THE THREAT OF CYBER ATTACKS IN URBAN CONURBATIONS

Marta BACHOR
m.bachor@akademia.mil.pl
Faculty of National Security
War Studies University, Warsaw, Poland

Abstract

This paper investigates the threat of cyber attacks in urban conurbations. The first section attempts to define cyberspace and to identify potential objects of attack in the city. The second section analyses the history of past cyber attacks, and the final section gives an overview of activities performed by states and organisations with a view to countering and eliminating cyber threats.

Keywords: cyber attack, city, security

Introduction

The beginnings of the internet can be traced back to the late 1970s and the first attempt to send data undertaken at California University. That event marks the starting point of the rapid growth of the internet and cyberspace. In recent years, the range of services offered on the network has been extending and includes: e-mail, search engines, social networking sites, and multimedia-playing websites. The growth of the internet has been correlated with the increase in the number of web users. According to a report published by *We are Social*, he number of internet users has grown by 7.8% in 2018.

The figures are unsurprising, bearing in mind that an increasing number of people and entities have decided to transfer their everyday life and business to the virtual world. Modern life would be practically impossible without access to the most recent news, e-mail, contacting family in a distant part of the world, online shopping, and e-banking. The importance of the internet is such that it is nowadays considered as a basic utility, along with the classic trio: water, electricity and gas.

Unfortunately, the soaring numbers of users give rise to increasing numbers of negative activities. Developed to make people's lives easier, cyberspace provides anonymity, which conceals the illegal activities of terrorists, criminals and states.

In this context, owing to the fact that these are cities that are the focal point of political power, central banks, and critical infrastructure in a broad sense, these are also cities that are in particular danger from cyber attacks. Destabilising efforts may be undertaken not only during wartime and crisis, but in peace time as well. Therefore, the provision of cyber security should be the priority of every city.

Considering the aforementioned background, this paper will begin with an attempt to demonstrate the essence of cyber attacks and to provide a definition of the term *cyberspace*. Subsequent sections will focus on identifying cyber threats and their implications for city security, and give selected examples of interference in cyberspace by different countries. Finally, the attention will move to solutions adopted by countries and international organisations to eliminate cyber threats.

The essence of cyber attacks

Prior to delving into the subject matter, we need to define the term *cyberspace* and attempt to determine potential objects of cyber attacks in cities. The term *cyberspace* was coined by William Gibson, who first used it in his 1984 novel *Burning Chrome*. The expression is regarded to have entered common language in the 1990s. According to Andrzej Nowak, *cyberspace* "has been created entirely by human hand, by combining information systems into networks, which enable communication by electronic means. In addition, each participant in this battlefield exerts full control over the properties of this environment" (Nowak 2013, p. 6). An

alternative definition refers to *cyberspace* as "communication space created by the system of Internet links via networked computers and information memories, which encompasses all systems of electronic communication (Grenda 2013, p. 200).

Yet another definition considers cyberspace as the fifth domain – another dimension for influencing the adversary, along the classic arenas, such as the land, the sea, outer space and air space. Cyberspace is an "information battlefield" which enables a free flow of information. Any activities performed in cyberspace are aimed at gaining informational advantage over an adversary, and may be broadly classified into offensive and defensive. Defensive activities are undertaken in order to protect one's own information resources, whereas offensive activities aim to destroy or intercept the adversary's information system (Bielawski, Radomska 2017, p. 37).

Although the term *cyberspace* was coined relatively recently, particular states have attempted to propose their own definitions. The United States Department of Defense defines it as: "the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Nowak 2013, p. 7). Great Britain's approach to cyberspace is defined in the 2011 document *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*, which states that: "cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services"(Wasilewski 2018, p. 49). The European Union has put forward its definition of *cyberspace* in an official EU glossary, which describes the term as "the virtual space in which the electronic data of worldwide PCs circulate." The National Cybersecurity Agency of France (ANSSI) has proposed a short term defining cyberspace as "the communication space created by the worldwide interconnection of automated digital data processing equipment. (Nowak 2013, p. 8).

In Polish legislation, the term is defined by the Act of 29 August 2002 on Martial Law and on the Competences of the Commander-in-Chief of the Armed Forces and the Rules for his Subordination to the Constitutional Authorities, as "the space

for processing and exchange of information, made up of data communication systems."

As previously mentioned, despite the great convenience offered by cyberspace in a broad sense, it does provide the space for organising and performing cyber attacks. What is understood as a cyber attack are all activities or crimes executed in the form of electronic operations. The direct targets of such attacks are IT security systems and data protected by them; furthermore, cyber attacks often prove to be connected with the illegal dissemination and sharing of data (Grenda 2013, p. 200).

