UDC: 327.84:004.493
Professional paper

CYBER ESPIONAGE CONSEQUENCES AS A GROWING THREAT

Abdulla CIVULI[1*], Shkurte LUMA-OSMANI[1], Eip RUFATI[1], Gjulie ARIFI[2]

[1]Department of Informatics Faculty of Natural Sciences and Mathematics, University of Tetova
[2]IT Center, University of Tetova
[*]Corresponding author e-mail: a.civuli319019@unite.edu.mk

Abstract

Cyber espionage is the new arena in the world of espionage. Cyber espionage, or cyber spying, is a type of cyber-attack in which an unauthorized user attempts to access sensitive or classified data, intellectual property (IP) for economic gain, competitive advantage, political reasons or military advantage. This project makes a detailed exploration related to cyber espionage, targets and tactics used in cyber espionage, ethics, what motivates people to spy against their own government. These events in the Balkans show how unprepared these countries are to protect themselves against cyber-attacks. Some cases of cyber espionage are also elaborated, with an emphasis on the cases in North Macedonia and Albania. The last part of the paper covers the ways to defense against cyberespionage as well as its positive and negative impacts.

Keywords: APT, Stuxnet, Spyware, Spycraft, Covert Messages, Ciphers.

1. Introduction

Rulers, governments and corporations have been doing it for centuries. Spying to gain information, assess potential threats, stop attacks and gain the upper hand [1]. Throughout history, nation states have been trying to undermine each other through clandestine activity, whether its spying, sabotage, or subversion. The rapid growth of the internet during the 1990s opened up a new frontier in the arena of international espionage, and it wasn't long before we began to read ominous warnings about cyber warfare. Could a country's enemies shut down its power grid, take out its telephone system, or even hijack its nuclear missiles [4]?

Cyber espionage attacks can be motivated by monetary gain, they may also be deployed in conjunction with military operations or as an act of cyber terrorism or cyber warfare. The impact of cyber espionage, particularly when it's part of a broader military or political campaign, can lead to disruption of public services and infrastructure, as well as loss of life [2]. The first documented case of cyber espionage pre-dated the web itself. In 1986, Clifford Stoll, who at the time was an astronomer managing computers at Lawrence Berkeley National Laboratory in California, noticed some strange activity in computing time records. This eventually led him to a hacker who appeared to be systematically targeting computers at military bases around the U.S. looking for military secrets. Clifford Stoll created a trap for the hacker, luring him in with a cache of fake information. Later the hacker was identified as Markus Hess, a West German who had been selling stolen information to the KGB [4]. The first major cyber espionage by a state intelligence agency was codenamed "Moonlight Maze" in the mid-1990s. U.S. investigators concluded the attackers were Russian, although Russia denied it [3].

Between 2000 and 2003, a series of widespread cyber espionage attacks code-named Titan Rain were launched against the American defense infrastructure, targeting high- level organizations like NASA, Sandia and Lockheed Martin. The cyber-attacks extradited vital information, and left behind virtually undetectable beacons on compromised systems, allowing them to reenter at will. Investigators discovered the cyber breaches were part of state sponsored cyber espionage attacks conducted by China [1].

2. Cyberespionage targets

Today, cyber espionage is used by intelligence agencies and adversaries alike, and has proved a useful strategy in the collection or corruption of data, stealing technology and patents, disrupting critical infrastructures, and allowing for advanced warning of an enemy's attack [1]. The most common targets of cyber espionage include large corporations, government agencies, military intelligence, academic institutions or other organizations with valuable IP.

Cyber spies most commonly attempt to access the following assets:

- Research & Development data and activity
- Academic research data
- IP, such as product formulas or blueprints
- Business goals, strategic plans and marketing tactics
- Political strategies, affiliations and communications
- Military intelligence [2].

2.1. Common Cyberespionage tactics: In an age when billions of people, governments, and rouge states are digitally connected today scientists and hackers have discovered that it is possible to use malware to steal data off your digital device that completely evades the protections built with cryptography. When intelligence agencies don't have access, they get creative [1].

