Associate Prof., Eng. Mariusz Frączek, PhD
Pomeranian Academy in Slupsk
ORCID: 0000-0002-2216-8053

DOI: 10.26410/SF_1/22/10

THE IMPACT OF INFORMATIONAL TECHNOLOGY DEVELOPMENT ON INFORMATION PROTECTION – CONSIDERATIONS IN THE CONTEXT OF HOMELAND SECURITY

Abstract

The publication presents basic issues related to information protection in the aspect of access and common use of various information technologies. There was presented a wide spectrum of their influence on the security of information and data of the global network user as well as the main threats. The author pointed out the issues of growing challenges, accepted and existing areas of their influence. The general impact of modern technologies on information security was also presented. An important thread of consideration is to indicate the basic principles of information protection, which should be taken into account when using the Internet.

Keywords

information security, information technology, threats, protection

Introduction

The state telecommunication system is designed to provide information for the needs of organizations, institutions and citizens in all states of its functioning – in times of peace, crisis and armed conflict. The foundation of the system architecture is the ICT infrastructure, which integrates various means and devices of communication and information technology, creating a network for transmitting information. In times of peace and crisis, the leading role is played by ICT service providers (mobile, Internet and cable operators). During war, dedicated systems and ICT networks are used for the most important people in the country and the armed forces, adapted to the organization of command and operations[1]. Experts in internal security issues have knowledge about their purpose and distinctiveness of the services provided. A common feature of most modern services is the use of the latest information technology based on both modern equipment and software to exchange information.

The dynamic development of information technology and the phenomenon of convergence of services between telecommunication and computer networks makes it more and more common to combine these two networks into a single entity and create a one ICT network[2]. Nowadays, this is reflected in the capabilities of each citizen in terms of individual abilities to create, collect, process and transmit information in digital form. The limitation is the type of equipment owned (finances), the ability to use it (knowledge), access to network infrastructure and the amount of time needed to implement a given service. One of the important reasons for this state of affairs is the continuous growth of users' expectations in terms of speed and quality, but also the continuous development of modern technologies. The author focused his considerations solely on the use of information technology in peacetime and its impact on information security, taking into account the potential and identified threats, as well as trying to identify ways to counteract them.

The presented problem situation makes it necessary to answer the question: How to make the users (institutions/ citizens) of modern information technologies aware that their incompetent use may affect information protection and internal security?

Methodological and methodical assumptions

The goal of the article is to demonstrate the need for studying the impact of informational technology development on information protection in the context of homeland security.

This involves a research problem, formulated as a question: How to make the users (institutions/ citizens) of modern information technologies aware that their incompetent use may affect information protection and internal security?

Due to the complexity of the goal and research problem, the research process employed theoretical and empirical methods, techniques and research tools. Various re-

[1] More: Regulamin działań wojsk lądowych, DWLąd 115/2008, Warszawa 2008.

[2] M. Frączek, Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych, Warszawa AON 2015, p. 31.

search methods, techniques and tools were used in the research process accompanying the preparation of this article.

The following were primarily used during the research:

- inductive reasoning where general statements are derived from detailed information, which made it possible to formulate new conclusions;
- analysis, which is a research process consisting in the decomposition of the whole into component or separating individual elements of the whole to learn the whole by learning individual parts, which made it possible to identify the scope of projects that constitute the rationalization of activities in the area of internal security.

An important source of knowledge for the author was also the analysis of documents for collection of research material and direct observation.

Security of ICT network and cyberspace

Security – the meaning of this term in the aspect of organization and functioning of ICT networks, along with the constant development of information technology, cannot be defined unambiguously. It has an interdisciplinary meaning, and this is a result of its various interpretations available in the literature[3]. According to the author, information and communication network security should be identified with ensuring, in a given place and time, the state which means no risk of information loss. Thus, it is "a state obtained as a result of an organized (organizational and technical) protection against possible threats, expressed in the ratio of the possessed potential intended to ensure information protection and the possibility of using forces and means appropriately to the scale of threats"[4].

The challenge facing all users is to determine the importance of protecting the virtual space to provide them with the desired services. The author has a number of doubts related to the interpretation of the term "cyberspace" contained in the literature[5], because according to the Polish law it is also defined heterogeneously, and no unambiguous and accepted definition has been developed. Usually, cyberspace is defined as the space of production and exchange of information created by ICT systems.

