Cyber Attacks and Combat Behavior

Carataș Maria Alina
"Andrei Saguna" University of Constanta
mariacaratas@saguna.eu
Spătariu Elena Cerasela
"Ovidius" University of Constanta
ebarbu2001@yahoo.com
Gheorghiu Gabriela
"Ovidius" University of Constanta
gabrielag3110@yahoo.com

Abstract

Cyber terrorism is an intangible danger, a real over the corner threat in the life of individuals, organizations, and governments and is getting harder to deal with its damages. The motivations for the cyber-attacks are different, depending on the terrorist group, from cybercrime to hacktivism, attacks over the authorities' servers. Organizations constantly need to find new ways of strengthening protection against cyber-attacks, assess their cyber readiness, expand the resilience capacity and adopts international security regulations.

Key words: cyber terrorism, cyber-attack, cyber resilience, cyber readiness
J.E.L. Classification: K40, M20, M48, O34.

1. Introduction

Cyber terrorism consists in using new technologies to cause major injuries by organized groups and is an enormous threat to individuals, companies, and governments all over the world. Information stored online, computers and entire networks are constantly threatened or attacked and the phenomenon appeared when terrorism occurred encountered cyberspace. Nowadays, the incidence of attacks is on the rise, in the last year important attacks hit the entire globe, showing how vulnerable we are in front of cyber risks.

Cyber-attacks can take several forms, like online identity theft, hacking, malicious code, intellectual property loss, deliberate damage on computer systems

2. Attacks motivations

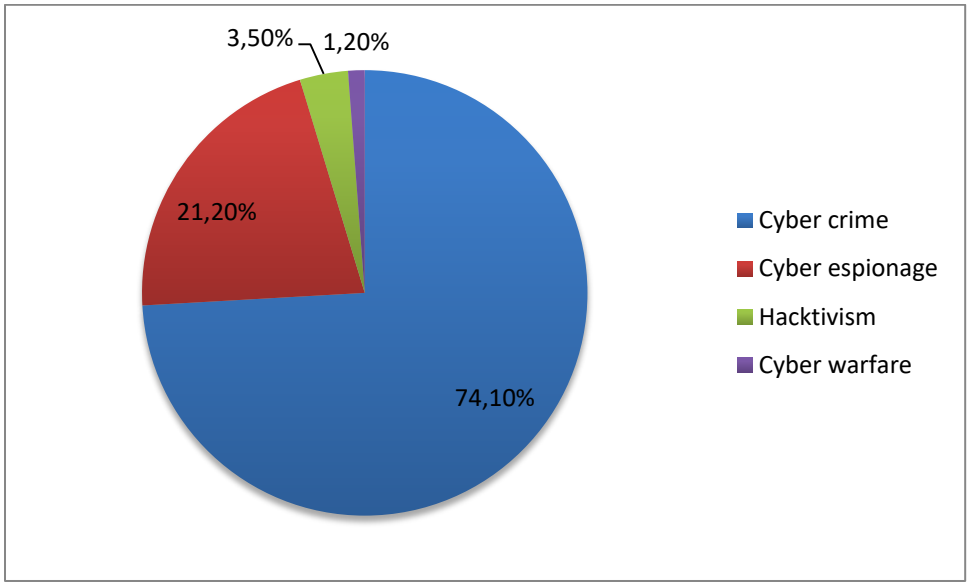
There are four main reasons behind the cyber-attacks according to statistics on hackmageddon.com, for April 2017:

Table no. 1 Motivations behind cyber attacks

Motivations	Percentage
Cybercrime	74,1%
Cyber espionage	21,2%
Hacktivism	3,5%
Cyber warfare	1,2%

Source: Author's projection after Hackmageddon statistics

Figure no. 1 Motivations behind attacks



Source: www.hackmageddon.com

Weimann associated cyberterrorism with a cloud, as we know the cloud is there in the sky and it may come but we do not know when it will come.

The online environment is very wide and offers the main tools for perfected attacks, as terrorist groups are trending all over social media, through group chats and forums, websites, YouTube, there are even online manuals about terrorism, there is access to ultimate speed tools in causing major harm.

3. Damages on organizations

Analyzing the influence of cyber-attacks on the organizations, we consider aspects of costs depending on the impact of the event and its nature. Some examples of damages that are difficult to quantify as they bring hidden costs are:

- the theft of intellectual property,
- data destruction,
- Economic cyber espionage.

The damage of the events counts additional costs, like:

- increases in the insurance premiums,
- a higher cost for credit due to lower credit-rating after an attack,
- operational dysfunctions due to the need of repairing equipment,
- arrange new infrastructure, business interruption
- losing credibility and value on clients relationships
- the loss in revenues from renewing contracts
- financial damage from branding devaluation

4. Cyber resilience

Organizations must reshape their cyber security regulations, going from prevention to a more active defense by preventing, detecting and responding strategy, evaluations, shaping a rigorous internal audit system.