Most cyber espionage activity is categorized as an Advanced persistent threat (APT). An APT is a sophisticated, sustained cyber-attack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization and evade existing security measures for long periods of time.

Most cyber espionage attacks also involve some form of social engineering to spur activity or gather needed information from the target in order to advance the attack. These methods often exploit human emotions such as excitement, curiosity, empathy or fear to act quickly or rashly. In doing so, cybercriminals trick their victims into giving up personal information, clicking malicious links, downloading malware or paying a ransom [2].

2.2. Spyware: Spyware is a software that can be planted by adversarial parties on your system. They have the ability to collect information. They can collect your passwords or record your conversations. If you are making webinar calls using your computer, they can turn on your camera and record anything that you are doing. This is all spyware activity, and can be used against a person or government.

2.3. The man in the middle attack: One of the first things many of us do when we land at an airport is immediately turn on our phone. Intelligence services use a technique called "the man in the middle" attack. And what they create is a small little mini tower that may exists in the executive lounge of the airport. It may exist in the concourse. And once we turn on our phone on, rather than contact the closest major tower, it reaches out this mini little tower that's controlled by an intelligence service. It, in turn, contacts the major cell tower, but because it's in the middle, it can download everything on your phone and it can put a virus on your phone in exchange, and you will never, ever be aware of it. And there are multiple cities in the world in which that happens on a regular basis [1]. One country that's collecting detailed profiles on all of its citizens by applying recent advances in artificial intelligence and data mining to their surveillance capabilities is China. Along their robust arsenal of surveillance devices, they've also developed drones that looks like real birds. They're using data to analyze everything at their people, in terms who you are, who do you talk to, what are your opinions about the regime, what you blog about, what you search what you like what you don't like. And that assesses a credit score or risk score to you. An example of how social credit systems have been theorizes to be used is, if you have a high credit score, you qualify for the best scholarships, the best jobs. You're allowed to travel overseas. But if you have low credit score or you associate with the wrong folks, or you post negative commentary against the regime or governmental policies your credit score takes a hit. That means in some cases, you can't qualify for certain jobs, you can't qualify for certain academic institutions or loans, or you're restricted in terms of where and when you can travel inside the country or abroad [1].

3. Ethics in cyberespionage

Is intelligence gathering ethical? Eight years after the Snowden revelations on mass surveillance and 16 years after the emergence of extraordinary rendition scandals, the debate on the role of ethics in intelligence gatherings has never been as prominent, and is dominated by opposing perspectives. On the one hand is the view that the very nature of intelligence work is unethical, but such work needs to be done to protect national security. On the other is the view that it is precisely this unethical nature that undermines the legitimacy and security of democratic states, and therefore is unacceptable.

The response from the public and civil society actors to scandals around extraordinary rendition and mass surveillance has been a resurgence of a fundamental debate on the extent to which democratic laws and values are being compromised to protect national security [7]. Espionage may have been defined once primarily as an external activity of a state but by now that meaning has long since been overwhelmed by other forms of espionage, including industrial espionage perpetrated by corporations and individuals, as well as by states [6]. The data targeted in cyber-attacks is often personal and sensitive. Cyber security professionals have access to the sensitive personal data they were hired to protect. So it's imperative that employees in these fields have a strong sense of ethics and respect for the privacy of your customers. Many companies focus only on the technical abilities of a candidate for hire, but it's not enough that the staff have knowledge of technology and hacking techniques. They must also demonstrate the ability to maintain their moral standards while processing customer data or handling other grey areas of data management and cyber security [5].

One possible explanation is that cyber espionage is just so very easy and it has become so pervasive that we can no longer assign it a moral character. Maybe we have become morally numbed by the sheer volume and character of these intrusions.

