ISSN: 2450-6869

eISSN: 2719-6763

No. 12, 2021

DEFENCE SCIENCE REVIEW

http://www.journalssystem.com/pno/

DOI: 10.37055/pno/150838

The Influence of Cyberwars on Socioeconomic Activity of Residents of Central and Eastern Europe

Original article

Received: 2022-05-30

Revised: 2022-05-31

Accepted: 2022-06-09

Final review: 2022-06-09

Peer review:

Double blind

Keywords: cyber-attacks, cyberspace conflicts, social behaviour, cybersecurity, cyberwar

Jolanta Połeć[1,A-F]
ORCID 0000-0003-1038-5728

Wojciech Trzaskowski[2,A-F]
ORCID 0000-0003-2204-3952

A – Research concept and design, B – Collection and/or assembly of data, C – Data analysis and interpretation, D – Writing the article, E – Critical revision of the article, F – Final approval of article

[1] Military University of Technology in Warsaw, Poland

[2] PKP Polskie Linie Kolejowe S.A., Poland

Abstract

Objectives: The purpose of this article is to investigate and present the issue of cyberwar and its impact on the socio-economic activity of inhabitants of Central and Eastern Europe.
Methods: The main method used in this study is a systematic review of international and Polish political literature in the fields of cybersecurity, sociology, military, international relations and international politics.
Results: The analysis enabled identifying the importance of the cyberspace driven by the technological development. Article discusses key terms, the concept of cyberwar, categorization of cyberattacks and their influence on the socio-economic activity of the inhabitants of Central and Eastern Europe. The last part examines examples of cyberattacks in Kosovo, Estonia, Georgia, Bulgaria and Ukraine.
Conclusions: The technological progress impacts the emergence of cyberthreats such as cybercrime, cyberterrorism or cyberwars carried out through the newest technology. These actions are affecting both state institutions and citizens. The examples prove that cyberwar is already being used to damage the big-scale national projects. A cyberattack often targets a politically inconvenient opponent, not to physically eliminate them but to cause chaos and a breach of trust among their adherents. Some countries use cyberattacks to influence the internal affairs of another country. Even if thoroughly planned and carried out, an attack can still change or strengthen the current government. Neglecting the threat of cyberattacks may affect the citizens gravely. It may increase the awareness of the danger or give an institution greater control over personal freedom of citizens. Cybersecurity is best achieved through education and raising awareness.

Corresponding author: Jolanta Połeć – Military University of Technology, ul. Kaliskiego 2, 00-908 Warsaw, Poland; email: pjola@vp.pl ; Wojciech Trzaskowski– PKP Polskie Linie Kolejowe S.A., ul. Targowa 74, 03-734 Warsaw, Poland; email: wtrzaskowski23@wp.pl

Introduction

Each epoch governs according to its own laws, norms, and rules. Each has its own governance documents.

One of the main challenges of the present day is to create a sufficient and reliable security system through granting security and protecting data. Information security, despite being of the greatest importance to society, is difficult to achieve in light of cyberwars and cyberterrorism.

There are numerous definitions of the term cybersecurity. It may be defined by both particular Internet users and companies. However, it is the state which sets glories and takes steps to protect its citizens from cyberterrorism threats found in cyberspace (Jaroszewska, 2017).

Today's technology is developing at a progressively faster pace. The present 'fourth' digital revolution stems from the invention of the first computers and the first decentralized net called the ARPANet Advanced Research Project Agency Network (1969), which was the Internet archetype established in 1990. The full potential of these technologies was not been exploited until the 1990s. It was then that the new e-services have been launched (e.g.: e-mail, e-banking, electronic signature, social and entertainment media). Companies have started to offer their products or services on their websites. This phenomenon leads to the virtualization of reality and the "digitalization" of human life. The sign of times is the processing of data from the maximum amount of particular people and their activity in various teleinformatic systems. The technological progress of the last 30 years has facilitated human life on many levels. Thanks to the Internet, globalisation has become faster and more efficient in connecting the farthest corners of the world, which may be reached with one click of the mouse. However, in addition to visible advantages, technological progress also involves new threats. It suffices to be a particular computer user to get access to virtual knowledge. Although previously accessible only to states, the technology of the computer network has become so widespread that it was only a matter of time how fast it will be used for destruction purposes, such as criminal or even terrorist activity. Today, cyberattacks are becoming more and more common. They occur on an enormous scale in, for example, the state infrastructure, banking, transportation, communication, energy technology, or social services. The issue of cybersafety is no longer a secret.

The objective of the authors is not to carry out a complete discussion on the subject but rather to present subjectively the issue of cyberwar, which is gaining momentum and importance in current and future armed conflicts. The importance of the current state of affairs has forced the authors to study and reflect on the past and forego cyberwars.Moreover, the authors of this article have attempted to define the phenomenon of cyberspace and cyberterrorism and assess its importance for state security as well as the threat it poses.

