Research Report

MUNISH ‘12

Please think about the environment and do not print this research report unless absolutely necessary.

Forum: General Assembly First Committee

Issue: Preventing and prosecuting cyber warfare

Student Officer: Sandra Smits

Position: President of the General Assembly, MUNISH 2012

Introduction

The online community is changing fast and we are starting to see what has been happening behind the screens of our computers: a world of cyber warfare. Cyber warfare dates back to the existence of the Internet. In worst cases, it leads to a complete destruction of a country's system. It has become a more than considerable issue; it is a new type of warfare that is rapidly spreading. Non-Governmental Organizations (NGOs) and some governments are already attempting to solve this crucial problem using different methods. Cyber warfare is an issue that should not be underestimated because of the vulnerability of the universal reliance on networks, more specifically power networks and Internet. Anyone who is specialized in computers could easily hack into a variety of different systems from banks, governments, confidential database etc. This could cause terrible consequences which could then de-stabilize an entire nation and create an immense chaos in the nation's infrastructure and framework, thereby affecting civilians. In other words, cyber war can be provoked very easily and create a horrendous disaster with huge catastrophic impacts. These cyber wars can sometimes affect nations so dreadfully that these countries are not able to recover easily. Sometimes it doesn't have to be so large-scale, cyber warfare and also endanger certain individuals, even civilians.

Definition of Key Terms

Preventing

Preventing something is to keep it from happening, so in this case preventing cyber warfare means to make sure that it does not happen.

Prosecuting

When we prosecute someone, we initiate civil or criminal court action against them so that they get punished for their actions. Prosecuting cyber warfare involves taking hackers and those committing cyber warfare to court and ensuring fair punishment.

Cyber warfare

Richard A. Clarke, a government security expert, defines cyber warfare as “actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.” It is a conflict based on the Internet involving political attacks on specific networks and information systems. These attacks can easily disable complex systems, websites or even essential services. They can also steal secret classified data and communicate it to adversaries. They even have the potential to destroy financial systems, in other words create macro economic crises.

Hacker

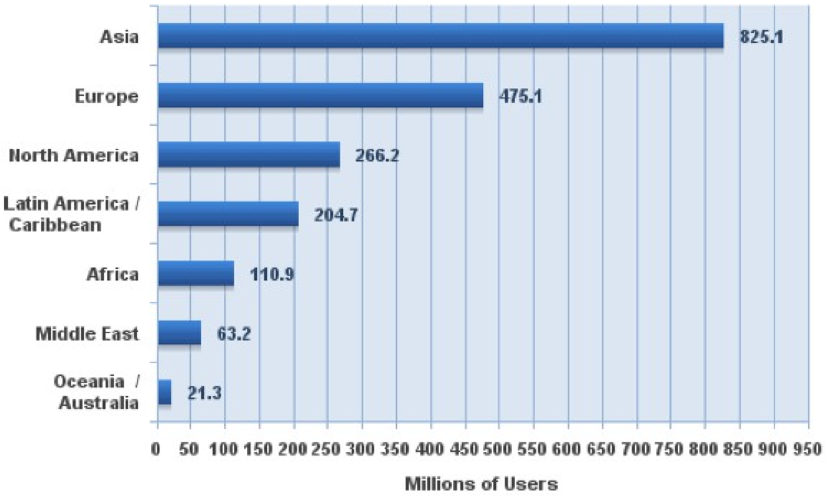
A hacker is known as a person who is specialized in computers and usually attempts to hack in other people’s computers in one way or another. Hackers are sometimes able to hack into very complex cyber systems.

General Overview

Internet

In cyber warfare the core of the issue is *internet*. Internet is basically where cyber warfare originates. It is a very unsafe system that any human being can access. No nation or individual can be protected from Internet. According to the Internet World Statistics, the Internet is used by approximately 2 billion people in the world. All these human beings, whether civilians or not can be affected or involved into various types of cyber warfare.

Internet Users in the World
by Geographic Regions - 2010



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Estimated Internet users are 1,966,514,816 on June 31, 2010
Copyright © 2010, Miniwatts Marketing Group

Cyber warfare between individuals

Cyber warfare between individuals is very similar to cyber warfare between nations. Individuals use mal-ware hosting websites to hack into many computers. Not long ago a young man managed to hack into the white house's system. This proves that any specialized person in computer can hack into any network or systems such as banks and governments.

With so many civilians using the internet, it has become inevitable that civilians will get involved in or effected by cyber warfare. The civilian realm is at risk, noting that the security breaches have already gone beyond stolen credit card numbers, and that potential targets can also include the electric power grid, trains, or the stock market.

Hackers are now focusing on gambling sites but also networking sites. This field is very interesting to them because there is a lot of information to be collected. Facebook or any other social networking site can easily be hacked, a hacker can add you as a friend and gain information about you, or simply send you a file infected with mal-ware.

