economic, cultural, political, and technological interdependence among national institutions and economies. It is also characterized by the fewer irrelevancies of conventional national border which consequently lead to the freer flow of goods, services, capitals, people and ideas across the globe (Wild and Wild, 2016).

On the other hand, according to McGrew (1990) in Reich (1998), a notable professor of International relations from University of Southampton stated that globalization constitutes as:

“Multiplicity of linkages and interconnections that transcends the nation states (and by implication the societies) make up the modern world system. It defines a process through which

events, decisions and activities in one part of the world can come to have a significant consequence for individuals and communities in quite distant parts of the globe (McGrew, 1990, as cited in Reich, 1998)."

Therefore, to sum up two definitions above, in simple words globalization is basically a phenomenon which is illustrated as the increasing trend of interconnectedness in many aspects of world such as economy, politics and many more aided by the advancement and the utilization over technology consequently create a world that is borderless and more integrated where an event that happens in a particular area can significantly influence people and communities in another place.

Furthermore, tracing back the history, although there is no concrete agreement about when exactly the term of globalization has been coined, the idea of globalization can be found even several decades ago. Many scholars have agreed upon a statement that since globalization marked by the existence of lower trade barrier of trade and investment (Wild and Wild, 2016). The year of 1940s is the very focal point that pushes the globalization to be widespread since those years particularly 1944 were marked by the Bretton woods meeting by political leaders of several states which largely initiated by Britain and United States along with other forty-four nations (Ikenberry, 1993). This fruitful meeting was successfully held and produced several output including the establishment of International Bank for Reconstruction and Development known as World Bank and General Agreement of Tariff and Trade or GATT that later known as World Trade Organization.

The following years, the notion to promote the removal of trade and investment barriers is highly echoed by many countries around the world especially states that disagree with protectionism-economy which being claimed to be the reason of slower economy growth (Ferrini, 2012). Thus, the falling barriers of trade and investment are bringing both challenges and opportunities, for example, in one hand, the falling barrier of trade and investment is simultaneously influencing the competition of states in term of trade which brings certain challenges for the domestic economy of many states, including in term of the emergence of competitor of local products. While in the other hand, it is also able to provide citizens of home countries varied choices of products with relatively reduced prices. In general, the freer trade also helps the home state-countries to bring certain products that are more beneficially efficient to be imported rather than produced alone by the state itself (Ferrini, 2012).

Meanwhile in the present time, globalization has pretty wider scope. It is due the fact that as the time goes by, the advancement of technology has key important role in becoming the factor for the widespread of globalization. Technological innovation in this extent has facilitating the movement of data in easier, faster and less costly way (Wild and Wild, 2016).

Furthermore, this technological aspect is also important for measuring so-called globalization index, an inquiry which performed by researchers in order to measure the extent of globalization by giving rank to the observed states using several measurement aspects as organized below:

Table 2.1
Measurement Categories and Variables that are used in Measuring the Globalization Index

No.	Measurement Categories	Example of Variables
1.	Economic Integration	trade, foreign direct investment, portfolio capital flows, and investment income
2.	Personal contact	international travel and tourism, international telephone traffic, remittances, and personal transfers (including compensation to employees)
3.	Technological connectivity	internet users, internet hosts, and secure servers
4.	Political engagement	Memberships in international organizations, personnel and financial contributions to U.N. Security Council missions, international treaties ratified, and governmental transfers

Retrieved From (Wild and Wild, 2016, p. 36)