There are several indicators that IT professionals, regardless of nationality, have (on average) lower ethical standards than people outside the field when it comes to protecting IT users' interests. This appears to arise because of the higher priority assigned by IT professionals to exploiting technologies to their full potential often in disregard of other considerations. This reality appears to have been confirmed with the linked cases of Facebook and Cambridge Analytica in the recent scandal over accumulation and exploitation of user data for the purposes of electoral manipulation [6].

3.1. What motivates people to spy against their government or company: The act of gathering information from an enemy is rarely carried out by an intelligence officer in person. Instead they recruit agents who have access to information they need. Finding the perfect agent for the task is the first and the most crucial step in the process. The intelligence services of all countries recruit foreign spies because it's the foreign spies who have access to secrets. When an intelligence officer is looking for a person to recruit him as a spy, one of the things he is looking for is what is this person's vulnerabilities? Do they have money problems? Do they have marital problems? Do they have substance problems? And they want to identify these. Whether is face to face meetings or identifying potential recruits via online sites like LinkedIn, the process takes time. A faster approach is to attack the source directly, which is what China did when they gained access to some of America's top-secret files by installing malware into the network of the United States Office of Personnel Management, the OPM in 2015. Chinese hackers were then able to exfiltrate whatever information they needed. The audacious cyber-attack wasn't just a national security threat, but a threat for spy recruitment as well. With that information they had the Chinese were able to know not which of the employees had clearances, but how much income they have, how many children they have, what they income debt ratio may be. So now they can use that potentially, as targeting. People become spies for many different reasons, and historically intelligence services have used the acronym MICE. Where each letter stands for a motivation to spy, it can be for money, ideology, compromise or ego.

The Soviet Union discovered very early that American's lust for money made them very vulnerable to being bought as spies. There are many cases where people working for government institutions, intelligence agencies or military have fallen into debt. And the position they have held in these institutions they have used it to spy against their government in the return of money. Because they had information that ordinary people do not have, like government secrets or military intelligence. They have gained millions of dollars for spying against their government, in some cases they were rewarded with silver bars or diamonds.

Money isn't the only reason someone becomes a spy.

Ideology is also a powerful incentive. This was true especially during the Cold War, were spies were motivated by support for the ideological positions of either the western world or the Communist bloc. Ideology can be a great motivator for treason, and so is compromise or black mail. This method was used by all services, to some extent, through the Cold War. It happens when someone is threatened to spy otherwise he will be blackmailed. Ego, on the other hand is a powerful motivator. It's a really powerful driver of what makes for men choosing to do what they do in life. Ego and greed is what drives most people to become a spy [1].

4. Some cases of Cyberespionage

4.1. Edward Snowden: Edward Snowden is an American former computer intelligence consultant [13], he was an employee and worked as a contractor for the National Security Agency, as a systems administrator in Hawaii. The position he had there gave him a great deal of latitude and freedom in operating system, he was the one that was guarding the system, and he in turn was collecting information from that system. Snowden allegedly copied over a million highly confidential and sensitive documents onto thumb drives and smuggled them out of the NSA, and then, he leaked them. In 2013, Snowden created a false story that he had needed treatment for epilepsy, and he traveled to Hong Kong. Snowden had a meeting with several reporters. He claimed he passed all of his thumb drives to them. But some sources says that he also was secretly meeting with the representatives of the Russian government. But Snowden later claimed that he took no thumb drives with him. The existence of secret information-gathering programs by the US National Security Agency, leaked by Snowden shed light on the reach of surveillance, not just for national security and espionage operations, but on the civilian population [1].

4.2. Cyber-attacks in Estonia: The other case is the Russian attack on Estonia a tech-savvy nation of 1.3 million people, in April 2007. The Russians virtually attacked the infrastructure of Estonia. They shut down the newspapers, the broadcasts the parliament, ministries. ATM's stopped working. The internet didn't work. The society of Estonia was dependent on the internet. The Russians basically shut down the e-economy, electronic-based economy of Estonia for a period of time. For this attack they used ping floods and botnets usually used for spam distribution.

