Forum: Special Conference

Issue: Countering the Rising Cyber Security Threat

Student officer: Daria Leus

Introduction

It is difficult to imagine our lives without the Internet. Both – private customers and legal entities depend on global network. Undoubtfully, the Internet is a distinctive invention, yet not everybody is aware of the dangers it may have. Perhaps, one of the main and most frequent concerns is cyber security. In the past few years this question has become even more vital, with the rise of hacking, cyberattacks on governmental institutions and online fraud, which have affected private consumers, as well as big companies. Indeed, cybercrime is a huge sector and it continues to grow. Something needs to be done with this issue as soon as possible.

Definition of key terms

Cybersecurity - the protection of internet-connected systems, including hardware, software and data, from cyberattacks.

Cybercrime - a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes); cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes.

Computer hacker - any skilled computer expert that uses their technical knowledge to overcome a problem. While "hacker" can refer to any skilled computer programmer, the term has become associated with a "security hacker" - someone who, with their technical knowledge, uses bugs or exploits to break into computer systems.

Phishing - the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

Spamming - the use of messaging systems to send an unsolicited message (spam), especially advertising, as well as sending messages repeatedly on the same site. The most widely recognized form of spamming is email spam.

Child pornography - a form of child sexual exploitation; federal law defines child pornography as any visual depiction of sexually explicit conduct involving a minor (persons less than 18 years old); images of child pornography are also referred to as child sexual abuse images.

Hate crime (also known as a bias-motivated crime or bias crime) - a prejudice-motivated crime which occurs when a perpetrator targets a victim because of his or her membership (or perceived membership) in a certain social group or race.

Malware - any software intentionally designed to cause damage to a computer, server, client, or computer network.

Background information

To speak about cybersecurity, it is necessary to know how it all began. Here is the brief history of the Internet, as it is where cybercrime was born and has been developing ever since.

A communication network was first created in the 1960s by the United States Advanced Research Project Agency (ARPA). The primary goal of the network was to enhance the speed and effectiveness of government research teams, allowing scientists and researchers to share information and collaborate at a distance. New devices were added, and the network's existence was eventually publicized in 1972 at the International Computer Communication Conference. As more and more devices were added to the network, the ARPANET would eventually grow into Internet. In little more than two decades after the first successful tests of ARPANET, the Internet had been opened up to the public, and it had already begun to affect the lives of so many[i].

That is when hackers were "born". To the general public a "hack" became known as a clever way to fix a problem with a product, or an easy way to improve its function. The

first hackers started to learn about the computer code and ways of changing it. Some of their hacks were so successful that they were able to replace the original code or system.

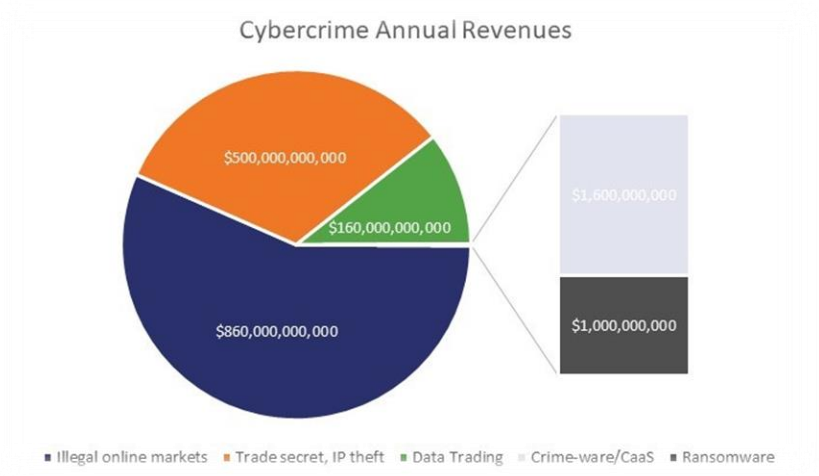
Hacking first became associated with crime when the early computerized phones became widely used. These hackers (at the time called “phreakers”) discovered the correct codes and tones that would help them get free long distance service. Basically, they stole long distance telephone time. And as more complex communication became available, cyber crime got more and more opportunities to develop.

A very big case was the discovery of the Morris worm virus, created by Robert Morris, a Cornell University student. This virus damaged more than 6,000 computers and resulted in estimated damages of $98 million. More incidents began to follow, so The Congress of the US passed its first hacking-related legislation, *the Federal Computer Fraud and Abuse Act*, in 1986. The act made computer tampering a felony crime punishable by significant jail time and monetary fines[ii].