The present article is mostly based on Polish academic publications. Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie written by Agnieszka Bógdał-Brzezińska and Marcin Florian Gawrycki which discusses the typology and characterization of cyberterrorist attacks. The key part of the article is to present the causes of cyberwars and their influence on the socio-economic activity of the inhabitants of Central and Eastern Europe.

1. Definition of Cyberspace

The author of this term is generally thought to be William Gibson, an author of science fiction stories, who introduced it in a story from 1982 entitled ‘Burning Chrome’ and his novel “Neuromancer”. In “Neuromancer”, Gibson introduces his readers to, defining it as: “Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity”. (Gibson, 1999).

However, coming from a work of fiction, the cited definition has not only developed the concept of cyberspace, but also described key elements of this environment: global reach, collecting of all the recourses in one enormous database, its complexity, and infinity. In his definition, Gibson accurately conveys the very essence of global cyberspace not as a virtual but rather as a real and substantial being. This state is achieved through exposure to the Internet and its uncontrollable spreading.

The current possibilities for the development of cyberspace subside legislators not only at home but also internationally, with numerous challenges (Jaroszewska, 2017).

Initial research and educational objectives have evolved, and cyberspace has reached the dimension of an international carrier of information, and in consequence, the number of threats of cybercrime has increased. This required the introduction of further precautions.

Up until the 1990s, European countries lacked proper regulations and legislation which would guarantee their users’ safety. The cyberspace of the 21st century is a cross-border term and, as such requires international regulations (Grzelak and Liedel, 2012).

Cyberspace was formed by the following processes (Sienkiewicz, 2009):

- the process of the integration of the base forms of partition and presentation of the information,
- the process of convergence of information and communication systems and electronic media,
- the process of the integration of technology leads to the formation of the integrated teleinformatic platform.

2. Cyberterrorism as a method of combat

The term “terrorism” refers to the threat of violence or its use, to achieve political or economic goals. The media play an important role in the consolidation of this term. To foul up a person or an organisation, the media, which tend to be prejudicial, often overuse the term ‘terrorism’. Attention has become one of the main characteristics of contemporary terrorism.

The development of cyberspace had led to the emergence of a new phenomenon called cyberterrorism. The common element of terrorism and cyberterrorism is the threat of violence or the use thereof, usually targeted at the civilian population.

Cyberterrorism is a relatively new phenomenon and method of combat.

In fact, any object that functions in cyberspace may be its target. Both terms, cyberterrorism and cyberspace, first appeared in the 1980s. The term ‘cyberterrorism’ was coined by Barry Collin. He defined cyberterrorism as a shift of terrorism from the real world to the virtual world (Tafoya, 2011). The term ‘cyberspace’, on the other hand, was introduced by the aforementioned William Gibson. Cyberspace lies within the framework of cooperation, which has both positive and negative aspects.

The first relates to the increase of satisfaction of social needs in all the areas of life: education, social interactions, and the economy. The negative side has become a source of new threats to external (international) and internal (national) security. Among these phenomena (Sienkiewicz, 2009), there are:

1. Cybercrimes (use of cyberspace for criminal purposes; particularly in the context of organized crime).
2. Cybervigilance (public control through teleinformatic tools).
3. Cyberwars (cyberspace as a new dimension of the conduct of hostilities).
4. Cyberterrorism (use of cyberspace for terrorist purposes).

Cyberwar, as well as cyberterrorism, is an increasingly preferred method of combat in contemporary international confrontations. The shift of attackers to cyberspace is caused by the expenses of carrying out such an attack. The only cost to the attacker is the cost of computer hardware. Several levels of cybernetical war can be foregrounded. Some of them are as follows:

- a cyberwar accompanying military operations,
- a restricted cyberwar, where the teleinformatic infrastructure of a state is a main target of the accompanying hostilities;
- a non-restricted cybernetic war, is characterized by a wide range of operations and raids, which may come from any place on earth and target both military and civilian infrastructure.

The area of particular vulnerability to cyberterrorist attacks is the critical infrastructure of states, organizations, or communities. The critical infrastructure is required for the proper and efficient functioning of state bodies and, above all, citizens. Examples of critical infrastructure are energy and fuel supply systems; the communication and teleinformatic systems; the bank and financial systems; the food and water supply systems; the healthcare system; the transportation system; the rescue systems; the storage and disposal of chemical and radioactive substances systems (Kowalewski and Kowalewski, 2014, p. 28).

All of those elements are at particular risk of being cyberattacked. The disturbance of their functioning may lead to both material and personal losses.

The following breakdown of the attacks may be deployed:

- attacks that happen only in cyberspace (attacks on software),
- physical hardware attacks (Wilson, 2008).

