Committee/Council:	**Disarmament and International Security Committee**
Issue:	**Developments in the fields of information and telecommunications in the context of international security**
Student Officer:	**Alkistis Giavridis**
Position:	**Co-Chair**

Introduction

Throughout the 1990s there was a major information technology boom, endorsing a whole new form of communication, providing easier and faster access to information while creating a whole new work sector. Ever since, there have been astonishingly rapid advancements in technology, and as of today we, the human race, are predominantly dependent on Information Communication Technologies (ICTs). All of our information and data is stored on digital devices, we use technology to communicate with one another and even when it comes to financial resources, all of our money is deposited in bank accounts. This dependency on ICTs makes us extremely vulnerable as the latest technological innovations can also lead to an expansion of the crime scene on a digital level in the form of online theft of identity, economic fraud, stalking, cyber bullying, hacking, phishing, data and information piracy, etc.

But apart from our personal lives, ICTs also have the power to outstretch the challenges to international security. Constant updates and ameliorations of cybertools facilitate the disruption of international peace and stability by the use of technology as a weapon and therefore the endorsement of a whole new level of war, cyberwarfare. Both state and non-state actors have the ability of using ICTs for malicious purposes such as the gathering of knowledge, the enlisting, planing and arrangement of attacks, the wiedespread of ideology, propaganda, the recruitment of child soldiers, the forbidden access to sensitive information concerning a country's security, the manipulation of data as well as the leaking of false information about a country's security or army plans.

Therefore it is of salient significance to move towards the increase of transparency and confidence-building measures as well as the clarification of the application of international law to state and non-state behavior in cyberspace. Similar to when nuclear technology was first invented, cyberspace has also changed armaments and warfare, which underlines the importance of creating international norms, treaties and agreements that prevent the risk of cyberwarfare and enhance the secutiry of ICT infrastructure, globally.

Definition of Key-Terms

Cyber Warfare

Cyber Warfare is described as “the fifth domain of warfare”, and refers to virtual conflict instigated for political reasons by either state or non-state actors with the goal of attacking an enemy’s information systems. Cyber Warfare involves attack methods such as sabotage, electronic espionage and/or security breaches as well as electrical power grids.

Cybercrime

The term cybercrime refers to crimes (illicit activities), which involve the use of digital devices and/or computer networks. Crimes falling under this specific category go from rather harmless crimes such as the unlawful downloading of music or movies, to more severe crimes such as identity theft or credit card account theft.

Information Technology security

Information Technology security, otherwise referred to as cyber security, deals with actions that have to be done in order to protect and safeguard computer networks, computer systems and/or data from cybercrime.

Information Communication Technology (ICT)

Even though there is no universally accepted definition for ICT, the term mainly refers to all the technology used by individuals or organizations to get access to information through telecommunications such as radio, television, wireless networks, cell phones, satellite systems, computer and network hardware and software, and other communication mediums. Compared to Information Technology (IT), the term Information Communication Technology is usually used associated with education.

Hacker

Strictly speaking the term “hacker” describes a person with an excellent expertise in the field of programming. In spite of that, it is usually used when referring to someone that has illegally hacked into (broken into a computer system, file and/or network) in most cases for malicious purposes.

Surveillance

Surveillance is commonly practiced by the authorities and deals with the permanent observation of a person or a group, who is suspected of a crime, as well as the continuous supervision of a certain place where the suspects are likely to gather.

Dark Net

Dark Net is short for “Dark Internet”. The Dark Net is a collection of private networks and/or Internet services, where the network and IP-address of participants are anonymous. This allows users to communicate freely, download and share illegal files (often including illicit content such as child pornography), or trade illegal products such as guns or drugs without the fear of being discovered, tracked and/or identified.

Malware

Malware is short for “malicious software”. It is an umbrella-term that is used to define any software that is designed to disrupt and damage a computer system, server or network no matter if it’s a virus, a worm, a Trojan horse or spyware.

Computer Virus

A computer virus is a man-made software program or piece of programming code designed to spread from one computer to another and create, move and delete files, as well as cause the computer to not function properly. The most common ways to get a computer virus are opening infected emails that contain malicious code, surfing unsafe sites or downloading infected software.

