Romana Oancea – Ilie Gligorea – Aurelian Raţiu
– Isabela Dragomir[1]

Cybersecurity

Nowadays, the Internet is integrated into society both through social interaction and business transactions, so the need for data protection and security has become increasingly important. In addition, not only computers, but also most hardware devices are networked, and regional geographical boundaries are no longer maintained. Communication and/or interaction between different countries is now very easy and the protection of data flow has become a concern for all countries and organisations.[2] The change in paradigm regarding the environment in which everyday activities relate to work, communication, collaboration, and even learning are carried out, has led to an increase in the amount of illicit activity on the Internet. In addition, increased speed, anonymity and national laws that are not always applicable to the Internet have brought about changes in the typology of cyberattacks. To underline the seriousness and danger the society is experiencing today, the concept of cyberspace has been introduced and defined as "the interdependent network of information technology, infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical infrastructure industry".[3]

Cybersecurity fundamentals

In NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), cyberspace "is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks".[4] In other words, cyberspace is "the interdependent network of information technology infrastructures",[5] which makes it the arena for political, economic and

[1] "Nicolae Bălcescu" Land Forces Academy.
[2] SWD 2020.
[3] The White House 2008: 3.
[4] Klimburg 2012: 8.
[5] The White House 2008: 3.

DOI: https://doi.org/10.36250/01195_07

military interaction and some actions in this space can have a negative impact on social stability, national security and economic development. In cyberspace, digitalised data is created, stored and shared by using an infrastructure that allows data flow.[6] This environment is prone to cyberattacks, cybercrime and de-cyber warfare. When discussing cybercrimes, we generally refer to attacks launched by individuals for financial gain, while cyber warfare actors, such as states or governments aim for political advantage, strategic advantage or destabilisation.[7] The purpose of cyberspace actions by one state or group against another focuses on a broad spectrum of threats that can harm a nation's interests. Threats range from espionage to illicit actions directed at critical infrastructure that can destroy, disrupt or destabilise the work of structures vital to society. Cyberattacks have recently increased in intensity and complexity and have a variety of targets. The difference between the terms cybercrime and cyber warfare is delineated by the motivation of the actors involved, the situation and the context in which they operate. Actions in cyberspace, referred to as cyber warfare, are a form of hybrid warfare and aim to weaken the enemy country by compromising its core systems. In addition, these actions are supported by organised groups or states and are generally identified only after significant damage has already been done. Cyberwar incidents are increasing, not only among states, but also among terrorist groups and political or social organisations. The tools and techniques are the same regardless of whether the cyber incident is classified as cybercrime, cyber warfare, cyberterrorism or hacktivism. However, cyber warfare involves more resources and time. The complexity of actions in cyberspace and the negative effects they have in all areas have made cybersecurity a priority on the international agenda. Due to the necessity of digitalisation for all sectors, cyberspace has become the area of choice for the conduct of most of the activities. "Cyberspace is, in all truth, the battlefield on which the war of the future is currently being fought."[8] By utilising this environment, cyber operations will probably play a vital role in hybrid warfare, especially for mass manipulation and intelligence gathering, espionage, sabotage or economic disruption, destroying military resources or organisations, and targeting critical infrastructures that are vital for a developed society. In order to counter or reduce cyberattacks, actors such as the EU, NATO or the USA are focusing their efforts on ensuring

6 Singer–Friedman 2014.
7 Polyakova et al. 2021.
8 Cunningham 2020: 2.

a high level of cybersecurity by improving cyber resilience and incident response capabilities.[9] "If you know the enemy, and know yourself, you need not fear the result of a hundred battles. If you know yourself, but not the enemy, for every victory gained, you will also suffer defeat. If you know neither the enemy nor yourself, you will succumb in every battle."[10] Cybersecurity is a great umbrella term referring to protect the confidentiality, integrity and availability of system, data and information. So, when the data is transmitted through the Internet or when data is saved locally on a device, it needs to be protected. Protected data means maintaining confidentiality, integrity and availability.[11]

Figure 1: The CIA Triad
Source: Cyber One 2019

The CIA (Confidentiality, Integrity, Availability) model describes three important goals of cybersecurity such as confidentiality, integrity and availability:[12]

- Confidentiality – means that the information is not accessible for unauthorised access even if the access is required by devices, processes or people. In other words, confidentiality means keeping data and information secret. The main way confidentiality is accomplished is through encryption. Confidentiality is a complex task which presupposes that information and data need to be protected against unauthorised

[9] European Parliament 2022.
[10] Tzu 1910.
[11] Oriyano–Solomon 2020.
[12] Chai 2021.

access, data is not intercepted by a third party, only authorised people can access data, and that there must be a mechanism that allows the verification of the identity of the entity with access.[13] By way of example, a breach of confidentiality means that someone gains access to information which they should not have access to, regardless of whether the breach is voluntary or involuntary.

- Integrity – refers to the authenticity of information, provided the information is not altered, and the source of information is genuine. It means that data and information in transit, saved or processed has not been altered accidentally or intentionally.
- Availability – means that information, services or resources are accessible to authorised users. Availability can be defined as timely access to genuine data and information for authorised users.

Different tools can be used to ensure the confidentiality, integrity and availability of information. Each tool can be utilised as a part of the information security process. Authentication, authorisation and nonrepudiation are tools which can be used to maintain system security with respect to the CIA triad:[14]

- Authentication – involves proving the user's identity. Authentication can be accomplished by identifying someone through one or more of three factors such as something they know (a password or a private key), something they have (a physical key, a smart card), something they are (face, fingerprint), or something they do (how they walk, how they pronounce a passphrase). For security reasons, combinations of two or more elements of these categories are used (2FA – two factors authentication) in order to prove the user's identity.
- Authorisation – is the step that follows authentication. Authorisation refers to the specific permissions that a particular authenticated user should have, given his/her authenticated identity. Each user or process has associated privileges, so authorisation means establishing privileges. For instance, in case of cyberattacks, the hacker has the target's privileges. If the user used an administration account, the hacker has all the privileges, and they can do everything. In planning authorisation, it is important to follow

[13] Shakarian et al. 2015.
[14] Graham et al. 2011.

the principle of least permissions – each person should have only the permission that she/he needs to do their job.
- Auditing – is collecting information about an individual's activities. Specifically, tracking is similar to Auditing. Every action made by a user is recorded in log file and these files can be analysed.

In sum, authentication proves the user's identity, authorisation assigns permission to individuals, and auditing analyses the user's behaviour and activities.

