ΚΕΔΙΣΑ KEDISA

ΚΕΝΤΡΟ ΔΙΕΘΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΑΝΑΛΥΣΕΩΝ

CENTER FOR INTERNATIONAL STRATEGIC ANALYSES

Cybersecurity as a challenge of XXI century

Aleksandra Pecak

Research Paper No. 65

ΚΕΔΙΣΑ KEDISA
ΚΕΝΤΡΟ ΔΙΕΘΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΑΝΑΛΥΣΕΩΝ
CENTER FOR INTERNATIONAL STRATEGIC ANALYSES

Research Paper no. 65

Cybersecurity as a challenge of XXI century

Aleksandra Pecak

Analyst Kedisa

Cybersecurity as a challenge of XXI century

I. Introduction

The concepts of cyberspace and cybersecurity are often discussed yet rarely understood. Through the years, cyberspace has come a long way to become a second reality. Along with the increasing interest in cyberspace, crime has also developed in this area. Selected aspects mentioned in this article are the components of the present situation in this regard.

II. Actors in Cyberspace

Cyberspace protection is focused on criminal acts, which are performed by individual states, initiates numerous pathologies and deviates from the norm. It causes the rise of plenty of new illegal acts (identity theft, terrorism, blackmail). Crimes in cyberspace are on the agenda, it is proven by numerous publications as well as events taking place in the international arena.

The dependency of cyberspace is dictated by many features such as: unlimited range, universalism or low operating costs; it results in individuals being more open and willing to move their activities to the Internet(sale, product placement and work).

The state of an individual's awareness about cyberspace does not equal a high level of interest. The lack of basic knowledge about cybersecurity, safety of data or your own safety in the web implicates further problems, because this process of continuous technological and developmental changes, many, if not the most of the society can not function without Internet access. Chats, e-mails, social portals are the focal point, which undergoes the process of sustainable development.

Without any doubt, the opportunities contribute to many important achievements, but it would be unwise to take only one part into consideration. On the other hand are threats, which are a natural consequence of forbidden acts such as leading the illegal actions against local and even international regulations. Terrorists and criminals, protected by-anonymity, do not hesitate to cooperate in order to achieve a main goal which is a financial gain. For the purposes of this article, I have selected three types of actors which can be spotted in cyberspace, which common denominator will be cybercrime.

Activists	Terrorists	Criminals
Declaring support for an idea by aggressively promoting, using tools of wide range and coverage.	Engaging activities by single states or groups for selfish political objectives. Their main weapon is intimidating and invoking the state of threat. They are using cyberspace to recruiting volunteers or spreading propaganda.	In this aspect the scene has only changed. The criminal main goal is to achieve a financial gain, or any other private gain by frauds, thefts or scamming.[1]

[1] https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/

Each one of those violations is regulated by the penal code. Despite numerous social campaigns that make citizens aware, crimes are still being committed. False domains or apps are benefiting the ignorance of users, who are not fully aware, as I proved in the beginning. Crimes such as scam or theft are mostly carried out on these types of websites. It is happening everyday, but the major problems are cyberattacks targeted at the important institutions in the government. To visualise the severity of the problem I will show a few examples of the most popular cyber attacks during last years.

