Projekt finansowany w ramach umowy 857/P–DUN/2016 ze środków Ministra Nauki i Szkolnictwa Wyższego przeznaczonych na działalność upowszechniającą naukę.

Nazwa zadania:
Stworzenie anglojęzycznej wersji publikacji

Ministerstwo Nauki
i Szkolnictwa Wyższego

Zeszyty Naukowe
Wyższej Szkoły Bankowej w Poznaniu
2017, t. 72, nr 1

Paweł Majdan

War Studies University in Warsaw
Faculty of National Security
e-mail: p.majdan@akademia.mil.pl
phone: +48 22 261 814 365

Cyberterrorism as a Modern Security Threat

Abstract. *The 21st century has ushered in a period of rapid change that can be seen in nearly every aspect of life. In most cases, they have a positive impact on society. However, one cannot help noticing that in an era of tremendous growth there are also a number of challenges and threats. One of them is cyber-terrorism. This is a new, rapidly growing form of terrorism, which takes place in cyberspace, with possibly devastating consequences are for people, states and international organizations.*

Keywords: *terrorism, cyber-terrorism, security, threats, cyberspace, cyberterrorist attacks*

Introduction

In rapidly changing times of the present day, characterised by development in many spheres of life, society is facing numerous challenges and, unfortunately, also threats. It is a crucial problem, which constitutes a major barrier to the development of countries and societies.

More importantly, the world is experiencing the effects of globalisation, as well as a rapid growth of information technology. This raises the question of security associated with the evolution of information systems. Modern society relies on increasingly complex information systems, which are gradually replacing older technologies in various areas. These systems perform many important functions. Above all, they facilitate the process of decision making, help to formulate strategies and improve the effectiveness of performing tasks. Nowadays almost everyone uses all kinds of electronic access cards or uses online banking services. Professional information systems are an important factor in the day-to-day operation of corporations, enable air traffic control, or help to manage transport and logistics. The modern-day world is becoming of a world of information technology. However, despite the numerous conveniences, information technology is also associated with many threats. For one thing, it has become an inseparable part of our daily lives. It is enough to think of ubiquitous video surveillance systems (CCTV), which are used to monitor people and buildings. While these systems offer many benefits, they are also exploited by criminal groups for their own purposes. The virtual world is growing and evolving to ever closely resemble the real world. The virtual reality has also become home to "new terrorists", known as cyberterrorists. Just a few years ago nobody would have thought that educated citizens "armed" with just their laptops could become terrorists in cyberspace.

In view of the above, the present article aims to present the key facts about cyberterrorism and its main characteristics and to highlight its spread as a tool of modern-day activities that pose a threat to national security. The article also discusses different methods of attacks used by cyberterrorists. To achieve this goal, the following research methods will be used: analysis, synthesis, generalization and inference.

1. The nature of cyberterrorism

One of the increasingly common threats in cyberspace is cyberterrorism. In information society it is viewed as the main threat to telecommunication security of countries and international organisations. It is both a national and international threat. Judging by recent events, it can be said that cyberterrorism is constantly evolving.

Although terrorist activities as such have existed for many years, it is only since the September 11, 2001 attack on the World Trade Centre that the world has started paying attention to it. Following a wave of recent terrorist attacks, the phenomenon has become a household name and one of the major threats of the 21st century. Although cyberterrorism seems to be a relatively recent development, it has already reached an unprecedented scale.

Like terrorism, cyberterrorism is difficult to define. The literature provides a number of different definitions. This diversity is due to the following factors:

– the lack of one commonly accepted definition of cyberterrorism,

– the lack of one definition of terrorism, which leads to various ways of defining cyberterrorism,

– unclear relationships between concepts of cyberterrorism and information warfare,

– a tendency to negate the need for the term "cyberterrorism."

Let us start from reviewing different definitions of cyberterrorism. The term was originally coined in 1980s by Barry Collin of the Institute for Security and Intelligence. DE defined cyberterrorism as "intentional abuse of an information digital system, a computer network or component, with the intention of supporting or facilitating a terrorist action" [Bógdał-Brzezińska & Gawrycki 2003: 64].

