Forum: General Assembly 1

Issue: The question of cyber security and protection against cyber warfare

Student Officer: Daniel Park

Position: Head Chair of First Committee

Introduction

The development of technology is extending to its maximum; its presence improves the quality of lives of humanity. Even, military reliance on information and computer technologies (ICTs) is indefinitely increasing to the point of introducing a “fifth” domain of war-fighting besides the formerly known land, sea, air and outer space. However, recent year’s technological innovations had been operated for indiscriminate surveillance causing political disputes between nations, as means of conducted cyber-attacks. The purposes disrupt the maintaining of international stability and security. Victims are continuously becoming more vulnerable due to the increasing access to technologies and Internet. Yet, the international society has no clear solutions, instead raises questions such as, to what extent can existing international law be transposed to the cyber domain.

Cyber warfare potentially includes attempts to access, damage, undermine, and sabotage other nation, organization’s data. In 2007, a catastrophic cyber warfare occurred in the Republic of Estonia. It is believed that the operation was led by the Russian Federation. The attack had malfunctioned over 1 million computers throughout the nation including those of the government, business, and the media. As an aftermath, Estonia was left with a loss estimated to be ten million euros, forming a bilateral political tension between the two nations. Thus, the financial loss recognizes the potential harm cyber warfare can impose. Moreover, in March 2013, the Republic of Korea became a victim to cyber warfare. Its cyberspace had experienced a wave of cyber-attacks including hacking information systems of major broadcasting corporations and banks. This had cost South Korea an estimate of seven hundred million U.S dollars.

Taking into consideration of these incidents of cyber warfare, nations and the United Nation (UN) have responded. These include, forwarding of draft resolutions on different aspects of cyber security to the United Nations General Assembly (UNGA), enforcements to existing cyber security by proposing new legislations. Yet, cyber warfare is still a concern not only to public sectors of nations, but also private sectors of individual companies and organizations. Hence, recommends member states to produce constructive, practical and efficient solutions that potentially enhance cyber security and the protection against cyber warfare.

Definition of Key Terms

Cyber warfare

The action targeted at a specific body by a nation-state or international organization considered as an assault to deliberately damage its information networks.

Cyberspace

The domain of all IT systems characterized by the utilization of interconnected networks to store, modify and exchange data.

Cybersecurity

The body of technologies, procedures, and practices intended to secure networks, computers, programs and data from cyberattacks or unauthorized access.

IP Address

A code made up of numbers separated by three dots assigned to specific devices in a network.

Server

A computer program that coordinates the flow and serving of data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet.

Denial-of-service (DoS) attack

DoS attack is a form of cyber-attack often used by hackers since the mid-1980s. A DoS attack aims primarily at specific sites and networks, rendering the entire site or network unavailable by denying access of users.

International Telecommunication Union (ITU)

The ITU is an international organization that is a part of the UN system in charge of technical and policy matters related to global telecommunications network and service.

Computer Network Operation (CNO)

CNO is a broad military computing concept that incorporates procedures, tools and methodologies to optimize, utilize and retrieve strategic benefits from computer networks. CNO provides private and military organizations with protection, defense and retaliation as response to computer related assaults that originate from enemy network or information system.

North Atlantic Treaty Organization: Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE)

Established on May 14, 2008 it reached the status of International Military Organization on the 28th of October, 2008. Hence, NATO CCDCOE is an authorized research and training facility dealing with consultations, education, research and development of cyber security. Their mission is to enhance the capability and cooperation for sharing information among member nations of NATO and its partners in cyber defence.

Background Information

The history of cyber warfare

1988- Morris Worm

The very first cyber-attack was a virus labeled as the Morris worm, created by Robert Tappan Morris who was a student at the time and now works as a professor at MIT. This virus is recognized as the first ever to affect the world's dawning cyber infrastructure. Professor Morris claimed that his intention of the development of this virus was to gauge how big the Internet was. However, it had targeted computers all over the United States, causing them to slow down to a point where they would be unusable. Its mechanism was to use weaknesses in the UNIX system Noun 1, and replicate itself rapidly to spread at a fast rate.