Cyber resilience can be assessed by:

- measurements computed metrics,
- experiments,

- analytical judgment,
- Resilience capacity.

Strict security regulations can prevent cyber-attacks and forgery attacks. The General Data Protection Regulation program was adopted in 2016 and will be operating from May 2018 as a security data protection for European Union individuals. The program obliges companies to implement cyber security measures.

Big data security analytics is one of the cyber security solutions, by combining analysis of real and historical time so it identifies incidents, anomalies and providing solutions on vulnerabilities.

IT security or cyber security provide other security solutions for companies, by scanning the systems on a regular basis, monitoring them and in the case of identifying cyber-attacks and counter them by disconnecting the devices from the network and alerting the information owners about the danger.

Also, the G20 issued an *International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms,* aiming international stability in cyberspace. The act refers to the behavior in cyberspace according to the international law, promoting free will regulations of trustworthy state behavior during peacetime, developing and implementing confidence-building measures (CBMs) aiming stability in cyberspace, minimizing risks of wrong perception and escalation.

The program contains a series of tools available to counter cyber threats, like:

- diplomatic tools – communication with enemies is forbidden, assistance from allies is encouraged;
- use of law enforcement tools for crime investigation and prosecution of spiteful cyber players including international cooperation and mutual assistance, promoted by the Budapest Convention (2001);
- economic tools by applying financial sanctions;
- military capacity;
- Intelligence abilities.

A real challenge in counteracting cyber-attacks consists in delimitation between the cyber espionage and electronic surveillance. By using means of electronic surveillance is extremely easy to interfere with privacy invasions, intellectual property theft and violate either the International Covenant on Civil and Political Rights ICCPR and/or European Convention on Human Rights ECHR.

There are also legal framework against cyber-attacks or exploitation like the Economic Espionage Act (EEA) and Computer Fraud and Abuse Act (CFAA) in the United States, and Cybercrime Convention signed in Budapest

Analyzing all conventions we find it challenging to separate security espionage of surveillance and the main solution can be promoting domestic laws adapted from the international laws.

ISACA, formerly named as Information Systems Audit and Control Association is a nonprofit independent organization providing guidance and tools to information systems users. They realized a survey on the State of Cyber Security and gathered the findings in a report. The main ideas are the following:

- Companies find it difficult to hire professionals in cyber security positions
- The budgets on cyber security are growing but on a slowly manner
- The threats are expanding, the environment is unfriendly
- Major concern of cyber-attacks over the (IoT) the internet of things, replacing the mobile threats
- Ransomware – a malware that prevents the user in accessing their data by locking their devices until a ransom is paid (usually the attacker asks payment in cryptocurrency).

5. Conclusions

Cyberspace will always encounter risks, it is impossible to create an immune cyber system. But we can always improve the cybersecurity, making it stronger on attacks, keeping a continuous active cyber deterrence state. Companies need to work on response procedures for ransomware attacks. Also, organizations need to invest in their cyber security infrastructure, in training for the employees, even if they have problems in hiring qualified cyber security specialists.

We need to develop cyber readiness and cyber resilience as cyber-attacks are on the rise and get more and more sophisticated and prevention is the utmost security strategy. We also need to adopt both as individuals and especially in enterprises education programs for online behavior.

Scareware or ransomware is a developing business and we need to be perfectly conscious of this fact when searching for means of combat or response.

6. References

- *Banks W.C. Cyber espionage and electronic surveillance: beyond the media coverage, http://law.emory.edu/elj/_documents/volumes/66/3/banks.pdf*
- Convention on Cybercrime, 23.XI.2001 http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
- Convention for the Protection of Human Rights and Fundamental Freedoms. Rome,1950
- Convention on Cybercrime, 2001
- *Deloitte, 2017, Risk management, strategy and analysis from Deloitte, Seven Hidden Costs of a Cyberattack RISK & COMPLIANCE JOURNAL, http://deloitte.wsj.com/riskandcompliance/2017/05/17/seven-hidden-costs-of-a-cyberattack/?mod=WSJBlog*
- International Covenant on Civil and Political Rights, 1996, U.N.T.S. 171
- ISACA State of Cyber Security 2017: Part 2: Current Trends in the Threat Landscape, www.isaca.org
- *Weinmann G., 2015Terrorism in Cyberspace: The Next Generation, Woodrow Wilson Center Press with Columbia University Press*
- *http://www.hackmageddon.com/ accessed at 17th May 2017*