CURRENT TRENDS OF CYBER TERRORISM IN THE MIDDLE EAST AND NORTH AFRICA

Florentina-Ștefania NEAGU*,
Anca SAVU*,
Tiberiu TĂNASE*

Abstract

The phenomenon of cyber terrorism has grown globally and the states of Middle East and North Africa have not been circumvented, a major cause of the spread of the phenomenon is Internet users' access, so that in North Africa in 2000 the number of Internet users was 710,000 and in 2017 there were 102 million users; this means 45% of the total population of the region. Another factor is legislative shortcomings or even their absence, for many years Tunisia did not have a law on cybercrime instead of using the law on e-commerce. The same thing is happening in Morocco that uses the trade law.

Algeria and Egypt have no cybercrime laws, but publicly announced that then declare the cyberspace domain of national priority. The only states where there is no law on cybercrime, communications regulation or other laws on new technologies are Libya, Syria, Yemen, Iraq, and Kuwait. Attackers' motivations are money-related, infecting devices by sending malware via e-mail, commercial and industrial espionage. The tools they are using include: web app attacks, ransomware, targeted attack, defacement, espionage, insider threat, theft and physical damage, DDos, phishing and malware. Taking into account the political and economic evolutions in the region as well as globally, there is an upward trend in cyber terrorism.

Keywords: *cyber terrorism, dark web, information warfare, intelligence, risks.*

* PhD Student, Bucharest University of Economic Studies, Romania, Email: stefanianeagu15@yahoo.com

* PhD Student, National Defence University "Carol I", Bucharest, Romania, Email: ancasavu91@yahoo.com

* PhD Researcher, Division of the History of Science of the Romanian Committee for History and Philosophy of Science and Technology - CRIFST of the Romanian Academy, Romania, Email: tiberiutanase26@gmail.com

Introduction

Worldwide, the IT industry is experiencing steady growth by employing an increasing number of staff due to the emergence of new types of malware. According to Panda Security, daily, 230,000 new malware attacks are recorded at 39 seconds time interval. Most attacks have taken place within the retail and technology industry, small and medium-sized enterprises, but also against government institutions, because they have access to a high level of personal data but also because large amounts of money can be earned by providing the data decryption key. Attacks targeting companies include phishing, social engineering, bootnet, malware, Hackers' medium time to access a company's servers is 22 minutes (Ziffer, 2019). The main cause of these vulnerabilities in 95% of cases is given by human errors. At the end of 2018, the total cost of cybercrime was over 1 trillion dollars.

The main tools used by hackers

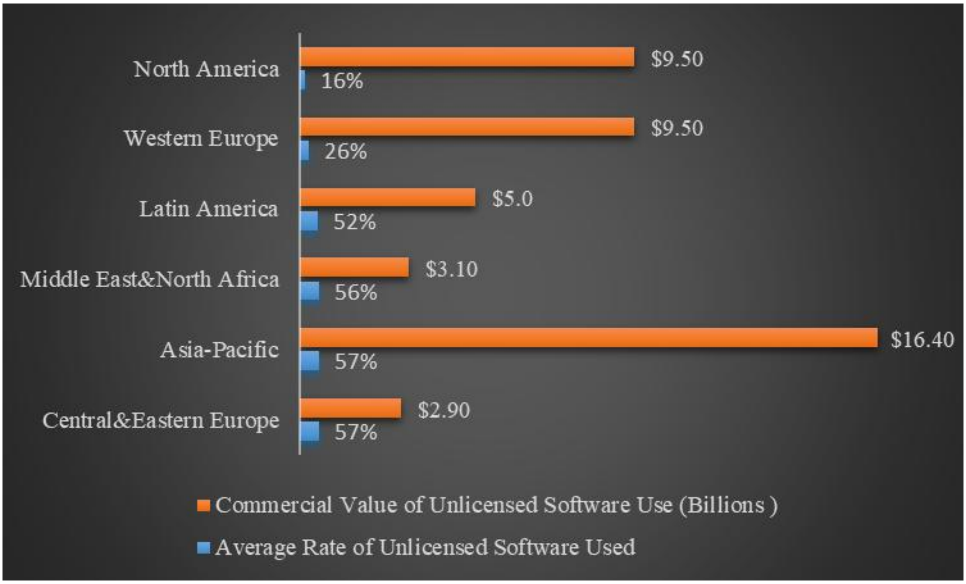
A study conducted by SciDevNet shows that there are 450 million internet users in Africa, which indicates an increase of 9.941% from 2000 and to 2018 with a penetration rate of 35.2%. The high level of Internet connection is accompanied by a high rate of software piracy, especially among African and Middle East countries. Cyber criminals mostly use infected computers fed to pirated software. In 2013, International Data Corporation conducted a study which showed that 33% of global software is counterfeited, valued at $ 114 billion worldwide. The countries with the most affected IT infrastructure were: Libya (92%), Algeria (84%) and Nigeria (82%).

