Forum: Commission on Crime Prevention and Criminal Justice
Issue: The question of preventing cybercrime against governmental institutions
Main chair: Jakob Magnusson
Deputy chair: Alice Biscuola

---

1. Introduction

With the world around us modernizing exponentially as new technologies and techniques are invented and used, the western life has now evolved into revolving around the use of personal computers and the Internet. With so much knowledge available at our fingertips, we are living in a golden age of information. However, this comes with some very exploitable consequences.

Ever since the invention of the Internet, that many electronic devices are linked together and share a cloudspace, it has been possible for individuals with a vast knowledge of computing to access anything an individual, company, or governmental institution might hold dear. Personal photos, passwords, business strategies, nuclear launch codes - all of these have the potential of being accessed, obtained and used by hackers. Acts of accessing other people's information or causing havoc through hacking are classed as cyber-crimes.

Codebreaking is an age-old practice, however with the Internet being a relatively new technology, cybercrimes follow suit with its age.

Although cybercrime is prevalent on many different levels and scales, this research report will be focusing on cybercrimes on governmental institutions from both national and international sources.

2. Definition of Key Terms

Cybercrime: Criminal activities carried out by means of computers or the Internet.

Cyberwarfare: The act of launching attacks on other states and/or organisations through the usage of computer or the Internet to sabotage their activities and systems.

Computer crime: Committing an illegal offense by using computers and the Internet.

Worm (computer worm): A worm is a form of **malware** that self-replicates and then spreads from computer to computer through networks. Can have various uses and effects on infected machines.

Malware: Software that is specifically designed to disrupt, damage, interfere, or gain access to a computer system.

Software: Programs used by a computer that are installed within the components of a computer (as opposed to **hardware** which are the parts that make up a computer).

Trojan: A Trojan is something that pretends to be something else - the name comes from the fabled Trojan horse and the battle for Troj. Basically a piece of software that tricks the user into downloading it by looking like something the user would need, such as a fake anti-virus program.

Distributed denial of service (DDOS): A DDOS attack is when a network is attacked through the hacker sending countless (usually million or hundreds of thousands) of requests in very short intervals repeatedly to either view a website or access a file, which overloads its servers and makes the website or file unviewable and unusable.

3. History

The origin of cybercrimes

Cybercrimes are one of the most modern methods for committing illegal acts. The first acts of modern cybercrimes started around the 1970s, with programs such as “The Creeper”, which resembles a modern computer virus with the end goal to simply cause annoyance.

A very famous worm that surfaced in the late 1980s is the Morris Worm. This, now infamous, piece of malware gained access to over 6000 computers from government institutions and university systems. The creator of the worm, Robert T Morris Jr was a university student at the time and was eventually fined 10 thousand dollars and had to live through three years of probation.

The premise is that a new technology always attracts people that try and use it to cause havoc. This is no different when looking at computers and the Internet as a medium of spreading the chaos created by hackers and other software engineers. The computer just happened to be a very exploitable technology since it became so integrated in everybody’s daily life and jobs.

Modern examples of cybercrimes

In 2006, the city of Los Angeles experienced a strike where all the traffic engineers refused to work. Scared of someone tampering with their systems, the city blocked access to the computers that controlled the city’s traffic lights. Two of the strikers managed to hack themselves in though, changing around the timing of the lights in some key intersections to cause massive traffic blocks that ruined the traffic in the areas affected. No one was harmed, however it several days before city officials knew what was going on and fixed the problem.

In 2013, the US Navy was hit by an attack from people allegedly working for Iran. The hack was devastating as it exposed the weaknesses of the Navy’s systems and allowed access to many navy documents. The cost for the USA to remove the hackers was substantial as well, as they hired contractors to aid them in their efforts. The total cost was multiple millions of dollars.

One can see that as the Internet and computer technology has progressed throughout the years, so has magnitude of what a cyberattack can achieve.

One of the most well-known modern examples of cyberattacks and cybercrime are the alleged hacks of Russia tampering with the USA's elections to promote Trump. Although it has been proven that the Trump administration has worked with Russians throughout his campaign, proving that Russia tampered with the election is no easy feat.

4. Key Issues

The key issues when dealing with cybercrime can be grouped into different categories:

- Proving who/what the source is
- Increasing security
- Prevention of cybercrimes

Proving who/what the source is

On the international scene, many cyberattacks have occurred in our recent history. Some examples are when the US and Taiwan allegedly hacked their way to access files belonging to the Chinese Ministry of State Security, Russia allegedly hacking into Georgian computer networks and damaging official governmental websites, and in 2011 when 24,000 files were stolen digitally from the US Department of Defence by unknown hackers.