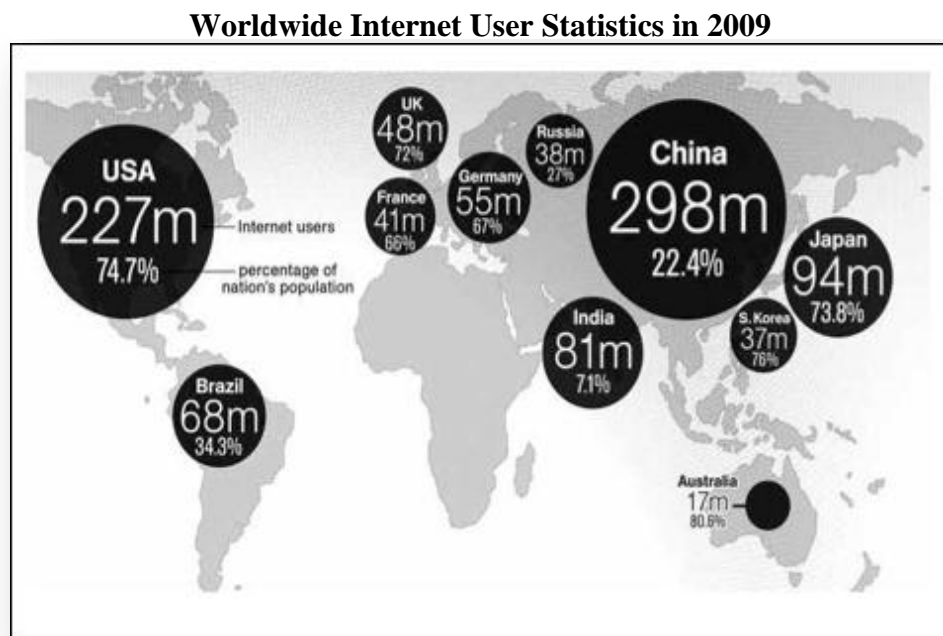
Hence, based on table above we can see how basically technological connectivity is as important as other elements in measuring the globalization index especially in present time where the phenomenon of globalization is hugely influenced by many technological advancements. Among them are included the invention of e-mail, videoconference and most importantly the internet and World Wide Web or abbreviated as WWW.

Specifically, internet according to Oxford Dictionaries can be defined as a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols (Oxford, 2016). As the time goes by,

internet in fact, is the fastest growing information mechanism in human history compared to earlier innovation such as radio, television and personal computer (Choucri, 2012, p. 52)

The figure below is illustrating the statistic data of worldwide internet user based on States in the top rank in the proportion of the number of internet user as well as its percentage out of total population per country in the year of 2009.

Figure 2.1.



Retrieved from (Choucri, 2012, p. 52)

From the figure as illustrated above, it can be understood that the biggest percentage of internet user belongs to Australia where around 80.6 % which is around 17 million of citizens out of 21.69 million populations are having connection to the internet. Meanwhile, the biggest number of population that are connected to internet belong to China where around 298 million people connected to the internet. However, the percentage is only

about 22.4% due to the fact that the population of China at the moment is already on the number 1.3 billion people. In the average, there are South Korea, USA, Japan and UK who are having 70% above in percentage and in the lower rank are Germany, France, Brazil, Russia, China and India where the percentage are 67% and below.

Therefore, from the data above the percentage of internet user out of total population is considered important in measuring the globalization index because it is one of the variables that can illustrate how advance is a particular state in term of its connectivity to the internet because internet in this extent also plays a key role to connect people individually and even government in a statehood level to the cyberspace.

In one hand, within the individual level, people can easily get a cyber access because of the facts that the mobile technology utilization is getting more advanced day by day. Mobile technology is referring to the use of cellular communication commonly perceived as cell phone. The growth of the mobile users in term of number is consequently leading to the increase of people's involvement in cyberspace both in developed and developing world which its simplest form is the access over social media like facebook, twitter and many more (Choucri, 2012).

Meanwhile, in the statehood level, many researchers argued that state is the major organizing device that needs to balance the exploration of the real kinetic world such as in the matter of state engagement with other states in a conventional way as well as in term of cyber features within the international

relations itself (Choucri, 2012, p. 91). Furthermore, in this twenty-first century realm, there is a fact that there is growth of the utilization over cyber venue in term of government service which is usually recognized as e-governance. UNESCO defines the term E-governance as below:

“Governance refers to the exercise of political, economic and administrative authority in the management of a country’s affairs, including citizens’ articulation of their interests and exercise of their legal rights and obligations. E-Governance may be understood as the performance of this governance via the electronic medium in order to facilitate an efficient, speedy and transparent process of disseminating information to the public, and other agencies, and for performing government administration activities (Grievances, 2008).”

