Name of the committee : Security Council
Issue : Discussing a framework for international response in mitigating potential conflict escalation in cyberspace
Name of the chairs : Jeanne Puech, Michael Miller

Discussing a framework for international response in mitigating potential conflict escalation in cyberspace

Introduction

Facebook, Twitter, LinkedIn… Digital networks are embedded in all our economies and our political and social life. They have become a central tool for human activity and the functioning of governments. These networks form cyberspace - the new potential battlefield of the 21st century. They hold information of immense value, and they control machinery that provides crucial services. Even though they create immense economic benefits, they are also a major source of risk to countries. Because of the newness of this technology in our world, the lack of explicit agreement among states, and the rise of cyber-espionage and cybercrime, this unstable environment invites miscalculation and misinterpretation, and inadvertent escalation of conflict. Changing this requires identifying which instruments of statecraft are most effective and where we may need new institutions, norms, and laws. Progress in cybersecurity requires manipulating complex international processes to change what governments consider to be acceptable behavior in cyberspace.

a. Key words (Definitions)

Cyberattack: A cyberattack is a software program transmitted over digital networks and installed on a target machine to disrupt data or services or even destroy machinery.

Cyberwar: A cyberwar is the application of force between two or more major actors using cyber techniques. It is a very recent form of conflict.

Hacker: A hacker is a person with great computer skills who uses computer software to gain access to illegal and classified data. The hacker can have diverse motivations, including political ("hacktivism", cyber-terrorism…), personal, or financial reasons.

Cyberspace: Cyberspace is the virtual computer world where communication over computer networks occurs. It allows users to share information, interact, swap ideas, play games, engage in discussions or social forums, conduct business and create intuitive media, among many other activities.

Virus : A computer virus is a written program with the aim of spreading sneakily and quickly to other computers. It disrupts, more or less severely, the functioning of the infected computer.

Overview of the issue

b. History and origins of cyber attacks

i. First worms and viruses

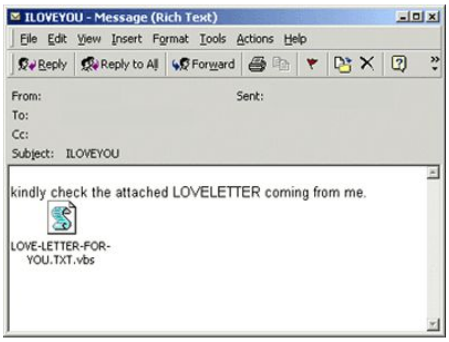
1. First computer worms

The first computer worm was created in 1988, by Robert Morris. In less than a day, the worm affected approximately 10% of the 60,000 Internet-connected computers across the United States. Even if the infected systems were cleaned or rebooted, the worm would return and re-infect them. Each infection reportedly cost between $200 and $53,000 to remove and, according to the U.S. General Accounting Office, as much as $100 million may have been lost due to the Morris worm.

The Morris worm served as a wake-up call for the information security industry. But it also draw attention all around the world to the potential danger posed by computer viruses and the need for strong protections.

2. First viruses

ILOVEYOU is one of the most well-known and worst computer viruses of all time. It was spread through an email with a subject line that said “I love you” in 2000.

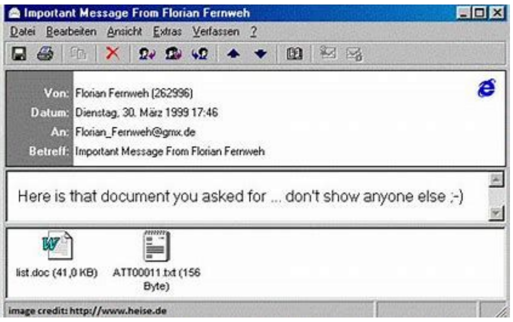

ILOVEYOU - Message (Rich Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

From: Sent:
To:
Cc:
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

LOVE-LETTER-FOR-YOU.TXT.vbs

Melissa is a fast-spreading macro virus that is distributed as an e-mail attachment. It was accompanied by the message “Here is the document you asked me for... do not show it to anyone”. In just a few days, it starred in one of the most important cases of massive infection in history, causing damage of more than 80 million dollars to American companies. Companies like Microsoft, Intel and Lucent Technologies had to block their Internet connections due to its action.