Additionally, the literature suggests a different categorization: (Bógdał-Brzezińska and Gawrycki, 2003)

1. Category I, the traditional use of technology: communication, information gathering, obtaining financial means;

2. Category II - the old methods of aggressive The examples are: the use of violence against computer hardware:

3. Category III, - the use of technology to destroy it, for example, by means of computer viruses.

There are numerous types of attacks. In practice, several main tools used to carry out different types of attacks on IT systems can be distinguished (Bógdał-Brzezińska and Gawrycki, 2003):

- malware – (viruses, bugs) – programs that spread through the IT system and wither change the way it works or reproduce and occupy the processor's memory, disk space, and other resources and, as a result, block access to data;
- logic bombs, which activate new functions of the logical elements of the computer and may lead to the destruction of hardware and software;
- trojans are programs that can perform unwanted actions without the user's knowledge and consent, e.g., deleting files, formatting disks, copying data, etc.;
- spoofing - Impersonation of someone authorized to access the system performed with the intention to destabilize the system;
- chipping – placing chips containing programs that prevent unauthorized access
- or create design defects in computers;
- backdoors – a method of fixing errors to later use them to hack into the computers
- of users using affected software;
- masquerade - pretending to be one of the system’s users performed by a hacker, by means of modifying the data packages during connection to the system or similar method;
- Hijacking - gaining access to the data being transferred between computers;
- Sniffing - Tracking network traffic;
- Denial of Service (DoS), Distributed denial of service (DDoS), a result of the blocking of access to a website by sending a huge amount of data packages from various locations to the website, which causes the server to crash.

The typical process of a cyberattack consists of three fundamental phases (Sienkiewicz and Świeboda, 2015, p. 224-262). First, it involves ‘sampling’, a way to understand the weak sides of the system. The second is related to gaining access to the contents of the system. The third contains the execution of a particular plan of action, for example:

- theft - gain control of the contents of the system by an unauthorized person without copying,
- copying - unauthorized copying of the files,
- deletion - the destruction of the target,
- reading - unauthorised access to information,
- modification - modification of the data or the profile of the target,

- omission - bypassing the system security process.

Due to safety reasons, information has its attributes, such as confidentiality, integrity, and availability.

Every attack poses a danger to all of the above or its combinations. The perpetrators of information hazards may be divided into two categories (Sienkiewicz and Świeboda, 2015, pp. 224-262):

1. Perpetrators of the so-called 'structured' threats, which include: state organizations, terrorist organisations, and different types of criminal groups;

2. Perpetrators of the so-called 'unstructured' crimes, for example, criminals, frustrated persons, hackers, vandals, etc.

The attacks that occur in cyberspace are of sudden, unexpected and surprising nature. Pointing out the source of the attack, especially those of a criminal, psychological, or terrorist nature, is often impeded.

The Internet user tends to fall victim to three threats (Ait Maalem Lahcen, Caulkins, Mohapatra and Kumar, 2020):

- loss of confidentiality (data theft) which may target databases, backups, application servers, or system administrators.
- loss of Integrity (Alter Data), which includes hijacking,

Change in financial data, theft of large sums of money, redirection to payments, and the threat to the image of the organization:

- loss of availability (denial of access) includes distributed denial of service (DDoS), distributed reflected denial of service, and physical destruction.

Fig. 1. shows three main types of cyber threats and their combination.

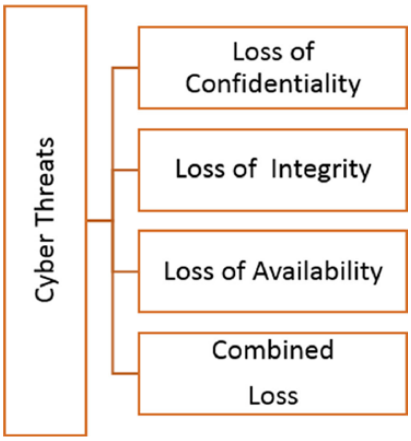

Fig. 1. Three main types of cyber threats

3. The social and psychological effects of cyberattacks

Every user of a computer or a person functioning in a country which can be characterised as a developed country may become a victim of a cyberattack. The means of communication and all the tools of today require rapid usage of all the contents of the system and facilitate daily life. The society which is used to convenience and rapid functioning is quick to fall into different states of mind in a case of deprival of the boon of the cyberworld.

The observations have shown that members of society are more prone to reacting to the effects of a cyberattack than to the attack itself. The invasion of malware may not be of particular concern to the individual; however, its effect will have a direct impact on one, for example, in the form of power blackouts and lacks heating, leading to the impossibility of preparing food.

The social and psychological (emotional and behavioural) effects of cyberattacks must be considered.

The social effect of a cyberattack is related most of all to disturbances in everyday life. Causes feelings of anxiety or distrust of cyberspace or technology. The psychological effect may be based on the social effect and can encompass more personal aspects like anxiety, grief, anger, anger, indignation, depression, etc.

Beliefs constitute an important element of the present analysis. It is because the user's reaction to threat and the motivation to use securing mechanisms depend on beliefs in this area as well as the degree of danger of exposure, the vulnerability to danger, the evaluation of own's effectiveness and expected costs. The type of actions taken to prevent or moderate the effects of the cyberattack depends on the fear culture related to crime and related possible unknown threats. Fear of crime may cause people to change their mindset. The usual attitude towards the fear of the crime is to take care of flight. Such behaviour may lead to different types of phobia and generate enormous stress that intensifies the anxiety, delusions, and public fear of crime and danger, regardless of the actual presence of such threat.