III. The biggest hackers attacks

- Estonia DDoS

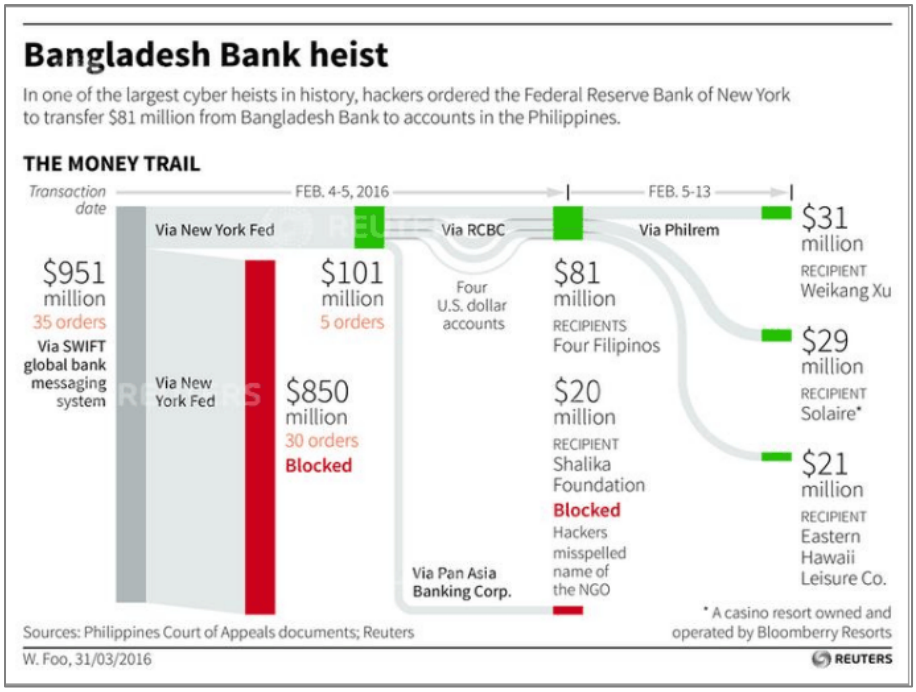
It started in 2007 when the most wired country in Europe - Estonia, was a victim of a long lasting hacking attack. So far, this event is widely regarded as the first ever act of cyber warfare in the world. The spontaneous actions of pro-Russian actors targeted Estonian governmental, financial, political and online services. The attacks were dynamic, synchronized, changing in response to counter-measures and ceasing at a precise time. The diversity of attack tools nearly blocked the whole Estonia's internet.

The attack was a response to the relocation of a Soviet war memorial - The Bronze Soldier. This Baltic country lost productivity, opportunity cost, remediation, even the alternative web hosting at emergency rates estimated in billions of Euros. The attack could have costed the government losing trust of their citizens, but the quick response and the support from NATO surely prevented widespread public distrust.[2]

- Bangladesh Central Bank

Hackers ordered about 30 transfers in the name of Bank of Bangladesh using the SWIFT authorization codes. BAE[3] proves that vulnerabilities in SWIFT made it easier for hackers to attack. They got caught by making a mistake in the name of one of the receivers of the transfer. The money was stolen from a Bank of Bangladesh account using the Federal Reserve Bank of NY.

[2] Andreas Schmidt, "The Estonian Cyber Attacks", January 2013
[3] BAE Systems - electronics, security, information, technology and support services.



- River City Media

In 2016 an improperly configured backup accidentally placed the entire database online. That accident was the largest single data breach in history. About 1.4 million addresses and records were placed online. This highlights how easy a simple mistake can go from private to public within seconds.

- Sony Entertainment

In November 2014, Sony Pictures was hacked by “Guardians of Peace". A group working for North Korea was trying to commit an act of terrosism against movie theaters. The hackers had taken a lot of private databases, deleted the movie copies from the servers, and left threatening messages. The main reason was the upcoming movie *The Interview* - a comedy about assassination Kim Jong Un. After this situation, Sony Entertainment was struggling for days to repair the damage.

The US government position was clear: North Korea was responsible for the attack, even though they denied it.

After several weeks, the "Guardians of Peace" posted files they had stolen from Sony's servers such as Sony movies, confidential documents about upcoming performances, employees, and their salary, but the company decided to release the movie in some theaters. Month after they got 8 messages demanding to "stop showing the movie of terrorism"[4]. In Mid-December the FBI announced that "has enough information to conclude that the North Korean government is responsible for these actions."[5] Which made the GOP to stop their actions.

This situation clearly shows us that the accident still establishes a precedent that makes it harder to get the risky projects made.

- Yahoo

The cyber attack on one of the biggest companies is not accidentally in the first place. It took place in 2014 and has the same background as The River Media attack. Hacker known as "Peace" was showing the world that he is going to sell 200 milion Yahoo accounts. Emails, phone numbers, names, passwords were owned by "Peace". During the following days, the number was still increasing to stand by 500 million users' data.