Reading that you might have noticed how in all three examples either the word "allegedly" or "unknown" was used. This is because it is very hard to find the source of cyberattacks, since there are numerous ways of masking one's tracks so it becomes near impossible to identify the source with 100 % certainty.

Increasing security

This goes along with the previous point about finding the source of cyberattacks. Since our most valuable institutions are at risk every day by hackers, it is a natural reaction to evolve modern computing to become more secure, to prevent attacks. The problem is that while

security becomes more complex, hackers get better. Although this can be seen as motivation and incentive for making security systems better, it also means that nothing is ever really 100 % secure.

Prevention of cybercrime

It is said that hackers, those who commit cyber crimes, hack because of one of the following reasons: They want to test their skills against the best security systems in the world (think Pentagon), they want to gain information otherwise inaccessible to the public (think WikiLeaks), they want to sabotage or promote something to further a cause (think Anonymous) or they want a monetary gain (think viruses that force you to pay money). Although this is a generalisation, it fits in with most cases of cybercrime.

The best way of dealing with cybercrime is to make sure it does not occur in the first place. Most viruses that computers get infected with are caused by sources such as malicious pop-up ads, virus-infected emails, and trojan software. To prevent these from becoming a problem, it is important that people are educated about the common and less common gateways for viruses to get into a computer. This is especially important since this topic focuses on cybercrime against governmental institutions, since a nation's most valuable information can be found in such places.

Apart from education, tracking and shutting down hacker groups is another option. This option does come with a lot of problems however, since all a hacker really needs to do damage is a laptop with access to the Internet. One's location is not very important.

Seeing as this might be too problematic for the police force to deal with, the only option that persists is to upgrade security, which was discussed above.

5. Major Parties Involved

The major parties of this issue include the United States of America, the People's Republic of China, the Islamic Republic of Iran, The Russian Federation, the State of Israel, the United Kingdom of Great Britain and Northern Ireland, The Democratic People's Republic of North Korea, and the UNODC.

The United States of America

The United States of America has in recent years expanded their focus on cyber warfare immensely through investments in education for staff, centralising the cyber-capabilities of the army, navy, marines, and air force under the same roof. Throughout the years the US has been accused of espionage and cyber attacks on multiple nations. One of the most well known cases is the so called “Stuxnet” worm that caused massive damage to the Iranian nuclear program back around 2009, which is around the time it was discovered. However, it is said that it had been developed since 2005 and been active since around 2007, meaning that it had lived for quite some time before that. Although it has been linked to the US and Israel, it has not been proven nor confirmed by any governmental agency where it originated from.

The US are currently taking many steps towards preventing cyber crimes, as stated, with the homeland security emphasising it, where they have the goal to stop cyber warfare as a whole.

The People’s Republic of China

China has lately been involved in multiple accusations of cybercrimes. There have been a large series of attacks on Australian governmental institutions that are being blamed on China for quite some years now. In March 2013 they allegedly hacked into the headquarters of the Australian Security Intelligence Organisation, while in 2015 they allegedly attacked the Bureau of Meteorology, and in 2016 the Australian government’s computer network was breached, to mention some of the events. China has naturally denied all these reports that have also been coming from Canada, India, and the US.

The Russian Federation

Much like the People’s Republic of China, the Russian Federation has allegedly committed their share of cyber crimes throughout history. As the common theme seems to be however, Russia has denied every single allegation. Many of these cyber attacks have been on other countries, such as two attacks, one in 2007 and one in 2008 on Estonia and Georgia respectively. The attack on Georgia is especially important to keep in mind since it was the predecessor to the Russo-Georgian War in 2008. During and before this war, Russia had

allegedly issued numerous DDOS attacks, which rendered sites such as the official Georgian President's website. An official from the Russian Defense Ministry once stated that "The issue of cybersecurity is a most topical one at present. It is particularly important to prevent the militarization of the virtual space; whereas the Tallinn Manual is a step in exactly that direction. Its approach to the issue at hand is far from perfect. And the assessments made in it appear one-sided". In the quote the official Konstantin Peschanenko was referring to the Tallinn manual, which is a document containing international rules on cyber terrorism, cyber space, and cyber-attacks. The statement can be seen as Russia's official view on cybercrimes, however with all the cases where Russia has allegedly performed numerous cybercrimes one might find it hard to believe that they are actively trying to put a stop to the issue.