According to estimates made in 2011, the percentage of pirated software in the Middle East and Africa was 58%, while Microsoft estimated software piracy on Kenya's IT market of 78%, which means a loss of $ 120 million. One of the causes that facilitate software piracy is the outdated or outdated operating systems. Counterfeit software and applications can be easily exposed to cyber-attacks. At the level of Africa, about 80% of user computers are infected with malware, viruses, and other programs. The most common tools used by hackers are key loggers that benefit from encryption and file protection. The value of a key logger is $ 35 and can be easily purchased from Dark Net.(BSA Global Software Survey, 2018)

In figure 1, we can see the commercial value of unlicensed software and the average rate of unlicensed software around the world. The highest commercial value is in Asia-Pacific, North America and Western Europe and the smallest in Central and Eastern Europe and the Middle East and North Africa. The main threat worldwide has proven to be Cryptominers, which have affected 42% of the world's companies, generating $ 2.5 billion. The operating mode of these cryptominers has evolved from Facebook's Messenger, Youtube to Google Play announcements, which infected tens of thousands of websites, personal computers and mobile applications. (BSA Global Software Survey, 2018) Many types of malware have integrated mining capabilities into their operating mode, ransomware, and bank trojans, including Panda and TrickBot, which target not only bank accounts, but also encryption wallets and trading system accounts, adding features of credit theft cryptocurrency in the operating mode.

Cryptominers are also a threat to cloud services that involve data seclusion and information disclosure that stem from low security. Cryptominers target cloud infrastructure to exploit stored data and generate increased revenue for exploiters. In the first six months of 2018, cryptomers targeted two main components of the Docker and Kubernetes systems. One relevant example of attack by cryptominers is the internal cloud servers of the Tesla that have been infected with a Monero cryptomonitor (Check Point, 2018).

Figure 1: The value of Unlicensed Software Globally (Source: Author's own processing based on BSA Global Software Survey, 2018)



The evolution of cyber terrorism in the Middle East

With the development of information technologies, the threat of cyber-attacks and terrorism has emerged throughout the world, which in turn affects the decline of state and citizens security. Following the tragedy of September 11, the Western society has suffered a fear of terrorism coming from the Middle East. But what we should know is that only certain groups in the Middle East represent a terrorist threat. Undoubtedly, terrorist threats from groups like Al-Qaeda or the Taliban are constant for governments, especially the United States.

However, the evolution of technology and the Internet, as well as the embrace of terrorist groups of this trend, makes governments confront another type of terrorism, namely cyber terrorism. Cyber terrorism has expanded so much and quickly that it has become the first issue on the US national security agenda (Gielten, 2013). The danger of cyber-terrorism in the Middle East started when the former Al-Qaeda leader began using the internet to upload videos during certain speeches. In the present, the Islamic State collects all the Middle East titles.

