Introduction

For the last decade the development of IT has reached its highest, providing people with a greater quality of life. However it also created a silent war: a cyber war. Cyber attacks have been reported from countries all over the world, and many of these attacks were strong and provocative enough to cause political disputes between countries. Sabotages on organizations such as government body, military infrastructures, communication systems and financial markets may lead to serious outcomes. Increased access to technologies and Internet are making the victims more and more vulnerable and yet the international society has no clear solutions on the table.

One incident of disastrous cyber warfare took place in Estonia in 2007. The attack is believed to originate from Russia, and it jammed 1 million computers nationally including the governments, business, and media websites leaving ten million euros of damage. Consequently, the bilateral political tension built up between the countries at this time. This example illustrates how cyber attacks can lead to a physical damage including but not limited to financial losses. Another event, which took place in 2009 between South Korean and North Korea, was associated with military top secrets. South Korean government reported an attack on their country’s national military data. Claiming with high possibility that the attack was from North Korea, the government announced that the defense plans between South Korea and USA in the event of another Korean war may have been stolen by North Korean hackers.

This issue not only concerns the public sectors of countries, but also alarms the private sector and individual companies and organizations. Just like many government bodies, normal companies or any other organizations are not safe from cyber warfare. Anyone can be attacked at anytime by anyone, due to certain characteristics of cyber warfare. Cyber warfare is ‘asymmetrical’. In other words, attacks can come from anywhere. Detection, prevention, and response control to the attack has to take place in all places of data, control panels, and attack surfaces, and this is not as simple as it sounds. It is now the member states’ responsibilities to construct and discuss solutions that are effective, efficient and practical at the same time.
Definition of Key Terms

Corruption

Situation in which data and algorithms of an IT system are changed in an unauthorized way: deleting or editing the correct way of function of the system.

Disruption

Situation in which an IT system is edited to perform an operation that makes the system shut down, work at a fraction of their capacity, and interfere with its normal way of functioning in an unauthorized way.

Domain

Address on the Internet, which could be a mixture of numbers and alphabets, made to be easily recognizable to the owner and the visitors. Domain names are sold at registration center, so the domain can only be used by one person or a particular website so it cannot be used by multiple entities.

ISP

Internet Service Provider, computers or machines that inter-connect individual computers and networks to a World Wide Web.

Cyber warfare

The provocative acts targeted at specific body in order to disrupt the online system deliberately

Malware

Full name is Malicious Software, a program designed to enter a computer to damage, disable or hijack information in an unauthorized way.

Payload

Used to describe any damage that can be done when a computer or a system has been hacked.

Application (App)

Computer software designed to help performance of computers and technologies in a certain way

Server

A computer program which coordinates the flow of data in between linked computers, networks to a website or anywhere on the Internet.

Top Level Domain (TLD)
Category of domain names: .com, .edu, .gov etc. These are primary routing services for internet traffic.

Firewall

Software or program that does not allow unauthorized access to the computer or network - only allows authorized users to access the network.

Honeynet

Network of virtual computers created by researchers and professionals to study malware.

Honeypot

Virtual computer without any security of security program: they are designed to be infected by malwares to be studied by honey-net.

ISO/IEC JTC1

Joint organization between International Organization for Standardization (ISO) and International Electro-technical Commission (IEC) with a single aim of maintaining, developing and promoting standards in Information Technology.

ITU

International Telecommunication Union: an UN agency that is in charge of issues involving Information and Communication Technology.

Interface Manager

A layer of software between operating system and an application that allows the application to perform in a designed way.

IP Address

Internet Protocol Address: ID number assigned to specific computer in a network.

Unpack

Breaking through the deceptive coding that compresses and protects a malicious program.