Taking the time to be effective in dealing with potential threats facilitates the process. However, lack of conviction can lead to stress and avoidance of any preventive action. For example, in the event of a cybercrime incident, such as a fishing scam, individuals may consider that they do not have the skills or knowledge necessary to avoid such an incident, and thus avoid acting or taking any preventive action. If this is to happen on a large scale, it can have a noticeable social impact.

Behaviours conditioned by fear or avoidance can influence the perceived ineffectiveness of managing a situation. Human behaviour is largely regulated by self-beliefs in personal performance, people can perform their actions at the lowest level of self-efficacy despite the high level of fear induction, and they can take preventive action without having to wait for feelings of fear and excitement to appear. Different theoretical approaches explain fear control procedures or how people cognitively recognize fear or threat by changing their attitudes, intentions, or behaviours to avoid danger. The greater the threat, the greater the fear generated. The threat is also associated with a sense of fear, not efficiency. Perceived effectiveness only determines the nature of the response (fear or risk control), while perceived threat determines the intensity of the response (how much fear or risk control there is). For that reason, perceived threat and fear-mongering seem to be closely related.

The vast majority of victims of scams and computer abuse have only been victims once, and only a small fraction say they have suffered two or more times. Statistics support this claim, indicating that users can quickly learn from their mistakes when they become victims of computer crimes.

On the contrary, when the perceived threat is high but the perceived countermeasure effectiveness is low, fear control procedures are initiated. Initially, fear appears, and the threat becomes intense when people feel that they cannot prevent it. In this way, people are manipulated with their fear (defensive manipulation) by adopting reactions such as denial. When fear control procedures dominate, people respond to their fear, not to danger. Individuals can feel helpless and become a victim. While their lack of knowledge about cybercrime will lead them to accept the possibility of being victims or to deny this possibility in general.

An interesting issue in the context of the study of human behaviour on the Web is the creation by users of a completely different image of their person on the Web. In virtual reality, people say and do things that they would not normally do in reality. For example, they may relax, feel less self-conscious, and present more open attitudes, speaking directly about difficult problems. This phenomenon has become the definition of the so-called disinhibition effect. This is influenced by several factors. They take into account the fact that people can create a different identity online and may feel less vulnerable in the way they express themselves or behave. Furthermore, people may feel less visible online and therefore may engage in activities that they would not otherwise do. These factors influence our discussion of the effects, as the consequences of some online activities may not be fully tangible to people in the offline world (Ait Maalem Lahcen, Caulkins, Mohapatra and Kumar, 2020).

4. Emotional responses to cyberattack

Research indicates that current forms of cyberattacks can cause significant psychological effects. Depending on who is the attacker and who is the victim. The psychological effects of cyber threats can even be compared to traditional terrorism. Victims of online attacks can suffer emotional trauma that can lead to depression. There is also evidence of acute posttraumatic stress disorder (ASD) symptoms in crime victims. This manifests itself in similar reactions, i.e. intrusive memories, emotional dullness, and nervousness, especially in the case of victims of virtual sexual assaults (Bada and Nurse, 2019).

For example, the impact of identity theft can act on the victim on an emotional level and lead to the following emotions, i.e. feelings of worry/insult/betrayal, irritability, anger, and powerlessness. Often, victimization can lead victims to feelings such as outrage, anxiety, putting security before freedom, and little interest in using new technologies due to a loss of trust in virtual reality.

The victim can go into stages of grief and suffer from anger, or rage. In some cases, victims may even blame themselves and increase their sense of shame (sextortion, i.e., obtaining sexual material from someone and then extorting money or further content under the threat of publishing previously received photos or videos may be a perfect example of this). In addition, victims feel that they are partly or entirely to blame for the situation in which they are.

Due to the rather delicate psychological side of the victims and the shame, as a rule, about half of the victims do not contact anyone in search of help, and about a quarter can try to take action themselves. For example, by avoiding certain sites in the future. Other effects can also be self-isolation and even depression, especially in the case of financial loss.

It was found that victims of online scams consistently reported the emotional impact as greater than its financial impact. This shows how even nonlethal forms of cybercrime have a significant impact on attitudes. The victims under attack react not only with fear, as do the victims of crime, but also with the government's demand for protection regarding supervision and stricter regulations.

Based on data from the literature, less than 1 in 10 people say that they feel "very" safe online. Furthermore, only half of the adults interviewed would change the way they behave online if they became a victim. People can accept a situation even if it is unpleasant just because they don't understand it or don't know enough about it. Going in this direction, it can be concluded that individuals can accept cyberattacks because of a sense of "learned helplessness". Often, users can simply accept the possibility of being a victim. Indirectly, therefore, the key question arises whether they also accept the reality of influence and hope that the severity is low. The anonymous nature of cybercrime can lead to its acceptance and the acceptance that users at some point will become victims of cybercrime. What is more, feelings of learned helplessness can potentially also result in low assimilation of protective behaviours.