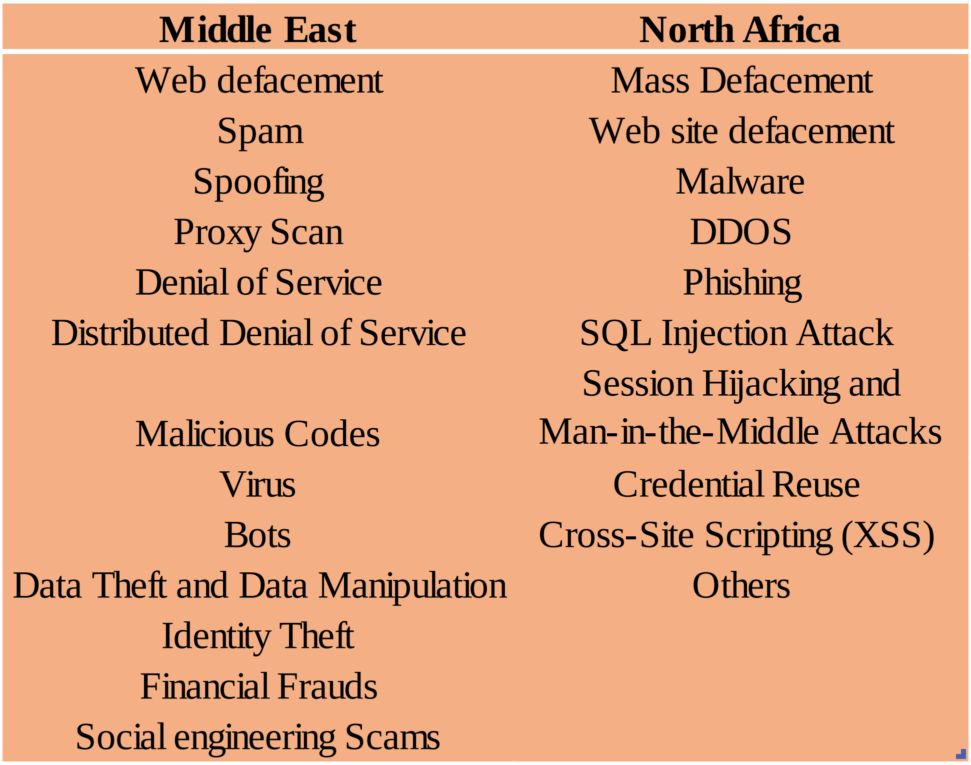
Different from Al-Qaeda, ISIS is more of a threat to countries around. With the evolution of the cyber war, the term "e-jihad" also emerged, which essentially means "electronic jihad". ISIS uses cyber space to preach Islamic ideas, spread ideologies or disrupt Israeli sites (Tereshchenko, 2013). The adoption of new technologies by terrorist groups helps them in recruiting staff, highlighting goals, spreading fear, and raising funds. Their purpose is to use the cyber platform to penetrate target networks easily, with low detection and low cost (McFarlin, 2014).

The Middle East region is an easy target for cyber-attacks, mainly due to the lack or low level of awareness of the threats posed by Internet users and the lack of legal regulations. The element generated by the number of attacks is the presence of numerous political, economic and social conflicts, but especially of religious and civilization conflicts. The most representative reason to be mentioned is the civil war in Syria, followed by the Saudi-Iranian conflict and the Arab-Israeli conflict. Many cyber-attacks or acts of cyber terrorism were caused by the parties involved in the Syrian war. The Syrian army has used various methods of social engineering and malicious software to attack users and anti-government organizations in Syria and other countries.

In Iran, the most common attack was in 2010 on energy infrastructure. This attack was produced by the Stuxnet virus, which destroyed the centrifuges used in the process of enriching nuclear fuel. After that, another virus that was discovered by the Iranian authorities is the Flame virus, which attacked the computers of Iranian officials. This virus was designed to spy out the Middle East cyberspace by attacking operating systems that used Microsoft Windows (Sanger, 2012). Another major attack was in August 2012, when Saudi Arabia's largest Saudi oil company was attacked with the Shamoon virus, killing more than 30,000 computers. (Microsoft, 2018) Two weeks later, a similar attack took place on Ras Gas in Qatar, a giant in the gas market. At a time when security professionals recommend last generation identity management techniques such as facial recognition and biometric identification, only 80% of large Gulf businesses continued to use usernames and passwords as the only means of connecting (Microsoft, 2018). Environments such as the gas, oil and utilities industries will still be at risk of being hit by cyber-attacks.

This year, the Middle East PwC study on the global information security situation shows that these security challenges are likely to grow only in the region, while sophisticated technology is continually expanding. Despite an annual increase in strategic initiatives to improve security among Saudi Arabian enterprises, it continues to be a hot target for cyber criminals, given the geographic, political and economic position of the region.