One of the most important documents defining the term "cyberspace" is the "Doctrine of Cyber Security of the

[3] Regulamin Działań Wojsk Lądowych, DWLąd Wewn. 115/2008, Warszawa 2008, Słownik definicji. Encyklopedia wiedzy komputerowej, Warszawa 2006, Biblioteczka Komputer Świat nr 3/03 (23), p. 213. Liderman K., Podręcznik administratora bezpieczeństwa teleinformatycznego, Warszawa 2003, p. 18. Liderman K., Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa 2008, pp. 11-12. Encyklopedia Nauki i techniki, Prószyński i spółka, Warszawa 2002, tom I, p. 139.

[4] M. Frączek, Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych, Warszawa AON 2015, p. 79.

[5] Dictionary of the English Language, Fourth Edition copyright ©2000 by Houghton Mifflin Company. Updated in 2009. Published by Houghton Mifflin Company, Random House Kernerman Webster's College Dictionary, © 2010 K Dictionaries Ltd. Copyright 2005, 1997, 1991 by Random House, Inc., Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010, p. 6, Ustawa z dnia 17 lutego 2005 roku „O informatyzacji działalności podmiotów realizujących zadania publiczne", Art. 3, pkt. 3., M. Frączek, Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych, Warszawa AON 2015, pp. 149-151.

Republic of Poland" [6] which "indicates the strategic directions for ensuring the desired level of security (...) in cyberspace" and further defines it as "the space for processing and exchanging information created by ICT systems (sets of cooperating IT equipment and software ensuring processing, storage, as well as sending and receiving data through telecommunication networks by means of telecommunication terminal equipment appropriate for a given type of network and intended to be connected directly or indirectly to the network's termination point) together with the links between them and relations with users"[7].

The aforementioned "Doctrine..." attempted to reconcile different environments and to develop a compromise on the functioning of the armed forces in cyberspace, among other things. Hence, another concept called cyber security environment appeared. It is defined as "the totality of conditions for the operation of a given entity in cyberspace characterized by challenges (opportunities and risks) and threats to the achievement of the adopted objectives"[8]. Thus, the meaning of the term cyberspace is constantly evolving and can be identified in many ways[9]. It should be noted the ongoing heated discussions among experts and academics on the origins and meaning of the term cyberspace. There are still different, not always uniform interpretations of it, because the precise characterization of cyberspace is difficult, which is due to different premises. It is also worth noting that in the ICT networks of telecommunication operators it is erroneously assumed that protected assets are only information in electronic form containing various data exposed to cybercrimes[10], fear-inducing cyberterrorism[11] and hacktivism. The author's professional experience indicates that this is a much broader area, also for scientific research about the impact of modern technologies on security.

Information technology – selected aspects of information protection

The current broadband market has gone through a long evolution in two respects:

1. Bandwidth growth – from PSTN telephone networks to ISDN to broadband access, i.e., from the technology of using copper cable to the use of fiber optics.
2. New applications – allowing to transmit first voice information, then text, next images and finally multimedia in form of video.

This has resulted in a rapid development of the ability to transmit information in the order of their origin: telephony, SMS, e-mail, chat boxes, use

[6] Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej z dnia 22 stycznia 2015 roku, wyd. BBN, wyd. Warszawa 2015. Przesłanie Prezydenta Rzeczypospolitej Polskiej.

[7] Ibidem.

[8] Ibidem, Wprowadzenie, p. 5.

[9] M. Frączek, Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych, Warszawa AON 2015, p. 151.

[10] A. Bógdal-Brzezińska, M.F. Gawrycki, Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Warszawa 2003, p. 325.

[11] D. E. Denning, Wojna informacyjna i bezpieczeństwo informacji, Wydawnictwa Naukowo-Techniczne, Warszawa 2002, T. Jemioła, J. Kisielnicki, K. Rajchel, Cyberterroryzm – nowe wyzwania XXI wieku, Wydział Wydawnictwa i Poligrafii Wyższej Szkoły Policji w Szczytnie, Warszawa 2009.

of websites (Internet – mainly various thematic Internet portals, instant messaging and online shopping), UMTS and VoIP connections, videoconferencing, teleworking, telemedicine, or VOD platforms (movie libraries). It should be noted, with some new services being created at the same time.