Major Parties Involved and Their Views

North Atlantic Treaty Organization (NATO)

NATO is very involved concerning cyber warfare because they consider it as a very pressing issue. Over the last few years, NATO has been dealing with several cyber attacks. They have decided to take measures in order to combat these attacks and protect their information bases. In order to defend their databases against hacking they implemented very high standards of defense, such as a cyber defense policy which consists of people hired to analyze serious threats and regarding their information.

McAfee .Inc

McAfee is the largest company in the world that provides internet security against any type of virus. In 2010, they released The Annual Virtual Criminology Report (VCR), it mentioned that cyber warfare was not an issue that should be underestimated because it had officially moved from 'fiction to reality'. It also mentioned that many nations were secretly spying on each other's systems and that they were all individually developing very sophisticated cyber weapons that they were planning to use in the future. The president of McAfee.Inc said that "There is little doubt that the impact of cyber war will extend beyond military networks. As our dependence on Internet technology grows so does the need for thoughtful discussions on political conflict in cyberspace."

The People's Republic of China

China is rapidly moving towards incorporating cyber warfare into its military actions. Ever since 1997, they have used the concept of Net force, meaning a strong reserve force of computer experts trained at universities, training centers and sometimes academies, these chosen people are usually quite young and very bright. China's cyber warfare is expanding so fast that it caused a deep concern in some other member's states military leaders as it could increase the amount of cyber attacks they receive. China's military have used civilian computer experts in clandestine cyber attacks aimed at American companies and government agencies.

The Russian Federation

Russia as a nation is very divided on the issue of cyber warfare. Some believe it is a very severe crime, ranking it right after nuclear warfare in terms of severity. However, the other portion believes that cyber warfare is a weapon that can be used wisely and see it as a great advantage on their enemies because they can view secret information and databases. In the past Russia has used cyber attacks to disarm its enemies. They have used it against Estonia in 2008, during the South Ossetia War, and they have also cyber attacked Georgia.

United States of America

The USA has been very involved in cyber warfare, especially regarding cyber weapons and specific defense to combat cyber attacks. They have used cyber warfare several times against Iraq in attempts to destroy their financial system. In order to fight terrorists or decrease the level of terrorism they have also used cyber attacks to spy on their cell phones, computers and other various types of communication devices that the Taliban might have been using to spy on them. After numerous very successful cyber attacks the USA are also a great target for their adversaries. So many Americans citizens are connected to internet that they could easily lose a cyber war against a nation with fewer internet users.

Israel

Due to the unstable situation of Israel, cyber warfare has occurred a lot over the past few years. The Israel Defense Forces (IDF) decided to take action in cyber warfare because they realized which big impact it had . During the 1990's they created a specific infrastructure for cyber warfare, this helped Israel acquire very destructive cyber weapons. This made Israel one of the leading countries in the cyber warfare. Not only they were attacking other nations with their cyber weapons but they also had a very clever defending system that the Israel Security Agency (ISA) created to protect themselves from cyber attacks.

United Kingdom

The United Kingdom have recently implemented the Regulation of Investigatory Powers Act (RIP) . This allows the UK to read and intercept any e-mail and if there are any suspicions they can require a decryption of the personal file found.

Timeline of Events

Date	Description of event
1982	The Soviet spies stole computer control system from the Canadians; this made the Soviet pipeline line explode.
1998	The United States hacks into Serbia's air defense control to facilitate the bombing of Serbian targets
1999	NATO accidentally bombs the Chinese embassy in Belgrade, spawning a wave of cyber attacks from China against U.S. government web sites
2005	Brazil receives a very destructive cyber attack that affected tens of thousands of people by an unknown attacker
2006	During the war against Hezbollah the Israel Defense Force (IDF) used cyber weapons against them to have an advantage on their strategy.
2007	McAfee accuses China of cyber attacks towards India, The United States and Germany
2007	Israel cyber attacks Syria for war reasons
2008	Cyber attackers hijack government and commercial web sites in Georgia during a military conflict with Russia
2009	The United States and North Korea were violently cyber attacked by an unknown nation
2009	The U.S. enters into talks with the Russian Federation about cyber warfare and security
2010	Cyber war breaks out as Iranians hack into Chinese search engine
2011	IMF targeted in big cyber attack

UN involvement, Relevant Resolutions, Treaties and Events

- Threats to international peace and security caused by terrorist acts, 2010 **(S/RES/1963)**

- Creation of a global culture of cyber security and the protection of critical information infrastructures, 2003 **(A/RES/58/199)**

- Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures, 2009 **(A/RES/64/201)**

Evaluation of Previous Attempts to Resolve the Issue

The UN's General Assembly wrote a resolution about the hostile use of technology. There has been a lot of controversy because barely any nations agree with each other on the matter. Some nations do not want it to be forbidden as they use it often to spy on their rivals, whilst other nations want it to be forbidden or at least well regulated because they receive varieties of cyber attacks.

Some experts use this resolution as a base started to try and find constructive solutions by first developing a much clearer understanding of what exactly is cyber warfare because not all member states and non member states agree on what is actually classified as cyber warfare. This was a first small step towards solving the issue of cyber warfare. According to Jose Cancela, the Chairman of the Disarmament and International Committee, many delegations were looking forward to create a treaty in order to create a strong cyber security. This was only in 2010 so the treaty is still on its way to being composed.