Virus

Harmful software program which is able to generate and multiple itself to be spread over the network, and each virus has a payload that is activated under certain instructions and corrupts, changes or destroys the data.
History

The beginning of cyber-warfare

1988 - First ever virus attack

The Morris worm, created by a student at Cornell University called Robert Tapan Morris who later became a professor at MIT in United States, was the first virus recognized by the world. The targets were the computers all over United States, and the virus caused computer systems to slow down to the extent of turning them unusable. Its mechanism was relatively simple, as it interrupted one part of the whole system called the UNIX system. The virus replicated itself rapidly and it has spread at a very fast rate. Professor Morris claimed the aim of development of this virus was to find out how big the Internet was at the time. He became the first man in the history to be convicted under the US’s computer fraud and abuse act.

Caption: Robert Tapan Morris

Between 1990s - late 2000s

As technology developed and uses of Internet and computers became more widely spread both in government bodies and individuals at home, there was a relatively high number of cyber warfare incidents between 1990s and late 2000s compared to that in 1980s. As a result, in June 1997, the NSA (the National Security Agency of United States) conducts a test known as ‘Eligible Receiver’ assessing the vulnerability of national bodies and militaries against the cyber attacks. The research showed that at that time most of the important governmental websites were exposed to attack at relative ease. Usual commercial computers and software could do the hacking of these sites. To resolve this problem, countries started to set up their own laws and regulations in order to prevent damages from the attacks. For example, in December 2006 the United States government agency NASA (The National Aeronautics and Space Administration) was forced to block emails with attachments before shuttle launches as a precautionary measure to prevent hackings. This measure was followed by the report issued by the Business Week, which announced that foreign hackers had obtained the plans for the latest US space launch vehicles.

The increased awareness of the issue has made the protection stronger and more effective. In April 2007, Estonian government network was harassed by an anonymous denial of service attack. Several government online services as well as the online banking services were disrupted. The reason behind the attack was found to be the country’s spat with Russia over the removal of war memorial. The new term ‘cyber riots’ evolved; such acts were classified separately from crippling attacks. However, the Estonian government responded very well,
bringing back the services within hours after the attack. As this example illustrates, around late 2000s, the people’s responsiveness to cyber attacks has gotten much better. However, as the protections improved the skills of hackers improved as well. Silent arm race was going on between people trying to protect, and people trying to hack.

Problems were exacerbated, and reasons of attacking started to vary even more. Nevertheless, most of the international cyber warfare cases were developed from political issues. The Chinese through wide and broad attacks demonstrated this type of political attack in March 2009. Canadian researchers at Munk center for international studies at University of Toronto announced that the Chinese hackers have penetrated 1,300 computers in 103 countries. These computers include the ones in embassies, government offices, and military computers. They have stolen many top-secret national and international documents. This was the largest hacking operation identified until 2009. (Link for more details on this incident: http://www.nytimes.com/2009/03/29/technology/29spy.html?pagewanted=all&_r=0)

Recent cyber-warfare

**Between 2010 - 2011**

In 2011, the three big cyber attacks shocked the world. In May, Sony the Japanese electronics company reported the Congress that hackers had penetrated the Play Station network to steal and misuse the personal information of at least 77 million users worldwide. It left the company with financial loss of 170 million USD, and also harmed the owners of the personal information hacked. The criminals were found to be the members of an anarchist-activist group known as ‘Anonymous’. In the next month, IMF (International Monetary Fund) officials announced its hit by ‘a very major breach’ of its computer systems, and there were several evidences suggesting it was an act of Chinese hackers. Later in the year, around December, the incident from which the term ‘malware’ originated took place. Malware is named after the Massiah in Islam, and it hacked 800 computers of government officials, embassy and employees across Iran, Israel, Afghanistan, United Arab Emirates and South Africa. The method of hacking performed by malware was via the software sending an email to users with attachments; once attachments are opened, every other email and messages of the user can be viewed on the hacker’s computers.