The Estonian Cyberwar

On April 26, 2007, the small Baltic state of Estonia and its government networks were harassed by a wave of denial-of-service (DoS) attacks coordinated by the Russian Federation. It was also accompanied by riots in the streets; it was a protest against the Estonian government for removing the Bronze Soldier monument, a Soviet war memorial in Tallinn. The cyber-attacks targeted influential government websites, websites of banks, universities, and Estonian newspapers. The Estonian government undertook measures as response, hence successfully relaunching some of the services within hours.

The development of cyber security

Computer Emergency Response Teams (CERTs)

In response to the very first cyber-attack, the Morris worm was the establishment of CERTs at the Carnegie Mellon University under the U.S government contract in 1988. The small organization is the central point for coordinating responses to emergencies and Internet security incidents. Their group now has more than 150 cybersecurity professionals dedicated to improve the security and resilience of computer systems and networks. They partner with government, law enforcement, industry and academia for the development of advanced methodologies and technologies to combat cyber threats. Additionally, the information retrieved from their research and analysis of data gathered from the CERT division also assist in developing applicable solutions that are then available for those in need. Hence, contributes to the efforts of improving software security. Elaborating on their contribution in national and global standards, they previously provided direct aid to the Department of Defense (DoD) through ways such as, projects designed to improve the security networks, increasing global situational awareness from working collaboratively with the Defense Information System Agency.

The Global Cybersecurity Index (GCI)

The Global Cybersecurity Index launched by the United Nations (UN) International Telecommunication Union (ITU) in order to measure the status of cybersecurity worldwide. Furthermore, they inspect the level of commitment each nation in cybersecurity of five main areas: legal, technical and organizational measures, capacity building with national and international cooperation. The GCI partnered with ABI Research aiming to close security gaps in the short-term particularly for developing countries, also in the long-term it intends to drive the efforts in the implementation of cybersecurity on a global scale.

Key Issues

Impact of cyber warfare

Ever since the development of ICTs, for many years the term cyber warfare is brought up with conjuring images of malicious programs. The programs are designed to cause computer systems to stop, weapon systems to fail, etc. Vandalism, propaganda and Denial of service are typical forms of cyber warfare. During elections is when vandalism is most often used. In the nation of Kyrgyzstan, any computer users who relate with any non-government friendly comments or posts are hacked and attacked, corrupting their data within their server. The weaker type of cyber warfare is propaganda. It is not a direct assault or nor does it interrupt the system in any forms, but it manipulates people's responses to satisfy the attackers' intentions and change the opinions and views of people on specific things. The form that cyber warfare takes most commonly is denial of service. Though, these attacks are hard to defend against. Basically, an overload number of requests are created to the server that paralyzes a whole system. In 2013, the NASDAQ trade market had shut down. News had reported that it was from a substantial disruption to their processing system that went on for more than three hours. This had prompted NASDAQ with a $10 million fine, more importantly lack of confidence had emerged influencing the investor sentiment associated with the technical elements of the trading system.

Lack of cyber security

Noting cyber warfare is a developing prominent issue with potential detrimental threats, protection from it is questionable. Sophisticated systems that interconnect through international borders are being increasingly targeted by cyber terrorists such as, criminals, terrorist groups and foreign governments in pursuit to steal secretive data. Governments and international businesses have just woken up to the terrorizations from cyber warfare like such. The establishment of the European Network and Information Security Agency (ENISA) in 2004 was one of the first in EU to enhance European coordination on information security through addressing common risks and vulnerabilities. The EU has also become aware of the potential danger posed by cyber warfare, so International cyber security policies are now distinguishing between cyber threats to national or European security and whether they are threats to the private property or the functioning of the market economy. Among the public and organizations, awareness of cyber threats are still limited and not in state of sufficient implementation.

Cooperation amongst nations and organizations

The process of cooperating with major entities that control electrical grids, transportation systems and telecommunications networks are critical. Researchers considered it as one of the barriers from further refining defense for infrastructures from cyber warfare. Cooperation and communication between government officials and private sectors like the military is essential. The military possesses higher knowledge with superior preparation for response against cyberattacks. Yet, not only are relationships between nations and organizations defective, there are presence of severe lack in partnership amongst developed nations and developing nations. Less economically developed countries (LEDCs) struggle financially, pending reliance on other nations for support. Generally, the more economically developed countries hold information on the most effective measure when combating cyber warfare. Though, such benefits do not exist amongst the LEDCs because of such lack of partnership.