In May 2010 the Secretary General of the International Telecommunication Union (ITU) proposed to create a treaty to regulate cyber war with the aim of stopping cyber warfare completely between nations. No nations were obliged to help create that treaty or to agree to it so of course the nations using cyber warfare as an advantage did not see the point in contributing to the construction of such a treaty. In the end, barely any nations were wishing to help compose this treaty so the project was abandoned. One of the main problems that makes the issue of cyber warfare so difficult to tackle is that international cooperation is what would be required to address it, and so far nations have not shown willingness to cooperate with each other.

According to this new report by the East-West Institute, an international treaty to establish regulations for computer security might be unattainable. "It could take years to arrive at a global treaty on cyber security, since many states are not ready for it, and perhaps never will be.”

Possible Solutions

“A cyber war would be worse than a tsunami - a catastrophe,” the UN official said. Action needs to be taken to prevent and prosecute cyber warfare. Although it is a very complicated issue which leaves many nations in disagreement, there are numerous possible solutions to help prevent and prosecute cyber warfare. These solutions come in a set of four: prepare, defend, detect and legal consequences. We can prevent it if countries guarantee to protect their citizens and their right to access to information, promise not to harbour cyber terrorists and should commit themselves not to attack each another. In order to prevent it, cyber reports could be published; indicating which networks and data should be off-limits. Also, educating civilians to be careful when communicating significant information via unsafe networks should be considered. In terms of defense and detection, computer systems should be strengthened and nations should develop offensive weapons in the means of increasing security codes to prevent mal-ware. The UN must prosecute cyber warfare in order to prevent it as well. Legal consequences should be strictly enforced against those that do not comply with cyber restrictions in order to effectively prosecute hackers and those committing cyber warfare. The other possible solution would be the challenging one of creating a proper international treaty in order to regulate cyber warfare.

Bibliography

"Cybercrime and Cyber Warfare and the Effect on the Society | Cyber Warzone." *Cyber Warzone | Cyberwarfare and Cybercrime Revealed*. Web. 25 July 2011. <http://www.cyberwarzone.com/cyberwarfare/cybercrime-and-cyber-warfare-and-effect-society>.

"Cyberwarfare." *Wikipedia, the Free Encyclopedia*. Web. 25 July 2011. <http://en.wikipedia.org/wiki/Cyberwarfare>.

"Cyber Warfare." *Wikia.com*. IT law wiki, n.d. Web. 25 July 2011<http://itlaw.wikia.com/wiki/Cyberwarfare>.

"Cyberwarfare Market 2010-2020." *Companiesandmarkets.com*. N.p., 25 July 2011. <http://www.companiesandmarkets.com/ Summary-Market-Report/cyberwarfare-market-2010-2020-195409.asp>.

"Cyberwarfare and Its Damaging Effects on Citizens." *Infosec Island*. Web. 25 July 2011. <https://www.infosecisland.com/documentview/11904-Cyberwarfare-and-Its-Damaging-Effects-on-Citizens.html>.

Dewalt, Dave. *Virtual criminology report 2009*. 2009. PDF file."INTERNET USAGE STATISTICS The Internet Big Picture World Internet Users and Population Stats." *Internetworldstats.com*. miniwatts marketing group, June 2010. Web. 25 July 2011<http://www.internetworldstats.com/ stats.htm>.

IQPC. "CYBER WARFARE 2011: EUROPE'S LEADING CYBER WARFARE CONFERENCE." *cyberwarfare-event.com*. N.p., n.d. Web. 25 July 2011. <http://www.cyberwarfare-event.com/Event.aspx?id=386992>.

Motley, Setton. "In the event of cyber attack, Let's rely on and trust...the government?" *Washingtonexaminer.com*. N.p., 2010. Web. 25 July 2011. <http://washingtonexaminer.com/blogs/examiner-opinion-zone/ event-cyber-attack-let-s-rely-and-trust-government>.

Ophard, Jonathan A. "CYBER WARFARE AND THE CRIME OF AGGRESSION: THE NEED FOR INdivIDUAL ACCOUNTABILITY ON TOMORROW'S BATTLEFIELD." *Law.duke.edu*. Duke law & technology, 2 Feb. 2010. Web. 25 July 2011. <http://www.law.duke.edu/journals/dltr/articles/2010dltr003.html>.

"Various case histories." *wikipedia.org*. N.p., 2010. Web. 25 July 2011.

<http://en.wikipedia.org/wiki/Cyberwarfare>.

"What is cyber warfare?" *Searchsecurity.techtarget.com*. Tech Target, 25 July 2011 <http://searchsecurity.techtarget.com/ sDefinition/0,,sid14_gci1405599,00.html>.

Zimmerlin, S. "Improving regulations concerning cyber warfare." Special Political and Decolonisation Committee. January 2011. HMUN 2011.