**Between 2012 and today**

During the late 2012 and early 2013, the major cyber attacks targeted United States. In September 2012, nine banks in United States including Bank of America, JP Morgan Chase and Wells Fargo were attacked by Islamic hackers group called: ‘Izz ad-Din Al-Qassam Cyber Fighters (also known as Al-Qassam Brigades)’. The world famous magazine, The New York Times, was also a major prey of hackers from all around the world. After publishing an article about the investigation of families of former prime minister of China Wen Jia Bao who benefitted
financially from state contracts, The New York Times has experienced a major attack. The hacking included gaining access to the paper’s computing system. Later on, they made an official announcement that the purpose of the attack was to monitor the newspaper’s China coverage.

**Key Issues**

**Different motivations for attacks**

**Military:** More than half of world’s cyber warfare is military-related, either aiming to interrupt the system of a military body through denial of services, or to obtain military secrets of other nations. These kinds of acts build up political tension between countries, and destabilize the world peace.

**Terrorism:** There have been claims that cyber warfare is better described as ‘cyber terrorism’, because hackers carry out the attacks without informed dates or time, and for most of the time, anonymously. Furthermore, cyber weapons used during the cyber warfare are known to be as equally destructive as biological weapons in real life terrors. Its disruption on political situations as well as the relationships between countries can lead to terror attacks in real life.

**Civil:** Apart from cyber warfare in a country’s national bodies, attacks and sabotages can also target the ordinary citizens. Disruption of computers and laptops at businesses and homes through web server hackings and network equipment hackings can disturb the well being of the general public.

**Different types attacks**

**Vandalism** – A typical example of vandalism related to cyber warfare is vandalism during election. In a Central Asian country Kyrgyzstan, computers or users who post government-unfriendly posts or comments are usually hacked and attacked, resulting in corruption of data within their server.

**Propaganda** – This is a weaker type of cyber warfare, since it is not a direct form of attack, it does not disrupt the system or does anything similar. Propagandas are designed to manipulate and achieve people’s responses that suit the attackers’ intentions and often change the views and opinions of people on certain things. Cyber propaganda is a form of cyber warfare as the propagandas are published through out the web, emails and file-sharing sites and causes social disputes.

**Denial of Service** – This is the most usual form of cyber warfare as its implementation is relatively easy. However, it is hard to defend against these kinds of attacks. Basically, the attacker creates an overloaded number of requests to the server that paralyzes the whole system.
server cannot handle all the incoming strains with connections being cut. The domain and the website are permanently damaged and do not function until they are manually fixed.

**Major Parties Involved and Their Views**

**Major Countries Involved**

*United States*

United States is one of the countries that receives the most cyber attacks globally. As a result, the country had to come up with solid solutions and methods to deal with the cyber warfare. In 2009, President Barak Obama described America’s digital infrastructure to be a ‘strategic national asset’, and in May 2010, the government established the new US Cyber Command (USCYBERCOM) under the direction of NSA (National Security Agency). The main role of the organization is to protect its military networks and to attack other countries’ systems. US incessantly expressed its concern on exposure of the country’s key sectors in both private and public sectors (public and private facilities, transportation, banks, education sector and most importantly, the government) to cyber warfare. Throughout the century, the US government has actively tried to combat cyber warfare. In August 2010, they publicly warned and criticized the act of Chinese military hacking their military networks. However, other countries claim that the US government is contradicting itself by attacking other nations, as the New York Times reported in 2012 that President Barak Obama has given orders to attack the Iran nuclear systems.