A different definition of cyberterrorism was proposed by Dorothy Denning, who described it as „unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" [Bógdał-Brzezińska & Gawrycki 2003: 64]. Moreover, according to Denning, a cyber-attack is committed when it causes immediate damage to person or property or is sufficiently significant as to cause fear, death, injury, an explosion, plane crash or financial loss. Otherwise, it will not be regarded as a cyber-attack. Many scientists disagree with this definition arguing that it disregards the phenomenon of what is known as soft terrorism, i.e. the use of online propaganda, communication or recruitment.

In an effort to explain the nature of cyberterrorism, it is worthwhile to quote observations made by Ernest Lichocki, who defines terrorism as "a phenomenon at the interface between different fields, such as:

– telecommunications security,

– information and communications technology,

– personal security,

– physical security,

– national and international regulations,

– personal data" [Lichocki 2008: 2].

Another definition worth citing was formulated by a specialist of the US Department of Defence, Rod Stark, who defines cyber terrorism as "a premeditated and unlawful use of politically, socially, economically or religiously motivated cyber warfare or cyber-targeted violence, conducted by non-state agents or state-sponsored groups for the purposes of creating fear, anxiety and panic in the targeted population and the disruption of military and civilian assets. It is an attack aimed at digital information systems, regardless of whether it is conducted by means of a computer or not" [Bógdał-Brzezińska & Gawrycki 2003: 65].

According to the US Federal Bureau of Investigation (FBI), cyberterrorism is an premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agent [Bógdał-Brzezińska & Gawrycki 2003: 65].

In Poland, the responsibility for counteracting cyber terrorist attack rests with the Internal Security Agency (ISA). According to the Department of Telecommunications Security, cyberterrorism is defined as "activities intended to block, destroy or distort information processed, stored and transmitted through telecommunications systems as part of information or psychological warfare" [Biaoskórski 2011: 256]. The definition was already formulated in 2002, when cyber-attacks were still rare. According to a more recent definition, created by ISA in 2010, cyberterrorism is "the use of information technology in order to cause harm."[1] Based on its knowledge and experience, ISA recognises that cyberterrorism is an increasingly common tool of political and ideological struggle.

Analysing attacks that occur in cyberspace, ISA believes that a new type of conflict is emerging, known as Internet wars. They are waged in the virtual reality of cyberspace by hackers with specialist knowledge. Their actions can disrupt or paralyse the functioning of a country or its crucial elements. According to ISA, a high level of technological development is constantly contributing to improving the way various aspects of political, social and economic life are managed. However, at the same time, this development makes the state dependent on the efficiency and security of the critical infrastructure. An attack against one element of this system can disrupt the operation of the others since they are all interrelated.

Typically, cyber-attacks can be directed against systems that support the functioning of:

– state administration,
– internal security,
– national defence,
– telecommunications,
– energy supply,
– water supply,
– financial networks,
– rescue services.

Apart from faults and shortcomings of technical solutions, among the possible sources of threats for telecommunications networks, ISA has identified the following deliberate activities:

– disruption of systems,
– unauthorised data input or copying,
– breaking security measures to take control over particular infrastructural components.

A rather general definition of cyberterrorism is also included in "The Cyberspace Protection Policy of the Republic of Poland." According to the updated

[1] www.abw.gov.pl/portal/pl/88/306/Cyberterroryzm.html [access: 10.08.2016].

version of the document from 2013, cyberterrorism is defined as "an offence of a terrorist nature committed in cyberspace". Cybercrime is defined as "an offence committed in cyberspace" [The Cyberspace Protection Policy 2013: 5].

Summing up the above definitions and based on the Polish criminal law, it can be concluded that cyberterrorism is a crime which:

– involves serious intimidation of many people,

– involves actions that force a government agency of the Republic of Poland or another state or an agency of an international organisation to undertake or cease particular activities,

– causes serious disruption to the political system or economy of the country.

Given the above definition, cyberterrorism involves different kinds of politically and/or ideologically motivated terrorist actions which are conducted or planned in cyberspace by individuals or terrorist groups. These actions are directed against states, international organisations or transnational entities, and cause or can cause directly or indirectly damage to person or critical infrastructural elements.