Thus, it can be concluded that the notion of technology is a key feature that enables government to move forward in managing its statehood lives ranging from the process of computerization within the government office until the government connectedness to the network that enables government itself to share data between government entities as well as in the activities of maintaining its interactivity with its citizens and even government of the other states which is also being perceived as cyberpolitics (Grievances, 2008).

Nevertheless, the existence of cyberspace and state involvement in cyberpolitics is in fact involving a complex and dynamic development as these many types of actors were having different capabilities and intentions in their own objectives (Choucri, 2012, p. 125). As a result, it is admitted that particular states is not only focusing on how to lift up their own capability and maximize the utilization of the cyberspace but also even seek to do

surveillance and control over their opposition non-allied groups or states using the cyberspace itself (Choucri, 2012).

Therefore, the fact that cyberspace is a space with relatively undefined borders, the increasing involvement of state, for example the one performed by political elites through sending email and links to discuss political matters is providing opportunities for particular actors with biased intention to threaten not only personal lives but also state government. These challenges obviously bring influence towards state security in general especially in this realm of twenty-first century where cyberspace is considered the new battlefield of the non-traditional security issues (Choucri, 2012).

B. The Development of Cybersecurity Issues

The experience of being in numerous war and conflicts had been hugely influencing our live until today especially within the aspects of International relations study. Numerous armed conflicts that happened from the ancient to the present one have been leaving the society the negative image of state relations that seemed to be quite conflictual and put the security of state and citizens in risk (Heurlin and Kristensen, 2002). Since then, security has been a major discussion in International relations study where many schools of thoughts have their own specific way in defining this term.

As described by oxford dictionary, security can be defined as the state of being free from danger or threat (Oxford, 2016). Conventionally, our way of thinking about national security in specific usually refers to the military term such as security of national borders and also the ability of a country to

defend itself against military attack. However, in this twenty-first century, many scholars have argued that there is a need to reconsider the traditional concept of security itself (Choucri, 2012). It is due to the fact that nowadays, the coming of globalization and the advancement of technology has brought the new realm on the security issues especially due to the shifting trend of government in managing its statehood living by utilizing the cyberspace.

Thus, there is an emergence of a term called as cybersecurity that can be defined as a set of activities and other measures intended to protect a country from attack, disruption, or other threats of computer networks, related hardware and devices software and the information they contained and communicate including software and data as well as other elements of cyberspace (Fischer, 2016).

Therefore, in order to examine the development of cybersecurity in world so far, the fact that cybersecurity is developing side by side as the technology cannot be neglected and any aspect attached to it is also developed. As the very first generation of computer called ENIAC was designed in 1946 by John William Mauchly, the following decades were seemed to be filled with much advancement in the computer world which was very dynamic until its peak in 1975 where personal computer with smaller physical features is getting more common in the society for example Altair 8800 and the earliest generation of Apple introduced by Steve Jobs (Symantec, 2006).

Moreover, the existence of falling price in this computer commodity was consequently leading to the fact that there was an increasing number in the usage of personal computers in the society (Gercke, 2012). However, more people that were connected having more risk because of threat that might be addressed towards those people or also known as with the term cyberthreat. Cyberthreat itself is a term that describes how certain actors exhibiting the strategic behavior and capability in order to exploit cyberspace purposely to harm life, information, operations, the environment and/or property of others (Robinson et al, 2013 p.5).

At the beginning of the development, the threat that used to be potentially harmed the stored data in computer was coming from physical damage of the computer itself instead of in form of cyberattack as we found the following decades after 1960s. The example of the case happened in Canada when a riot of student was causing fire in a school in 1969 and destroyed computer data-storage of the university (Gercke, 2012). Thus, the security during this period was seemed to be relied on concrete security guard instead of being protected by certain program of software as nowadays being attempted by many states.

However, many inventions in technology in computer aspect were adding the complexity of the security system as well as threat that potentially gives risk over it. The decade of 1970s is the focal point where the beginning of computer fraud was coming into the surface as the estimated number of computer usage in U.S. was reaching 100,000 numbers and thus marked the

shifting trend of crime in the 1960 that identically called as traditional property crime against physical damage. However in 1970s the crime was more to the act of manipulation over electronic data and illegal use of computer. This new trend of crime has pushed many governments with high usage of computers to respond by creating legal act just like what had been done by U.S. government that discussed draft bill to address this kind of new emerging cyber crime (Gercke, 2012).