Users are asked to make many safety-related decisions daily that can cause anxiety.

Preventive behaviours to prevent a potential attack include, for example,

(a) not to open an email from a sender they are unable to recognize;

(b) lack of access to unknown attachments;

(c) only downloading and running programs from reliable sources;

(d) use of anti-virus and security software (e.g. firewall);

(e) regular backups.

Some of these decisions can also cause the user to be anxious because of a lack of knowledge about the possible consequences of making wrong decisions.

5. Potential public response to the cyberattack

The public response to a cyberattack is based on several cyber-specific variables such as the identity of the attacker, the identity of the target, the scale of the attack, and the timing of the event's disclosure. Social reactions may vary depending on the identity of the attacker revealed. The main categories are terrorist, hacktivist and criminal.

Criminals are, on average, less likely to publicly reveal their identity (assuming any identity or nickname). What is more, the target identity can influence the public response. For example, if a series of abuse incidents randomly affect individuals, it can be expected to cause less panic or outrage compared to a targeted attack on national finances, utilities or health care.

Furthermore, the scale of the attack will affect the strength of its impact. The full range of the attack may not be visible immediately, especially if the second- and third-order systems have failed. Finally, the way the government communicates the cyberattack and the timing of the disclosure of the malicious event will affect the level of public response. This information can influence the direction and dynamics of the public response. The ways the public learns about a cyberattack also have an impact. Different levels of public response can be caused by, for example, loss of service, public announcements by an attacker, or government announcements.

Fear and panic may not be the defining features of public reactions to future cyberattacks.

As mentioned above, members of the public are more likely to respond to an event (e.g., loss of service) than the cyberattack itself.

6. The impact of disinformation on social behaviour

Recently, systematic large-scale disinformation has had a significant impact on social behaviour. It poses a major strategic challenge to European democracies. Disinformation and fake news can lead to divisions in society, sow distrust, and even undermine social cohesion and trust in democratic processes.

New technologies and software make it possible to spread disinformation easily and relatively cheaply through social networks and other online media. Disinformation typically focuses on sensitive topics that can polarize public opinion and arouse strong emotions and therefore is more likely that such misinformation will spread.

These topics include health issues (e.g., anti-vaccine campaigns), migration, climate change, and social justice. Disinformation aims to polarize voices in democratic debate, create or increase tensions in society, and weaken electoral systems. It has a wide impact on European societies and security. Ultimately, it harms the freedom of opinion and expression.

Disinformation is often financed by actors in third countries whose aim is to destabilize European societies and democratic systems (Lehne, 2020).

7. Examples of spectacular cyberattacks in History

Cyberattacks have intensified in recent years. This increase is indirectly related to the growth of Internet users and the increasingly bold actions of various sides of the conflict in the virtual space. In particular, it is about the interference of one country in the sensitive infrastructure of another, e.g., power plants, control of railway lines, or paralysis of airports.

Below are some examples of activities in the sphere of cyberspace that have caused confusion in the societies of many countries.

Kosovo 1999

The first online war was triggered by the conflict in Kosovo. Cyberattacks in Kosovo began even before Operation Allied Forces, organized by NATO forces (North Atlantic Treaty Organization) in March 1999.

In October 1998, a Serbian group Black Hand carried out attacks on an Albanian website and threatened the subsequent attacks, also on the websites of NATO (Mitnick and William, 2003, p. 24). The Serbs have sent thousands of emails to various media, organisations, and governments of the NATO member states. The emails were called to stop the shelling. Some of the emails were anti-NATO and anti-American, others focused on massacres carried out by NATO planes. The main burden of the virtual clash was focused on the activities of various hacker groups that support Serbs or Albanians from Kosovo.

The Americans have analysed the possibility of cutting Yugoslavia off the Internet altogether. However, such a plan was abandoned because it was believed that as a result of such an action, the population would be deprived of access to the Internet network, which would prevent them from confronting the incoming messages and would be 100% dependent only on the fully propagandistic message of the authorities.

March 27, 1999, the Russian website (gazeta.ru) reported an attack on the White House website, which was denied by the United States with the information that the site was closed due to equipment failure.

During the shelling of Yugoslavia, almost 100 NATO servers were attacked. These were mainly attacks on servers made available to the public, so the situation did not have a major impact on the functioning of NATO, which informed the public that it did not intend to respond to such attacks. However, in response to pressure from the US public, actions were taken mainly aimed at manipulating bank accounts and carrying out attacks on Yugoslav antiaircraft defences.

In the final phase of the battle, the content of the sites was replaced. Black-Hand activists attacked artbell.com websites condemning NATO's attack on Yugoslavia. According to NATO specialists, hackers hired by Yugoslavian militias are at least partially responsible for the attacks. The activities of the Serbian hackers were supported by Russian and Chinese colleagues who, e.g., on the American website Orange Coast College posted vulgar information about President William J. Clinton.

In the ongoing ‘cyber games’, attacks were also carried out on mine portals. Department of the Interior, Department of Energy and National Park Services.