2. Characteristics of cyberterrorism as a threat to national

According to experts on telecommunications and national security, cyberterrorism should be treated as one of the most important threats and challenges of the 21st century. It is therefore necessary to identify the cause of this phenomenon and explain why terrorists choose to operate in cyberspace. The most obvious reasons for the greater popularity of cyberterrorism compared to traditional forms of terrorism include:

– a wider impact,

– low costs,

– the disappearance of borders (states are losing their sovereignty and attacks can be launched from any place in the world provided it has access to the Internet),

– minimal risk of a planned attack being discovered,

– the possibility of conducting sudden and unpredictable actions against completely unaware and unprepared victims,

– complete anonymity, which enables the spread of misinformation,

– lower risk of terrorists themselves being affected by the attacks,

– counteracting terrorism requires improved coordination,

– a difficulty to distinguish between real and virtual threats,

– minimal risk of retaliation on the part of the state,

– the possibility of a parallel attack against selected targets, without the need to travel to or stay in the target location,

– avoidance of collateral damage, which can be exploited as part of propaganda to influence public opinion

– growing access to the Internet.

As can be seen, there are many “benefits” of a terrorist attack. Computer software turns out to be a very good tool of collecting and exchanging information as well as maintaining communications. Thanks to the use of cyberspace, cyberterrorists remain anonymous, can encode or conceal information in text or graphics files, which do not raise suspicions. Unauthorised access to systems makes it possible to intercept relevant information and can help terrorists to conduct conventional attacks. As it turns out, cyberterrorist actions are a perfect tool that enables terrorists to achieve their objectives at low cost and without being detected.[2] Unfortunately, for terrorists it is a very safe way of operating, since it does not require the use of life-threatening resources, such as weapons, explosives or chemicals. Moreover, in order to launch an attack terrorists do not have to change their location and, even if it is necessary, all they need to do is find a place with Internet access. The availability of tools required to conduct cyber-attacks enables terrorist attacks because:

– the ownership and use of a computer is legal,

– software used by cyberterrorist groups is available in the Internet,

– terrorist groups which do not have the necessary IT skills can easily employ specialists,

– it is not feasible for a state to register all civilian IT specialists.

Another advantage of cyber-attacks over conventional terrorist attacks is the fact that they often go undetected; thus, the relevant counter-terrorist agencies cannot be informed.

3. Classification of cyberterrorist activities

An almost unlimited development of civilization and technology creates new possibilities that are exploited by cyberterrorism. Scientists from The Naval Postgraduate School in Monterey identified three levels of cyberterrorism capability:

– simple, unstructured – cyberterrorists perform simple hacking attacks into information systems using Internet tools developed by others. A terrorist organisation has a very limited capability of analysing targets which are being attacked, commanding, controlling and learning new methods of attacks in cyberspace,

– advanced, structured – cyberterrorists conduct more sophisticated attacks against computer systems and networks. In addition, they are capable of modifying or creating their own tools required to launch an attack in cyberspace. Moreover, unlike cyberterrorists at the previous level, they can analyse their targets,

[2] M. Narojek, *Cyberterroryzm*, http://sbn.republika.pl/cyber.html [access: 20.08.2016].

– complex, coordinated – cyberterrorists conduct complicated attacks with an aim of causing mass disruption against integrated heterogeneous defences. They are also capable of creating sophisticated tools designed to attack targets in cyberspace and analyse them, they can maintain effective command and control and are capable of self-improvement [Bógdał-Brzezińska & Gawrycki 2003: 87].

As can be expected, the threat of first level cyberterrorism is the most likely, owing to its simplicity and relatively minimal resources required to conduct such actions. Very often, because of their small scale, effects of such attacks are not serious and do not attract much attention, partly because hackers have limited capabilities of analysing their targets.

Attacks representing the second level of cyberterrorism are more sophisticated. What makes them potentially very dangerous is the fact that this category of cyberterrorists can develop their own software to conduct hacking attacks.

Third level cyberterrorism is the most dangerous variety, since it usually leads to a complete disruption of a system, as well as other targets.

In addition to the three levels of cyberterrorist capabilities and the associated level of risk, electronic attacks can be classified into two brad categories"

– electronic warfare,

– cyber warfare.

Electronic warfare involves the use of physical properties of electronic systems. Typical examples include radio jamming or electromagnetic pulse attacks (EMP), which consist in generating short bursts of electromagnetic energy, which can destroy electric or electronic circuits.

Cyber warfare consists in attacks against the logical layer of electronic and information systems with the intention of disrupting the flow of information or taking control over it. Typical targets include operating systems, software, communication protocols, network infrastructure, as well as user accounts or any other digital targets.