Background Information

Russia’s attack on Georgia

In August 2008 Russia was accused of being responsible for the denial-of-service attacks on the Georgian government websites and on other commercial Georgian sites. The cause of the cyber attacks was believed to be the at-that-time-ongoing-armed South Ossetia-conflict between the 2 states. Researchers claimed that the group responsible for the website attacks was a “multi-faceted cybercrime organization”, the Russian Business Network (RBN), as it was very similar to Russia’s cyber attack on Estonia in 2007. Responding to the cyber attack, the Georgian Ministry of Foreign Affairs said that numerous websites in Georgia had been seriously affected by Russia’s cyber warfare campaigns and also U.S. President Barack Obama demanded that the cyber attacks should come to an end. The Russian embassy in London on the other hand, described the case as a misunderstanding, denying the existence of a military attack by the Russian Federation and describing the activity in South Ossetia as peace enforcement.

Flame Virus

The Flame Virus was discovered in 2012 by the Russia-based security firm Kaspersky, and is one of the most powerful weapons in cyber space. Its main tactic to gaining access to valuable information is cyber espionage, more specifically the remotely manipulating of computer settings, the collection of stored files, the capturing of audio conversations and instant messaging conversations as well as the taking of screenshots. The espionage toolkit's target group does not only include individuals, but ranges from certain state-related organizations to educational institutions. Flame's attacks have been mainly focusing on nations in the Middle East and North Africa, and the person, organization or nation behind the incidents has not been identified, as the servers are well protected and hidden. The Flame virus was going around and spreading from computer to computer for two entire years while infecting millions of systems, without even having been discovered.

The National Security Agency (NSA)

Verizon and PRISM

In April 2013 a top secret court order by the foreign intelligence court of the U.S. forced the communication technology company Verizon to hand over all of its information regarding phone calls in its systems to the NSA. This information contains caller ID, receiver ID, call duration as well as the time and place the call was made from. The type of the order was untargeted and widespread, in other words the NSA could basically spy on every single Verizon user's phone call data, no matter if that user even was a suspect for any cases of unlawful behavior. In early June 2013 the allegations of the Electronic Frontier Foundation (EFF) and many others, about the NSA's surveillance purposes, were proven to be true, as The Guardian published the exact court order, asking Verizon to turn over "all call details or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls". Shortly after those revelations, 2 other articles by the Washington Post and The Guardian followed, revealing that the U.S. was also using a surveillance program called "PRISM". This information was leaked by former NSA contractor, Edward Snowden stating that with the system PRISM, the NSA basically looked into the servers of nine popular Internet services including Facebook, Google, Microsoft, YouTube, Skype and Yahoo, gaining access to the systems' user's communication. The existence of PRISM was also confirmed by the director of the Defense Intelligence Agency, James R. Clapper. Despite that there has been a lot of discussion and controversy concerning PRISM, first and foremost the companies that are allegedly a part of this scandal, all denied that they participated or even knew about this program, claiming they did not allow the government "direct access" to their data. The Guardian and the Washington post both claim that the program does not only give the NSA metadata information like Verizon did, but also gives them insight into the content of conversations. The New York Times and others on the other hand claim that PRISM only collects and analyzes data that was legally requested by the NSA. After this case of phone surveillance became public, countless civilians complained, saying the actions of the NSA were first of all unnecessary, as they were not targeting a specific group of criminals, and secondly an invasion of privacy, as call details are something personal. The President of the United States Barack Obama responded to this incident, saying it was just an action to enhance security within the U.S. by preventing further terrorist attacks from happening after 9/11. In November 2013 a review group on Intelligence and Communication Technology proposed amendments to the Obama Administration on the U.S. spying policy, so as to safeguard the Americans, while not invading on their privacy.