Major Parties Involved and Their Views

United States

The United States of America (USA) is one of few nations that receive the most cyber-attacks. Thus, as a result they are also the most active participant in promoting cybersecurity. In 2009, America's digital infrastructure was described to be a 'strategic national asset' by President Barak Obama. In May 2010, the government had established a new command, named U.S Cyber Command (USCYBERCOM) under the direction of the National Security Agency (NSA). The purpose of this was to organize cyber resources, protect its military networks and also synchronize attacks to other nations' systems. The exposure to cyber warfare of USA's key sectors of both private and public are constantly expressed as its concern. These sectors are such as; public and private facilities, banks, education sectors, transportation and the government. Over the past few decades, the U.S government has relentlessly invested in combating cyber warfare.

In July 2011, a framework for the U.S military strategy for cyber warfare called the Five Pillars has been published. The first pillar is to have recognition of new domain for warfare similar to those in the battlespace. The second pillar is proactive defense opposed to those as passive defense like, computer hygiene or firewalls. These require the usage of sensors to provide active defense with rapid response to detect and annihilate any cyber-attack on a system. The third pillar is critical infrastructure protection (CIP), which is to ensure the protection of critical infrastructure. The fourth pillar is the application of collective defense, which provides the early detection, incorporating them into the cyber warfare defense structure. The fifth pillar is to maintain and enhance the advantages from technological change, additionally improving computer literacy and increasing artificial intelligence.

In April 2015, the U.S Department of Defense (DoD) published its most recent cyber strategy expanding upon the Five Pillars. The cyber strategy concentrates on building capabilities to ensure, secure and defend USA's DoD networks system and information. However, recently being involved in the NSA political controversy, USA has been accused for secret surveillance and spying on a global scale.

The European Union

The European Union perceived cybersecurity as a secondary issue resulting from the growing reliance on ICT. Though, this had changed in the aftermath of major cyber-attacks from terrorist groups in the U.S and E.U. Thus, now the E.U is proactive in ensuring protection from terror like the one on Estonia in 2007 for all E.U citizens and industries, promoting international policy on cybersecurity. The E.U's cybersecurity policies are modelled to balance effective strategies to counter new cyber threats. Their objectives are to protect individual liberties and the capability of informational self-determination and also democracy in general. However, given the E.U's successful cyber security and defense strategies formed from consistent and predictable cooperation between governments and private sectors, their belief in the censorship and mass surveillance on acceptable policies and measures are yet to be confirmed. In 2013, Cyber Security Strategy for the E.U was established, where currently it has been implemented in the governmental policies of 18 member nations of the E.U. The Cyber Security Strategy outlines the following priorities:

- Achieving cyber resilience
- Significantly reducing cybercrime
- Developing cyber defense policy and abilities, whilst preventing copies with NATO activities
- Promoting a Single Market for cybersecurity products, including the development of

industrial and technological assets for cybersecurity

- Setting up a coherent international cyberspace policy for the E.U and advancing core E.U values

The People's Republic of China (PRC)

China is recognized as to be responsible for numerous cyber-attacks on both public and private sectors of countries such as United States, Russia, France, Canada and India. As a result, China is attributed for many past international cyber warfare incidents. The majority of the incidents were cyber-spying which is quite detrimental in the trust amongst nations. This increased political tension between the countries. However, despite many accuse China for the attacks; there is no specific evidence that they were accountable to China, the Chinese government expresses their innocence. Additionally, the Chinese government claims that they are also a victim of the cyber warfare, rather than an international threat to other nations. Noting that the ability of hacking and spying with the application of technology of the Chinese government is yet to be evaluated and proven. The opinions of other nations on the importing of foreign high-tech cyber spying and attacking facilities are remained unsupported.