Important Message From Florian Fernweh
Datei Bearbeiten Ansicht Extras Verfassen ?

Von: Florian Fernweh (262996)
Datum: Dienstag, 30. März 1999 17:46
An: Florian_Fernweh@gmx.de
Betreff: Important Message From Florian Fernweh

Here is that document you asked for ... don't show anyone else ;-)

list.doc (41,0 KB)
ATT00011.txt (156 Byte)

image credit: http://www.heise.de

The Melissa and ILOVEYOU viruses infected tens of millions of PCs, causing email systems around the globe to fail, all with little strategic objective or clear financial motivation.

These threats led to the development of antivirus technology in order to spot the signature of the virus and prevent it from executing. Equally as important, these threats also played a huge role in driving the awareness of computer users of the risks of reading emails from untrusted sources and opening their attachments.

ii. Cyberwar between nations

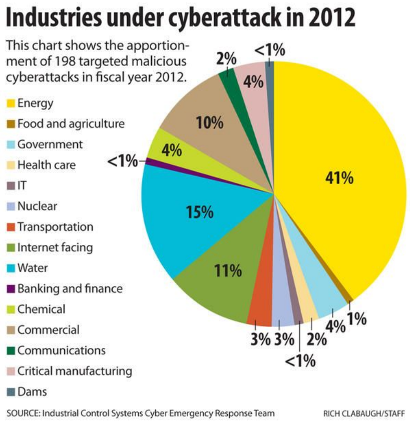
Organized hackers based in China were responsible for a series of hacks against American government offices and businesses. In 2015, the United States Office of Personnel Management was hacked which resulted in over 20 million government employees' sensitive information being leaked, including some confidential information about intelligence community officials. While government officials and experts have told the press that the evidence demonstrates that the Chinese government was responsible for this breach, the US government has not made an official statement on Chinese government involvement, and Chinese state media has denied any government involvement in the hacks, stating it was carried out by criminals within China. In recent years, numerous hacks against businesses around the world have also been identified, perpetrated by groups ranging from underground hacking collectives like Anonymous, to cyber-wings of military organizations such as the Syrian Electronic Army or ISIL. The objective of these hacks has been to steal government secrets, cripple infrastructure, or co-opt communications systems, which angers corporations and governments wishing to protect their interests, their information, and their security.

Sometimes cyber attacks can have more tangible effects. In 2009, the US and Israel allegedly launched the Stuxnet virus against Iranian nuclear enrichment facilities and destroyed roughly a fifth of all Iranian centrifuges by making them spin out of control. In 2007, Estonia was targeted by Russian sympathizers for wanting to remove a Soviet statue from the capital, Tallinn. Several prominent government websites were hacked, and essential government services were disrupted. In December 2013, he credit and debit card information was stolen from over 40 million shoppers at Target stores over the holiday season. After it was announced, people avoided shopping at Target and the company lost 46% of its profits and had to pay over $10 million in damages to affected shoppers. Some analysts warn this is only the beginning. As the internet and internet-linked technology become more widespread, the potential danger of cybercrimes increases. If nothing is done to combat this scourge, almost nothing can be considered safe. Smartphones could provide hackers with a wealth of financial and other private information from its users. Stock markets could be manipulated to wipe out entire economies overnight.

Clearly this is an issue which needs to be addressed and the only way to address it is through international dialogue and cooperation.