The State of Israel

An article published in 2013 claimed that experts have estimated that Israel is faced with roughly 100,000 cyber-attacks daily. Because of this, the Israel Electric Company set up state of the art so-called "Cyber Gyms" where they are training IT professionals in how to combat cyber warfare. The state of Israel seems determined to develop new countermeasures to combat cyber-attacks. Israel does however not escape any allegations of them performing cybercrimes themselves, as they are linked to the Stuxnet virus (more info in the section on the US).

The United Kingdom of Great Britain and Northern Ireland

As it seems to be a hard task finding cases where the UK allegedly performed cybercrimes, the UK has one of the world's largest intelligence agencies. This said, the UK has very recently been the victim of hacking attempts allegedly from North Korea and Russia, where UK banks, energy companies and the UK parliament have been targets. The UK does have the so-called NCCU, the Nation Cyber Crime United, which responds to and provides countermeasures for combating cyber crimes.

The Democratic People's Republic of North Korea

As mentioned in the previous paragraph, North Korea has allegedly been involved in a series of cyber-attacks on the UK, and South Korea especially. These alleged attacks have been

used to put North Korea in a more powerful position in the world, as they have now recently been in the spotlight following their Nuclear threats towards namely the US.

The United Nations Office on Drugs and Crime (UNODC)

In 2013 the UNODC produced a comprehensive study on the topic of cybercrimes, which marked their start of involvement in the issue. The UNODC mainly work with afflicted by cybercrimes and cyber-attacks to help combat the attacks and the issues that arise from them. They do not only work with national agencies, but also regional agencies to help solve problems related to cybercrimes.

6. Timeline

1971	The Creeper virus is spread
1988	The Morris Worm spreads across the US, causing massive problems for those infected by it
2006	The city of Los Angeles' traffic engineers go on strike with two of the strikers hacking the traffic light systems, causing massive congestions at key intersections
2006	Nasa blocks all received emails that have attachments in fear that they could sabotage a shuttle launch
2007	Russia allegedly hacked the Estonian government's systems, causing problems to the country's banking systems and online services
2007	The US secretary of Defence's email was hacked and information which would later

	lead to attacks on the Pentagon
2007	The US and Taiwan allegedly hacked their way into obtaining files belonging to China's Ministry of State security
2008	Russia allegedly hacked Georgian computer networks using DDOS attacks in order to make certain services unavailiable
2009	Russia allegedly hacked into Israel's infrastructure during the Gaza strip offense
2010	The Stuxanet virus was found
2013	First edition of the Tallinn Manual was released, which provided a study on how international law applied to cyberspace
2013	Allegedly North Korean hackers hacked financial institutions and a broadcasting channel in South Korea
2013	UNODC Produce the "Comprehensive Study on Cybercrime"
2017	The second edition of the Tallinn Manual was released, so called Tallinn Manual 2.0, which expanded upon the original Tallinn Manual
2017	UK was targeted by hackers that allegedly came from North Korea with the intentions of embezzling money and cripple networking systems

7. Evaluation of Previous Attempts

Since the problem of cyberattacks still is very prevalent today, we can assume that it has been hard trying to find ways of stopping attacking and dissuading people from not performing cyber-attacks.

The Tallinn Manual is a great example of how to solve the problem. It includes information on how cybercrimes are related to international crimes. Although Russia has deemed the first edition of it to be a good step, it was not good enough to satisfy them. Luckily, however, the producers of the Tallinn Manual have worked on improving it, releasing the second edition called the "Tallinn Manual 2.0", which is supposed to be an improved version of the first release.

As great as one can think the Tallinn Manual is, it has the great drawback of not being legally binding, meaning that it is up to each state whether or not to follow the guidelines it presents. This can be seen as both a success and a failure. The success being that there are now guidelines for states to follow regarding the legality of a topic that is too many people very ambiguous. The failure however is that it is, once again, not legally binding.

Another previous attempt is the NATO creating the Cooperative Cyber Defense Centre of Excellence. The goal of the CCDCOE is to develop the defensive capabilities of protecting those at risk from cyber-attacks through the mediums of cyber warfare and cyber terrorism. This has succeeded through its ability to bring states together to cooperate and develop existing defence systems. The CCDCOE is perhaps not a failure in itself, however it is a part of NATO, which limits the group who are member of it, something one can see as counterproductive.