In Russia you have the hacking community, who have complete freedom from the Russian government to do what they want and steal as much as they want. But with one condition. If the government wants them to do something for them, they must do it. And this happened with Estonia. They did not utilize their military or intelligence assets. They used the criminal underground [1]. Estonia responded to Russia's DDoS attack simply by suspending certain services to computers with Russian IP addresses [11].

4.3. Wikileaks: On 7 March 2017, WikiLeaks started publishing content code-named "Vault 7", describing it as containing CIA internal documentation of their "massive arsenal" of hacking tools including malware, virus projects, weaponized "zero day" exploits and remote-control systems to name a few. Leaked documents, dated from 2013 to 2016, detail the capabilities of the United States Central Intelligence Agency (CIA) to perform electronic surveillance and cyber warfare, such as the ability to compromise cars, smart TVs, web browsers (including Google Chrome, Microsoft Edge, Mozilla Firefox, and Opera Software ASA), and the operating systems of most smartphones (including Apple's IOS and Google's Android), as well as other operating systems such as Microsoft Windows, macOS, and Linux [12].

4.4. Stuxnet: Stuxnet is a computer worm that was specifically written to take over certain programmable industrial control systems and cause the equipment run by those systems to malfunction. Stuxnet was designed to attack Siemens 7 operating system that ran in a Windows environment in the nuclear plants in Iran, where they spun the centrifuges to enrich the uranium. The Stuxnet attack which allegedly was done by combinations of Israel, United States and Western Europe, attacked Iranian development nuclear production capabilities, and brought down various systems basically by being able to infect them with a virus. As result this attack destroyed a significant component of the Iranian system for enriching uranium [1]. Stuxnet was a surprise because it was highly sophisticated and because it was the first major cyber-attack that could inflict damage on the physical world as well as the digital world [11].

4.5. Cyber-attacks in North Macedonia: One of the cyber-attacks taking place in North Macedonia, were cyber-attacks on elections in 2020. The website of North Macedonia's State Election Commission (SEC), or to be more exact the site's election section, was targeted by hackers immediately after polls closed in the snap general election on July 15, leaving the question of who stands behind the attack?

The SEC was hacked immediately after voting ended at 9pm on Wednesday. The election section then recovered for few minutes but the results disappeared again, preventing journalists and other interested people from monitoring the election results, which were announced with a huge delay a day after the election. The type of attack was "DDoS attack".

The attack was stopped as soon as Austrian telecommunication company A1 Austria, which has a unit in North Macedonia, A1 Makedonija, whose network SEC is using, intervened. Most countries take measures to protect their electoral infrastructure in order to provide the maximum security on election day, which was not the case here in North Macedonia [8].

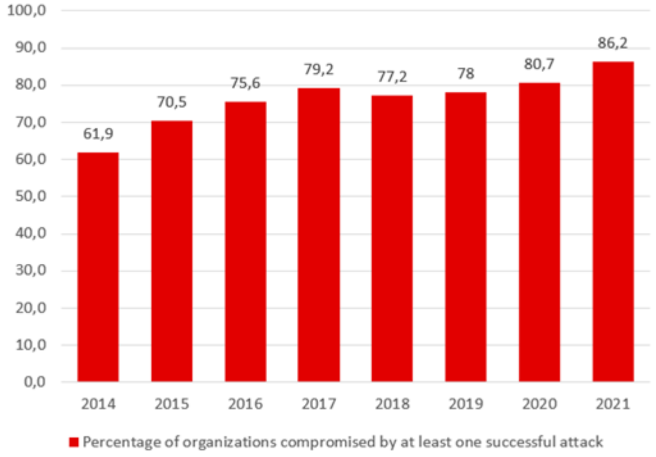

Fig 1. Percentage of organizations compromised by at least one successful attack. Source: [17]

4.6. Massive data leaks in Albania: Data leaks and cyber-attacks are becoming increasingly frequent in southeastern Europe. One of the more recent examples is a data leak from Albania, which compromised the personal data of several thousands of Albanian citizens. In the end of December 2021 a database with private information of salaries, job positions, employer names and ID numbers of some 630,000 Albanian citizens, from both the public and private sectors started to circulate online via excel files sent through social media platforms like WhatsApp. There will be severe consequences because the data can then be used to access personal accounts by private companies that may wish to target individuals for advertising, monitoring, social media targeting, and more. Also the risk of blackmail is very high [9].