Critical infrastructure in a broad sense is for certain obvious reasons among the objects at the highest risk of attack. These systems are mostly concentrated in urban areas. The term *critical infrastructure* is defined in the Polish Act of 26 April 2007 on crisis management as "systems and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance for the security of the state and its citizens, as well as serving to ensure efficient functioning of public administration authorities, institutions and enterprises, which includes the following:

- energy, fuel and energy supply systems,
- communication systems,
- tele-information network systems,
- financial systems,
- food supply systems,
- water supply systems,
- health protection systems,
- transportation systems,
- rescue systems,
- systems ensuring the continuity of public administration activities,
- systems of production, storing and use of chemical and radioactive substances, including pipelines for hazardous substances."

The existing infrastructure is a network of interconnected systems, damage to one of which can result in damage to the others. Therefore, practically any element of the system is a potential object of attack. The common feature of terrorist attacks of the modern age, carried out by terrorists, criminals or other states, is their unpredictability in terms of the place and time of strike.

Fuel and energy supply systems can be regarded as one of the key systems of the critical infrastructure. The energy system is made up of energy and fuel production, transfer and distribution systems. A cyber attack on this system would probably involve targeting the strategic energy stations and lines in order to cause extensive damage (Żuber 2014, p. 180).

Compromising the tele-information network system could not only jeopardise the functioning of the city, but also the life and limbs of citizens. The gravity of such an attack results from the fact that the system is responsible for maintaining the operation of such elements as: finance, transportation, water supply, health protection and energy. The main objective of a cyber attack would be to disrupt the information chain.

The financial system of the state is high on the list of potential targets for a cyber attack. The system is composed of such institutions as: the central bank, commercial banks, cash machine networks, mints or stock markets. A cyber attack on such extensive infrastructure could be performed in order to disturb cash flow, money theft, conceal debt or current financial situation, manipulate the currency trading system, or to grant access to savings for enterprises or private actors. Were any of the aforementioned to come to fruition, it would be likely to cause panic or spread instability, which could in turn trigger mass withdrawals of assets (Żuber 2014, p. 181).

Another element of critical infrastructure, the food supply system, is one of the fundamental components of the national economy, which is of considerable importance to state economic security. Weakening this system could lead to hunger, epidemic or disease. The food supply includes such systems as: plant production, processing, transportation, foodstuff storage, food production and distribution. Depending on the targeted stage of the production process, the attack on food supply systems could disturb the food supply chain, or food production. Owing to the fact that modern food producers rely heavily on advanced technologies, the majority of machines involved in the process are computer-operated through IT systems. Any external interference in the food supply system could considerably disrupt society, and cause food shortages, which in turn would certainly cause food prices to soar.

Consequences of a similar character should be expected in potential interference with the water supply system. Composed of drinking water and waterworks, the system is critical to maintaining hygiene and the health of citizens. If destabilised, it would surely create favourable conditions for epidemics and diseases to spread, leading to loss of confidence in authorities and, as a consequence, the destabilisation of political and social structures.

The health protection system is responsible for ensuring sufficient levels of health care not only for the weak, old and sick, but also for any individual in dire need of treatment. Having gained access to the system, a potential attacker could target medical databases containing information on the medical history of patients and their personal data. Moreover, a cyber attack could be intended to take control over medical equipment: a hospital with no access to medical lamps, heart rate monitors and other instrumentation in operational condition would be incapable of performing its health care functions (Żuber 2014, p. 182).

Another system under threat from cyber attack is the transportation system. Transportation, *i.e.* movement of loads or people by means of railway, road, air, pipeline, sea or inland transportation systems, could be attacked in order to: disrupt traffic control systems or ticket services, give false information with the intention of manipulating the operation of navigation equipment or traffic light controllers. These activities could result in transportation disasters in each area of transport. Such events would probably lead to a heavy death toll and cause extensive damage to road and sea transport, or the aviation infrastructure, not to mention leading to natural disasters.

Rescue systems are quite complex and include: crisis management centres, the fire service and emergency ambulance service. Attacks on these systems could destabilise them and enable assuming the control of rescue operations and their coordination. Intercepting any of the elements of critical infrastructure in a broad sense may have far-reaching consequences. It may cause lack of trust in state authorities and affect people's sense of security.