Attacks on EU offices and UN Computer Networks

In August 2013 the German Magazine "der Spiegel" disclosed that the NSA had been spying on UN computer networks in New York and on EU internal computer networks in New York and Washington D.C. The Magazine reported, that it had been shown documents by Edward Snowden that proved those allegations. Some of the "top secret" files also pointed towards the fact that the NSA has been digitally eavesdropping on the EU Council of Ministers and the European Council in Brussels. This was done by cracking into the encryption system of the UN and then hacking into a private communication network used by diplomats of the EU. Although the U.S. has been trying to deemphasize the spying actions on foreign government officials, German Chancellor Angela Merkel, whose phone was also allegedly intercepted by the NSA, and French President François Hollande demanded that such actions should not be repeated and spying on each other's allies is unacceptable.

Hacks on China

In May 2013, after the U.S. sought his arrest, former NSA contractor, Edward

Snowden escaped to Hong Kong and revealed information about the U.S. hack attacks that targeted Chinese mobile systems, universities and businesses to the South China Morning Post. He said that many of the 61,000 hacking operations the NSA had globally conducted, were targeting China, especially mobile phone companies and the Tsinghua University in Beijing, one of the top research institutes in the country. Snowden's way of proving that the allegations were true, was by presenting pieces of information that he could have only found by a foreign security office or by gaining physical access to China's computers. He also claimed that this wasn't the first breach on Chinese computer systems, and that the spying on China has been going on for several years. Snowden added that the surveillance also included Chinese mobile phones, more specific phone messaging data.

The Sony Pictures hack

In October/November 2014 there was a major hack on Sony Pictures' computer systems. The hackers stole private information about recent film productions of the company, and exposed them in the Internet, open for anybody and everybody to read. Apart from that they also used malware to damage sensitive data on the computer devices of the company. Bloomberg reported that the hack was practiced by the so-called Guardians of Peace (GOP), and that it was an act of blackmail. Although Sony became aware of the hack in November 2014, a former employee of the group claimed that the GOP had been stealing data from the incorporation for a longer period of time. On 19 December 2014 the United States officially confirmed that the government of the Democratic People's Republic of Korea (DPRK), also referred to as North Korea was being behind the cyber attack. The possible motive behind the attack is believed to be the Sony-backed movie "The Interview". The movie was rather provocative to the DPRK, as its plot evolved around the assassination of the DPRK's leader Kim Jong-un. On the 16th of December 2014 the GOP once again blackmailed Sony, threatening to attack screenings of the movie. Due to those threats, many theatres refused to show the movie and therefore Sony cancelled the theatrical release of it. Two days after that incident, the hacker group demanded that the movie should never be "released, distributed or leaked in any form of, for instance, DVD or piracy". Everything even related to "The Interview" (including trailers, scenes of the movie, etc.) should be obliterated. The President of the U.S. thought that the cinema release of the movie should not have been canceled and responded to the scandal saying that "We cannot have a society in which some dictator some place can start imposing censorship here in the United States". Eventually the film was released on Christmas Day 2014 in a couple of theaters and on several digital platforms including YouTube, Google Play and later Netflix. Sony itself justified the fact that they cancelled the release at first, saying that it was the theaters' decision to not screen the movie, and not the company's.

The use of ICTs for terrorist purposes

In many cases ICTs and especially the Internet pose great assistance not only to our daily lives, but also to malicious groups such as terrorist organizations. Because of the fast speed of the Internet information can travel in the speed of light from one person to another. Many terrorist organizations such as ISIS, Al Qaeda and the Taliban are also aware of this and use the Internet and social media websites to spread propaganda, ideology, recruit and also for financing purposes. They use video and audio material to promote their organization's beliefs while targeting vulnerable groups of people, trying to get them to become a part of their illegal activities.

17-year old ISIS recruiter

One of the more recent examples of the influence of the ISIS propaganda machine on our society, happened in June 2015. A 17-year-old boy from Virginia pleaded guilty in federal court for helping the terrorist group ISIS by using his Twitter account to radicalize others, telling them how to financially aid the terrorist group and he even propelled one of the followers of his account to join ISIS in Syria by putting him into contact with an ISIS fighter overseas and even financing his plane ticket. John P. Carlin, the acting assistant attorney in charge of the Justice Department's National Security Division said that "This case serves as a wake-up call that ISIS propaganda and recruitment materials are in your communities and being viewed by your youth". And this just enhances the need to work on the field of Information and Telecommunications in order to prevent the misuse of ICTs from happening, and ensuring a safe cyber space for the future generations as well.