Figure 2: Types of cyber-attacks observed in the both regions (Source: Author's own processing based on EG-CERT Report and International Institute for Counter-Terrorism)



Middle East	North Africa
Web defacement	Mass Defacement
Spam	Web site defacement
Spoofing	Malware
Proxy Scan	DDOS
Denial of Service	Phishing
Distributed Denial of Service	SQL Injection Attack
Malicious Codes	Session Hijacking and Man-in-the-Middle Attacks
Virus	Credential Reuse
Bots	Cross-Site Scripting (XSS)
Data Theft and Data Manipulation	Others
Identity Theft	
Financial Frauds	
Social engineering Scams	

This makes it difficult for companies to identify when an attack occurre. Many are identified when third parties or customers report suspicious messages or requests for funds. But early detection and effective incident handling require a comprehensive and integrated security plan that takes into account all critical parts of an organization. It's just that all these things are not enough if the organizations personnel are not trained to cope with incidents, as attacks range from direct theft of data through hacking, spamming, phishing, DDoS attacks etc. Attackers are becoming more and more innovative and are using innovative types of attacks, which makes it easier to access systems. There is no limit of the negative impact that a cyber incident may have on an organization in today's digital age.

From loss of customer and employee data to financial losses caused by fraud or business interruptions, the list of risks is long. Each company or institution has a unique exposure to digital risk that is closely related to the nature of the organization and should, therefore, be identified and mitigated fully and carefully at all levels.

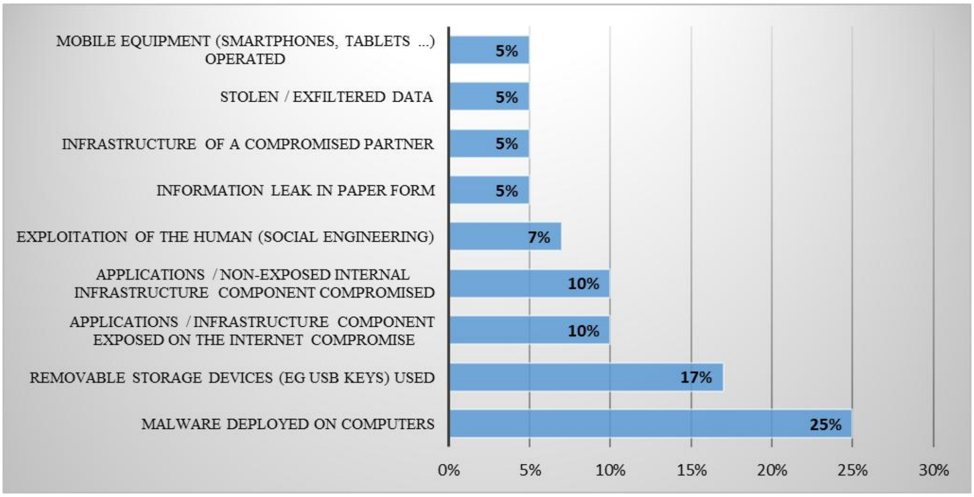
Trends in North Africa

Algeria has made significant progress in the IT sector in the recent years. Following strong investments made over the last three years, the country has updated its legal framework and has introduced a number of new regulations to support the growth of the IT sector. Like other states in the region, the Algerian government has identified a number of cyber security issues in the sense that there is no well-grounded legislative framework that provides measures to counter cyber terrorism and that some of the population is considered vulnerable to possible threats. Like the European states, Algeria has improved its legislation on personal data protection and the creation of mechanisms to prevent online fraud and copyright infringement (Oxford Business Group).

With regards to Egypt, the main cyber threats faced it are threats of intrusion and sabotage of IT infrastructures, cyberterrorism, cyberwar, digital identity threats, and theft of private data. At the end of 2018, the Supreme Council of Cyber Security (ESCC) has launched the National Cyber Security Strategy. According to the strategy, a period of four years, the government will implement six specific programs to guarantee the citizens' security on the Internet and of electronic payment systems. According to the Global Cyber Security Index, Egypt is Africa's leading cyber security and cyber-awareness campaigns among the population (Ecofin Agency, 2018).