Apart from the critical infrastructure, cyber attacks could also target enterprises and production facilities, with the aim of halting production. Cyber terrorists have developed elaborate methods of attacking prosperous and resourceful businesses. These inconspicuous attacks are predominantly targeted at the ignorance

and gullibility of employees, urging them to access infected websites or open e-mails, thus enabling the perpetrator to take over the system. The obtained access consequently allows them to steal company data or financial reserves and may subsequently bankrupt the business.

The elements of critical infrastructure, companies and production facilities described in this section are based predominantly in cities, which are by far the most-developed locations in the world, occupied by a considerable number of people who own countless electronic devices. Moreover, it ought to be mentioned that these are urban conurbations that are internet hubs, which further intensifies the network traffic in the area. The high concentration of such critical objects and facilities makes cities an attractive place for people, fostering their development and fulfilment of opportunities; however, this simultaneously makes cities an ideal target for attack.

Major cyber attacks in history

To support the theoretical explorations conducted in the previous section of this paper and to emphasise the gravity of cyber threats, this section will give notable examples of the most notorious cyber attacks.

Estonia was the object of one of the most serious cyber attacks targeting the entire state. Estonia is a country with an exceptionally high level of informatisation. Each Estonian citizen holds an electronic identification document, which allows them to use public offices. What is more, students do not need to appear at a university to sit exams, as virtually any matter can be resolved online, including accessing exam results, setting up a company or voting. In fact, Estonians were the first citizens to elect their government through online voting. Although the advanced level of IT solutions makes the lives of Estonians easier, it also attracts a considerable amount of attention from cybercriminals. The Estonian cyber attack commenced on 27 May 2007 and lasted for over 10 hours, during which numerous websites were blocked, including government sites, the President's, several newspapers, banks and the Police. As a result, Estonians were unable to access their online banking systems and money. The criminals were found to have employed the DoC-type virus that attacks selected servers by flooding the targeted machine with excessive

amounts of data, which leads to overloading and eventually blocking the system. It was widely reported that the attacks were carried out by Russia; however, a 5-year investigation has failed to prove that the cyber terrorists followed instructions from Russia. Nevertheless, it has been shown that the source of attacks was external (Nowak 2013, p. 10).

Another instance of cyber attacks aimed at states and, what is more, connected with Russian hackers, took place in Lithuania. The attack is believed to have been organised in response to the decision of Lithuanian authorities to prohibit the use of Soviet symbols. The main objects of the attacks were the website of the Lithuanian Parliament, the Ministry of Finance, the Ministry of National Defence and the Ministry of Agriculture. As a result, the attacked websites were daubed with images of the Soviet red flag and indecent texts directed at Lithuanian authorities (Nowak 2013, p. 12).

It is not only Europe that has become the target of cyber attacks; the USA was targeted by cyber terrorists in 2004. The attacks were primarily aimed at networks of the US departments of defence, state, energy, and homeland security, and also at companies providing equipment for the US Department of Defense. Although the conducted investigation revealed that the source of attacks was China, no organisation has officially accepted responsibility for the crime.

Physical critical infrastructure systems have also been targeted by cyber attacks, as exemplified by the attack on the tele-information network system of an electric power plant in Iran. The attack was carried out with the use of the Stuxnet virus, which infects the system in a two-fold process.

The first phase of infection is spreading while simultaneously attempting to conceal its presence from the security system. The virus spreads through removable storage devices, particularly in such environments as strategic infrastructure of *e.g.* nuclear plant systems, which are not connected to the worldwide web for safety reasons.

Phase two consists in searching for the control station, which is typically a standalone machine, monitoring and controlling industrial control systems (otherwise programmable logic controllers – PLC). The virus is known to conceal the implemented changes and its presence prior to undertaking to modify the industrial control system (Nowak 2013, p. 14).

It ought to be remembered that espionage should be considered as one of the cyber threats. Cyber-espionage primarily targets people in possession of sensitive information, attractive for the terrorist or criminal, which typically is crucial to *e.g.* national security. An example of such activities is a mass worldwide cyber-espionage attack that has been aimed at diplomatic and governmental institutions. The activity was detected owing to extensive efforts of a leading anti-virus software provider, Kasperskhy, and began to be referred to as "Red October." The main objective of the attack was to obtain information from computers and smartphones. "Red October" is capable of adjusting to a particular scenario owing to its modular structure. Each module is responsible for a different activity, *e.g.*: intercepting passwords, copying e-mail addresses, or monitoring keyboard activity. According to Kasperskhy, "Red October" successively attacked connected computers of key figures: military persons, diplomats, politicians, and lawyers (Nowak 2013, p. 145).

Poland is a frequent recipient of cyber attacks, and one of the notable instances was the one targeted at LOT Polish Airlines. The cyber attack was focused on the ground operation system responsible for organising the flight schedule. During the 5-hour breakdown, the airport was at a standstill, approximately 11 flights were postponed and passengers were unable to check either the online flight schedule or the schedule normally shown at the airport terminal. Similar problems occurred in Frankfurt, where the German airline Lufthansa's baggage check-in system was affected by a cyber attack.

The tele-information systems in Poland have also been targeted by hackers. The cyber-attacks were carried out using simple methods: a potential victim would receive a fraudulent e-mail message from their commander asking them to open the attachment. Once opened, the virus infected the entire IT system (Wybranowski 2014).

The given examples of cyber attacks exhibit specific targeting of attack objects, which are predominantly connected institutions and companies that are of critical importance to the state, and which are mainly located in cities. Typically, an attack on one object triggers immediate destabilisation of other systems within the network, whereas rapid dissemination of viruses is facilitated by the location of infection. Considering the level of technological advance, the implications

of cyber attack threat are even more serious. It is therefore imperative that the contemporary institutions responsible for security in urban conurbations cooperate in the search for optimal solutions.

Means of preventing and countering cyber threats

The overview of cyber attacks in the preceding section appears to indicate that the growth of the internet and cyberspace in a broad sense have facilitated the emergence of cyber threats. It is of great importance to develop optimal solutions in order to counter and prevent them. Considering the global range of this phenomenon, it appears necessary to look at the approaches adopted by various states and organisations around the world.

On 21 May 2010, the American government announced the establishment of the United States Cyber Command, *USCYBERCOM*, within the framework of the US Army. *USCYBERCOM* is responsible for protecting American military networks and organising information resources. The organisation employs 6,000 specialists working in 133 teams (Grenda 2016, p. 184).

Currently, the United States is continuing its efforts to improve the implemented solutions. The United States House of Representatives and the US Senate have proposed a 2019 defence policy bill that includes important regulations concerning the cyber security environment. The bill specifies the countries that are the main actors influencing the sense of cyber security, *i.e.*: China, Russia, Iran and North Korea. In order to ensure that the reaction to cyber threats posed by these countries is rapid and commensurate, the bill approves the use of adequate response should the threat be identified. Moreover, the bill introduces a number of regulations concerning Russia, *e.g.* it allocates additional funds to minimise the activities of Russian IT operations. The developed bill will be presented to the Parliament and subsequently to the President (Boguszewski 2018).

In Poland, on 1 February 2008, Polish authorities set up the Computer Security Incident Response Team *CERT.GOV.PL*. The major objective of the team is to coordinate the process of reacting to computer incidents in the sphere of public administration and the critical infrastructure in a broad sense. The team monitors

the security levels of websites and eliminates detected threats. The CERT.GOV.PL website contains information regarding current threats, forms of cyber attacks and measures of defence against them (Iskierka 2014, p. 87).

In addition, another Polish initiative designed to regulate the security issues in cyberspace took the form of a document *Poland's Cyber-Space Protection Policy*. The primary objective expressed in the Policy is for Poland to attain an acceptable security level for the national cyberspace. The document furthermore specifies particular steps that should be undertaken, including: increasing security level, bolstering threat detection and elimination capabilities, diminishing the effects of past incidents in cyberspace.

As is the case with numerous other countries, defence of cyberspace is also a priority in France. *French Cyberdefence Policy* recognises two interconnected domains: civil and military. No entity alone is capable of providing the adequate level of protection without cooperation with other services, including: IT service providers, network operators, and government functionaries. On 1 January 2017, French authorities unveiled a new cyber-warfare unit *CYBERCOM* subordinate to the ministry of defence. The unit is primarily responsible for three key missions: cyber information, cyber security and cyber attacks. According to the French government's plans, the unit will employ 3,200 frontline soldiers and 4,400 reservists by 2019 (Grenda 2016, p. 185).

Attempts towards systemisation of cyberspace defence activities are also undertaken by international organisations such as NATO. The cyber attacks on Estonia attracted the attention of NATO to the problem of cyber threats. The interest has prompted NATO to define cyber threats as a potential stimulus for performing joint operations. It has been concluded that the defence of the critical infrastructure of the alliance is the responsibility of all member states and that it should be performed in cooperation. NATO has created the Cooperative Cyber Defence Centre of Excellence based in Estonia. The Centre is the hub of cooperation and shares the expertise of not only member states but also other actors aiming to improve their capabilities through research, education and consulting (Urbanek 2016, p. 27).