Types of cyberattacks

The cybersecurity kill chain stages model, derived from the military model of anticipating possible enemy actions in order to neutralise the target, is the basic model used for tracking and preventing cyber intrusions at various stages.[15] In defence strategy, the goal is to understand how the enemy will act and then move on to identify the appropriate technique. The instrumentation of a cyberattack is time-consuming and involves the use of various techniques depending on the vulnerabilities identified in the host systems. Cybersecurity kill chain provides an overall picture of the phases commonly invoked in a cyberattack. In general, a cyberattack, whether it is an illicit action against a person, group, organisation or nation includes the following steps:[16]

- Reconnaissance – it involves passive information gathering without interaction or potential exploratory contact with the victim by using a phishing technique. Public sites such as Facebook, Twitter, LinkedIn or official sites are generally used to collect information regarding a potential victim, in order to identify his/her possible weaknesses.
- Scanning – acquiring more technical detailed information. Most activities are focused on identifying weaknesses in target systems, such as configuration settings. Known vulnerabilities, applications and weaknesses in general depend on the software or hardware components installed on the target device.

[15] Diogenes–Ozkaya 2019.
[16] *ATT & CK Matrix for Enterprise* s. a.; Diogenes–Ozkaya 2019; Oriyano–Solomon 2020.

- Weaponisation – different "weapons" are built in order to attack the victims at different stages. The instruments created for this purpose depend on the vulnerabilities identified after scanning. For instance, an infected file can be created and sent to the victim.
- Infiltration and Privilege Escalation – trying to exploit one or more identified vulnerabilities in order to gain access to a resource and then escalating access privileges. Hardware, software and human factor vulnerabilities are exploited in order to gain access. Of the three types of vulnerabilities, humans are the most vulnerable, so they can be targets of social engineering attacks such as phishing, spear phishing, etc., for gaining access. Often network access can be done through unprivileged access which restricts or makes it impossible to run a malicious code and an account with higher privileges is sought. Privilege escalation can be both vertical and horizontal. For vertical escalation, an attacker needs to perform actions that involve administrative access, so the purpose is to gain admin privileges higher level rights. In horizontal escalation, the attacker uses a normal account to access an account with high privileges. The purpose is not to upgrade the privilege of an account, but to access an account with higher privileges.
- Exfiltration – is the phase where the adversaries apply different techniques to steal data, modify or delete sensitive files, or obtain configuration information. The action depends on the purpose of the attack. Once an attack has reached this phase, it is considered successful. The exfiltration of the data identified in the system can be done either via email, downloaded directly to another device or saved on external drives, or using malware to infect a target and send the data from the victim's computer.
- Access extension – additional exploit can be installed in order to grant permanent access to the system. In general, techniques such as rootkit or similar tools are used to provide easier silent access.
- Assault – the purpose of this stage is to cause damage by removing or modifying critical configuration files or parameters in order to alter the way in which a device operates. This stage is not present in all attacks.
- Obfuscation – is covering the tracks, which is often a very important step especially when the aim is to collect information and return to the system in the long term or when the action is to remain "secret". This is one of the most difficult steps and it requires advanced technical knowledge.

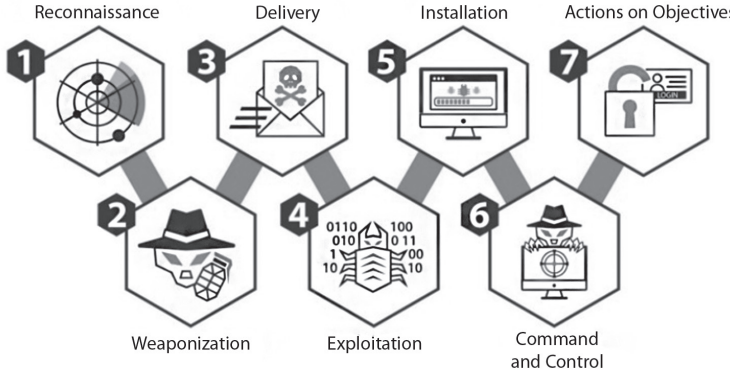

Figure 2: Cybersecurity kill chain stages developed by Lockheed Martin, 2011
Source: ATT & CK Matrix for Enterprise s. a.

A cyberattack and a cyber defence could be conducted at any scale: from the state level by the military to an organisation or even an individual level. The steps to instrument the tactics used in the cybersecurity kill chain also apply to illicit actions initiated by one state against another nation. When referring to nation state threat actors the most common tactics are:[17]

- Propaganda and information propagation – attempting to control people by spreading lies in order to make people lose trust in their country.
- Espionage, reconnaissance and information gathering between countries – monitor other country's communication systems to steal secrets, data or information.
- Sabotage – the competitors can take advantage of information theft in case of research and development, or military, economic or technological data.
- Denial-of-service (DoS) or Distributed DoS attacks – flooding a server with illegitimate requests in order to prevent it from responding to the legitimate ones.
- Malware – can disturb the proper functioning of the critical infrastructure.

The motivation for these types of attacks can be military if the aim is to control key elements of an enemy nation, or civilian if the target is a critical infrastructure with direct impact on society, or hacktivism if the aim is related to ideological

[17] Geers 2008; Fortinet 2022.

promotion. Propaganda used in psychological warfare uses misinformation as a method to create panic among the population or to manipulate their behaviour. The most common medium for propaganda is social media and the internet. Social networks such as Twitter, Facebook, LinkedIn, Instagram, etc. are often used to manipulate public opinion, spread diverse political views and even go "deep behind enemy lines".[18] In the digital society, there are not any totally effective methods of countering propaganda unless the rights to information and free expression are violated. There are states such as Russia, China or North Korea that are trying to secure their national information space by introducing suppression measures targeting social networks and media.[19]

Figure 3: Disinformation and propaganda
Source: Bayer 2019

There are situations when both Russia's and China's internal and external efforts have been effective. Propaganda and disinformation serve multiple purposes and even use political bots to intentionally distribute false information on and through social media.[20] Disinformation campaigns are often used in hybrid attacks and lately there has been an increase in the number of attacks given that the majority of daily activities take place mainly online. The availability of services and resources can be an issue in the case of Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks. A DoS attack occurs when a legitimate user is

[18] Bayer 2019: 38.
[19] Geers 2008.
[20] Bayer 2019; Woolley 2020: 89–110.

unable to access information, resources, devices or services due to the actions of malicious cyber threat actors that generate synthetical traffic.[21] For instance, due to the DoS attacks, legitimate users have no access to the information displayed on a website, or they cannot use the email service or their online account. DoS are considered effective weapons in cyber warfare. DoS attacks involve flooding the target host or network with illegitimate requests and the target cannot respond to legitimate requests made by legitimate/regular users. A more complex type of DoS attack, using multiple hosts to launch the malware, is the DDoS attack, which has a similar effect – overloading and crashing, or lowering the target's performance intentionally. The essential difference between a DoS and a DDoS attack is that instead of launching an attack from one location, the target is attacked by using multiple connected devices. DDoS attacks typically use botnets. A botnet is a collection of compromised computers often referred to as 'zombies', infected with malware that allows an attacker to control them.[22] The attacker controls and coordinates all the infected hosts in a DDoS. The infected hosts are usually called zombies.