Major Countries and Organizations Involved

The United Nations Office for Disarmament Affairs (UNODA)

The influence of ICTs on international peace and security is an issue that the UN has dealt with since 1998, when a resolution, introduced by the Russian Federation, was firstly adopted on that topic. Ever since, there have been several resolutions and reports on information security, some by the Secretary General presenting the diverse opinions of member states and others by a Group of Governmental Experts (GGE) analyzing the potential threats of ICTs and proposing solutions that could lead to a more secure coexistence of nations in cyber space. The 2012/13 report by the GGE mainly focuses on tackling the issue by creating norms and rules that define responsible and cooperative state behavior in cyber space, so as to reduce the risk of cyber warfare. It also points out the necessity to use International Law, particularly the United Nations Charter in order to ensure a safe and cooperative ICT environment. The UN plays a significant role in addressing this complex issue, as it has the power to enhance communication and dialogue between the different states, and therefore urge them to work together on a common problem. The different attempts by the UNODA, to find the best possible solutions can be found on their web site, that deals particularly with making improvements in the field of Information and Telecommunications in the Context of International Security.

The United Nations Office on Drugs and Crime (UNODC)

While reports by the UNODA mainly focus on maintaining international peace and security through improving State behavior in cyberspace, the UNODC emphasizes on preventing terrorist groups from using the Internet as help for their unlawful activities. Those activities range from spreading ideology, recruiting and financing to attacking states or gaining illegal access to sensitive information. A report entitled “The Use of the Internet for Terrorist Purposes” was launched on October 22nd 2012, and explicitly offers guidance to member states on national and international level, mainly through endorsing the enhanced collaboration between criminal justice systems and private companies, in order to stop the use of the Internet for terrorist purposes.

The Islamic State of Iraq and Syria (ISIS)

The Islamic State of Iraq and Syria, also referred to as The Islamic State of Iraq and the Levant, is the most cruel jihadist terrorist organization of our time. The group’s goal is to establish a broader Islamic Caliphate, and it is willing to take brutal measures so as to achieve that goal. The Internet was one of the major factors that has led to the huge expansion of the ISIS community. The Islamic State has been using apps and social media tools such as Facebook, Twitter, Skype and YouTube to spread propaganda, and to reach young, naïve children as well as unknowing civilians outside of the Middle East. Their tactic consists of 2 main points; The first one is to post videos of bombings, shootings and beheadings on renowned websites like YouTube in order to first and foremost horrify and scare their enemies, but also demonstrate and express their power to the rest of the world. The other tactic that ISIS uses is portraying themselves as this immense, strong “family” by posting images of smiling children and comparing their fights to real-life computer games, and therefore propelling people to want to be a part of that forceful community, rather than being slaughtered by it.

Iran and the Stuxnet Worm

In the years 2009 and 2010 there was a major cyber attack on Iran's nuclear centrifuges, destroying approximately one fifth of them, and setting back Iran's nuclear program an estimated 2 years. The countries behind this attack are believed to be the United States and Israel. None of the 2 states has publicly stated that they are responsible for the attack, but anonymous U.S. national security officials came forward and assured that there has been collaboration between the Idaho National Laboratory in the U.S. and Israel, concerning the uranium enrichment plant in Natanz, Iran. Therefore the U.S. and Israel are accused of being responsible for the designing of Stuxnet. Stuxnet was discovered in June 2010, by the Belorussian anti-virus vendor VirusBlokAda. It is an Internet worm that spreads via USB sticks and targets Windows computers by attacking certain industrial control systems, made by Siemens, that are responsible for many kinds of automated process in chemical plants, nuclear plants, oil refineries, pipelines, etc. In October 2010 over 50,000 computers had already been infected by the worm, and 14 infected control systems had been reported by Siemens, the majority of which was in Germany. According to security researchers, Stuxnet was also responsible for the destruction of the Indian broadcasting satellite INSAT-4B in July 2010. In the case of Iran, first speculations stated that the worm was created to steal electrical blueprints of industrial control systems, but after thoroughly looking into the case, researchers found out that the worm also had the ability to make alterations in those control systems. Responding to the Stuxnet attack, Iran has been making major developments its cyber capabilities since the beginning of the year 2014 and according to a 2014 Mandiant Report, Iran poses an "ever-increasing threat due to its historical hostility towards US business and government interests".