Cyberterrorist attacks are closely connected with cyber warfare, as they rely on the same tools and mechanisms of operation. Their distinguishing feature is the motivation for the attack. Of course, cyberterrorism has a lot in common with cybercrime – both rely on the same set of tools. However, as in the case of cyber warfare, the difference lies in the motivation. Cybercrime is not concerned with ideology or has no interest in influencing governments or society. Their attacks are intended to bring profit from criminal activity, such as identity theft, credit card fraud, extortion or commercial blackmailing.

A perfect example illustrating this new kind of threat is the activity of the group called Anonymous. It is an anonymous, international group of Internet activists and hackers. Membership in the group is based on self-identification with their values and goals. The organisation does not have an internal hierarchy or one strictly defined philosophy. Its members identify with anarchist tendencies, oppose Internet censorship and control, or the political *status quo*. The Anonymous Group is responsible for many politically and ideologically motivated attacks, which were conducted in response to events incompatible with values shared by its members. Among their targets were governments of many countries, child pornography sites, The Church of Scientology or media companies or websites of various organisations.

One of the most commonly used method of attack in cyberspace is a distributed denial-of-service (DDoS), which is carried out using a network stress testing application called Low Orbit Ion Cannon (LOIC).

Cyber-attacks can be divided into two categories: attacks targeted at computer systems (syntactic attacks) and attacks against users (semantic attacks)

Syntactic attacks exploit the characteristics of the system itself, i.e. loopholes or vulnerabilities of operating systems, software, network protocols and network traffic management systems in order to take control over a computer system or disrupt its operation. This category of attacks include hacks exploiting loopholes in operating systems or Internet browsers in order to infect a computer, self-spreading viruses, worms as well as DoS attacks. For example:

– **zero-day attac**k is an attack in which exploits a undisclosed computer software vulnerability to hack computer running this software and gain unauthorized access,

– **SQL injection** is an attack against data-driven applications or databases, in which nefarious SQL statements are inserted into an entry field for execution.

Semantic attacks involve actions aimed at damaging the credibility of target resources or deceiving users. One example of this type of attack is ‘pump and dump’ (P&D), in which false and misleading positive statements from an allegedly credible source is used to encourage investors to buy stocks whose price is being artificially inflated. Semantic attacks can also include different techniques intended to obtain sensitive information by disguising as a trustworthy entity. In fact, this category provides most opportunities for criminals to show their creativity to continue producing new techniques of attacks.

4. Methods of attacks in cyberspace

In addition to the methods described in the previous section, one list the following techniques of cyber-attacks:

– **email spoofing** is an attack which exploits a vulnerability of email protocols – the lack of authentication mechanisms – and involves sending emails with a forged sender address to disguise as another person;

– **phishing** is an attempt to obtain sensitive information, such as usernames, passwords, PIN codes, by disguising as a trustworthy person or institution. The phishing website imitates the real website and asks for the required confidential information. The unsuspecting user enters their login information which is sent to the criminals, who can now access the victim's online accounts or use their credit card to make unauthorised purchases;

– **spear phishing** is a form of phishing, which is a personalised attack directed against a specific individual or company, which relies on personal information gathered by attackers about their targets, their friends or professional contacts. The purpose of spear phishing is to make the communications appear legitimate and deceive the victim, who could become suspicious when confronted with more impersonal methods of deception;

– **pharming** is a cyber-attack in which the user's browser is redirected to a different IP address with a fake version of the original website in order to obtain access credentials to the authentic website.

The list above includes just a handful of techniques used to carry out cyber-attacks and there are many more. The most common ones include Trojan horses, logic bombs, hardware backdoors, sniffing backdoors, DoS attacks or Van Eck Phreaking.

As can be seen, there are many techniques of conducting cyber-attacks. In most cases, they go unnoticed, cause damage and disruption to many systems, institutions, states and international organisations. It can be expected that innovative technology combined with expert skills can pose a serious threat and a real danger to the way the modern world functions. Man has always been known to be the weakest link in all kinds of processes, and human errors are part and parcel of our lives. Unfortunately, this is just what terrorists are waiting to exploit.

Summary

In summary, it should be concluded that in the course of time, with the development of digitisation and the spread of information technology in society, the threats of cyberterrorism are bound to escalate. According to predictions, they may become the most serious non-military instrument of soft power in the world. Unfortunately, this threat can become increasingly widespread, since cyberterrorists are constantly looking for new solutions and improving their IT skills.