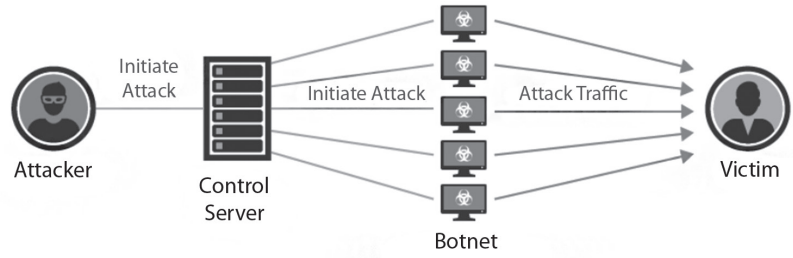

Figure 4: A Distributed Denial-of-Service Attack
Source: Imperva 2017

DDoS attacks are often considered effective weapons due to the technical requirements and low costs, but the effects can be very serious. These attacks are frequently launched by hackers wishing to express their ideological disagreement, or by other groups that intend to limit access to information, to disrupt communication, to paralyse the activity of websites or even of critical

[21] CISA 2021.
[22] Radware s. a.

infrastructure in an "enemy" country.[23] Espionage is a common practice in the military as well as in industry, economics or technology and focuses on:[24]

- stealing state secrets and trade secrets
- intellectual property rights
- sensitive information in strategic fields

Threats to cybersecurity are on an upward trend and, in addition, the complexity and impact of cyberattacks is increasing. Furthermore, as the problems facing society become more complex and diverse, companies are forced to operate predominantly online. It has been observed that cyber espionage has received a boost and new opportunities for cyber criminals have emerged.[25] A cyber sabotage attack can be defined as an illicit action financed or coordinated by a state actor against a country aimed at disrupting communications services, economic activities, military activities or at destroying critical infrastructure. This type of attack may have physical consequences.[26]

Cyberattack case studies

The battle for supremacy is fought in every field, be it military, economic or technological. For instance, Russia is trying to improve its power position across the globe through its cyberspace-funded actions, as demonstrated by its attacks on Estonia, Crimea and Ukraine. Moreover, it is conducting a powerful influence and disinformation campaign using social media. China is concentrating its efforts on stealing intellectual property based on illicit actions in cyberspace to provide economic comfort and/or technological progress. Government organisations in North Korea have made a name for themselves by launching cyberattacks especially on entities that attempt to denigrate their national image.[27] After a successful cyberattack, it is quite difficult to identify how it was orchestrated and especially who the actors directly involved were. Thus, if the attack is not claimed by any state or group, assumptions are made to identify the actors

[23] Radware s. a.
[24] Enisa 2020.
[25] Enisa 2020.
[26] Molina 2022.
[27] Cunningham 2020.

depending on the mode of attack, the geopolitical context and the evidence identified. There are quite a few instances where the U.S. or U.S. governmental organisations have been accused of unlawful actions directed against a state or a nation. Articles in specialised literature point out that cyber warfare started in 2010 with Stuxnet, considered the first cyber weapon to cause physical damage, which was allegedly launched by the U.S. against Iran's nuclear program.[28] After this incident, the series of cyber warfare attacks continued and most of them were instrumented using developed malicious code, such as Trojans, worms, or combinations thereof. Propaganda is an old tactic used in modern warfare by many states. If radio and television were used in the Cold War, nowadays propaganda also employs modern electronic techniques to manipulate or influence people's perceptions. The techniques used in propaganda vary depending on the goal to be achieved, so stealing and revealing private information, hacking different devices, creating and spreading fake news are the most common techniques targeting politicians, influential people or private organisations.[29] Propaganda is considered a type of cyberattack because social media landscape allows misinformation to spread further and possibility to create social network false accounts. In addition, using bots to spread false information, database and device hacking for stealing critical data, recruiting new members into violent and dangerous movements by using social network are specific to cyberattacks approaches. Disinformation and propaganda campaigns have Russia as the main actor. Russia has frequently been suspected of using fake social media accounts for disinformation and propaganda campaigns. Many of the disinformation campaigns by various Russian groups have been aimed at influencing public opinion and undermining the credibility of governments in several countries such as the United Kingdom, the United States and the European Union.[30] The campaigns have been carried out at crucial moments, especially in the run-up to elections, and have used social media as a landscape.[31] After a series of attacks that were instrumented using various social networks and aimed at misinforming and undermining public confidence in national values, Facebook and Twitter started to develop new technologies to reduce propaganda through social networks. Methods of protection against propaganda are primarily concerned

[28] CSIS 2022; Cunningham 2020; Fortinet 2022.
[29] Trend Micro 2017.
[30] CSIS 2020.
[31] Satariano 2019; Stubbs 2020.

with public awareness. People need to be informed about the repercussions that can arise if seemingly harmless information is shared on social media, the common practices used by malicious individuals or groups on social media, and the possibilities for securing information saved on various devices. Even more so, information should only be retrieved from trusted sources. Starting with the Internet era, there have been many cyber incidents politically motivated that were aimed at data and information theft in order to gain technological knowledge or other states' secrets. When these espionage actions are planned and/or supported by the nation, intangible damage often cannot be estimated at first assessment. Some of the most notorious attacks, which have been supported by state actors and which have taken cyber espionage to another dimension are Operation Aurora (2010) and Red October (2012). Operation Aurora was a series of cyberattacks from China that targeted U.S. private companies such as Google, Yahoo, Dow Chemical, etc., and the goal was to steal trade secrets.[32] On January 2010, Google announced that it had been the victim of a cyber espionage attack launched by China and multiple Google email account had been hacked into. After the announcement made by Google, several companies publicly admitted that their systems had also been hacked by the same adversary. The attack was very complex. During the first stage – reconnaissance – company or other official websites were most likely browsed for employee information, focusing especially on email addresses. Then, networks were scanned for hardware and/or software vulnerabilities. During the weaponisation stage, a Trojan (Hydraq Trojan) designed to steal intellectual property was most likely constructed.[33] The Trojan was based on a software vulnerability identified in Microsoft Internet Explorer so that in the first phase all Windows-based systems were affected. It is assumed that the attack was based on a link from a 'trusted' source to a malicious website. Employees, following spear phishing campaigns via email or chat, received a link to a malicious website hosted in Taiwan. By exploiting a vulnerability in the Microsoft Internet Explorer browser, a malicious JavaScript code (Hydraq Trojan) was downloaded locally, where it executed another exploit that had the ability to open a backdoor on a compromised system, enabling the attackers to receive unauthorised access to the