*China*

A lot of the past international cyber warfare incidents are attributed to China. China is known to be responsible for attacks on both public and private bodies in countries such as India, United States, France, Russia and Canada. Several of the incidents were major and they have increased the political tension between countries in the past. Despite the majority of countries suspecting China for the attacks, the Chinese government claims its innocence on cyber-spying. The government even argues that China is the victim of the attacks, rather than an international threat of cyber warfare. In fact, the Chinese government’s technology, hacking skills and spying abilities are yet to be evaluated and proven. Hence, other nation’s opinion on how China is importing foreign high-tech cyber spying and attacking facilities and skills are remained to be mere opinions rather than facts.
India

India has established The Indian Computer Emergency Response Team (CERT-In) under the department of Information and Technology in 2004 in order to combat the cyber warfare. In 2011, the government introduced a new division under CERT-In, called National Critical Information Infrastructure Protection Center (NCIIPC), to control hacking against specific areas in the country such as telecom, transport, banking, defense and others. This new formation of NCIIPC aimed to effectively divide the protection even more within the country. Another subdivision of CERT-In is National Power Cooperation of India (NPCIL), which is in charge of protecting the nuclear weapon sector. Indian government is clearly putting an enormous effort to protect the country from various types of cyber warfare. Recently in February 2013, NCIIPC finalized its policies on domestic security solutions. The solutions include reducing its exposure to foreign technology, isolating its security agencies and having all these performed under the control of a National Cyber Security Coordinator. This attempt has been successful, as from that month and onwards, India has not been damaged significantly both economically and socially in any cyber attacks.

South Korean and North Korea

South Korean government has expressed its interest in improving its cyber warfare protection. The tension in Korean Peninsula has built up recently due to suspected acts of North Korea’s cyber attacks targeted at the South. In March 2013, South Korea’s major banks, such as Shinhan, Woori and Nong-hyup, and major broadcasting companies, including KBS, MBC and SBS were attacked; as a result, at least 30,000 computers were affected. It was the biggest attack South Korea ever experienced, and the government suspected that the attack was linked to North Korea. As North Korea has been investing huge amount of capital in training high quality hackers with South Korea felt that it was sensible for them to do the same in order to prevent future damages. The military secrets between the joint practice of United States and South Korea have also been exposed to North Korea through hacking. Therefore, United States and South Korea have planned to discuss the topic in depth in Security Consultative Meeting (SCM) in the future.

Iran and Middle East Countries

Iran is famous for its heavy investment on cyber warfare capacity. Although some say China and Russia have the highest quality cyber warfare related skills, in fact, Iran is playing a leading role in cyber warfare. Iranian hackers are known to be leading majority of attacks targeting United States, followed by Chinese hackers. Iranian government reported that it has invested 1 billion USD annually in recent years to build what is called ‘cyber muscles.’ Furthermore, Iranian authorities have openly stated that they welcome any hacking expertise that
is willing to work for the Islamic Republic for good and revolutionary activities. This shows how motivated Islamic Republic as a whole is for improvement in its cyber welfare facilities.

**Timeline of Relevant Resolutions, Treaties and Events**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of event</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>22nd January 2001</td>
<td>UN GA3 Resolution (A/55/593, 55/63)</td>
<td><a href="http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf">http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf</a></td>
</tr>
<tr>
<td>23rd January 2002</td>
<td>UN GA3 Resolution (A/56/574, 56/121)</td>
<td><a href="http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf">http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf</a></td>
</tr>
<tr>
<td>31st January 2003</td>
<td>UN GA2 Resolution (A/57/529/Add 3, 57/239)</td>
<td><a href="http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf">http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf</a></td>
</tr>
<tr>
<td>February 2003</td>
<td>ITU (International Telecommunication Union, an UN agency) led World Summit on Information Society (WSIS) in Geneva</td>
<td></td>
</tr>
<tr>
<td>30th January 2004</td>
<td>UN GA2 Resolution (A/58/481/Add 2, 58/199)</td>
<td><a href="http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf">http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf</a></td>
</tr>
<tr>
<td>February 2005</td>
<td>ITU WSIS summit in Tunis</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>ITU puts the issue of cyber-agenda in combating cybercrime and cyber defenses</td>
<td></td>
</tr>
<tr>
<td>17th March 2010</td>
<td>UN GA2 Resolution (A/64/422/ Add 3, 64/211)</td>
<td><a href="http://www.citizenlab.org/cybernorms/ares64211.pdf">http://www.citizenlab.org/cybernorms/ares64211.pdf</a></td>
</tr>
</tbody>
</table>
Evaluation of Previous Attempts to Resolve the Issue