Advanced techniques were not employed during the conflict in Kosovo. Most of the attacks were mainly e-mail bombings and website substitutions. The Internet was used for propaganda, demonizing the opponent (disinformation), attacking with viruses, Distributed of Service (DoS), Distributed Denial of Service (DDoS), and hacking websites.

Estonia 2007

The Estonian teleinformatic network is one of the most developed in Europe. The constitution grants the right to access the Internet. The Estonian government decided that all the administrative business should be carried out through the Internet.

The first cyberattack on a mass scale occurred in 2007, during the conflict between Russia and Estonia. The displacement of the monument of the Brown Soldier, a commemoration of the Red Army, from the centre of Tallinn acted as an excuse. For Russia, the monument was a symbol of Soviet soldiers who had lost their lives while regaining Tallin from the Nazis. For Estonia, however, it was a symbol of the Soviet occupation. The decision concerning fate has caused a political disagreement between Tallinn and Moscow. On one hand, the disagreement was manifested by aggressive public demonstrations and street fights between the activists and law enforcement services; on the other, a regular war has started in Estonian cyberspace. On 27 April 2008, the Russian hackers attacked the Estonian government servers by means of blocking access to the government websites (DDoS type of attack). In addition to government websites, hackers attacked also websites of political parties, the largest banks, the police and independent media (Lakomy, 2010, pp. 55-71).

The attacks happened on May 9th, a day celebrated in Russia as Victory Day, an anniversary of the end of world war two. Internet traffic in Estonia rose more than twenty-fold. Attacking the baking system made it impossible to carry out any transactions. The two largest banks, Hansapank and SEB Ühispank, had to suspend their online services and international transactions. The attacks were coordinated and carried out from numerous locations in the world, from countries with varying attitudes towards cyberterrorism of hacking. It was the first time in history that a sovereign state has been a victim of a cyberattack. The investigation, along with additional sources, has confirmed that the attack had been carried out by Russia. However, the country denied participation.

As more than 95% of transactions in Estonia are done online due to the high level of technological development in the country, the attack had a massive impact on society.

Moreover, its psychological effect was enormous not only for Estonians but also for the international public.

For an average Estonian, the attacks were more irritating than dangerous. They hindered communication and information flow, for example, by blocking access to banks. The scale of the attacks had caused an enormous financial disaster, mostly concerning internet banks. The methods used were rather primitive, but the psychological effect was achieved.

The suspension of banking services didn’t need to take long to disturb an ordinary citizen of Estonia.

The cyberwar, which took three weeks, has proven how defenseless a society is in a small country before the cyberterrorism. Estonian defence minister Jaaka Aaviksoo summed up the whole event very aptly, saying: "for the first time it happened that cyber-attacks posed a serious threat to the security of an entire nation (Davis, 2007).

Estonia is a member state both of the North Atlantic Treaty Organisation (NATO) and the European Union. However, neither organisation was able to fight such an attack, forsee its scale or influence on the whole society (Czepielewski, 2009).

As a consequence of the attack, the Estonian government has taken legislative and organisational steps, to prevent a similar situation from happening in the future.

The member states of NATO have sent specialists in the field of cybersecurity to Estonia. As a result, a special unit destined to protect the virtual space has been appointed.

Georgia 2008

Apart from Estonia, the country most affected by the open cyberwar was Georgia.

The first mentions of virtual aggression have emerged on August 5th,2008. Georgia’s IT systems were attacked as Russian troops approached Tbilisi for several dozen kilometers, where fighting was taking place between Georgia and Russia with the participation of the pro-Russian separatist republics of South Ossetia and Abkhazia. In fact, however, the first attacks had happened earlier, on July 20th, when the content of several government websites had been changed, for example, the website of the Georgian president. His photo was replaced by that of Adolf Hitler.

In retaliation, Georgians blocked access to the Ossetian news portals and governmental radio. The Georgian media started to broadcast information through a Georgian station Alania TV.

The Russians did not remain passive. They carried out a series of types of DDoS attacks (distributed denial of service) and broadcast fake news from BBC and CNN The main targets were government websites (for example website of the President Mikheil Saakashvili), but also websites of banks, embassies of countries supporting Georgia (UK, USA), scientific institutions were under attack.

As a result of the attacks, Georgia has lost the possibility of presenting its point of view to foreign societies regarding the ongoing conflict. The actions of the Russian hackers resembled the situation in Kosovo in 1999 when there was also a plan of cutting Yugoslavia off the Internet. In the case of Yugoslavia, access to the Internet remained allowed In Georgia, however, the citizens were satisfied with the access to information on the current events, which led to the widespread Russian propaganda.

Georgian telecom operators had to join forces to survive attacks on their networks, and the global CERT community actively supported the only CERT in Georgia at the time, CERT-GE, in defending them.

The attacks were carried out by services clearly involved in the Internet underworld which carry out criminal activity on the Internet. The attacks on Georgia in 2008, were carried out by the website StopGeorgia.ru. Most of the attacks were related to the famous criminal network, Russian Business Network, which has its own Wikipedia page: http://en.wikipedia.org/wiki/Russian_Business_Network.