[32] Council on Foreign Relations 2010.
[33] Shakarian et al. 2015.

system.[34] Probably only privilege escalation was required to move from unauthorised access to locating the intellectual properties repository and stealing company secrets. After investigating the attacks, the indicators pointed that Operation Aurora was executed with the full knowledge or even under the directive of the Chinese Government and the attack target.[35] To reduce and minimise the damage in case of espionage attacks, it is recommended that applications be updated regularly, and sensitive information be secured. In addition, employee awareness sessions about spear phishing or email attachments or links can make the difference between failure or success for a hacker. A typical example of espionage is the cyberattack called Red October. Red October was a large cyber incident whose main objective was to gather intelligence from diplomatic, governmental and scientific organisations in different countries. It was discovered in October 2012 by a team from Kaspersky, a Russian company. It is believed that the attack was launched in 2007 or earlier against Eastern European countries, former USSR Republics, countries in Central Asia and others. In the first stage, before launching the attack, the victims were carefully selected and analysed, then after the reconnaissance and scanning stages, the weaponisation stage was carried out. In the weaponisation stage, a malware was built, consisting of distinct modules with various objectives and functions such as to steal encrypted files or to recover and steal deleted files, to recover deleted files from an USB stick, to monitor when a USB stick is plugged in, etc. For the malware to reach the system and infect a target, spear phishing email was used and vulnerabilities in MS Office and Microsoft Excel were exploited. Once a system has been infected, attackers have often used information exfiltrated from the infected target so as to get into other systems. Targets were not only traditional workstations, but also mobile devices because the malware was designed so that it was able to steal information from mobile devices, and the malware was also able to steal information from various configuration equipment such as routers or switches. A detailed analysis of the malware indicated that Russia was behind the espionage attack dubbed Red October.[36]

[34] Enigma Soft 2010.
[35] Shakarian et al. 2015.
[36] Kaspersky Lab 2013.

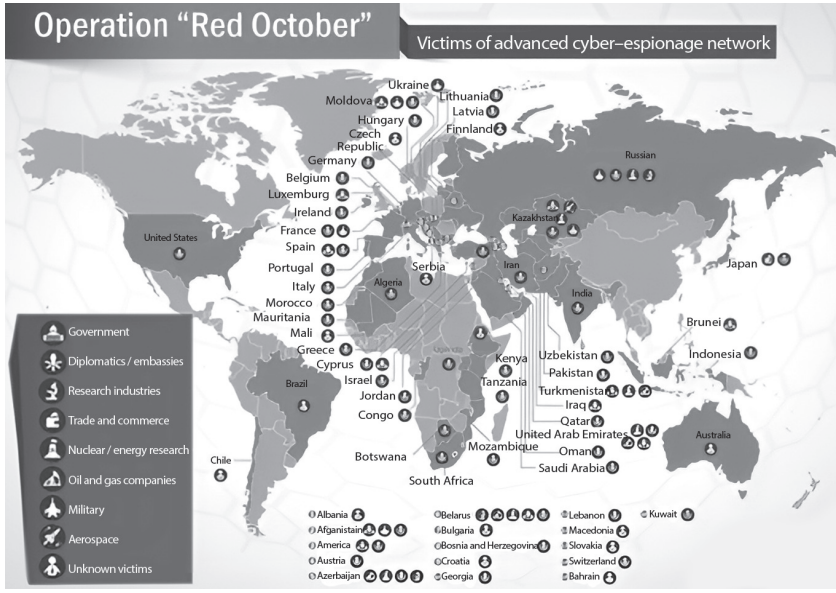

Figure 5: Victims of Red October
Source: Max 2013

These cyber espionage attacks were the first in a series of large-scale attacks, but events have not stopped. Lately, the number of nation states backed cyber espionage attacks targeting the economy are on the rise and this trend is likely to continue.[37] Protection methods, which could reduce or minimise the risk of a cyber espionage attack, primarily involve creating security policies for employees, actions and the organization and training staff on the policies developed. Regular assessment of risks and vulnerabilities to identify possible security breaches and, last but not least, regular updating of installed software.

DoS and DDoS attacks can be weapons in cyber warfare and are intended to disrupt communication channels between government institutions and citizens in order to decrease public confidence, demoralise residents and introduce an element of panic and instability. In addition, they aim to disrupt critical infrastructure such as energy utilities, transportation, hospitals, banks, water supply and so on, and produce panic, chaos and instability. In other words,

[37] ENISA 2020.

DoS attacks prevent legitimate users from accessing services or resources of a website by flooding it with fake requests. Servers are unable to deal with a large number of illegitimate requests and cannot distinguish between a legitimate and an illegitimate request, and, consequently, they become inoperable. These types of attacks disrupt critical operations and block access to website by both military and civilian people.[38] DoS and DDoS attacks are quite common because they are not necessarily costly and there are services that allow DoS attacks to be launched. Moreover, botnet codes can be found on the Dark Web. Among the string of attacks aimed at destabilising lines of communication between government and citizens are:[39]

- The May 2007 attack on the websites of the Estonian government institutions, following the decision by Estonian officials to move the World War II bronze memorial statues.
- The 2008 cyberattack targeting the websites of government institutions in Georgia. The attack took place in the immediate aftermath of the war between Russia and Georgia.

In April 2007, a series of DDoS attacks were launched against Estonian websites following the government's decision to relocate the bronze statue of the Soviet Soldier in the centre of Tallinn. For Russian minorities, the statue represented 'liberation', while for many Estonians it represented Moscow's dominance and oppression; therefore, the relocation led to disputes between the police and the opponents of the government's decision.[40] In addition, the economic relations between the two states were deteriorating, various events were directed at Estonian embassy employees in Moscow and ethnic tensions in Estonia led analysts to assume that Russia was directly involved, but it remained only at the level of supposition because Russia never admitted its direct involvement.[41] Amidst internal and external discontent, between 27 April 2007, and 18 May 2008, Estonia faced a series of DDoS attacks aimed at rendering government websites unavailable and paralyzing various communication networks. The first attacks were carried out from IP addresses outside Estonia, but later attacks were also launched from inside the country. Hackers provided people involved in the