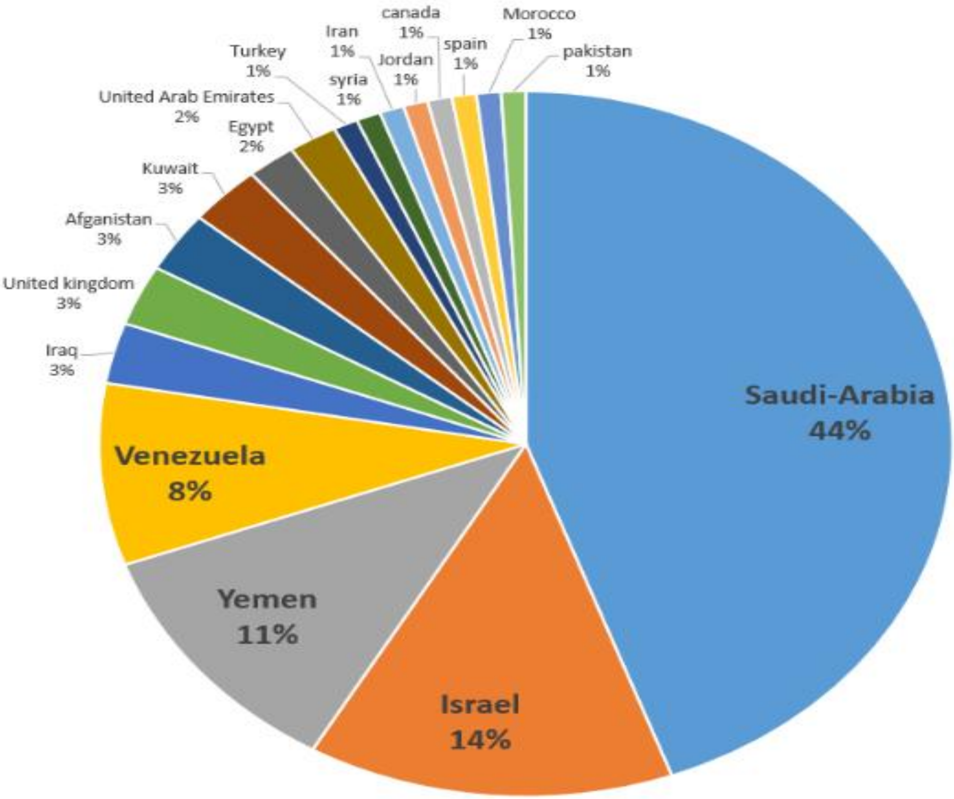
Cyber-crime has become a concern for Moroccan IT companies as well as industry, service and communication. According to a study by PwC for IT companies, the results showed that more than 70% of respondents believe that their security systems do not meet all the standards of the global cybernetic system. Moroccan companies face a challenge caused by the digitization of almost all activities, but also by the fact that they do not have the technical ability to detect the actions of cybercriminals early on. (PwC, 2018)

Figure 3: The nature of the incidents detected in Morocco (Source: Author's own processing based on PwC Global State of Information Security Survey 2018)



A threat that has been faced by Tunisia since the outbreak of street protests in 2011 is the impact of social networks on young people and their possible radicalisation. Through these networks, terrorists have been able to easily identify target groups and disseminate their propaganda messages. In addition to the techniques underlying terrorist activities such as commissioning, communicating, training and executing attacks, these groups have increased their defence capabilities through websites. Among the most common online risks faced by citizens, institutions and companies are: compromising personal information through espionage, piracy and theft. In order to prevent cyber incidents and to inform the public of the risks they are facing on the Internet, the government has launched in September 2018 the e-portal "Tunisians against Cyberterrorism" (Centre for Applied Policy Research, 2018).

Figure 4: Cyber target distribution by country
(Source: Clear Sky Cybersecurity Report, 2015)



Major Cyber breaches in the Middle East and North Africa

The most active hacker groups are Iranian. Below we will detail the major attacks committed by these:

- Saipem in Italy was attacked with a Shamoon malware program and its servers were directed to Middle Eastern countries by Iranian groups. This program was previously used in an attack on 30,000 computers by the Saudi Aramco oil giant (Brewster, 2018). Iranian groups have been behind attacks on the Government and communications infrastructure, dozens of Internet sites belonging to Middle East, North Africa, Europe, and North American entities (Tweed, 2019).
- In February 2014, a group of hacked-ups attacked Sands in Las, through computers and mobile phones (Bloomberg, 2014). In 2015, a cyber spying campaign called the Thamar Tank was launched against Middle East University researchers, defence and security companies, journalists and human rights activists (Clear Sky Security, 2015).
- In 2017, the APT33 group entered the servers of an American airline, a Saudi Arabian airline, and a South Korean petrochemical company, where it stole commercial secrets (O'Leary et al., 2017). In 2018, the Oil Rig cyber spy group, which acts primarily in the Middle East, has carried out an APT attack and data theft against several states (Lee and Falcone, 2018).
- In May 2017, an attack against the HBO television station was made through a data theft scheme and it resulted with the loss of $ 6 million by the use of Bitcoin (United States Department of State, 2017). In 2018, the Leafminer group has attacked government organizations and companies across the Middle East using security grids, trying to access email addresses, servers, and sensitive information databases (Symantec, 2018).
- March 2018, a report from the UN showed that North Korean hackers have been trying to compromise the

email accounts of members of a UN commission that applies trade sanctions against North Korea. (Centre for Strategic & International Studies, 2019)