There is a lot of evidence to support the hypothesis that the attacks were inspired by the Russian government and that special forces such as military intelligence (GRU) or civilian intelligence (FSB) were involved.

To protect itself from cyberattacks, the Georgian government transferred its computer resources to the USA, Estonia and Poland (Korns and Kastenberg, 2009, pp. 60-76).

Bulgaria 2019

The biggest Russian attack targeting personal data has happed in Bulgaria in 2019. It was carried out by Kristian Boikov, who stole personal dates from millions of Bulgarian citizens, from the National Income Agency, causing chaos in the country. It was demonstrated that the real party responsible for the attacks, might be Russia. This is due to the fact that it occurred while Bulgaria was purchasing F-16 planes for the United States. The incident was read in terms of the political influence that Russia could achieve through the possibility of exerting pressure on decisions taken in NATO and the EU thanks to Bulgaria's membership in these organizations. The analytics confirm these speculations. Ognyan Shentov, director of the Center for Democracy Studies in Sofia, pointed out that Bulgaria in 2020 was Russia's closest ally among all EU member states: "We have always stood halfway between the Visegrad Group and Russia" (Stępniewski, 2020).

Ukraine 2022

The ongoing armed conflict in Ukraine has revealed a considerable potential and enormous influence on the carrying of hostilities through cybernetic activity. Both before and during the war, numerous incidents of attacks in cyberspace have occurred. Those attacks aimed to physically exhaust the adversary, access their crucial data and foul them.

One of the most spectacular successes of cyberwar was the immobilisation of a train transporting Russian warfare to the territory of Belarus.

The hacking of the train had actually happened before the outbreak of the war, that is, January 25th, 2022. The objective was to stop the transport of Russian soldiers and warfare to the Belarussian-Ukrainian border. It was not the first attack on carrier systems. Before, during military maneuvers, similar incidents had occurred. The operation was carried out in late January by a Belarussian cyber-guerrilla group as part of “the Hell”, a campaign that has been running for several months The attackers offered The researchers from the CuratedIntelligence asked the group for a sample of the malware used in the attack. They did not receive it; the Cyber Guerilla, however, shared with them details about one of its previous breaks. The analysis of CuratedIntelligence proved that hacktivists possess the tools and skills required to successfully hack the railway. The members of CuratedIntelligence shared their position on the CyberScoop website with a specialist from SentinelOne, interviewed by Ars Technica. The operator of the Belarussian railway did not acknowledge the attack, nor did it start negotiations. The systems started working again on their own, but not for long. The operations carried out by Cyber Guerrilla may be followed on popular social networks, such as Twitter. The group’s actions have forced the superintendent of the Belarusian Railway to switch to manual control mode, and therefore to a definite decrease in the efficiency of the railway network there (Madrjas, 2022).

The attack was not only targeted at the control of the traffic systems but also, by means of blocking an app used for internet ticket sales, at civilian users of the Belarussian Railway This situation compelled the authorities of the Belarussian Railway to hire more staff for the ticket offices on the railway stations. As a result, many passengers were forced to spend hours queuing to buy a ticket.

Worldwide known Internet activists, such as the Anonymous hacker group, have also been engaged in the fight for the Ukrainian cause. Anonymous is renowned for its spectacular actions related to cyberattacks. The hacker group has members throughout the whole world. They call themselves ‘hacktivists’. As they say, they are not affiliated with any party and their goal is to promote free speech and oppose government control and censorship.

Until now, the group has carried out numerous operations, such as (PAP, 2022):

- hacking Russian satellites. The Ukrainian agency Ukrinform has informed that Roscosmos, the Russian space agency, has lost control over its own spying satellites;

- revealing personal data of Russian soldiers participating in the invasion;
- cyberattacks of websites on well-known brands that did not withdraw from the Russian market after the announcement of international sanctions. Those are brands such as Leroy Merlin, Auchan, Nestle, and many more;
- hacking thousands of private user printers and transmitting through their messages the propaganda lies about war and advises how to combat it which special software called Onion Router, which can be downloaded for free, installed, and used to gain access to 'true media' not censored by Russia;
- blocking websites of the Ministry of Communication and Digitalisation, the State Office of Military Industry, and the Armed Forces of Belarus, as well as the websites of the Pension Fund, the Border Guards, and the public services of Russia;
- there were also reports of hacking Putin's yacht. Furthermore, hackers intervened with the data on maritime traffic so that it looked like the yacht crashed on the Ukrainian Snake Island and then changed its course to "hell";
- instead of propaganda programs, the hackers emitted Ukrainian patriotic songs and real videos from the ongoing war on Russian Television.

Only the most famous and spectacular of the actions of the Anonymous group carried out in the name of Ukraine were listed.

Conclusions

Technological progress has had a significant impact on the emergence of new cyber threats leading to new forms of terrorism. Cyberterrorism, related to acts of terror carried out by means of the newest teleinformatic devices, is one of them.