38 Imperva s. a.
39 SUNY 2022.
40 Ottis 2008.
41 Herzog 2011: 49–60.

'movement against Estonia' with clear instructions on how DDoS attacks can be launched, and websites have also been set up for this purpose. All instructions were in Russian and advised people how to attack government websites with ping flood, UDP floods,[42] email spam, etc. which indicated that the Russian Government itself was behind the groups. The peak of the DDoS attacks on Estonia was considered to be 9 May 2007, the day when Russians celebrate 'Victory Day'. On May 19, the attacks suddenly stopped.[43] Typically, DDoS attacks are intended to distract the attention of the victim from the hacker's true motive because, while the victim is focusing on the DDoS attack, other illicit actions, such as collecting sensitive information, may be undertaken. After the attack Estonian officials asked Russia to investigate Russian IPs, but no response to the request was received. Experts from the EU and NATO were brought in to prove the Russian involvement in the attacks on Estonia, but the Kremlin's involvement could not be clearly proven.[44]

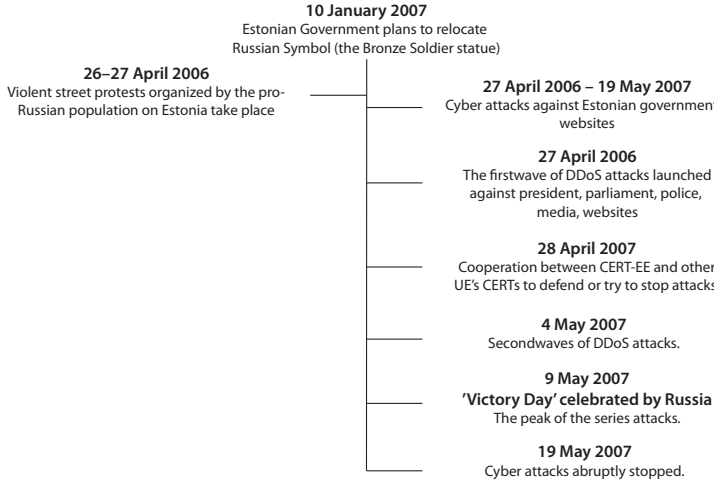

Figure 6: Timeline of the DDoS key element attack on Estonia 2007
Source: 2007 Cyber Attacks on Estonia

[42] Types of DoS or DDoS attacks. The target is overwhelmed with specific illegitimate requests and becomes inaccessible to legitimate requests.

[43] Herzog 2011: 49–60.

[44] Herzog 2011: 49–60.

Following the DDoS attacks against Estonia, NATO and EU member states' agenda included discussions on new cybersecurity guidelines and punishments for nations that engage in digital warfare. In addition, the 2008 Bucharest Summit created the Cyber Defence Management Authority in Brussels (CDMA), tasked to "centralize cyber defense operational capabilities across the Alliance" and established the Cooperative Cyber Defence Centre of Excellence (CoE) in Tallinn, responsible for the "development of long-term NATO cyber defense doctrine and strategy".[45] Furthermore, in May 2008, the Estonian Ministry of Defence implemented the National Cyber Security Strategy.[46] On 8 August 2008, Russia decided to go to war on the side of South Ossetia, in response to Georgia's military actions against the separatist Ossetian regime. Against this background, Georgia detected a series of DDoS cyberattacks against government and media websites. The aim of these cyberattacks was to isolate Georgia from the global community and "silence" important Georgian media organisations. The DDoS cyberattacks against Georgia were carried out in two phases:[47]

- In the first phase, DDoS attacks against government and media websites were reported, that were carried out using botnets. A botnet is a malicious piece of code able to infect other computers and turn them into 'zombies' so that they can be coordinated from a central 'command and control' server.
- During the second phase, the list of victims of DDoS attacks was extended. In addition to government and media victims, the list included financial, business and education institutions. Moreover, public email addresses were used for spam email campaigns and SQL Injection attacks were launched in order to identify as many possible recruits' emails as possible.

During these phases, a number of individuals were recruited and trained to continue to launch DDoS attacks against Georgia. As with the attacks against Estonia, recruits were instructed on how to launch targeted attacks and websites were created containing tools for launching DDoS attacks from private machines. Among the websites accessed by the recruits were StopGeorgia.ru and XAKEp.ru.[48] During the attacks, the websites in Georgia were temporarily unavailable,

[45] Hughes 2009: 2.
[46] *2007 Cyber Attacks on Estonia.*
[47] Kozlowski 2013: 237–245.
[48] Shakarian 2011: 63–68.

which meant that communication in the country was severely disrupted, which also affected the government's link to the outside world. Moreover, fake messages were displayed on the official websites that were still 'working'. The DDoS attacks against Georgia which aimed to "isolate and silence", suggest coordination between ground military operations and cyberattacks, although Russia did not want to be associated with the cyberspace activities. There is a difference in analysis as compared to the Estonian attacks for "the Russian cyber campaign in Georgia in August 2008 represents actions occurring simultaneous with major conventional military operations".[49] No clear evidence was found that the DDoS attacks against Estonia and Georgia were supported by the Russian Government. However, given the context and the relations between the two countries, the support of Russia for the Russian group that 'orchestrated' the attack is not entirely ruled out. In 2017, Russia's military admitted the scale of its information warfare effort, which makes the assumptions about the Russian involvement to become more certain. The 2022 events in Ukraine demonstrated the effectiveness of state-sponsored attacks in launching politically-motivated DDoS against critical infrastructure and government institutions.[50] In 2010, a malicious software worm called Stuxnet disrupted the Iranian nuclear program and the Stuxnet worm was detected in multiple computers in Iran. The main target of the attack was aimed at centrifuges used in the uranium enrichment process at the Natanz nuclear power plant in Iran, and the purpose of the worm was not espionage but sabotaging the production of enriched uranium.[51] At the time, Iran did not officially state the reason why some of the nuclear power plants temporarily stopped production. The biggest problem stems from the way programmable logic controllers (PCLs) that control the automation of physical manufacturing systems were accessed, controls that are also used to automate nuclear centrifuges, located in top-secret locations and not connected to the Internet. The Stuxnet worm was distributed only via infected USB sticks and exploited four 'zero-day' vulnerabilities[52] in the Windows operating system.[53] Moreover, the malware used two valid digital certificates from manufacturers

[49] Shakarian 2011: 68.

[50] Nicholson 2022.

[51] Baezner–Robin 2017.

[52] A weakness of a system discovered and not patched yet. These types of vulnerabilities are often used by cyberattacks and the attacks are called 'zero-days'.

[53] Naraine 2010.