[4] Emily VanDerWerff, Timothy B. Lee, *The 2014 Sony hacks, explained* https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea#:~:text=In%20late%20November%202014%2C%20Sony,information%20off%20of%20Sony's%20network. 3.01.2015

[5] FBI National Press Office, *Update on Sony Investigation*, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation 19.12.2014

One of the problems is a weak link in digital defences. Many server domains ask similar security questions which is not a problem for a hacker. The stolen data is only a part of that program making. User information such as the email address might be a potential tool for a hacker to break into your bank account.

It was easier for "Peace" because many people on Yahoo had the same password everywhere. Unfortunately, as soon as one password had been broken, all of them were. After this huge data leak Yahoo invalidated cookies used in the security breach, and asked users to change their passwords.

Those few examples prove how careful we need to be while taking next steps.

IV. Cyberspace - an alternative reality

Related to the process of globalization, the Internet during last years has become an alternative reality; transaction making, selling, trading, interpersonal contacts all these factors make up the whole cyberspace.

Data transfer runs smoother and faster between individual institutions or countries so the term "cybersecurity" goes beyond a single state. It becomes a complex problem for all states, who are taking part in the process. Comprehensively provided service helps to strengthen both sides of the relationship. Enriched with the knowledge of attacks on the most popular companies, we pose an important question: Can a real threat of a cyber attack result in use of the NATO article 5?

"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."[6]

It changes the imagination of an attack that we know of. Before the era of the Internet, an attack was associated with using force or arriving troops into the enemy's country. After the beginning of the Internet, the concept has been redefined because of the following questions: How can an attack which takes place in cyberspace be described? How can we clarify an act of committing a crime that we have not seen?

Cyberspace does not have a specific address or a real localization. There is no clear answer to one of the questions above. However, there is an answer that exhaustively explains and regulates international cooperation.

[6] North Atlantic Treaty, Washington D.C, 04.04.1949

As a member of the North Atlantic Treaty Organisation it is our responsibility to follow the third article: "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack."[7] It is, without any doubt the best answer which even commands us to cooperate with member states in case of any danger.

V. Expansion of terrorist groups

Preventing terrorist attacks is an absolute priority of each state, for example the terrorist threat against the US government remains persistent and acute. Threats are posed by foreign fighters, also recruited from the US, traveling to join the Islamic State of Iraq and the Levant (ISIL). ISIL shows how aggressive they are, promoting their campaign, attracting like-minded extremists all around the world. ISIL has persistently used the Internet to communicate and spread its message. From a security perspective, it is ISIL's widespread outreach through the Internet and particularly social media which is most concerning. The organisation blends traditional media platforms, glossy photos, and social media campaigns that can become popular just in a few seconds. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago. The clue is to spread the message as fast as possible.[8]

The first and basic capability, access to the Internet, has changed the way individuals radicalize and plan attacks. As an example I will lighten the Islamic State in Malaysia. They are focused on training and tactical planning involving basic tools like cars or knives, which can be used by everyone in each part of the globe. This combination made terrorism available for masses. Malaysia's technological background is important but not crucial for operations with less innovative barriers.[9]

The key to ISIS development is the terrorist intent. In this case, external and internal pressures have influenced a completely new generation of people who are ready to use technology for terrorist reasons. The geographical threat area is expanding due to ISIS transitions to more conventional terrorist networks. As a result, policy makers would and definitely should make some adjustments to technological conditions into their project of emerging ISIS hotspots. Malaysia is providing a significant case study in the showing up threat of remotely inspired attacks in spite of a widespread internet access, encrypted message service or proliferating use of VPN's. There is only one purpose: to mobilize single states into movement.[10]

---

[7] North Atlantic Treaty, Washington D.C, 04.04.1949

[8] Colin P. Clarke, *How ISIS Is Transforming*, https://www.rand.org/blog/2017/09/how-isis-is-transforming.html 25.09.2017

[9] Seth Harrison, *Evolving Tech, Evolving Terror*, https://www.csis.org/npfp/evolving-tech-evolving-terror.