Despite all efforts, we are not able to curb the threats resulting from the intensively growing virtual reality. Cybercrime and cyberterrorism are increasingly affecting both state institutions and regular citizens. Even the best protection is rapidly becoming obsolete and not adjusted to the requirements of contemporary cybercriminals and cyberterrorists. The selected examples prove that cyberwar is already a means to cause damage to big-scale national projects.

The tools used for a cyberattack very often become a weapon targeted at a politically inconvenient opponent. Such a weapon does not aim at the physical elimination of the opponent but rather at causing chaos and a breach of trust among its adherents. Some countries make use of this type of action to influence the internal affairs of another country. The end result depends on the public reaction. Even if an attack is not planned accurately and thoroughly carried out, it can still lead to, either, a change in the political fraction governing at the given moment, or its strengthening. An example of the latter is Russia. The presently governing fraction has only strengthened its position since the onset of the war with Ukraine despite the fact that the results of the cyberattacks carried out is not as expected. Neglecting the threat of cyberattacks may have very serious consequences that directly affect the complacency of society. People who feel unsafe may be open to change to regain their peace. It may lead to either increase in awareness of the danger of granting the state or other institutions greater control over personal freedom. It seems that the best way to cybersecurity is through cybersafety education combined with the continuous rising of the citizens' awareness.

References

Ait Maalem Lahcen, R., Caulkins, B., Mohapatra R. and Kumar, M. (2020), Review and insight on the behavioral aspects of cybersecurity, Springer Open.

Bada, M. and Nurse, J. R. C. (2019), Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press, in: The Social and Psychological Impact of Cyber-Attacks, Benson & McAlaney (2019/20).

Bógdał-Brzezińska, A. and Gawrycki, M.F. (2003), Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie.

Clay, W. (2008), Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, Available at: http://wlstorage.net/file/crs/RL32114.pdf.

Czepielewski, M. (2009), Cyberterroryzm jako element społeczeństwa informacyjnego (na przykładzie Estonii), in: Cyberterroryzm. Nowe wyzwania XXI wieku, ed. Jemioła, T. Kisielnicki, J., Rajchel, K.

Davis, J. (2007) Hackers Take Down the Most Wired Country in Europe, „Wired Magazine". Available at: http://www.wired.com/politics/security/magazine/1509/ff_estonia?currentPage=all.

Gibson W. (1999), Neuromancer.

Grzelak, M. and Liedel, K. (2012), Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, in: Kwartalnik Bezpieczeństwo Narodowe, nr 22, 02.2012, Biuro Bezpieczeństwa Narodowego.

Jaroszewska, I. (2017), Wybrane aspekty przestępczości w cyberprzestrzeni, in: KPP. Monografie. Studium prawnokarne i kryminologiczne.

Korns, S. W. and Kastenberg, J. E., (2009). Georgia's Cyber Left Hook, Parameters, Winter 2008-2009, XXXVIII (4), pp. 60-76.

Kowalewski, J. and Kowalewski, M. (2014), Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa, „Telekomunikacja i Techniki Informacyjne", no 1–2, p. 28.

Lakomy, M. (2010), Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku. Stosunki Międzynarodowe – International Relations, 3-4 (vol 42), pp. 55-71.

Lehne, K.H. (2020), Kompedium Kontroli Cyberbezpieczeństwo w UE i państwach członkowskich UE, the European Union.

Madrjas, J. (2022), Białoruska kolej po ataku hakerów. Wciąż nie można kupić biletów, Available at: https://www.rynek-kolejowy.pl/wiadomosci/bialoruska-kolej-wstrzymana-przez-hakerow-106382.html.

Mitnick, K. and William, S. (2003), Sztuka podstępu: łamałem ludzi, nie hasła. in: Helion, op. cit., p. 24.

Sienkiewicz, P. (2009), Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni, „Automatyka", vol. 13, of 2, Available at: http://journals.bg.agh.edu.pl/AUTOMATYKA/2009-02/Auto46.pdf (15.07.2015).

Sienkiewicz, P. (2009), Terroryzm w cybernetycznej przestrzeni, in: Cyberterroryzm. Nowe wyzwania XXI wieku, ed. Jemioła T., Kisielnicki J., Rajchel K.

Sienkiewicz, P. and Świeboda, H. (2015), Transformacje., Vol. 1/2 Issue 84/85, pp 224-262. Language: Polish. , Data base: Academic Search Ultimate.

Stępniewski, T. (2020), Rosja wobec państw Europy Środkowej i Wschodniej zagrożenia pozamilitarne, Instytut Europy Środkowej.

Tafoya, W. (2011), Cyber Terror, FBI Law Enforcement Bulletin, 2011, vol. 80, no. 11.

Electronic sources:

PAP (2022), Hakerzy z Anonymous znów pokazali siłę. Wykorzystali rosyjskie drukarki, Available at: https://businessinsider.com.pl/technologie/hakerzy-z-anonymous-znow-pokazali-sile-wykorzystali-rosyjskie-drukarki/2d28lf9.