JMicron and Realtek – one of the largest hardware manufacturers.[54] In the Windows operating system, a valid digital certificate is required when installing a driver and digitally signed software is considered 'clean' by antivirus or anti-malware solutions. In addition, using a digital certificate from a trusted manufacturer extends the time in which the virus can be detected. The existence of valid certificates in Stuxnet allowed the installation of the worm in computers when the USB stick was used, and then the search for Siemens Simatic WinCC/Step 7 software, an application used in the control of industrial equipment.[55] Windows vulnerabilities were exploited because programmable controllers are generally programmed from computers not connected to the Internet. If the logic components could be programmed via other operating systems, appropriate vulnerabilities associated with the desired system were certainly used. Although it is not known exactly when the programming of the Stuxnet worm began, there are sources that claim that it had been worked on as a team, for at least two or three years[56] or even as early as 2005,[57] so that after the classic reconnaissance and scanning stages, the weaponisation was completed. It can be assumed that the team members either had advanced knowledge of programming and industrial control systems developed by Siemens – an unlikely assumption – or they documented and identified vulnerabilities, or pieces of code capable of exploiting certain security holes. After identifying vulnerabilities in the Siemens physical equipment, vulnerabilities in the Windows operating system – the system used to connect industrial control systems – were sought. The identification of the four 'zero-day' vulnerabilities certainly led to the next step – the theft of valid digital certificates. For the theft of the certificates, a physical entry was probably performed. Analysing the modus operandi as well as the architecture of the systems that control the centrifuges used in the production of the enhanced uranium, it is likely that the infiltration stage initially used an attack directed at one or more material suppliers and equipment manufacturers, and then followed a waiting period before the Stuxnet worm reached its final target. Based on the modules identified in the worm, sources claim that the attack against Iran's nuclear program was carried out in three stages:[58]

[54] Eset 2010.
[55] Falliere et al. 2011.
[56] Baezner–Robin 2017.
[57] Fruhlinger 2022.
[58] Teixeira et al. 2015: 149–183.

- After entering the system via an infected USB stick, on the machine or network using Windows as operating system, the worm replicates itself.
- It looks for a specific software such as the Siemens Step 7 software, based on Windows, and used for programming industrial control systems (Supervisory Control and Data Acquisition – SCADA) that operate hardware equipment in particular, nuclear centrifuges used to enrich uranium.
- It compromises all programmable logic controls using 'zero-day' vulnerabilities that have not yet been publicly identified and modifies the operating parameters of the centrifuges, resulting in their destruction.

The detection of abnormal behaviour for the sample file received by VirusBlockAda, a Belarusian antivirus company, in June 2006, coincided with the date when the digital certificates expired. A month later, an announcement was made public notifying the company of 'zero-day' vulnerabilities being exploited, and the antivirus community began investigating this highly sophisticated malware. It is only in the closing months of 2010 that Iranian officials admitted that nuclear power plants have been infected with a virus and in November 2010, they completely shut down the Natanz plant without making public the reason. The detection of the Stuxnet cyberattack represented a reason for concern in most countries around the world as the attack was labelled as cyber "terrorism" and is considered to have paved the way for cyber warfare.[59] No state claimed responsibility for the attack, and in addition, no member of the team that worked on Stuxnet has been identified. The effects were both political and social and had a strong economic impact for Iran. Socially, fear and a strong sense of insecurity spread among the population because strategic points, where the level of security was considered to be the highest, were attacked. Although the final target was Iran, many computers around the globe were infected, creating the same sense of global insecurity among the worldwide population. The economic impact was disastrous for Iran, which had to delay its nuclear program and invest in security and cybersecurity measures. After the Stuxnet attack one question needs to be answered, namely: "Will cyber weapons such as Stuxnet proliferate?" Cybersecurity experts believe, however, that there is a possibility that Stuxnet variants will become common.[60]

[59] Kaspersky 2012.

[60] Shakarian et al. 2015: 14.

Defensive approaches of cybersecurity

If we refer to the measures that need to be taken to reduce or minimise risk in the face of cyberattacks or to increase the resilience of organisations or countries to threats in cyberspace, we need to refer to collective measures and then to measures that any organisation needs to consider, especially given that the cyber threat landscape is aggravated by geopolitical tensions. Cyberspace vulnerabilities can be reduced if the following minimum measures are observed:[61]

- increasing the security of information
- implementing data security standards
- increasing the number of specialists in the cybersecurity field
- coordinating actions at national and/or regional level
- developing and continuously updating global and national security strategies

In 2020, the European Union updated its cybersecurity strategy in line with the complexity of the threats posed by the increase of digitalisation and interconnectivity. The new strategy ensures an open global internet and provides safeguards to ensure not only security, but also the protection of European values and fundamental rights. Thus, the new EU cyberstrategy, in response to the complexity of the new cyberattacks, aims to implement three main instruments in three areas of EU action:[62]

"Resilience, technological sovereignty and leadership"[63] – critical infrastructures and services are increasingly interdependent and digitalised, only that infrastructures and services must be secure by design and resilient to cyber incidents, and any vulnerabilities detected must be eliminated. The focus is to build a European Cyber Shield. To this end, Computer Security Incident Response Teams (CSIRTs) and Security Operations Centres (SOCs) constantly monitor and analyse traffic to detect intrusions and anomalies in real time, and SOCs isolate suspicious events using AI and machine learning techniques. The EU proposes to build a network of Security Operations Centres across

[61] Bejtlich 2015: 159–170; Irwin 2021.
[62] European Commission 2020.
[63] European Commission 2020: 12.

the EU and support the improvement of the existing SOC centres. In other words, through collaboration and cooperation, a real cybersecurity shield for the EU can be created. These are just a few ongoing initiatives, but there are also initiatives to attract cybersecurity talent, a reinforced presence on the technology supply chain, an Internet of Secure Things, or an ultra secure communication infrastructure.

"Operational capacity to prevent, deter and respond"[64] – the EU's strategic initiatives aim to establish a Joint Cyber Unit; encourage a Member States' cyber intelligence working group within EU INTCEN; prevent and discourage malicious cyber activities; review the Cyber Defence Policy Framework; offer support for the development of an EU Military Vision and Strategy on Cyberspace as a domain of operations; reinforce cybersecurity of critical space infrastructure under the Space Program.

Cooperation to advance a global and open cyberspace – the "EU should continue to work to promote a political model and vision of cyberspace grounded in the rule of law, human rights, fundamental freedoms and democratic values".[65] Thus, the EU Strategic Survey is about defining a set of objectives in the international standardisation process; promoting international security and stability; providing guidance on the application of human rights and fundamental freedoms in cyberspace; strengthening and promoting the Budapest Convention on Cybercrime; expanding the EU cyber dialogue with other countries and regional organisations; strengthening structured exchanges with private sectors, academia and the civil society.