c. The impact of cyber attacks

i. Cyberattacks and the environment



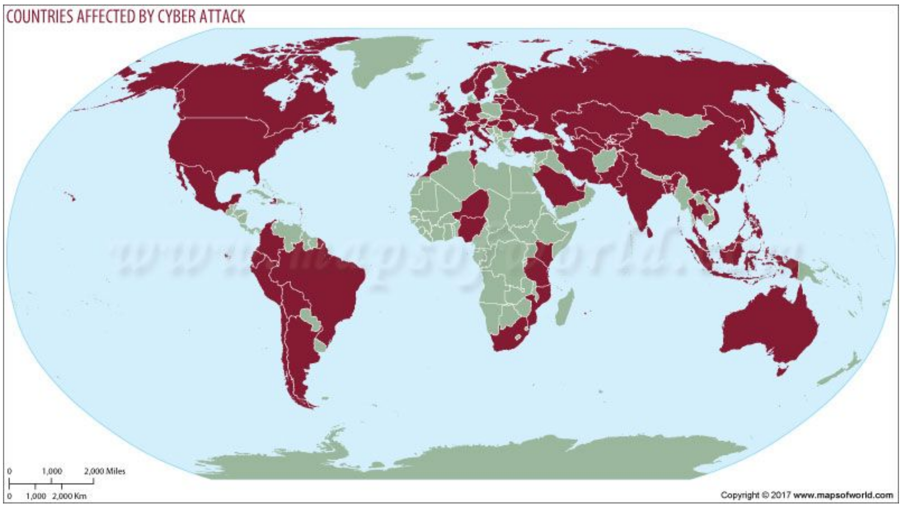
Managing cybersecurity is a tall order for industrial infrastructures and even taller for industries whose activities deal with natural resources: water treatment plants, oil drilling platforms, nuclear plants, etc. All of these sites are choice targets for hackers. If they fall victim to a cyberattack, the consequences for the environment could be disastrous. To prevent these risks these industrial sites must, at all costs, integrate cybersecurity into their processes.

Today, many industrial systems control installations that have an impact on the environment, whether water treatment plants or plants that use chemical processes, such as SEVESO sites. All activities within these infrastructures are run by interconnected automatic controllers which are sometimes connected to the internet. As a result, these systems are not always well protected and are extremely vulnerable to cyberattacks.

An attack on these types of infrastructures could have serious consequences above and beyond just a mere data leak. Verizon's report “Data Breach Digest” describes how hackers interfered with a water treatment plant in the United States by modifying the dose of chemicals used to treat water. As it's usually the case, the attackers narrowed in on an easy target with little protection but did not have an intention of causing damage to this particular plant. Unaware of how the pumps regulating doses worked and with little knowledge of how the plant ran in general, the attackers did not cause substantial damage. However, this example illustrates how carrying out a targeted attack with little to no preparation can have an impact on the general population.

d. Who is affected and in which way

If cyberwar happened, any society using computer networks to communicate or keep their data could be a victim of hacking, which means that every single nations would be in danger. All government data could be destroyed, taking out health care records, birth certificates, social care records and so much more essential information to the functioning of our societies. The transport system would be shut off, traffic lights would be blank, immigration would become chaos and all tax records could disappear. The internet could even be reduced to an error message and daily life as everybody knows it would be completely different. Power plants and water treatment facilities could be switched off, leaving people without basic necessities.


COUNTRIES AFFECTED BY CYBER ATTACK
www.mapsofworld.com
0 1,000 2,000 Miles
0 1,000 2,000 Km
Copyright © 2017 www.mapsofworld.com

Case studies :

A. “Patriotic Hackers” Attacks – 1999-2001

Actors Involved

- The United States and its North Atlantic Treaty Organization allies (NATO)
- Serb and Russian hackers
- American hackers
- Dutch hackers
- Chinese hackers
- China

Actions

During the Kosovo war, hackers from the United States, Serbia, Russia, The Netherlands and China attacked sites belonging to the belligerents and related actors.

Power Relationships

These attacks are perhaps the first instance where the episode can be called a “cyberwar”, because they were connected to the ongoing physical war in Kosovo.
The USA and Chinese responses to the cyber attacks originating from its territory were distinctly different. The USA made it clear to its citizens that it did not encourage

patriotic hacking, given that "such activity is illegal and punishable as a felony." China, on the other hand, did little to encourage its own hackers to stop. This is shows the dissimilar views of the Internet as a tool for foreign policy.

Evidence suggests that at least some of the hackers were regular citizens, not involved in politics, the military or espionage, and with very limited actual political or military power. Cyberspace offered them the opportunity to be actors in the war with very limited risks.