Nevertheless, China also realizes the importance in ensuring cybersecurity in order to secure their governmental and private resources. They are also open to work together with the international community, strongly believing in the institution of general and effective customs and procedures for their activities within the cyberspace. Resolutions potentially regarding the international code of conduct for information security and international deliberation with the UN framework of the General Assembly have been formed with the contribution of China.

South Korea and North Korea

After a cyber-attack suspected as an act from North Korea, the tension in the Korean Peninsula has developed, and the South Korean government has taken procedures for improving cyber security. The cyber assault happened in March 2013, where major banks in South Korea including, Woori, Shinhan, and Nong-hyup following up with major broadcasting companies such as KBS, SBS and MBC were attacked. The aftermath was the biggest that South Korea has ever experienced, at least 30,000 computers were affected. The South Korean government suspected North Korea because of the fact that North Korea had been investing in training quality hackers. South

Korea had thought that it was appropriate to do the same for preventing further damages. Another incident of the two nations regarding cyber warfare was that, prohibited information of the military between the US and South Korea was exposed to North Korea by measures of hacking. Thus, both nations have agreed to debate on the issue in the Security Consultative Meeting (SCM).

Timeline of Relevant Resolutions, Treaties and Events

Date	**Description of event**
November 2, 1988	The very first cyber-attack 'Morris Worm' was executed, causing computers all over the United States, to slow down to a point where they would be unusable.
1994	In response to the concerns of the International Security, an American computer services company, Netscape develops an encryption that secures online transactions, called the 'Secure Sockets Layer'.
2000	Another worm known as the love bug infects government and private systems worldwide. The U.S drives for the Council of Europe Cybercrime Treaty as response, also to harmonize computer laws between nations.
January 22, 2001	UN GA3 Resolution (A/55/593, 55/63) 'Combating the criminal misuse of information technologies' http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf
January 23, 2002	UN GA3 Resolution (A56/574, 56/121) 'Combating the criminal misuse of information technologies' http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf
January 31, 2003	UN GA2 Resolution (A57/529/Add 3, 57/239) 'Creation of a global culture of cybersecurity; http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

February, 2003	A pair of the UN sponsored conference on the information society; the World Summit on the Information Society (WSIS) took place in Geneva.
2003	DHS began procedures, forming the National Cyber Security Division.
January 30, 2004	UN GA2 Resolution (A58/481/Add 2, 58/199) ‘Creation of a global culture of cybersecurity and the protection of critical information infrastructures’ http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf
February, 2005	WSIS summit held in Tunis
April 26, 2007	A cyber-attack had taken place in Estonia, where its government networks were compromised by denial-of-service attacks. This had prompted the world in ensuring proper cybersecurity procedures.
2010	U.S Cyber Command goes into operation.
2010	World ITU summit in Guadalajara.
March 17, 2010	UN GA2 Resolution (A/64/422/ Add 3, 64/211) ‘Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures’ http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211
December 14, 2015	The UN General Assembly High-level Meeting takes place for an overall review of the implementation of outcomes proposed in WSIS summits.

Evaluation of Previous Attempts to Solve the Issue

Cyber warfare, a new domain of terror enforced many nations and organizations to take appropriate responses for ensuring protection of any valuable resources in their network system. The United Nations General Assembly has been drafting resolutions regarding the issue of cyber warfare and to promote cybersecurity. Moreover, they have established agencies and organizations fully under their control with an objective to deal with and problems relating with cyber warfare. Although these organizations support in forming resolutions, the problem is still on going and cybersecurity has more to be improved. Therefore, further meetings and summits are scheduled to develop the existing solutions and perhaps form better ones.

The current published resolutions focus on reinforcing the security of member state's individual networks and internet systems. In order to protect infrastructures from cyber threats, nations were to isolate their communication and information technologies. Despite the fact that sharing international knowledge like such was supported by the UN. The less economically developed countries found it difficult to maintain the same technology as the more economically developed nations. Due to these gaps financially, numbers of the attempts in promoting cybersecurity had failed. Moreover, Nations must take responsibility in assessing their current policies and legislations to guarantee that they consider cyber-attacks. However, due to the fact that the term cyber is defined and comprehended differently, the policies and legislations are to be suitable for each nation.