The Russian Federation

The Russian Federation has been accused several times of being responsible for internet surveillance via SORM technology, hacking attacks and numerous Denial-of-service attacks (e.g. Georgia, Estonia). In April 2015, Russia increased cyber attacks against the U.S. and the Ukraine, as the U.S. was trying to further intervene in the Ukraine. The attacks have not only been targeting a range of U.S. businesses but also the State Department and the White House networks, gaining access to President Obama's personal schedule. The U.S. security firm Crowdstrike announced that Russia had intruded over 10,000 times on companies globally, in the year 2015. Many experts claim that there has been an alteration in Russia's behavior in cyberspace. While in the past years the country's main tactic was to practice quiet and targeted hits with the goal of gathering intelligence data about the U.S., now it seems like the Russian Federation is not scared of being caught, on the contrary it sees exposure as a form of demonstration of power and willingness to also use that power.

China and The U.S.

Due to many cyber attacks between China and the U.S. in the past, there has been an ongoing cyber war between those two superpowers. After several hacking exploits by China, many targeting U.S. companies, and countless claims accusing China of cyber spying, the People’s Liberation Army admitted in May 2014 that their cyber security squad existed, even though they had routinely dismissed allegations at first. Later in May 2014, the cyber war between China and the U.S. exploded, as 5 Chinese military officials were accused of stealing vital trade secrets of six major American companies including firms in the nuclear energy and metal industry. As a response, China denies all kinds of accusations and points out that the real enemy is someone else, highlighting the historic revelations of Edward Snowden in 2013. Apart from that, China also indicates that the charges on its military officials would also have a serious impact on the cooperation between the two nations.

Timeline of Events

Date	**Description of event**

January 4, 1999	Resolution A/RES/53/70 submitted by the Russian Federation gets adopted without a vote
July 15, 2001	The Computer worm «Code Red» attacks computer systems running Windows 2000 and Windows NT, exploiting a vulnerability in those particular machines
November 2003	A series of cyber attacks on U.S. computer systems by a group of hackers, codenamed «Titan Rain» starts in November 2003 and goes on for roughly 3 more years. The attacks targeted military systems of the governmnet, trying to get access to sensitive information. The cyber assault was labeled as Chinese in origin.
June 6, 2004	At that time President, George Bush, creates a new division of the Office of Cyber Security & Communications, the National Cyber Security Division (NCSD). The NCSD is responsible for enhancing security of critical cyber infrastructure.
December 2006	The National Aeronautics and Space Administration (NASA) was forced to block all emails with attachements before of the launch of space shuttles, to assure that the launch plans would not be sabotaged by hackers.
April/May 2007	The Estonian government networks were attacked by several denial-of-service attacks, on popular government websites, two of Estonia's biggest banks, educational institutions and Estonian newspapers. The reason of the cyberattacks is believed to be the removal of a Soviet war monument constructed in 1947, and the group blamed for the attack is the Russian government.
June 2007	The email account of U.S. Secretary of Defense, Robert Gates, was hacked as a part of a series of attacks targeted on the Pentagon's networks. Officials accused China's People's Liberation Army of being responisible.
August 2007	German magazine «Der Spiegel» reported that Trojans had been inserted in Chancellor Angela Merkel's computer systems and three other ministries. Hackers associated with Chinese espionage systems are held responsible for the incident.
September 6, 2007	Israel attacked a Syrian air defense network to later target an alleged nuclear facility near al-Kibar, Syria.
October 2007	China's Ministry of State Security blames the U.S. and Taiwan for stealing information from Chinese key areas.
November 2007	The head of Britain's Security Service (MI5), Jonathan Evans warned several business companies of cyber attacks launched by the Russian Federation and China, with the goal of «stealing sensitive technology on civilian and military projects»