Outcome

One main consequence of this series of episodes is the emergence of cyber as a domain for warfare. Although shows that the consideration of cyber defense since at least two decades before 1999, the potential consequences should Kosovo related attacks been more successful "could have been devastating"; this in turn showed the world, and military powers in particular, that "the Internet is no longer just a side issue."
Most of the attacks concerned in this case have been classified as cyber terrorism. The official response of the USA was to shut down the DOE website until clarifying how the hackers managed to gain access. The White House also closed its site for a few days as a preventative measure following hijacking attempts.

B. Chinese Cyber Espionage, 2005-2012

Actors Involved

- China Agencies include "the Ministry of State Security (MSS), the Ministry of Public Security (MPS), the Second Department of the People's Liberation Army General Staff Department (2PLA), or the Liaison Office of the General Political Department."
- Hacker groups based in China
- The United States, its allies, and over a hundred countries as the targets of the attacks
- Private firms in diverse economic sectors, mostly in technology

Actions

Mainland China-based groups perpetrated intrusions into systems in the United States, its allies, and other countries, both for commercial and State-sponsored espionage.

Power Relationships

The head of the US National Security Agency and Cyber Command has estimated the loss for American companies in intellectual properties at 250 billion per year. This is an enormous incentive to denounce and try to stop the Chinese espionage.
That, however, has not been the case, with few exceptions such as Google denouncing what has been called "operation Aurora". In the private actors case, denouncing China could lead to Beijing making it harder for them to do business there.

Considering the rapid Chinese economic expansion, and the fact that the middle class there is larger than the entire population of the United States, it is a commercial choice not to publicly denounce Chinese intrusions.

The USA and China, as the world's two biggest economies, are also economically interdependent. Only in USA Treasury Bonds, China is reported to own 1.25 trillion. This, and the need for cooperation in geopolitical issues such as Syria and Iran, may complicate USA government public attempts at denouncing Chinese cyber espionage.

Outcome

Companies might have other reasons for not defying China publicly: although the intellectual property fight seems to be rising in the United States, fighting that fight in China may be more difficult; besides the different Chinese framework for intellectual property, there might be little gain in trying to prosecute a Chinese hacker and recover the loss, since any enforcement would require diplomatic efforts, which may not be available for small companies.

The Cox Report, the result of a US House of Representatives commission, concluded that China had gained access to "advanced US thermonuclear weapons."

A small California-based company (Cybersitter) claims its software was basically stolen by the Chinese government for use in the Green Dam Project, the massive firewall preventing millions of Chinese users to access contents ranging from pornographic sites to politically oriented portals. The company states the Chinese government owes it 2.2 billion. The suit, however, had limited chance of success because it was done in a U.S. court, with the alleged criminal activities taking place in China. Following the suit, the company received a cyber attack, presumably from China. The Chinese hacking group identified by Mandiant (a cybersecurity firm) as APT1, is involved in economic espionage, attacking companies in many industries, and stealing commercial information.

C. Estonia receives cyber attacks from April 17th to May 18th, 2007

Actors Involved

- Estonia
- Russia
- Estonian private actors, including newspapers, technical associations, banks and individuals
- Public and private actors from NATO allies, particularly Finland, Israel, Germany and Slovenia
- Russian and Russian-Estonian hackers

Actions

Following an ongoing political controversy over a World War II monument, Russians conducted a series of attacks to official and commercial websites in Estonia.

Power Relationships

The motivation for the attacks can be traced to earlier in 2007, when Estonia had announced it would move a WWII monument (the Bronze Soldier) from the center of its capital Tallinn, to a cemetery outside the city. The monument carried strong symbolism for ethnic Russians living in Estonia and Russians alike, as it represented the Soviet victory over Nazi Germany (Russian decision-makers asked Estonia not to move the monument). For some other Estonians, however, the monument was a symbol of Russian oppression during the USSR regime (Estonia became independent only six years earlier in 1991).
As Estonia qualified the attacks as being of Russian origin, International cooperation, including several European countries and Finland in particular, arose.

This included individual foreign technical professionals, ISPs, network companies, and other private and public actors. The attacks were traced back to Russia, but the direct involvement of the Kremlin has not been proven. The price of hiring a botnet with sufficient bandwidth to perform the attacks was $75/day. This did not stop, however, Estonian politicians and senior media officials of attacking Russian government directly in the aftermath of the attack, and the event “continues to frame Russian-Estonian relations today.” The Estonian reaction may have been directed at discouraging future uses of cyber attacks to exert influence in international relations, particularly by Russia.