Further during 1980s, these decades were marked by the dynamic development on computer software which enabled new kind of crime in form of patent-related crime and software piracy. During this era the malicious software began to spread and many computers viruses were revealed. Thus, in order to manage and face this new development, many states were trying to enhance their legislation as legal responses towards those new crimes. In this era, several international organizations have also started to give focus on this cyber-issue especially on how to analyze related phenomena and possibility to respond toward any case in the future where OECD and European Union were among the noted international organizations back then (Gercke, 2012).

As more and more new technologies were being invented, the decade of 1990s was quite a focal point in the cybersecurity issues since the discovery of World Wide Web or WWW pushed the increasing number of internet utilization. Any kinds of information were easily published and being exchanged by different people in different parts of the world in relatively short time enabling cyber crimes to become such transnational phenomena.

The concrete example of crimes during this era was pornography. Thus, in order to ensure the cybersecurity during this period, there were so many attempts done by states in the world including the discussion in UN general assembly that produced a resolution called 45/121 that was adopted in 1990 mainly talking about prevention and control over computer-crime related issues (Gercke, 2012).

The following decades by the beginning of twenty-first century realm were marked with more and more complicated kind of technology, so did the crimes. Phishing was one of the examples which can be described as an activity of illegal practice by sending email pretending from a reputable company purposely to push an individual to reveal personal information such as passwords and other confidential (Cambridge, 2017).

Until now, where the twenty-first century has passed by bygone years, the complexity of cyber crimes are getting more intense in scale and practice. New crime is also emerging for example like hacking. It is an activity performed by hacker who illegally gains access and sometimes intervene information within the system for personal benefits (Merriam-Webster, 2017).

Hence, it is no wonder why many States as well as regional and international organizations are having the urgency to respond towards these growing challenges and put the cybersecurity related issues as top priority as important as the conventional security issues within a statehood live. The reason is mainly because of cybersecurity. If it is not being managed to be

well-secured, there will be so many possibilities of threat or imbalance that will be disturbing citizens' life as many sectors of government such as critical infrastructures are attached and being managed more by computers and networks.

To sum up, globalization as a widely-known phenomenon has given certain contributions towards the development of cybersecurity issues as the development of technology in the earlier and present era is somehow getting more complex and more people and government of states are in fact involved within this circle of cyber world. Along with the benefits that are brought by this technological advancement, the risks are also getting higher and more complex than ever.

As a global citizen, people should somehow start to realize how crucial cyberspace for our daily life is and how basically they are much depending on it. A secure internet as a platform to connect ourselves within the cyberspace needs to be prioritized by any domestic government in such globalized era as it is not only the benefit that could be trans-nationally transferred from one state to another and so does the threat. People should start to imagine how miserable it would be if for example one of our daily life infrastructure such as electricity or transportation that managed by cyberspace and computer networks is interrupted by irresponsible party. Surely, it must be really disadvantage for any common citizens and the pride of state is put in a risk.

Thus, it is no wonder that cybersecurity is categorized as a contemporary emerging phenomenon of non-traditional security issues including in International relations studies. The involvement from many actors in International relations

ranging from state to non-state actor in fact merely has purpose to create a harmony of responses which considered urgently needed to overcome the potential problem in cybersecurity issues either in domestic or international level. Cooperation and support from citizens as well as private corporations are also very crucial to determine the success of attempt in assuring the cybersecurity of a state.

Overall, cybersecurity in today's era has been marked as a new trend in International relations because of critical features it has. Thus, if it is not well-assured, the catastrophes shall happen and disturb state affairs domestically and internationally. That is why many states from developing to developed one are now starting to aware and pay their attention to this issue. European countries such as United Kingdom to Asian countries such as China and even Middle East and the American continent countries like United States of America are starting to focus on cybersecurity issues not only domestically but also playing active role in supranational level.