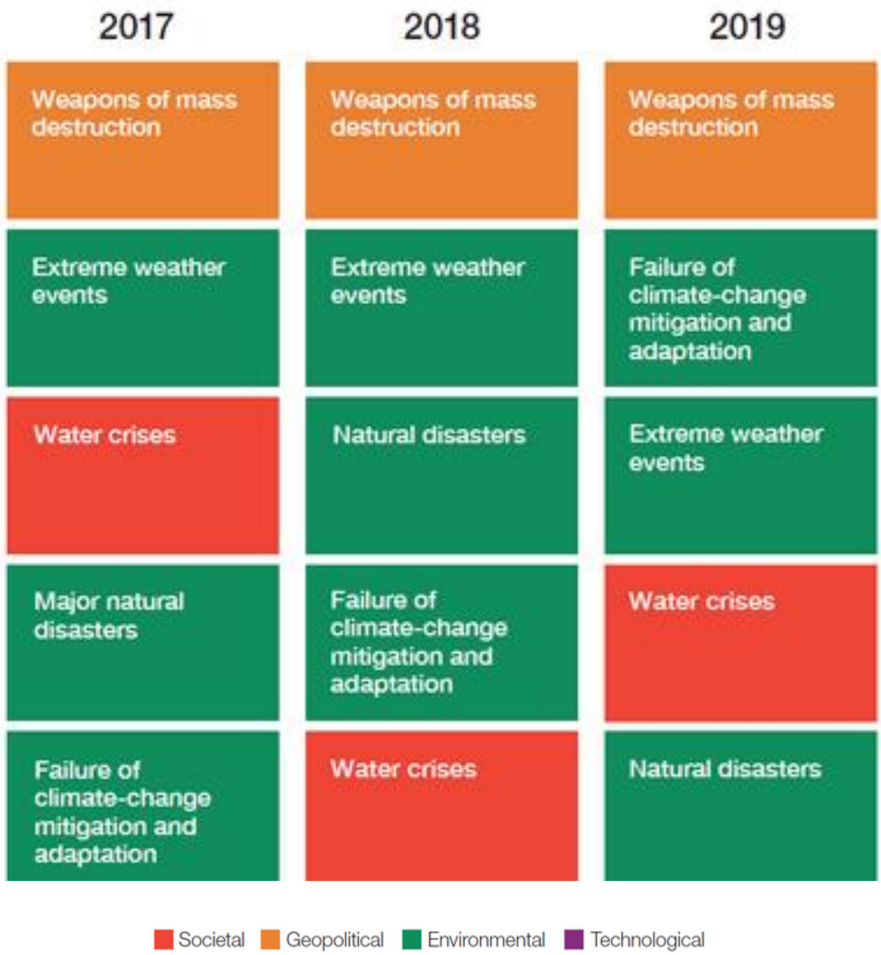
- April 2018 – Israeli cyber scientists have reported that Hamas has installed spyware in Fatah mobile phones that is a rival Palestinian faction. (Centre for Strategic & International Studies, 2019)
- November 2018 – The Chinese state's media said the country was the victim of multiple attacks by foreign hackers in 2018, including the theft of confidential emails, utility design plans, armed lists, and many other confidential information. (Centre for Strategic & International Studies, 2019)
- November 2018 – North Korean hackers have used various mauves to steal tens of millions of dollars from Asia and Africa. (Centre for Strategic & International Studies, 2019)
- December 2018 – North Korean hackers targeted the Chilean interbank network after an employee installed malware in a fake job interview. (Centre for Strategic & International Studies, 2019)
- December 2018 – Chinese hackers have compromised EU communications systems, retaining access to various diplomatic channels for many years. (Centre for Strategic & International Studies, 2019)
- December 2018 – North Korean hackers have stolen personal information from more than 1,000 North Koreans who live in South Korea. (Centre for Strategic & International Studies, 2019)
- December 2018 – The US, Australia, Canada, the United Kingdom and New Zealand have accused China of running cyber spying campaigns for nearly 12 years and are targeting the IP and business secrets of companies in nearly 12 countries. (Centre for Strategic & International Studies, 2019)