5. Defense against cyberespionage

In the world of espionage, collecting information is only half of the battle. The other half is counter intelligence and protecting the information you already have. Nevertheless, advancements in technology come with risks [1].

Deterrence is a useful counter-espionage strategy for nation-states with the authority and the resources to carry it out. Deterrence is when a nation convinces its enemy that it is willing and able to respond to cyber intrusions using military force. The purpose of this is to scare other nation-states from committing cyber-attacks in the first place and thus preventing the need for real retaliation. Finally, there is always the option to Fig ht fire with fire. Nation-states that experience a cyber-attack can always respond with their own cyber-attack. This is not always an available option, since many nations lack the technology to match their attacker, but a defensive cyber operation does not need to be sophisticated in order to make a point [11].

5.1. Ways to protect our data against cyber espionage attacks: As our society becomes more and more dependent on technology, we also become more vulnerable to potential attacks. When codes are broken more complex systems are developed to protect them [1]. Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as cipher text [10].

Codes and ciphers have played an important role in keeping information private throughout history. Breaking these codes and ciphers is crucial spycraft for successful espionage. What began with secret writings to hide information has progresses to electro-mechanical ciphers and then computers to send messages, and to decipher and break them. Next level technology seeks to override the safety measures of cryptography. As a result, ciphers have become increasingly more complex. Espionage is always described as a chess match you move the enemy countermove. The services themselves are always Fig hting. They're Fig hting either to steal secrets or Fig hting to protect secrets they have. There's never a moment you can relax [1]. Also, the costs of protection against cyber-attacks have increased. Cyber espionage also has a steep economic cost as well. In the United States alone the value of the information that is compromised due to international hacking is somewhere between 25 billion and 100 billion dollars annually [11].

6. Positive and negative sides of cyberespionage

A hostile organization having access to detailed information about a person or government is frightening. Cyber espionage is used by intelligence services to protect national security by preventing terrorist attack. It can also be used in war where the information collected from the enemy can be used for successful warfare.

In one case the Ukrainian soldiers Fig hting in eastern Ukraine are still using wire phones to communicate between posts, because Russian separatists are using electronic warfare so if the Ukrainians use signals phones to communicate, their positions will be revealed by the separatists, and they will be attacked with artillery shells. It’s not only government installations and organizations that are getting hit.

Cyber espionage attacks happen wherever there are loopholes or open ports that can be exploited, like our own personal devices.

Today, the variety of channels in which you can send covert message has exploded, especially with the growth of social media applications. On your phone you have multiple apps available for point-to-point encryption. You have WhatsApp you have Telegram, you have a variety of systems.

Every one of them is encrypted. The government has enormous difficulty and in some instances cannot break this encryption. But there's other ways that are complex and baffling. Digital applications make it easier to send messages and also allow spies to communicate secretly on otherwise benign platforms, such as digital gaming.

Through point-to-point encryption applications, terrorist groups who caused the attacks in France in 2015 were able to communicate secretly to each other without being detected by the authorities [1].

7. Conclusions

Cyber security is going to be a critical area of focus in 21st century. What we are seeing is, not only are government worried about this but more important businesses are starting to be worried as well, because if people spent billions of dollars in developing a certain product, all the research dollars, all the developments, all the testing, but if one of your competitors gets access to secret sauce or access to your plans and is able to beat you to market with reverse-engineered or better product for a fraction of the cost, that’s massive impact in the terms of GDP.

References

[1]. Spycraft (2021) Directed by Maria Berry, Jan Spindler, Marek Bures [Television Documentary]. Netflix.