The above considerations imply that each day increases the risk of a security threat that could disrupt public order. Consequently, there is a need for closer cooperation between agencies and institutions responsible for security in every aspect. People involved in the protection of cyberspace, particularly with respect to the exchange and use of information, should receive specialist training. Since cyber-attacks are a new threat, effective preventive measures that can predict a potential attack have not yet been developed. It is also necessary to improve legislation, procedures and increase competencies of specialists dealing with counteracting and combating cyberterrorism.

It should also be pointed out that it is developed and most technologically advanced countries that are mainly prone to these types of attacks. Among the countries that are particularly attractive targets for cyberterrorists are the USA, Russia, China, Japan or all European countries. The reason for this is the high level of information technology in these societies.

In the 1991 report published by the US National Research Council entitled "Computers at Risk: Save computing in the information Age," the authors write: "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." One of the most famous hackers, Kevin Mitnick, said: "I broke people, not passwords." He also believed that „the human factor is truly security's weakest link". Using his excellent IT skills, Mitnick was managed to steal confidential information and hack the most protected IT systems in the world. After spending five years in prison, he became a computer security consultant.

Nowadays, despite huge technological developments, there are no measures that would enable a complete control over cyberspace. Unfortunately, the virtual world does not have any borders, is not governed by any law, which is why everybody can remain largely anonymous. It turns out that every country can become the target of cyber-attacks and suffer as a result; potential damage will be the more severe, the more computerized its economy is. On the other hand, every country can carry out a cyber-attack if only there are professional hackers, able and willing to conduct it. The world is undergoing dramatic changes, technology is constantly advancing – no wonder, the same is happening to threats and challenges. Phenomena taking place in cyberspace go far beyond the technical dimension – they are affecting the social sphere of life. It has become banal to observe that that the 21st century is an age of the development of information technology. The traditional methods of communication are more and more frequently being replaced by new, more advanced information technologies. In the face of the progress of globalization and the development of technology and civilization, the scope of public security has expanded to include new aspects, such as information security or cyber security. Today, information security is identified with cyberspace, information space or telecommunications infrastructure. Therefore, one has to agree with the observation that "cybercrime, cyberterrorism, cyber warfare are no longer threats that one can read about in science fiction literature, but are real phenomena that we are witnessing more and more often" [Kwećka 2010: 209].

References

Białoskórski R., 2011, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa: WSCiL.

Bógdał-Brzezińska A., Gawrycki M.F., 2003, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa: ASPRA-JR.

Kwećka R., 2010, Strategia bezpieczeństwa informacyjnego polistrategią bezpieczeństwa podmiotu, w: *Metodologia badań bezpieczeństwa narodowego. Bezpieczeństwo 2010*, t. I, eds. P. Sienkiewicz, M. Marszałek, H. Świeboda, Warszawa: AON.

Lichocki E., 2008, *Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego*, Warszawa: PAN.

Narojek M., 2010, *Cyberterroryzm*, http://sbn.republika.pl/cyber.html [access: 10.08.2016].

Rządowy Program Ochrony Cyberprzestrzeni na lata 2011-2016, Warszawa: MSWiA.

www.abw.gov.pl/portal/pl/88/306/Cyberterroryzm.html [access: 15.08.2016].

Cyberterroryzm jako współczesna forma zagrożenia bezpieczeństwa

Streszczenie. *XXI wiek niesie za sobą ciągłe zmiany, które w dodatku następują bardzo dynamicznie. Zmiany te można dostrzec niemal w każdej dziedzinie życia. W większości przypadków mają one pozytywny wpływ na funkcjonowanie społeczeństw. Jednak należy mieć świadomość, iż w dobie ogromnego rozwoju powstaje również wiele wyzwań oraz zagrożeń. Jednym z nich jest cyberterroryzm. Jest to nowa, prężnie rozwijająca się odmiana terroryzmu, która odbywa się w cyberprzestrzeni, a jej skutki mogą być katastrofalne dla człowieka, państwa, a także organizacji międzynarodowych.*

Słowa kluczowe: *terroryzm, cyberterroryzm, bezpieczeństwo, zagrożenia, cyberprzestrzeń, ataki cyberterrorystyczne*