8. Possible Solutions

Seeing as it is hard to determine who did what and how they should be punished, due to alliances between many of the great and super powers in the world creating obvious biases, a favourable solution could be to make the UN's International Court of Justice mandate cases where two states are involved in some form of cyber conflict. Bringing up an issue previously mentioned, being able to tell who committed cybercrimes with absolute certainty is a

prerequisite for this to work however, since the ICJ must be able to put blame where blame is due, and not arrive at a sentence based on alleged blame. Because of this, it would be handy to develop some sort of system that makes it possible to track down the sender of cyber-attacks.

This could be done through the creation of a major IGO that would monitor and actively track the cyber activity of states.

Further research and development in computing and defence mechanisms should also be a favourable solution, whilst developing better offensive tools would be completely counterproductive. There is already ongoing cooperations with anti-virus software giants such as McAfee and Kaspersky, where they help research and develop defence systems. Creating an international research facility for this research could be favourable, albeit a bit risky, since representatives from many different states would be present and able to possibly spy on any progress.

Naturally, it is up to you as a delegate to form a solution that is both in the interest of your delegation and, preferably, the rest of the world. I can only hope that this rather lengthy guide has been somewhat useful in gaining an understand of the topic at hand. Please do use the sources I have used, and the useful links found in the “appendices” section to further your research. Looking forward to seeing you all in November!

//Jakob Magnusson - Main Chair of CCPCJ

9. Bibliography

1. *A Brief History of Cybercrime*, www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html.
2. Agt. "United Nations Office on Drugs and Crime." *United Nations Office on Drugs and Crime*, www.unodc.org/.
3. "CCDCOE." *CCDCOE*, www.ccdcoe.org/.
4. "China Military Seeks to Bring Cyber Warfare Units Under One Roof." *Bloomberg.com*, Bloomberg, 2015, www.bloomberg.com/news/articles/2015-10-22/china-military-chiefs-seek-to-unify-cyber-warfare-operations.
5. "Combating Cyber Crime." *Combating Cyber Crime | Homeland Security*, www.dhs.gov/topic/combating-cyber-crime.
6. "Creeper." *Malware Wiki*, malware.wikia.com/wiki/Creeper.
7. "Cyber Crime." *FBI*, FBI, 2017, www.fbi.gov/investigate/cyber.
8. Experts say it's still far too early to say whether North Korea was behind the outbreak of ransomware attacks that has affected hundreds of thousands of computers since Friday. "Ransomware: North Korea's History of Cyber Attacks." *CNNMoney*, Cable News Network, money.cnn.com/2017/05/16/technology/ransomware-north-korea-hacking-history/index.html.
9. Four Corners

   By Linton Besser, Jake Sturmer and Ben Sveen. "Chinese Hackers behind Defence, Austrade Security Breaches." *ABC News*, 2016, www.abc.net.au/news/2016-08-29/chinese-hackers-behind-defence-austrade-security-breaches/7790166.
10. "Full List." *Treaty Office*, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
11. Gavin, Harvey. "Hacking Warning: Kim Jong-Un's Henchmen to Step up Cyber Attacks and Target City of London." *Express.co.uk*, Express.co.uk, Jan. 2017, www.express.co.uk/news/uk/861007/north-korea-hackers-target-uk-banks.
12. "Iran Hacked US Navy Computers." *Security Affairs*, 2013, securityaffairs.co/wordpress/18171/hacking/iran-hacked-us-navy-computers.html.
13. "Israel's New 'Cyber Gym' Trains Cyber-Warfare." *Israel National News*, Dec. 2013, www.israelnationalnews.com/News/News.aspx/174712.
14. Landesman, Mary. "What Is the Stuxnet Worm Computer Virus?" *Lifewire*, www.lifewire.com/stuxnet-worm-computer-virus-153570.