The cyber attacks are the central issue, the physical counterpart during the concerned period was present in the form of riots and street violence. Even though the actual perpetrators of the DDoS attacks were also located outside Estonia (presumably members of the Russian diaspora), these actions were a part of an ongoing clash among different ethnic populations in Estonia.

Estonia was an ideal target for a cyber attack because 97 percent of bank transactions occur online; and in 2007, 60 percent of the country's population used the Internet on a daily basis.

Outcome

Estonia became a cybersecurity hub after the attack.
The suspicions of Russia being involved directly are not irrational. Former Soviet states, such as Estonia, are of particular importance in Russian foreign policy, and diminishing Western influence in the region is a very likely goal of the Russian government.
The volume of the attacks, and their coordination over time, also make Russia a viable suspect.

The use of “ globally dispersed and virtually unattributable botnets” , and particularly those including computers used without the owner’s knowledge (as was the case in

Estonia), obviously makes prosecution of the culprits very difficult: “Estonian authorities made a few in-country arrests but never uncovered the main culprits, who were allegedly operating out of Russia”.

Possible solutions :

Today, we have reached the position in which cybercrime is so sophisticated it seems almost impossible to prevent. The emphasis is now on how a nation responds once it has been breached.

There are many challenges to creating an international framework for cybersecurity. Though the challenges are great, the potential danger of not doing anything is far greater. The problems posed by cybercrime are serious, but they are solvable. It is hoped the international community can put aside their differences and create a free and open Internet which is safe from cybercrime.

It has been argued that the Internet needs to be governed by an international agency which is responsible for answering to the international system as a whole and not individual parties. The Non-Aligned Movement has stated the need for independent control of some parts of their internet to guarantee the protection of defense secrets as well as the ability to guarantee internet use for the growth of their economy. However, the makeup of such a body is still being debated.

Another major problem with guaranteeing cybersecurity is the issue concerning how to hold nations and international actors accountable for their actions in cyberspace. Nations like Russia and China believe cyberspace should be controlled locally by various national governments and should respect cultural norms and national policy agenda if a state determines the need for this. In much of the West, people believe in a free Internet, but in less democratic countries leaders may feel threatened by a free internet and wish to control it directly. Coincidentally, this has sparked debate around the world about how much freedom individuals are willing to give up in order to maintain security online. Originally, the Internet was a completely free place where individuals could express themselves and feel free to come up with applications never thought of before. As the technology has become more widespread and available, dangers have arisen. There is a large debate concerning how much freedom should be allowed in cyberspace. If governments took more control over cyberspace, they could most assuredly be more effective in improving cybersecurity, but there is a risk they would also decrease the level of freedom permissible on the Internet. This debate is especially pertinent in the European Union where individuals are asking where to draw the line between security and
freedom of expression.

One of the major problems with guaranteeing cybersecurity is the sheer amount of data that makes up cyberspace and, coincidentally, the difficulty in monitoring it all. The United States has been better able to monitor cyberspace than many other nations, but this has created some difficulties within the international system. Some nations have viewed America as the greatest protector of cyberspace while others view it as its greatest threat. Increasingly, individuals have become more worried about privacy issues and leaks of government information from Edward Snowden which demonstrated US spying practices on foreign leaders have only increased this worry. Also, since most of the servers which contain the Internet reside within the United States, there is concern that the US has an unfair monopoly in cyberspace ownership.

Main international actors :

a. Main NGOs

A huge difficulty in combating cybercrimes is the enormous amount of data that needs to be monitored in order to catch the cybercriminals. Many NGOs have tried to monitor cyber activities and report on cybersecurity issues. The International Association of Cybercrime Prevention, also provides information and training about cybercrime prevention.