[2]. Crowdstrike “WHAT IS CYBER ESPIONAGE?” April 1, 2021 [Online] Available: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/#:~:text=Cyber%20espionage%2C%20or%20cyber%20spying,competitive%20advantage%20or%20political%20reasons.

[3]. H.Cylinder, A Brief History of Cyber-Espionage January 18, 2021.[Online] Available: https://www.thebeacongrp.com/blog/a-brief-history-of-cyber-espionage

[4]. D.O’Brien, A short history of cyber espionage July 27,2017. [Online] Available: https://medium. com/threat-intel/cyber-espionage-spying-409416c794ec

[5]. Reciprocity, The Importance of Ethics in Information Security February 26,2021[Online] Available: https://reciprocity.com/the-importance-of-ethics-in-information-security/

[6]. G.Austin Ethics in China’s cyber espionage June 7, 2018. [Online] Available:https://theasiadialogue.com /2018/06/07/ethics-in-chinas-cyber-espionage/

[7]. S.Martin Spying in a transparent world: Ethics and intelligence in the 21st century October 28, 2016.[Online] Available: https://www.gcsp.ch/publications/spying-transparent-world-ethics-and-intelli genc e-21st-century

[8]. V.Dimitrievska Who hacked the website of North Macedonia’s state election commission on election day? July 19,2020. [Online] Available: https://www.intellinews.com/who-hacked-the-website-of-north-macedonia-s-state-election-commission-on-election-day-187756/

[9]. L.Cruz Massive Data Leaks In Albania Highlight National Cybersecurity Shortcomings December 29,2021 [Online] Available: https://theowp.org/massive-data-leaks-in-albania-highlight-national-cybersecurity-shortcomings/

[10]. Cloudflare “What is encryption? | Types of encryption” [Online] Available: https://www.cloudflare.com/ learning/ssl/what-is-encryption/#:~:text=Encryption%20is%20a%20way%20of,text%2C%20also %20known%20as%20ciphertext.

[11]. D.Rubenstein Nation State Cyber Espionage and its Impacts December 15,2014 [Online] Available: https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/#recent_attacks

[12]. Wikipedia WikiLeaks January 24, 2022 [Online] Available: https://en.wikipedia.org/wiki/WikiLeaks

[13]. Wikipedia EdwardSnowden January 29,2022 [Online] Available:https://en.wikipedia.org/wiki/Edward_Snowden

[14]. DW Edward Snowden still eying asylum in Germany September 14,2019 [Online] Available: https:// www.dw.com/en/edward-snowden-still-eying-asylum-in-germany/a-50429478

[15]. The Export Compliance Journal April 1,2021 U.S. expands military end-use export control law to cover ‘military intelligence’ in countries of concern [Online] Available: https://www.visualcompliance. com/blog/?p=2226

[16]. B. Vigliarolo Stuxnet: The smart person's guide August 15,2017 [Online] Available: https://www.techrepublic.com/article/stuxnet-the-smart-persons-guide/

[17]. P.Stainer Alarming Cybersecurity Statistics for 2021 and the Future April 5,2021 [Online] Available: https://www.retarus.com/blog/en/alarming-cybersecurity-statistics-for-2021-and-the-future/

[18]. Crunchbase Report: The Rise of Global Cybersecurity Venture Funding [Online] Available: https://about.crunchbase.com/cybersecurity-research-report-2021/

[19]. Ally Law Final Canadian Privacy Breach Regulations Include Mandatory Notification Rules May 7, 2018 [Online] Available: https://ally-law.com/final-canadian-privacy-breach-regulations-include-mandatory-notification-rules/

[20]. C.Nistor China now has 800 million internet users August 27,2018 [Online] Available: https://www.notebookcheck.net/China-now-has-over-800-million-internet-users.325616.0.html

[21]. S. Faris What is spyware? February 5,2021 [Online] Available: https://www.paubox.com/blog/what-is-spyware/