15. MacAskill, Ewen, and Rajeev Syal. “Cyber-Attack on UK Parliament: Russia Is Suspected Culprit.” *The Guardian*, Guardian News and Media, 2017, www.theguardian.com/politics/2017/jun/25/cyber-attack-on-uk-parliament-russia-is-suspected-culprit.
16. Markoff, John. “Before the Gunfire, Cyberattacks.” *The New York Times*, The New York Times, Dec. 2008, www.nytimes.com/2008/08/13/technology/13cyber.html?mcubz=0.
17. McCormick, Rich. “Iranian Hack of US Navy Network Was More Extensive and Invasive than Previously Reported.” *The Verge*, The Verge, 2014, www.theverge.com/2014/2/18/5421636/us-navy-hack-by-iran-lasted-for-four-months-say-officials.
18. Nakashima, Ellen, and Joby Warrick. “Stuxnet Was Work of U.S. and Israeli Experts, Officials Say.” *The Washington Post*, WP Company, Feb. 2012, www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.62a95172a3aa.
19. Nate Anderson
    - Jun 1, 2012 10:00 am UTC. “Confirmed: US and Israel Created Stuxnet, Lost Control of It.” *Ars Technica*, Jan. 2012, arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/.
20. “National Cyber Crime Unit.” *National Crime Agency - National Cyber Crime Unit*, www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.
21. Newtek - The Small Business Authority. “How To Prevent Cyber Crime.” *Forbes*, Forbes Magazine, Nov. 2014, www.forbes.com/sites/thesba/2013/08/28/how-to-prevent-cyber-crime/#226c03b3fffd.
22. “Pentagon Source Says China Hacked Defense Department Computers.” *Fox News*, FOX News Network, www.foxnews.com/story/2007/09/04/pentagon-source-says-china-hacked-defense-department-computers.html.
23. “Pentagon Source Says China Hacked Defense Department Computers.” *Fox News*, FOX News Network, www.foxnews.com/story/2007/09/04/pentagon-source-says-china-hacked-defense-department-computers.html.
24. Quarterly, David J. Smith inFocus. “Russian Cyber Strategy and the War Against Georgia.” *Atlantic Council*, www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia.

25. Siegel, Matt. “China behind 'Massive' Cyber-Attack on Australian Government: ABC.” *Reuters*, Thomson Reuters, Feb. 2015, www.reuters.com/article/us-australia-cybersecurity/china-behind-massive-cyber-attack-on-australian-government-abc-idUSKBN0TL08M20151202.
26. Smith, Ned. “The 3 Most Common Types of PC Virus Infections.” *LiveScience*, Purch, 2010, www.livescience.com/6355-3-common-types-pc-virus-infections.html.
27. “Tallinn Manual Process.” *CCDCOE*, Aug. 2017, ccdcoe.org/tallinn-manual.html.
28. “UN Rejects International Cybercrime Treaty.” *ComputerWeekly.com*, www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty.
29. “UNICRI :: United Nations Interregional Crime and Justice Research Institute.” *UNICRI :: United Nations Interregional Crime and Justice Research Institute*, www.unicri.it/.
30. Uhlmann, political editor Chris. “China Blamed for 'Massive' Cyber Attack on BoM Computer.” *ABC News*, Feb. 2015, www.abc.net.au/news/2015-12-02/china-blamed-for-cyber-attack-on-bureau-of-meteorology/6993278.
31. “WikiLeaks.” *Wikiwand*, www.wikiwand.com/en/WikiLeaks.
32. Williams-Grut, Oscar. “REPORT: Russia Hacked UK Energy Companies on Election Day.” *Business Insider*, Business Insider, 2017, www.businessinsider.com/russia-hacked-uk-energy-companies-election-day-2017-7?r=UK&IR=T.
33. Keith Breene, Formative Content. “Who Are the Cyberwar Superpowers?” *World Economic Forum*, www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

akara.umapornsakula.

34. “United Nations Office on Drugs and Crime.” *Cybercrime*, www.unodc.org/southeastasiaandpacific/en/what-we-do/toc/cyber-crime.html.
35. olga.lanchenko. “United Nations Office on Drugs and Crime.” *Use of the Internet*, www.unodc.org/unodc/en/terrorism/news-and-events/use-of-the-internet.html.

10. Appendices

The appendices section must include any relevant internet links or further areas of research that delegates should conduct. At least 3 appendices are required, and they must be numbered using Roman Numerals. All appendices must be hyperlinked.

I. The CIA Factbook - Great resource for information about states https://www.cia.gov/library/publications/the-world-factbook/

II. The United Nations Official Document System (ODS) - For finding previous resolutions https://documents.un.org/prod/ods.nsf/home.xsp

III. Article about combatting cybercrime produced by the US Homeland Security https://www.dhs.gov/topic/combating-cyber-crime

IV. Article about cybercrime produced by the FBI https://www.fbi.gov/investigate/cyber

V. Link to the EU convention on cybercrime http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

VI. Article by the UNODC about "Countering the use of the Internet for terrorist purposes" https://www.unodc.org/unodc/en/terrorism/news-and-events/use-of-the-internet.html

VII. Information about and a link to the Tallinn Manual 2.0 https://ccdcoe.org/tallinn-manual.html

VIII. Link to the CCDCOE https://www.ccdcoe.org/

IX. Link to the UNODC's "Comprehensive Study on Cybercrime" https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

X. Link to the UK website for the National Cyber Crime Unit (NCCU) http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit