Threats Posed by Cyberterrorism to Public Administration

PAULINA KRAWCZYK

Abstract The stable functioning and development of a global information society depends on an open and, most importantly, secure cyberspace. In the modern world, which is becoming increasingly computerised, the number of attacks in cyberspace is constantly increasing. In order for an attack to be classified as a cyberterrorist attack, it must have the definitional elements of acts committed using violence against persons or property and cause considerable damage in order to generate fear and social unrest. In addition, such attacks must be carried out for a specific purpose, e.g., be politically motivated. Cyberterrorism is a form of warfare, which is primarily characterised by low operating costs. Cyberterrorism poses a significant threat to modern public administration. It interferes with the structure of internal state security. The most important objective of state functioning is to ensure the security of all its citizens. In order to eliminate cyberterrorism, it is extremely important to protect classified information.

Keywords: • cyberspace • cyberterrorism • public administration • CSIRT

CORRESPONDENCE ADDRESS: Paulina Krawczyk, Ph.D. student, War Studies University in Warsaw, Academic Centre for Cybersecurity Policy, Aleja Generała Antoniego Chruściela "Montera" 103, 00-910 Warszawa, Poland, e-mail: p.krawczyk@akademia.mil.pl.

https://doi.org/10.4335/2022.2.14 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

© The Author(s). Licensee Institute for Local Self-Government Maribor. Distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 license (https://creativecommons.org/licenses/by-nc/4.0/), which permits use, distribution and reproduction for non-commercial purposes, provided th original is properly cited.

The protection of cyberspace has become one of the most addressed security issues. The stable functioning and development of a global information society depends on an open and, most importantly, secure cyberspace. Efforts to raise awareness in this area are undertaken in view of the rapid increase in the number of computer incidents and new types of threats. Poland, like European countries, has been presented with the challenge of ensuring the adequate protection of cyberspace. Apart from many positive aspects of the internet, the vast resources and its possibilities, cyberspace also carries enormous security threats. The more the world becomes dependent on modern technology, the greater the number of potential cyberterrorist attacks. The specific nature of the modern internet, which is extremely helpful to public administration users, may encourage terrorists to move their operations online. Technological progress in recent years has made cyberthreats a major concern for public administration. It might seem that cyberterrorist attacks have now displaced cybercrime, but nothing could be further from the truth. All critical infrastructures that rely on information technology are also at risk of cyberattacks.

In the modern world, which is becoming increasingly computerised, the number of attacks in cyberspace is constantly increasing, and what is more, they are very difficult to detect. The internet is a tool without which both citizens and the administration are unable to function. Thanks to computerisation, access to easily processed public information has certainly increased, as have communication possibilities.

There are numerous definitions of cyberterrorism in the literature. However, experts have highlighted the difficulties with defining this concept. The problem is that it is a diverse and dynamic phenomenon. Moreover, it occurs in many forms, and these forms change as human civilisation continues to evolve through technological progress (Olak, Krauz, 2014: 189).

The concept of cyberterrorism is widely believed to have been first coined by Barry Collin, an employee of the Institute for Security and Intelligence, who in the 1980s used this term by merging two concepts: cyberspace (Banasinski, 2018: 23) and terrorism (Szymczak, 1995: 463). According to him, cyberterrorism can be defined as the intentional abuse of an information system, network, or component toward an end that supports terrorist activities (White, Carlisle 1998: 10).

Dorothy Denning (Denning, 2002:79), on the other hand, argues that cyberterrorism is the unlawful attack on a computer network of users or a given information system aimed at instilling fear. Moreover, it can be said that cyberterrorist attacks are a form of an act of violence that cause serious damage to society and property (Fiktus et al, 2015: 481). Cyberterrorism aims to hamper, block or even distort the operation of IT systems. As a specific category of threats, it includes actions against communication and information systems undertaken to achieve specific terrorist objectives. Cyberterrorist attacks have already occurred in Poland many times. They mainly targeted government or computer systems in public administration, strongly destabilising the sense of security in the whole

country, not only within the area affected by the specific incident. This shows how strongly terrorist or, in this case, cyberterrorist activities affect people's sense of security (www.cybsecurity.org/wpcontent/uploads/2014/09/Do_rzeczy_nr38_2014_wybranowski.pdf) Cyberterrorism generally involves attacking computer systems using information technology. The use of such methods can cause computer systems to be blocked and lead to data loss (Aleksandrowicz, 2008: 23). The tools used for attacks include various forms of malware, such as viruses, bacteria, worms and server blocks, or conventional attacks. The above actions adversely affect cybersecurity, especially the security of state institutions, although terrorists may certainly cause damage in various areas of citizens' lives by attacking air traffic control systems, water supply systems, telecommunication systems, energy systems, water supply systems, transport and even power plants. These are just some of the areas that are a matter of concern for terrorists'. However, cyberterrorism is not just actions aimed at causing data loss. Cyberterrorism also manifests itself in propaganda and information campaigns, recruitment, the radicalisation of data exchange and sourcing. Terrorists use the internet to reach large numbers of people. Their main goal is to cause a disturbance of the peace in the form of protests and to disrupt the operation of government websites. In view of the constantly advancing computerisation, it is necessary to create effective systemic solutions at organisational and legal levels (Grzelak, Liedel, 2012: 136).

In order for an attack to be classified as a cyberterrorist attack, it must have the definitional elements of acts committed using violence against persons or property and cause considerable damage in order to generate fear and social unrest. In addition, such attacks must be carried out for a specific purpose, e.g., be politically motivated. Attacks on computers, networks or communication and information systems additionally entail serious damage to critical infrastructure, intimidation and attempts to force the government and public administration to yield to political and social demands. It should be remembered that cyberterrorism is a type of terrorism whose main distinguishing feature is that it is carried out in cyberspace and targets mainly communication and information systems or uses such systems.

Analysing all definitions, we can look at cyberterrorism in two ways. On the one hand – cyberterrorism as the use of information technology to mount a classic terrorist attack. On the other hand – cyberterrorism as an attack on computer systems as the main target of attacks rather than the tool to carry it out.

Cyberterrorism is a form of warfare, which is primarily characterised by low operating costs. To carry out an attack in cyberspace, no specialised equipment is required. Unlike terrorism, no weapons or explosives are used to mount a successful attack. Cyberterrorists only have a computer and internet connection.

Cyberterrorists also have a high degree of anonymity. It can be said that potential cyberterrorists can become anonymous online similarly to the standard internet users who go online on a daily basis. Cyberterrorists can easily adopt pseudonyms or impersonate

anonymous web users and make the identification of their real identity very difficult or even impossible. The difficulty here comes from the fact that terrorist organisations in the cyberworld have their own financial resources. Cyberterrorists are also well prepared for such attacks. Furthermore, they are characterised with great ease by which they mount cyberattacks. Cyberwarfare is now one of the modern battlefield dimensions. Technological progress has made it much easier for cyberterrorists to carry out their operations effortlessly. In addition, cyberterrorists know very well what they are doing and what their tasks are. Another characteristic of cyberterrorism is its global nature. A cyberterrorist attack can affect any country as long as it becomes the target of cyberterrorists. In the future, cyberterrorism may develop further still. One of the objectives of cyberterrorists is to draw the attention of media and to make sure the public is aware of their operations. Tracking and capturing cyberterrorists to punish them is extremely difficult but also expensive. To this end, special equipment is required and the people involved in combating this type of crime need adequate training and qualifications. A cyberterrorist can cause harm and hurt many people, not only from their own community, but also from many other countries around the world, without even walking away from their computer equipment. These people have the ability to cover their tracks so that their actions become as difficult to detect as possible. Last but not least, what makes cyberattacks increasingly popular is the fact that they involve a broadly defined information sphere. Cyberspace carries a considerable potential for furthering propaganda efforts. Modern technologies can be effectively used, for example, to disinform and manipulate public opinion.

Currently, three levels of cyberterrorist threats can be distinguished. The first is simple-unstructured, where cyberterrorists conduct basic hacking operations against individual ICT systems using tools created by someone else. The second level of threat is advanced-structured, where cyberterrorists conduct more sophisticated attacks against computer systems, as well as create by themselves, and modify, the hacking-tools they use to attack. They also have the capability to command and control attacks and refine attack methods. The third level is complex-coordinated, where cyber-terrorists conduct the most serious attacks, which are the most complex and coordinated, capable of causing mass-disruption against integrated, heterogeneous defence systems. They create and modify sophisticated hacking tools which they use to conduct future attacks. They also have command-and-control and learning capability (Oleksiewicz, 2018: 58-59).

The division of cyberterrorist threats by area of operation (Kowalewski, 2014: 28):

- attacks on military systems – these systems store information on the location of satellites, position of troops and military equipment, and on research on new types of weapons or communication systems. Most intrusions of this kind took place during the Cold War and the main perpetrators were usually agents of foreign intelligence services.
- attacks on enterprise systems – these systems store information relevant for a company's operations. It includes information about bookings, about a company's

clients and also about technologies used at work. The main perpetrators are usually employees who cooperate with competitors or feel the desire for revenge

- attacks on systems forming critical state infrastructure. The infrastructure includes the banking and financial, energy, telecommunication, water supply, transport and emergency services systems which store information relevant for national security. The perpetrators of such attacks may be the employees of companies related to these systems, and of course individual terrorists. At present, it is difficult to speak of elements of critical infrastructure which do not use technological support. The logical conclusion is that vulnerability to cyberterrorism is constantly increasing.

The use of the latest technology in the day-to-day functioning of the state means that the country may become more vulnerable to cyberterrorist attacks. Because of the Covid-19 pandemic that broke out in 2019, and other numerous problems occurring in the world, the community forgets more and more often about terrorist threats. They do, however, still exist and may gain in strength if using, for example, other threats such as the afore-said pandemic. This is confirmed, for instance, by Europol's latest report – "European Union Terrorism Situation and Trend Report 2021". This report emphasises that cyberterrorists use every opportunity to spread fear or propaganda. In this context, the Covid-19 pandemic and the accompanying increase in the use of the internet during this period proved to be a very favourable opportunity for them – on the one hand, to spread hatred, and on the other to integrate supporters. Since the use of the Telegram messenger is hampered, Islamists have struggled to find a universal communication channel and, as a result, their propaganda is scattered across various platforms. However, it still remains effective. The activity of other extremist groups, including extreme right and left-wing ones, is also increasing on the internet. Alongside traditionally addressed issues, they willingly take up new threads related, for example, to ecological, technological or pandemic issues (Analytical Report No. 33 of the Government Centre for Security).

At present, extremely rapid technological progress has taken place in the area of information technology. Nowadays it seems very difficult to function without instant messaging, search engines or access to email, especially on a daily basis. The dynamisation of the internet, as well as of the whole IT sphere, is the fastest-developing segment of social life (Hołyst, Jałoszyński, Letkiewicz, 2009: 120).

Some act for the benefit of times, many times facilitating and saving human lives, whilst others use the latest technology to kill and destroy, including state institutions (Pacek, Hoffman, 2013: 7).

In times of all these threats, the state must be extremely resilient to attacks and be aware of existing threats. The most important objective of state functioning is to ensure the security of all its citizens. For the state to function efficiently, all entities, institutions and services which are responsible for security in the country must be prepared for such threats. An inter-ministerial group of representatives from the Ministries of Digitalisation, National Defence, Internal Affairs and Administration, the Internal Security Agency, the

Government Centre for Security and the National Security Bureau have developed the Cybersecurity Strategy of the Republic of Poland for 2019-2024, which outlines "strategic objectives and relevant political and regulatory measures to achieve a high level of cybersecurity, principally a resilience to cyber threats of information systems used by operators of essential services, critical infrastructure operators, digital service providers and the public administration". This will also increase the level of national security (Cybersecurity Strategy of the Republic of Poland for 2019-2024 – Digitalisation of the Chancellery of the Prime Minister – Gov.pl Portal (www.gov.pl). The strategy is the result of the implementation of the Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, the so-called NIS Directive. Under the afore-said directive, in order to fight cyberterrorism effectively, activities should be coordinated primarily in the legal field, but also in terms of organisation. The protection of cyberspace is one of the fundamental tasks of public administration. An effective fight against cyberterrorism needs specialised institutions to use appropriate tools in order to monitor state security.

The authorities responsible for ensuring cyberspace security in Poland include the Ministry of the Interior and Administration, the Ministry of National Defence, the Internal Security Agency, the Military Counterintelligence Service and private entities.

In Poland, two institutions play a leading role in anti-terrorist activities: the Internal Security Agency (Journal of Laws of 2002) and the Police (Journal of Laws of 1990), which work closely together. The Internal Security Agency is a special service responsible for issues related to the protection of internal security of the state and its constitutional order. The main task of the Internal Security Agency is the protection of the state against planned and organised activities which might pose a threat to the independence and constitutional order of the Republic of Poland, as well as disrupt the functioning of the national government structure or jeopardise the basic interests of the country. The aim of this service is to combat various threats to the internal security of the state, such as the offences of espionage, terrorism, drug trafficking, organised crime or corruption. Measures to prevent the development of organised crime are based on granting powers to conduct operational and reconnaissance activities and criminal investigations to help to detect offences and prosecute perpetrators. Operational and reconnaissance activities, as well as analytical and information operations mainly serve the purpose of obtaining information to ensure state security and order as guaranteed by the Constitution of the Republic of Poland (Internal Security Agency – abw.gov.pl).

The Act on the National Cybersecurity System has established three Computer Security Incident Response Teams: CSIRT NASK, CSIRT GOV and CSIRT MON. Each of the teams is responsible for the coordination of incidents reported by entities assigned under the Act.

CSIRT NASK (nask.pl) – is led by the Research and Academic Computer Network – the National Research Institute.

The main tasks of the CSIRT NASK team include:

- recording and handling network security incidents;
- responding actively in a situation of immediate danger posed to users;
- cooperating with other CSIRT teams in Poland or worldwide;
- participating in national and international projects related to ICT security issues;
- conducting research on security incident detection methods;
- analysing malware and systems for the exchange of information about threats;
- developing proprietary tools for the detection, monitoring, analysis and correlation of threats;
- regular publication of the CSIRT NASK Report on the security of Polish internet resources;
- information and education measures aimed at increasing ICT security awareness.

The CSIRT NASK is obliged to coordinate incidents reported by the following entities:

- local government units;
- budgetary entities, local-government budgetary bodies;
- executive agencies, public-sector enterprises;
- public tertiary institutions and the Polish Academy of Sciences;
- the Office for Technical Inspection, the Polish Centre for Accreditation;
- the National Fund for Environmental Protection and Water Management, and regional funds for environmental protection and water management;
- commercial companies and partnerships carrying out tasks of general interest.

The CSIRT GOV (csirt.gov.pl) – led by the Head of the Internal Security Agency, it is the national-level CSIRT Team responsible for coordinating responses to computer incidents in the area indicated in Article 26 (7) of the Act of 5 July 2018 on the National Cybersecurity System.

The main tasks of the CSIRT GOV include the identification, prevention and detection of threats that compromise security and are important for the state's continuous functioning in terms of communication and information systems of public administration authorities or the system of ICT networks included in the uniform list of critical infrastructure facilities, installations and equipment, as well as communication and information systems of owners and possessors of critical infrastructure facilities, installations or equipment.

The CSIRT GOV is obliged to coordinate incidents reported by the following entities:

- public authorities, including government administration authorities, state inspection and law-enforcement authorities, and courts and tribunals;
- The Social Insurance Institution, the Agricultural Social Insurance Fund, the National Health Fund, the Polish Air Navigation Services Agency;
- the National Bank of Poland, Bank Gospodarstwa Krajowego.

The CSIRT GOV, together with the CSIRT NASK operate the ARAKIS-GOV system, which is an early warning system reporting threats emerging on the internet. This system has been developed through cooperation between the ICT Security Department of the Internal Security Agency and the CSIRT NASK team. The ARAKIS-GOV has been established to support the security measures protecting the ICT resources of public administration as a result of extending the ARAKIS system created by the CSIRT NASK by an additional functionality.

The CSIRT MON (csirt-mon.wp.mil.pl) – is led by the Ministry of National Defence. It is obliged to coordinate incidents reported by the following entities:

- entities subordinate to or supervised by the Ministry of National Defence, including entities whose communication and information systems or networks are included in the uniform list of critical infrastructure facilities, installations, equipment and services;
- entrepreneurs of special economic and defence significance, in respect of which the Ministry of National Defence is the authority that organises and supervises the performance of tasks aimed at ensuring national defence.

In addition to the afore-mentioned tasks of the teams, the Act on the National Cybersecurity System makes it possible to coordinate the activities of all CSIRTs in Poland. It enables them to cooperate with each other, jointly developing core elements of the procedures for handling computer incidents, the coordination of which requires cooperation. They specify, in cooperation with sectoral cybersecurity teams, how to cooperate with these teams, including how to coordinate the handling of incidents.

Simultaneously, CSIRT teams may, by way of agreement, entrust each other with the performance of tasks in relation to certain entities.

Another important element introduced by the Act in the area of cybersecurity is the possibility for CSIRT teams to perform device or software testing to identify the vulnerabilities which could be used to threaten the integrity, confidentiality, accountability, authenticity or availability of processed data, which may affect public safety or a vital interest of national security. On the basis of the afore-mentioned vulnerability testing, CSIRTs may provide recommendations to resolve vulnerabilities in devices or software used by entities within the national cybersecurity system (Computer Security Incident Response Team (CSIRT) – Digitalisation of the Chancellery of the Prime Minister – Portal Gov.pl (www.gov.pl).

The CSIRT GOV team is competent for handling incidents related to events of a terrorist nature, i.e., situations suspected to have developed as a result of an offence of a terrorist nature as referred to in Article 115 § 20 of the Act of 6 June 1997 – the Penal Code, or a threat of such offence (Article 2(7) of the Act of 10 June 2016 on Anti-terrorist Activities, Journal of Laws of 2019, item 796). Offences of a terrorist nature are defined as prohibited

acts committed in order to gravely intimidate many people, force a public authority of the Republic of Poland or of any other state or body of an international organisation to perform or refrain from performing certain activities, as well as to cause serious disturbances in the political system or economy of the Republic of Poland, another state or an international organisation – as well as a threat to commit such an act (the Act of 6 June 1997 – the Penal Code). The CSIRT MON is competent for handling incidents which are related to events of a terrorist nature and compromise the security of the national defence capabilities, affecting the Armed Forces of the Republic of Poland and organisational units of the Ministry of National Defence (Article 5 (1) (2a) of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service, Journal of Laws of 2019, item 687). If it is determined that an incident the handling of which is coordinated by the relevant CSIRT MON, CSIRT NASK or CSIRT GOV is related to the events referred to in paragraph one or two, incident handling coordination shall be taken over by the relevant CSIRT MON or CSIRT GOV (the Act on the National Cybersecurity System of 5 July 2018, Journal of Laws of 2018 item 1560).

In order to eliminate cyberterrorism, it is extremely important to protect classified information. Unauthorised access to this type of information may have serious consequences for the state. This is why cyberterrorists, when planning their attacks, initially use measures typical for cybercriminals. For example, they use techniques such as phishing, spoofing and hacking to extract data. This makes it easier to mount a complex and destructive cyberterrorist attack.

The key role in ensuring the protection of classified information is played by the Internal Security Agency and the Military Counterintelligence Service, which perform tasks related to the provision of personal security, i.e. conducting clearance proceedings, physical security, industrial security and ICT security.

Cyberspace has become a new security environment, prompting numerous changes, both in the pragmatic and in the legal and organisational dimensions of the functioning of security systems worldwide. In this context, it is particularly important to understand the dynamics of the changes in this environment. Building a legal system that constitutes the state's response to the opportunities and challenges of its presence in cyberspace is an extremely complex task.

There is a trend towards a shift from the traditional form of government-sponsored terrorism to a model in which the internet and other modern technologies are used, among other things, for propaganda, fundraising and recruitment of new members.

Cyberterrorism poses a significant threat to modern public administration. It interferes with the structure of internal state security. Nowadays, in times of globalisation, the expansion of societies, the flow of all goods, including information, this phenomenon should not be underestimated in any way. The state should take all available measures to prevent, at least to some extent, adverse phenomena such as cyberterrorist attacks. It is

the state's mission to implement appropriate systemic solutions in the area of prevention and to develop an early warning system against attacks. Institutions from both the public and private sectors should cooperate and coordinate actions to ensure security in cyberspace.

References:

Aleksandrowicz, T. (2008) *Terroryzm międzynarodowy* (Warszawa: Wydawnictwa Akademickie i Profesjonalne).

Banasiński, C. (2018) *Cyberbezpieczeństwo. Zarys wykładu* (Warszawa: Wolters Kluwer).

Denning, D.E. (2002) *Wojna informacyjna i bezpieczeństwo informacji* (Warszawa: Wydawnictwa Naukowo-Techniczne).

Grzelak, M. & Liedel, K. (2012) Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski-zarys problemu, *Bezpieczeństwo narodowe*, 22(2), p. 136.

Hołyst, B., Jałoszyński, K. & Letkiewicz, A. (2009) *Wojna z terroryzmem w XXI wieku* (Szczytno: Wydawnictwo Wyższej Szkoły Policji).

Kowalewski, J. & Kowalewski, M. (2014) Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa, *Telekomunikacja i Techniki informacyjne*, (1-2), p. 28.

Olak, A. & Krauz, A. (2014) Zjawisko terroryzmu we współczesnym świecie, *Kultura bezpieczeństwa. Nauka-Praktyka-Refleksje*, 15(15), p. 189.

Oleksiewicz, I. (2018) Cyberterroryzm jako realne zagrożenie dla Polski, *Rocznik Bezpieczeństwa Międzynarodowego,* 12(1), pp. 58-59.

Pacek, B. & Hoffman, R. (2013) *Działania sił zbrojnych w cyberprzestrzeni* (Warszawa: Wydawnictwo Akademii Obrony Narodowej).

Fiktus, P., Malewski, H. & Marszał, M. (2015) *Rodzinna Europa. Europejska myśl polityczno – prawna u progu XXI wieku* (Wrocław: E-Wydawnictwo, Prawnicza i Ekonomiczna Biblioteka Cyfrowa, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego).

Szymczak, M. (1995) *Słownik języka polskiego, t. III* (Warszawa: Wydawnictwo Naukowe PWN).

White, K.C. (1998) *Cyber-Terrorism: Modem Mayhem* (Carlisle: U.S. Army, War College), available at: apps.dtic.mil/sti/pdfs/ADA345705.pdf (January 5, 2022).