For more than ten years, the United Nations General Assemblies have drafted a few resolutions regarding the issue cyber warfare. Technically, the UN recognized the need to solve this problem as soon as it came up to the surface. Furthermore, UN has established a few organizations and agencies under its control to specifically deal with the issues concerning cyber warfare, cyber welfare and cyber defenses. With the help and aid of these organizations, they have produced resolutions and solutions at great quality. However, the problems still remain; additional meetings and summits are planned in the future to further discuss possible solutions to the issue.

Resolutions up until today generally focused on strengthening the security of each nation's individual networks and internet systems. They called for more efforts from nations to isolate their information and communication technologies in order to protect the infrastructures from foreign hackers. Although UN supported the sharing of international knowledge on these kinds of acts, it was hard for developing countries to catch up with the technologies in developed countries. More technologically advanced countries were more active in guiding less technologically advanced countries. However, due to the differences in financial situations and different attitudes towards the issue, a lot of these attempts were not successful.

Moving from the big picture of international interventions, to an intra-national approach involves asking cooperative work between public and private sectors of the countries. Specifically, the previous resolutions emphasized the importance of data sharing among the state and stakeholders of private firms. Highlighting the inter-connections between these two sectors, their cooperative acts were considered to be more effective in defending the nation from online attacks. Furthermore, the identification of networks and systems of any organization, be it a government body or a private firm, was also proposed. In order to protect an organization's system, individuals in the organization need to be fully aware of the system inside out. During this course of identifying and sorting out the networks, they once again secure their data and information for improved security.

Some of these previous attempts were very successful, as improving the security of the data and the whole system has been thought to be the core step to resolve this issue. However, as the security level increases, the skills of hackers improve well. Hence, views from different angles regarding the issue are needed. A solution that is beyond merely strengthening the system is required.

Possible Solutions

Definition of ‘Cyber Warfare’

One of the most basic but important problems to be solved today regarding the issue of cyber warfare is the definition and use of the term 'cyber warfare'. It is defined as the malicious act deliberately done online targeting a system or a network to disrupt its processing. However, the term ‘-warfare’ can
be misleading as it suggests an armed conflict, a mechanical force involved in the process; however, is this true? Some may say that the social disruptions caused by cyber attacks can be seen as an actual ‘war’ involving forces; however, to what extent is this subjective view applicable? Also, this idea of using forces not only is against the most fundamental charters of UN, but also invokes the rights of nations of self-defense under Article 15 of the UN Charter. Clarifying this issue with definition would be a crucial first step towards successful solutions for the topic.

**International Laws**

NATO (North Atlantic treaty organization) Cooperative Cyber Defense Center of Excellence has recently published its research report called ‘Tallinn Manual on the International Law Applicable to Cyber Warfare' (Link to the document: http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf) The solutions proposed in this manual are based on the three years of independent research conducted on this issue in detail. However, the solutions challenged the global society by allowing the states to kill hackers attacking their system. This is a very controversial part of the manual and it invokes the UN to intervene to prevent [what specifically?]. Just like this case of NATO Tallinn Manual, sometimes the existing laws need further amendments to be made. Furthermore, establishing brand new international laws regarding other aspects of cyber warfare is needed to solve the problem.

**Strengthening Online Security**

Measures to increase security of online data can be done through managing firewalls, anti-virus programs, email attachment scanning programs, safe and reliable connection to public internet via trusted Internet Service Providers (ISP). In addition to these primary methods of securing the data, public and individuals should be informed and educated about the availabilities and uses of these facilities.

*Caption: ISP spider web*
Bibliography

(Important ones in bold)