Therefore, although some of these previous attempts were proven to be successful in improving cybersecurity with procedures of the whole system thought out to resolve the issue. It must be understood that when security levels become higher and more advance, so will the skills of the hackers. Therefore, alternatives to currently existing solutions must be thought out, displaying views from different possibilities regarding cyber warfare.

Possible Solutions

Although, there are summits where nations get together to discuss possible solutions, there is no Geneva Convention for the internet. Thus, when it comes to the development of cybersecurity for proper protection from cyber warfare, it is essential for a greater openness and cooperation between nations and major organizations like the International Telecommunication Union. Furthermore, protection from cyber warfare can be conducted through measures where security of online data strengthens by ways such as, anti-virus programs, reliable and safe connection when using the internet in public via trustworthy internet service providers, etc. Yet, experts inevitably expect a cyber-war anytime in the future. Indeed forming protection or developing existing ones for cyber-attacks is necessary. Though, nations must also focus consistently in exterminating the problem of cyber warfare than relentlessly investing in cybersecurity. Therefore, there must be an emphasis on the ITU secretary general Hamaduon Toure's recent proposal; an agreement for an international cyber peace treaty must be executed where signatories agree that their infrastructure will not be at any use relating to cyber warfare.

Bibliography

"Arms Control Today." *The UN Takes a Big Step Forward on Cybersecurity*. N.p., n.d. Web. 11 Feb. 2016. <https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity>

"Countering Cyber War." *Countering Cyber War*. N.p., n.d. Web. 11 Feb. 2016. < http://www.nato.int/docu/review/2001/Combating-New-Security-Threats/Countering-cyber-war/EN/index.htm>

"Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at Conclusion of Thematic Debate Segment | Meetings Coverage and Press Releases." *UN News Center*. UN, n.d. Web. 11 Feb. 2016. <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>

"Defense Cybersecurity: Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses." *U.S. GAO* -. N.p., n.d. Web. 11 Feb. 2016. <http://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html?_r=0>

"Finding Solutions. Together." *Five Concerns and Five Solutions for Cybersecurity*. N.p., n.d. Web. 11 Feb. 2016. <http://www.global-economic-symposium.org/knowledgebase/the-global-polity/cybercrime-cybersecurity-and-the-future-of-the-internet/proposals/five-concerns-and-five-solutions-for-cybersecurity>

"132nd IPU Assembly: Resolution 1." *132nd IPU Assembly: Resolution 1*. N.p., n.d. Web. 11 Feb. 2016. <http://www.ipu.org/conf-e/132/res-1.htm>

"The History of Cyber Attacks - a Timeline." *NATO Review*. N.p., n.d. Web. 11 Feb. 2016. <http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>

"The History of Cyber Warfare." *The History of Cyber Warfare*. N.p., n.d. Web. 11 Feb. 2016. <http://online.lewisu.edu/msis/resources/the-history-of-cyber-warfare>

"International Telecommunication Union (ITU)." *TIA*. N.p., n.d. Web. 11 Feb. 2016. <http://www.tiaonline.org/policy/trade/international-telecommunication-union-itu>

"The Rise of Cyber Weapons and Relative Impact on Cyberspace - InfoSec Resources." *InfoSec Resources The Rise of Cyber Weapons and Relative Impact on Cyberspace Comments*. N.p., 05 Oct. 2012. Web. 11 Feb. 2016.

<http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/>

"Russia Pushes for UN Resolution on Cyberspace." *PCWorld*. N.p., n.d. Web. 11 Feb. 2016. <http://www.pcworld.com/article/240983/russia_pushes_for_un_resolution_on_cyberspace.html>

"UN." *CCDCOE*. N.p., 09 June 2014. Web. 11 Feb. 2016.

<https://ccdcoe.org/un.html>

"UN Resolutions." *ITU*. N.p., n.d. Web. 11 Feb. 2016. <http://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx>

"United Nations Launches Global Cybersecurity Index." *ITU*. N.p., n.d. Web. 11 Feb. 2016. <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/United-Nations-Launches-Global-Cybersecurity-Index.aspx>