Yet cybercrime continues its development, no matter what rules and legislations are set to discontinue these undoubtfully malicious actions.

Current situation

Today the problems have only become more complicated. The technological, monetary and human resources spent on cybercrime are huge. In 2018 alone, cybercrime has created over 1.5 trillion dollars[iii], the diagram shows the various aspects their income consists of:



As mentioned earlier, cybercrime is a quickly growing sector. Global cybercrime damages are predicted to cost over $6 trillion annually by 2021 (Official Annual Cybercrime Report 2017)[iv].

According to Cyber Security Media, 300 billion passwords will be used by 2020. That's a lot of passwords, all of which require cyber security protection. If not, that's 300 billion potential threats, worldwide.

By 2020, CSO Online predicts ransomware attacks will be quadruple. The healthcare industry gets attacked more than most industries. Healthcare industries should not give into demands and ensure their data is safe and backed up. Phishing emails are particularly common in this sphere.

Over 24,000 malicious mobile apps are blocked daily. Symantec's Internet Security Threat Report details that lifestyle apps are the main targets. The majority of these apps leak sensitive information like device location and the user's phone number. It would be completely impossible to monitor or check each of these apps for vulnerability issues. It's essentially an open ticket for cyber criminals to do their worst[v].

These are just several examples of how cyber criminals may steal our data, personal information and then use it to manipulate and compromise us.

Relevant information and UN resolutions

Internet protocol suite

A conceptional model which provides end-to-end data communication specifying how data should be packetized, addressed, transmitted, routed, and received[vi].

The Federal Computer Fraud and Abuse Act[vii]

A United States cybersecurity bill that was enacted in 1984 as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in *the Comprehensive Crime Control Act of 1984*.

Up until now, no resolutions concerning cyber security issues have been adopted by the UNSC (UN Security Council). The resolutions of other UN Committees (including the General Assembly) are recommendatory and legally non-binding on the Member States.

Since 1998, the Russian government has annually introduced a draft resolution in the First Committee (Disarmament and Security) on *'Developments in the field of information and telecommunication in the context of security'*. With gradual changes, the non-binding resolution has been adopted by the UN General Assembly (UNGA) each year.

UNGA resolution 2001: Developments in the field of information and telecommunication in the context of security[viii]

One of the points calls upon creating a group of governmental experts (GGE), consisting of experts from 15 states, chosen on the basis of equitable geographical distribution, for a study to consider existing and potential threats in the sphere of information security and possible cooperation measures to address them.

UNGA resolutions 2002[ix], 2003[x], 2009[xi]: Creation of a global culture of cybersecurity

The first resolution is a broader document, the last two are expanded to include the issue of protecting critical information infrastructures.

UNGA resolution 2000[xii], 2001[xiii]:

Combating the criminal misuse of information technologies - a specific focus on combating the criminal misuse of information technologies.

UNGA resolution 2013[xiv]:

The right to privacy in the digital age – emphasizes the responsibility of states to respect and protect privacy, and, for the first time, notes that the same rights that people have offline must be protected online[xv].

Possible solutions

1. States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;
2. Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;
3. Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

4. Legal systems should protect data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;
5. Cyber security courses should be held in all educational facilities in order to raise awareness in society.

Useful links and resources

[i] https://blog.eero.com/arpanet-foundation-internet/

[ii] https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/

[iii] https://www.thesslstore.com/blog/2018-cybercrime-statistics/

[iv] https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

[v] https://www.vpngeeks.com/21-terrifying-cyber-crime-statistics-in-2018/

[vi] https://en.wikipedia.org/wiki/Internet_protocol_suite

[vii] *https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act*

[viii] https://ccdcoe.org/sites/default/files/documents/UN-011129-ITIS.pdf

[ix] https://ccdcoe.org/sites/default/files/documents/UN-021220-CultureOfCS.pdf

[x] https://ccdcoe.org/sites/default/files/documents/UN-031223-CultureOfCandCI.pdf

[xi] https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf

[xii] https://ccdcoe.org/sites/default/files/documents/UN-001204-CriminalMisuseIT.pdf

[xiii] https://ccdcoe.org/sites/default/files/documents/UN-011219-CriminalMisuseIT.pdf

[xiv] https://ccdcoe.org/sites/default/files/documents/UN-131218-RightToPrivacy.pdf

[xv] https://ccdcoe.org/un.html