- December 2018 – US Navy officials have declared that Chinese hackers have repeatedly stolen information from the Navy contractors, including information and ship maintenance data and missile plans. (Centre for Strategic & International Studies, 2019)
- January 2019 – The United States Department of Justice has declared that an operation to disturb the media, aerospace, financial and critical infrastructure has come from North Korea. (Centre for Strategic & International Studies, 2019)
- January 2019 – A former American intelligence officer was found to work for the UAE to help the country learn more about diplomats, government officials, and their activists. (Centre for Strategic & International Studies, 2019)
- January 2019 – Security researchers have shown that Iran's hackers have been targeting the telecommunications and transport industries since 2014. Their purpose was to collect and supervise people in the Middle East, the US, Europe, and Australia. (Centre for Strategic & International Studies, 2019)
- January 2019 – The South Korean Ministry of National Defence declared that a group of unknown hackers compromised the information systems of the ministry's procurement office. (Centre for Strategic & International Studies, 2019)
- February 2019 – The airline Airbus said Chinese hackers, have stolen personal information to identify their European employees. (Centre for Strategic & International Studies, 2019)
- February 2019 – The Norwegian software firm Visma has declared that it was targeted by the Chinese Ministry of State Security hackers. They seem to have tried the commercial secrets of their business customers. (Centre for Strategic & International Studies, 2019)

Estimated trends of the next years

If the methods applied by traditional offenders in the physical world, such as extortion, armed robberies or drug distribution, have evolved over decades, cyber threats are subject to a rapid changing process, as cyber attackers use another type of attack every day.

Figure 5: Top 5 Global Risks in terms of impact
(Next 10 years, source: World Economic Forum Global Risk Perception Survey 2018-2019)



2017	2018	2019
🟧 Weapons of mass destruction	🟧 Weapons of mass destruction	🟧 Weapons of mass destruction
🟩 Extreme weather events	🟩 Extreme weather events	🟩 Failure of climate-change mitigation and adaptation
🟥 Water crises	🟩 Natural disasters	🟩 Extreme weather events
🟩 Major natural disasters	🟩 Failure of climate-change mitigation and adaptation	🟥 Water crises
🟩 Failure of climate-change mitigation and adaptation	🟥 Water crises	🟩 Natural disasters

🟥 Societal 🟧 Geopolitical 🟩 Environmental 🟪 Technological

In figure 5 we can see what cybernetic trends are in the next 10 years. The year 2017 was one in which new types of attacks arose, affecting three quarters of world countries, such as Wannacry, NotPetya, Locky, GoldenEye and Jigsaw, which spread around the world in a few hours, some of them targeting to show the vulnerability of systems while others aimed to gain cash rewards. These threats have continued in 2018 with the same intensity, causing major IT infrastructure damage all over the world.

The Trends for the coming years require the businesses to improve their capabilities to protect business information, as hacking groups are always looking for a new way to mount stolen information and access to servers. An example of this is the $ 81 million that disappeared following a cyber-attack from a bank in Bangladesh in just a few hours. Governments around the world must prioritize collaboration and information sharing to develop new cyber security programs. Also it should be maintained the communication with telecommunication companies and service providers in order to build together means of preventing cybercrime.

Conclusion

The Middle East and North Africa are the home of many cyber-attacks occurring around the world, but at the same time they are also beneficiaries of these attacks. Some countries have poor legislation and have an outdated and vulnerable technology against threats they are facing each day. Among the countries with strong legislation and an annual budget that grows from year to year precisely to deal with threats and companies benefit from competitiveness. And the trends in the next years are based on state-private cooperation to prevent cyber-attacks.

References:

1. Agbugah, F., (February 18, 2015). *Moroccan Banks Are The Latest Victims Of Cyber Attacks.* [Online]. Available at http://venturesafrica.com/moroccan-banks-are-the-latest-victims-of-cyber-attacks/ .