Finally, with regard to the activities within the European Union, the main development is the setting up of the Cybercrime Centre of Excellence Network

for Training, Research and Education, whose objectives are to predict cybercrime and accumulate knowledge and information in the field in order to support investigations in criminal cases and developing and disseminating systemic solutions within the European Union.

Conclusions

Modern society is undoubtedly an information society, as exemplified by the growing trend among people to transfer an increasing share of their everyday activities into the virtual world. As with people, the trend can be seen among other actors, such as: states, businesses, and international organisations. Although the benefits of extensive informatisation are unquestionable, they do, however, come with certain threats. The cyber security policy implemented by states and organisations is crucial to ensuring the necessary level of security in cities. Such complex organisms as urban conurbations must function in a secure environment; this, however, would not be possible without involving the central authority, whose responsibility is to develop a plan for the particular systems constituting the critical infrastructure with regard to cyber defence. Such a centralised solution would be particularly effective in the case of failure of one of the systems of critical infrastructure targeted by a cyber attack. In such an event, the affected system could be switched off to prevent a further spread of the cyber attack to other systems.

The modern threat of cyber attacks sets numerous challenges to the services responsible for the security of the state. The task becomes ever more difficult due to the lack of a uniform definition of cyberspace. Moreover, we must remember that in the face of the rapid technological advances, performing strictly defensive activities might prove insufficient and should be coupled with close analysis of former activities in order to boost the chances for immediate detection should such attacks be carried out.

Each cyber attack requires serious attention. The majority of the mentioned cyber attacks targeted particular elements of cities' critical infrastructure and businesses. The immense danger of such attacks results from the fact that they might not only expose classified information, but also endanger the economic situation and question the security of cities as investment areas.

References

Act of 29 August 2002 on Martial Law and on the Competences of the Commander-in-Chief of the Armed Forces and the Rules for his Subordination to the Constitutional Authorities (Dz.U. 2002 nr 156 poz. 1301).

Act of 26 April 2007 on Crisis Management (Dz.U. 2007 Nr 89 poz. 590).

Bielawski, R., Radomska, A., 2017. Selected models of information warfare in cyberspace. *Security and Defence Quarterly*, 14(1), 35-50.

Boguszewski, Ł., 2018. *Cyberbezpieczeństwo w USA w 2019 roku – NDAA.* [online] Available from: https://www.cyberdefence24.pl/cyberbezpieczenstwo-w-usa-w-2019-roku-ndaa-analiza [Accessed 8 Aug 2018].

Grenda, B., 2013. Cyber bezpieczeństwo operacji powietrznych NATO. In A. Czulda, R. Łoś, J. Regina-Zacharski (eds) *NATO wobec wyzwań współczesnego świata.* Warsaw-Łódź, 199-213.

Grenda, B., 2016. Obrona Cyberprzestrzeni NATO. In R. Wiśniewski, K. Waluch (eds), *Zarządzanie bezpieczeństwem danych,* 177-190, Płock.

Iskierka, I., 2014. Zapobieganie i zwalczanie zagrożeń ze strony cyberprzestrzeni. *Dydaktyka Informatyki,* 9, 82-90.

Kemp, G., 2018. *Digital in 2018: World's internet users pass the 4 billion mark.* [online] Available from: https://wearesocial.com/blog/2018/01/global-digital-report-2018 [Accessed 7 Aug 2018].

Nowak, A., 2013. Cyberprzestrzeń jako nowa forma zagrożeń. *Zeszyty Naukowe AON*, 3(92), 5-25.

The UK Cyber Security Strategy, Protecting and promoting the UK in a Digital Word.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [Accessed 1 Aug 2018]

Urbanek, A., 2016. Cyberwojna – zagrożenie asymetryczne współczesnej przestrzeni bezpieczeństwa. *Studia nad bezpieczeństwem,* 1, 5-32.

Wasilewski, J., 2018. *Cyberprzestępczość- wybrane aspekty prawnokarne i kryminalistyczne.* [online] Available from: https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/6538/1/J_Wasilewski_Cyberprzestepczosc.pdf [Accessed 7 Aug 2018].

Wybranowski, W., Ta wojna już trwa [online] Available from: https://www.cybsecurity.org/wpcontent/uploads/2014/09/Do_rzeczy_nr38_2014_wybranowski.pdf [Accessed 7 Aug 2018].

Żuber, M., 2014. Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego. *Rocznik Bezpieczeństwa,* 8 (2), 178-196.