Relevant UN Treaties, Resolutions and Events

(A/RES/53/70); (A/RES/54/49) (A/RES/55/28); (A/RES/56/19);

(A/RES/57/53); (A/RES/58/32); (A/RES/59/61); (A/RES/60/45);

(A/RES/ 61/54); (A/RES/62/17);) A/RES/63/37)(A/RES/64/25);

(A/RES/65/41); (A/RES/66/24); (A/RES/67/27); (A/RES/68/243)

Developments in the fields of Information and Telecommunications in the context of international security

(A/RES/55/63); (A/RES/56/121)

Combating the criminal misuse of information

(A/RES/57/239); (A/RES/58/199); (A/RES/57/239)

Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

Previous Attempts to solve the Issue

As apparent by the previous section, the UN has been passing resolutions regarding the topic of developing the ICT field in order to enhance international security since 1999. In those, several measures are proposed to tackle this extremely severe issue mainly focusing on creating general consideration and appreciation of the topic. Apart from that, there have been several reports by the GGE, carefully researching potential threats of the use of ICTs and proposing numerous ways to improve the situation such as creating norms and principles of responsible cyberspace behavior by States as well as working on confidence-building and capacity-building measures. The problem is that the countless attempts, by the Secretary General and the GGE, to enhance security in cyber space, have not been recognized by all of the member states, and this very complex issue is not taken serious enough by some of the states.

President of the U.S., Barack Obama has also taken the issue in his hands, by proposing a new law in January 2015, called the “Personal Data Notification and Protection Act”. The act basically forces companies and organizations to report any cases of data breaches or hacks within 30 days. This move by the President is most likely motivated by the recent increase in the number of cybercrimes against the U.S.. The only problem with the system is, that although sometimes people want to report e.g. a breach, they often do not know who exactly to address, and have to go through a multitude of law enforcement agency's websites to find someone who can redress the case.

The police of London have even gone a step further, by establishing the so-called "Action Fraud Center", and particularly by creating the FALCON response team, a group that people can easily and directly address, when they want to report breaches or hacks.

Possible Solutions

The first step to creating a safer ICT environment is to improve the situation on a national basis. Nations need to start educating their people on the problem of cybercrime, and what the best ways are to prevent it. Apart from that we also have to teach them how to easily spot a fraudulent email and in which way to deal with it, because often people, organizations and even governments transfer viruses on their programs, without even realizing it. It often happens that email attachments and other links are opened by us automatically and mindlessly, without the thought that the opening of those attachments might have serious consequences. Additionally we have to find a way to facilitate the reporting of cases of cybercrime. As stated above, all nations should try to create some kind of centralized body, comparable to the UK's Action Fraud Center, who organizations and individuals can directly address when they stumble across such a situation.

Apart from that it is a complete necessity to move towards international norms and treaties that clearly regulate responsible state behavior in cyber space, because at the end of the day, no matter how many anti-virus softwares or firewalls someone has used on their devices, if someone is really keen on gaining access to someone else's data, chances are he will. To conclude, what needs to happen is the creation of strict international laws on surveillance and cybercrime, as well as the defining of consequences that will follow in case those laws are not followed. Cyber security and cyber privacy need to be acknowledged as a basic human right, and the international community should see the violation of that right as unacceptable. The only way to stop states from committing cybercrimes is to have tougher consequences for such actions, than what the breach/hack is worth. Because if there is more at stake for nations, when committing such crimes, it is not as likely that they will commit them in the first place.

Bibliography

http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201

http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

http://www.cnn.com/2015/06/08/opinions/vishwanath-stopping-hacking/

http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/

http://www.un.org/disarmament/topics/informationsecurity/

http://www.theguardian.com/technology/cyberwar

http://techterms.com

http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html

https://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

http://www.hackmageddon.com/category/security/cyber-attacks-timeline/

http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T

http://www.wired.com/2012/05/flame/

http://www.kaspersky.com/flame

http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?_r=0

http://www.iar-gwu.org/node/65