[10] Michael Steinbach, *ISIL Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media, https://www.fbi.gov/news/testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media- 6.07.2016*

It is essential for terrorists to have the internet connection which changes the way of thinking and organising attacks. Most of the online servers offer more opportunities to accelerate the speed with which individuals radicalize and mobilize. Once a jihadist is mobilized he usues the web for communication and operational planning.

Internet usage in Malaysia is increasingly more common, 68% of citizens are connected to the Web. When it comes to the age of 18-34 year olds, that rate is even higher, almost up to 100%.[11]

Those outputs make ISIS choose the malaysian youth group as a main target of their recruitment efforts. They are starting from the sending device, through the cell tower and server, ending by the receiving device. In their applications all messages are encrypted which allows for every move because of the unprecedented operational security which is limiting law enforcement's ability to view or disrupt those informations. Finally, the same method works backwards, as a defence mechanism. The VPN network guarantees private connection to the internet by replacing the users provider address with one of the VPN providers. In consequence effectively anonymizes the activity of the user. This single tool prevents them from tracking their actions or intentions.

Similarly developed countries such as Malaysia have advocated for stronger key disclosure laws, which can protect their data or even called telecommunication companies to build a backup. In case of an emergency it gives the law enforcement access to the encrypted messages. More realistic approaches involve defensive counterterrorism resources.

The law enforcement should focus on new ways of preventing attacks and a possibility how to mitigate the effectiveness of attacks. A different perspective of this problem solving showed up in Europe right after several attacks using a ramming vehicle. This still increasing awareness of many types of violent attacks can be used as an instrument for preventive efforts and as a main key in featuring their threat assessments.

People have different opinions, experiences and importantly their past. For some, terrorists are irredeemable and the defence strategy should be fighting and murdering them, but not how intelligent people behave. Myriad citizens are thinking that counterterrorism strategy should focus on the fundamental definition of “terror”.
If counterterrorism will focus on technocratic character, apolitical approaches are required. Only a careful analysis of the technological possibilities fits right into this model. It shows both tactical and strategic considerations motivated by upcoming technologies and focusing even more on the defensive method. So the political questions are left aside.

[11] Suman Varandani, *ISIS Recruitment: 75% Of New Islamic State Group Supporters In Malaysia Are Recruited Online* https://www.ibtimes.com/isis-recruitment-75-new-islamic-state-group-supporters-malaysia-are-recruited-online-1936440 25.05.2015

However, as more people will have the internet access to the advanced technologies for eg. dark web. Counterterrorism efforts will need to stay flexible to easily adapt to a new situation.

VI. Conclusions

The development of cyberspace is, without any doubt, a positive impact for the civilization. It is beneficial as it has revolutionized the tech market. To accurately summarize, I will use the SWOT analysis as help. The opportunity is the increasing level of available resources, dissemination of the Internet as a way of communication and sharing data details on private servers. The threats are hackers working on behalf of individual organisations. The opposite effect is sharing sensitive data (bank accounts, addresses, phone numbers, contracts) with outsiders. Cyberspace became an alternative reality where there is no right institution as a position of power. So, hackers are fluently using programs or applications for identity theft or planning a terrorist attack. It changes the war as we know it from the past, and brings it to a different level. Dynamic changes are necessary to face the threat that awaits in cyberspace.

BIBLIOGRAPHY

1. https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/
2. Andreas Schmidt, “The Estonian Cyber Attacks”, January 2013
3. https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea#:~:text=In%20late%20November%202014%2C%20Sony,information%20off%20of%20Sony's%20network.
4. https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
5. North Atlantic Treaty
6. https://www.rand.org/blog/2017/09/how-isis-is-transforming.html
7. https://www.csis.org/npfp/evolving-tech-evolving-terror
8. *https://www.fbi.gov/news/testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media-*
9. *https://www.ibtimes.com/isis-recruitment-75-new-islamic-state-group-supporters-malaysia-are-recruited-online-1936440*