In order to reduce or minimise the risk of a cyberattack, whether the attackers are individuals, groups or nation states, organisations need to develop their own cybersecurity strategies. A good defence strategy is based on the "defence-in-depth" concept, which involves the application of different techniques, technologies and strategies to protect data and resources.[66]

64 European Commission 2020.
65 European Commission 2020.
66 Krause et al. 2021.

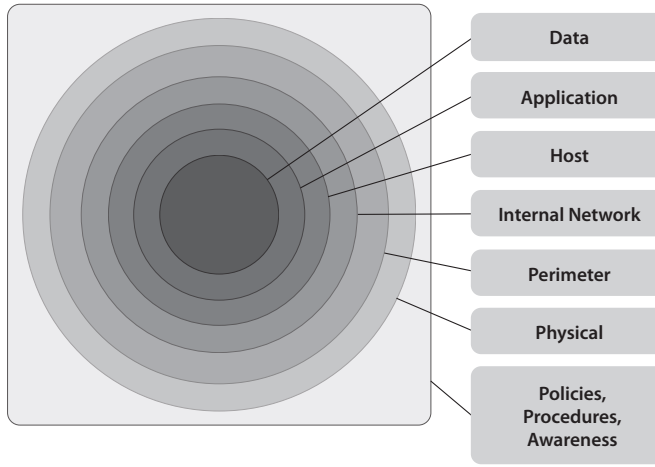

Figure 7: Defence-in-depth strategy
Source: Omoyiola 2019

The defence-in-depth approach, presupposes the existence of a number of defensive mechanisms aimed to protect data and information, especially since there is no single method to protect against any type of attack. Each method and mechanism contributes to reducing the risk of attacks arising from hardware, software and human resource vulnerabilities. Of the three types of vulnerabilities, the most exposed link is people, so developing policies, procedures, and awareness sessions for this factor is an extremely essential measure.[67]

Conclusion

Hybrid warfare is defined as a mixture of conventional and unconventional methods used against a much stronger adversary that aims to achieve political objectives that would not be possible with traditional warfare. This chapter pivots on the concept of cyber warfare, perceived as the first stage in hybrid warfare and one of the many unconventional ways in which an asymmetrical

[67] Oancea et al. 2019: 46–50.

fight can be carried out. The chapter starts by defining the fundamentals of cybersecurity, in the framework of the CIA triad, which encapsulates three main concepts such as confidentiality, integrity and availability, and the tools that facilitate their implementation. This section is dedicated to different types of cyberattacks and the stages any cyberattack presupposes – reconnaissance, scanning, weaponisation, infiltration and privilege escalation, exfiltration, access extension, assault, obfuscation. This section also discusses tactics used in cyber warfare and their potential consequences. By way of extended example, the case studies discussed in this chapter offer a comprehensive view to how various types of cyberattacks were conducted and how their tools were utilised so as to produce disruptive effects on organisations, institutions, governments and states. The last part of the chapter focuses on various modalities to counter cybersecurity threats and discusses international organisations' such as the European Union, as well as individual efforts aimed to increase resilience and mitigate the devastating effects of attacks in cyberspace.

Questions

1. Which are the elements of the CIA Triad and what does each of them refer to?
2. What are the generic stages of instrumenting a cyberattack?
3. What are the most common tactics utilised by one nation against another?
4. What are the goals of cyber propaganda attacks and of cyber espionage attacks?
5. What is the objective of a DoS attack?

References

2007 Cyber Attacks on Estonia. Online: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

ATT & CK Matrix for Enterprise (s. a.). Online: https://attack.mitre.org/

Baezner, Marie – Robin, Patrice (2017): *Hotspot Analysis. Stuxnet, Version 1.* Zürich: Center for Security Studies.

Bayer, Judit – Bitiukova, Natalija – Bárd, Petra – Szakács, Judit – Alemanno, Alberto – Uszkiewicz, Erik – Carrera, Sergio – Vosyliute, Lina – Guérin, Julia (2019): *Disinformation and propaganda. Impact on the Functioning of the Rule of Law in the EU and its Member States.* Brussels: Centre for European Policy Studies. Online: www.ceps.eu/ceps-publications/disinformation-and-propaganda-impact-functioning-rule-law-eu-and-its-member-states/

Bejtlich, Richard (2015): Strategic Defence in Cyberspace: Beyond Tools and Tactics. In Geers, Kenneth (ed.): *Cyber War in Perspective: Russian Aggression against Ukraine. Tallin: NATO CCD COE Publications. 159–170.*

Chai, Wesley (2021): *Confidentiality, Integrity and Availability (CIA Triad).* Online: www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

CISA (2019): *Understanding Denial-of-Service Attacks.* Cybersecurity and Infrastructure Security Agency. Online: www.cisa.gov/uscert/ncas/tips/ST04-015

Council on Foreign Relations (2010): *Operation Aurora.* Online: www.cfr.org/cyber-operations/operation-aurora

CSIS (2020): *Countering Russian Disinformation.* Washington, D.C.: Center of Strategic and International Studies. Online: www.csis.org/blogs/post-soviet-post/countering-russian-disinformation

CSIS (2022): *Significant Cyber Incidents Since 2006.* Washington, D.C.: Center of Strategic and International Studies. Online: https://csis-website-prod.s3.amazonaws.com/s3fs-public/221006_Significant_Cyber_Incidents.pdf?LnVEOhJ.dvbm2FkfowopP0XkTL7Crysq

Cunningham, Chase (2020): *Cyber Warfare. Truth, Tactics, and Strategies.* Birmingham: Packt Publisher.

Cyber One (2019): *What Is the CIA Triad?* Online: https://comtact.co.uk/what-is-the-cia-triad/

Diogenes, Yury – Ozkaya, Erdal (2018): *Cybersecurity – Attack and Defense Strategies.* Birmingham: Packt Publisher.

Enigma Soft (2010): *Hydraq Description.* Online: www.enigmasoftware.com/hydraq-removal/

ENISA (2020): *ENISA Threat Landscape 2020 – Cyber Espionage.* Annual report, 2020. Online: www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage

Eset (2010): *Why Steal Digital Certificates?* Eset research. Online: www.welivesecurity.com/2010/07/22/why-steal-digital-certificates/

European Commission (2020): *The EU's Cybersecurity Strategy for the Digital Decade.* Online: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Parliament (2022): *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).* Online: eur-lex.europa.eu/eli/dir/2022/2555/oj

Falliere, Nicolas – Murchu, Liam O. – Chien, Eric (2011): *W32.Stuxnet Dossier.* Symantec Security Response. Online: https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en

Fortinet (2022): *What Is Cyber Warfare?* Online: www.fortinet.com/resources/cyberglossary/cyber-warfare

Fruhlinger, Josh (2022): *Stuxnet Explained: The First Known Cyberweapon.* Online: www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Geers, Kenneth (2008): *Cyberspace and the Changing Nature of Warfare.* Online: https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf

Giles, Keir (2015): *Russia's Hybrid Warfare. A Success in Propaganda.* Berlin: Federal Academy for Security Policy. Online: http://www.jstor.org/stable/resrep22215

Graham, James – Howard, Richard – Olson, Ryan eds. (2011): *Cyber Security Essential.* London: CRC Press.