2. Elgin, B., Riley, M., (December 12, 2014). Now at the Sands Casino: An Iranian Hacker in Every Server," Bloomberg. [Online]. Available at https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas#p1

3. Brewster, T., (December 13, 2018). Warnings as Destructive 'Shamoon' Cyber Attacks Hit Middle East Energy Industry. Forbes. [Online]. Available at https://www.forbes.com/sites/thomasbrewster/2018/12/13/warnings-as-destructive-shamoon-cyber-attacks-hit-middle-east-energy-industry/#68e4e1713e0f.

4. Centre for Applied Policy Research (October 10, 2018). *Fighting Cyber Terrorism, improving Cyber Security in Tunisia*. [Online]. Available at https://www.cap-lmu.de/aktuell/events/2018/cyber-security-tunisia.php.

5. Centre for Strategic & International Studies, (2019). Significant Cyber Incidents from 2018 and 2019. [Online]. Available at https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

6. Check Point, (2018). *Check Point Cyber Attack Trends: Mid-Year Report 2018.* [Online]. Available at https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf.

7. Clear Sky Cybersecurity, (June 2015). Thamar Reservoir. An Iranian cyber-attack campaign against targets in the Middle East. [Online]. Available at https://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf.

8. Ecofin Agency, (December 12, 2018). Egypt *launches its 2017-2020 national cybersecurity strategy*. [Online]. Available at https://www.ecofinagency.com/telecom/1212-39420-egypt-launches-its-2017-2020-national-cybersecurity-strategy.

9. Gjelten, T., (2013). *Cyberattacks, terrorism top US security threat report*, [Online]. Available at, http://www.npr.org/2013/03/12/174135800/cyber-attacks-terrorism-top-u-s-security-threat-report. Accessed 10 November 2014.

10. McFarlin, J., (2014). *ISIS cyber ops: Empty threat or reality?* [Online]. Available at http://www.securityweek.com/isis-cyber-ops-empty-threat-or-reality. Accessed 11 November 2014.

11. Lee, B., and Falcone, R., (July 25, 2018). OilRig Targets Technology Service Provider and Government Agency with QUADAGENT, Palo Alto, [Online]. Available at https://researchcenter.paloaltonetworks.com/2018/07/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/.

12. Oxford Business Group, *Algerian ICT expands on digitisation and cybersecurity*. [Online]. Available at https://oxfordbusinessgroup.com/overview/increased-competition-alongside-digitisation-and-cybersecurity-efforts-arrival-new-players-has.

13. Panda Security, (January 25, 2016). *27% of all recorded malware appeared in 2015.* [Online]. Available at https://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/.

14. PwC, (May 2018). *Global State of Information Security Survey 2018.* PricewaterhouseCoopers France and Francophone Countries of Africa, p. 14. [Online]. Available at https://pwcmaroc.pwc.fr/fr/publications-communique-de-presse/comment-entreprises-maroc-apprehendent-cybersecurite.html.

15. Sanger, D.E., (2012). Obama order sped up wave of cyberattacks against Iran , http://www.nytimes.com/2012/06/01/world/middleeast/obama -ordered -wave -of -cyberattacks -against -iran.html?page- wanted=all, Accessed at October 10, 2015.

16. Symantec, (July 25, 2018). Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions, [Online]. Available at https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east.

17. Tereshchenko, N. (2013). *US Foreign Policy Challenges: Cyber Terrorism & Critical Infrastructure* [Online]. Available at http://www.e-ir.info/2013/06/12/us-foreign-policy-challenges-of-non-state-actors-cyber-terrorism-against-critical-infrastructure/. Accessed, 11 November 2014.

18. Tweed, D., (January 11, 2019). Iran Hackers Could Be Behind Wave of Cyber Attacks on Infrastructure: FireEye. [Online]. Available at https://www.insurancejournal.com/news/international/2019/01/11/514571.htm.

19. U.S. Department of Justice, (November 21, 2017). Press Release, Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO, [Online]. Available at https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting.

20. World Economic Forum, (2019). These are the biggest risks facing the Middle East and North Africa. [Online]. Available at https://www.weforum.org/agenda/2019/04/these-are-the-biggest-risks-facing-middle-east-and-north-africa/.

21. Ziffer, A., (February 19, 2019). *Cyber-attacks by foreign governments, malicious companies and enterprising hackers are on the rise. And the biggest problem is you.* [Online]. Available at https://www.abc.net.au/news/2019-02-20/cyber-crime-hits-consumers/10825970.