The Cyber Peace Foundation is another important NGO which is involved in “raising awareness, counseling, education, training and to reach out to citizens, governments, law enforcement agencies, private enterprises, NGOs working in cyber crimes and cyber security, universities, cyber security experts and bug bounty hunters; to provide a common platform on a global level.”

b. Countries

USA

The United States spent billions of dollars on joining the cyber capabilities of the Army, Air Force, Navy, and Marines. They are one of the top countries to be attacked in cybercrimes, and some of them are state-sponsored. But they are also one of the top countries that are able to cause a maximum of cyber-damage in a nation.

China

70 % of America’s corporate intellectual property theft is believed to originate from China.
The Foreign Policy magazine believes that the estimated range for China's "hacker army" personnel, is anywhere from 50,000 to 100,000 individuals.
Western countries have for a long time accused China of very aggressive espionage, and while investigations have traced various attacks on corporate and infrastructure computer

systems to have originated in China, "it is nearly impossible to know whether or not an attack is government-sponsored because of the difficulty in tracking true identities in cyberspace."

Russia
In 2018, Russian hackers successfully accessed U.S. Utility Control Rooms. Potentially state-sponsored hackers managed to breach one of the most significant systems, proving they have a powerful infrastructure.

Israël
About 10% of global sales of computer and network security technology comes from Israel. Technology is rapidly growing in Israel, with thousands of startups popping up every year. Tech companies bring immense value at tens of billions to israel.

UK
As a response to potential cyber warfare attacks from Russia as well as Iran, the UK plans to make their idea of becoming one of the world's top 5 cyber powers a reality.

Iran
Iran is behind attacks on dozens of sites from across the Middle East, North Africa, Europe, and North America. As stated in January 2019, Iranian cyber attackers could be responsible for a wave of hacks on government and communications infrastructure worldwide, one that will require a coordinated global response to fix.
This raises doubts about Iran's cyber warfare efforts being their latest contribution to global cyber crime statistics and trends. Additionally, Iran held its first cyber drill in 2012 and increased the budget dedicated to cyber operations by $20 million from 2013 to 2016.

c. Past actions in the united nations

The UN General Assembly, Economic and Social Council, and Security Council often stress the importance of cybersecurity and regularly call on member nations to fight cybercrimes. These organs usually refer responsibilities to the International Telecommunications Union (ITU) which is a UN agency based in Geneva and is responsible for coordinating efforts on those issues. They study cyber activity and set standards to which various governments are suppose to adhere to.

Guidelines for research :

It is important for delegates to keep the following questions in mind when brainstorming solutions to cybersecurity threats and potential conflict escalation in cyberspace:

a. What measures can be taken to improve the monitoring of cyberspace?
b. How can international actors be held accountable when they are found to have taken part in cybercrimes?

c. What steps can be taken to ensure a free, but safe Internet?

Bibliography :

Informations :

https://www.rand.org/pubs/monographs/MG1215.html
https://www.cfr.org/blog/avoiding-escalation-cyberspace
https://www.csis.org/analysis/conflict-and-negotiation-cyberspace
https://www.techopedia.com/definition/2493/cyberspace
https://thecyberwire.com/events/rsa2017/cyber-conflict-will-emerging-norms-keep-peace-with-escalation.html
https://news.un.org/en/story/2007/09/232832-estonia-urges-un-member-states-cooperate-against-cyber-crimes
https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/
https://thecyberwire.com/events/cycon-2017/international-law-and-confilict-in-cyberspace.html
https://www.sentryo.net/cybersecurity-and-environmental-risks/
https://www.theguardian.com/technology/2015/jun/05/cyberwar-hacking-attacks-nations-defence
https://www.newsweek.com/cyber-warfare-between-countries-look-488267
https://www.cybersecurityintelligence.com/blog/category/government-defence-11.html
https://cybertechaccord.org/uploads/prod/2019/04/FINALOASWP.pdf
https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2017/Sep-SEI/Ensuring%20Trust%

Pictures :

https://www.mapsofworld.com/calendar-events/technology-news/ransomware-cyber-attack-is-a-wake-up-call-warns-microsoft
https://www.cyberpeace.org/cyber-peace-dialogue/
https://www.pandasecurity.com/mediacenter/malware/most-famous-virus-history-melissa/
http://techviral.com/most-destructive-computer-viruses-ever/
https://www.paymentscardsandmobile.com/banks-merchants-struggling-keep-pace-cyber-threats/