Herzog, Stephen (2011): Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security,* 4(2), 49–60.

Hughes, Rex B. (2009): NATO and Cyber Defence. Mission Accomplished? *Atlantisch Perspectief,* 8. Online: https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/NATO%20and%20Cyber%20Defence%20-%20Mission%20Accomplished.pdf

Imperva (2017): *How to Identify a Mirai-Style DDoS Attack.* Online: www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/

Imperva (s. a.): *Denial-of-service (DoS) Attacks.* Online: www.imperva.com/learn/application-security/cyber-warfare/#examples-of-cyber-warfare-operations

Irwin, Luke (2021): 5 Ways to Improve Your Information Security. *IT Governance,* 11 February 2021. Online: www.itgovernance.co.uk/blog/5-ways-to-improve-your-information-security

Kaspersky, Eugene (2012): *The Flame That Changed the World.* Online: https://eugene.kaspersky.com/2012/06/14/the-flame-that-changed-the-world/

Kaspersky Lab (2013): *Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide.* Online: www.kaspersky.com/about/press-releases/2013_kaspersky-lab-identifies-operation—red-october—an-advanced-cyber-espionage-campaign-targeting-diplomatic-and-government-institutions-worldwide

Klimburg, Alexander ed. (2012): *National Cyber Security Framework Manual.* Tallin: NATO CCD COE Publication.

Kozlowski, Andrzej (2013): Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal,* Special edition (3), 237–245. Online: https://doi.org/10.19044/esj.2014.v10n7p%25p

Krause, Tim – Ernst, Raphael – Klaer, Benedikt – Hacker, Immanuel – Henze, Martin (2021): Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors,* 21(18). Online: https://doi.org/10.3390/s21186225

Kushner, David (2013): The Real Story of Stuxnet. *IEEE Spectrum,* 50(3), 48–53. Online: https://doi.org/10.1109/MSPEC.2013.6471059

Max, Eddy (2013): How the 'Red October' Cyber-Attack Campaign Succeeded Beneath the Radar. *PC Magazine,* 14 January 2013. Online: www.pcmag.com/news/how-the-red-october-cyber-attack-campaignsucceeded-beneath-the-radar

Molina, Jesus (2022): *Real Time Flames: Welcome to the Age of Cyber-sabotage.* Online: https://waterfall-security.com/welcome-to-the-age-of-cyber-sabotage/

Naraine, Ryan (2010): *Stuxnet Attackers Used 4 Windows Zero-Day Exploits.* Online: www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/

Nicholson, Paul (2022): *Five Most Famous DDoS Attacks and Then Some.* Online: www.a10networks.com/blog/5-most-famous-ddos-attacks/

Oancea, Romana – Bârsan, Ghiță – Giurgiu, Luminița (2019): Approach on Increasing User Security Awareness. *International Conference: The Knowledge-Based Organization,* 25(3), 46–50. Online: https://doi.org/10.2478/kbo-2019-0116

Omoyiola, Bayo O. (2019): The Hard Reality of Information Security. *IOSR Journal of Computer Engineering,* 21(6), 16–18. Online: https://doi.org/10.9790/0661-2106011618

Oriyano, Sean-Philip – Solomon, Michael G. (2020): *Hacker Techniques, Tools, and Incident Handling.* Burlington: Jones & Bartlett Learning.

Ottis, Rain (2008): *Analysis of the 2007 Cyberattacks against Estonia from the Information Warfare Perspective.* Tallinn: Cooperative Cyber Defence Centre of Excellence. Online: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Polyakova, Alina – Boulègue, Mathieu – Zarembo, Kateryna – Solodkyy, Sergiy – Stoicescu, Kalev – Chatterje-Doody, Precious N. – Jonsson, Oscar (2021): *The Evolution of Russian Hybrid Warfare.* Washington, D.C.: Center for European Policy Analysis (CEPA). Online: https://cepa.org/wp-content/uploads/2021/01/CEPA-Hybrid-Warfare-1.28.21.pdf

Radware (s. a.): *Botnet Definition: What Is a Botnet and How Does It Work?* Online: www.radware.com/security/ddos-knowledge-center/ddospedia/botnet/

Satariano, Adam (2019): Russia Sought to Use Social Media to Influence E.U. Vote, Report Finds. *The New York Times,* 14 June 2019. Online: www.nytimes.com/2019/06/14/business/eu-elections-russia-misinformation.html

Shakarian, Paolo (2011): The 2008 Russian Cyber Campaign against Georgia. *Military Review,* 91(6), 63–68.

Shakarian, Paolo – Shakarian, Jana – Ruef, Andrew (2015): *Introduction to Cyberwarfare. A Multidisciplinary Approach.* Amsterdam: Elsevier.

Singer, Peter W. – Friedman, Allan (2014): *Cybersecurity and Cyberwar. What Everyone Needs to Know.* Oxford: Oxford University Press.

Stubbs, Jack (2020): Facebook Says Russian Influence Campaign Targeted Left-Wing Voters in U.S. *Reuters,* 02 September 2020. Online: www.reuters.com/article/usa-election-facebook-russia-idUSKBN25S5UC

SUNY (2022): *International Cyber Conflicts.* The State University of New York. Coursera online course. Online: www.coursera.org/learn/cyber-conflicts

SWD (2020): Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation. SWD(2020) 115 final. Online: https://ec.europa.eu/info/sites/default/files/1_en_swd_part1_v6.pdf

Teixeira, André – Kupzog, Friederich – Sandberg, Henrik – Johansson, Karl H. (2015): Cyber-Secure and Resilient Architectures for Industrial Control Systems. In Skopik, Florian – Smith, Paul (eds.): *Smart Grid Security. Innovative Solutions for a Modernized Grid.* Amsterdam: Elsevier. 149–183. Online: https://doi.org/10.1016/B978-0-12-802122-4.00006-7

The White House (2008): The National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). Online: https://irp.fas.org/offdocs/nspd/nspd-54.pdf

Trend Micro (2017): *Cyber Propaganda 101.* Online: www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cyber-propaganda-101

Tzu, Sun (1910): *The Art of War.* Online: www.gutenberg.org/files/132/132-h/132-h.htm

Woolley, Samuel C. (2020): Bots and Computational Propaganda: Automation for Communication and Control. In Persily, Nathaniel – Tucker, Joshua A. (eds.): *Social Media and Democracy. The State of the Field, Prospects for Reform*. Cambridge: Cambridge University Press. 89–110. Online: https://doi.org/10.1017/9781108890960.006