The aforementioned possibilities of exchanging messages in their various forms would not take place without taking into account basic technical factors that affect security. The most important of these include[12] critical infrastructure of the state; telecommunication networks; computer network; Internet (global network / internet of things); ICT systems and networks; cell phone networks and their operators; data transmission; databases; globalization; modern technologies; social networks; development of information society; universal access to information and knowledge; convergence of services; cyberspace; development of electronics; miniaturization of consumer devices; power grid; renewable energy sources; e-banking; electronic exchange of documents and private correspondence; collection, processing and transfer of information; protection of classified information and sensitive (personal) data; artificial intelligence and quantum computers. Even a cursory assessment allows the conclusion that this is a very large spectrum of capabilities.

It was deemed appropriate to identify the fundamental issues of the impact of modern technology on information protection, which include:

1. The level of awareness of threats and the ability to identify them (internal/ technical [including electronic] organizational/for information sources) when using modern technological solutions.
2. Protection of classified information, which strictly defines by what means it is possible and even mandatory to ensure its security.
3. Protection of unclassified information, but… considered as particularly important… – unfortunately there is a noticeable lack of unambiguous legal regulations.
4. Protection of personal data:
   a. ordinary (name; surname; address of residence; PESEL, NIP, number and series of identity card, education, profession, sex, telephone number);
   b. sensitive (sensitive, particularly protected: racial or ethnic origin; political opinions; religious or philosophical beliefs; religious, party or trade union membership; health status; genetic code; addictions; sexual life; convictions, judgments of conviction, criminal fines and other decisions made in judicial or administrative proceedings).
5. Professional secrecy (for example, medical/ advocacy/ banking/ journalistic/ bailiff/ notary/ lawyer or judge) and effective access to data collected about them in digitized form.
6. The right to privacy and violation of personal rights.

[12] M. Frączek, Technical protection of cyberspace land force – general assumptions, ORCID: 0000-0002-2216-8053 Pomeranian Academy in Słupsk DOI: 10.26410/SF_2/21/7, Security Forum (ISSN 2544-1809), WSB University.

7. Consequences of breaking the law on the protection of (classified) information: revenue, reputation, data, customer trust, litigation.

It seems natural to ask where did the problems mentioned above come from? Well, in the XXI century we live in a world of digital surveillance, to which the vast majority of users agree:

1. Devices and tools: computers, laptops, netbooks, tablets, cell phones, CCTV cameras, artificial intelligence, databases...
2. Social media portals and platforms: Facebook, Instagram, Twitter, Tik Tok, WhatsApp, Messenger, YouTube, Skype, Google...
3. Lack of knowledge regarding cyber threats to digital citizens in terms of non-obvious ways to lose data and monetization it as a basis for business.

An example of such conscious actions is the fact that all Polish websites request their users to confirm that they voluntarily consent to the processing of their personal data, which is visible immediately after their launch. This consists of five points:

1. General information on the processing of data provided by the user when using services. Information on who is the controller of your personal data.
2. The use of cookies and other technologies and the scope of their use.
3. Information on how a website uses information from its user – direct marketing.
4. Brief information on how your information is used by the partners of a particular website and an indication of the long list of purposes for which the data is processed (storage of information on your device or access to it/ selection of basic advertising/ selection of personalized advertising/ profiling of personalized advertising/ profiling of personalized content/ selection of personalized content/ measurement of advertising performance/ measurement of content performance/ use of market research to generate audience feedback/ development and improvement of products/ provision of security, fraud prevention and error correction/ technical delivery of advertising or content. Special objectives: To provide security, fraud prevention and error correction, to tailor content available on the services to anticipated user preferences.
5. Information that as part of special features and functions, website partners may take the following actions: matching and linking offline data sources/ linking different devices/ using accurate location data/ receiving and using automatically sent device characteristics for identification.

According to the author, it is worth emphasizing that what threatens in computers – meets information technology users in the case of cell phones (smartphones), who often unreflectively allow various applications access to:

- cameras (front/ back);
- contacts/ location/ biometric data (fingerprint/facial recognition) and health data – sports and health monitoring apps;
- all media files (photos/ videos/music);
- all documents and data stored on your phone;

- instant messaging, including live chat (WhatsApp/ Signal/ Messenger)
- anonymous sending of data to owners of freeware.

What does total digital control of the citizen look like? Imagination suggests different scenarios, but we can try to define it as follows:

1. Users of the global network in the vast majority provide a lot of interesting data about their lives, for example, through their profiles on social networking sites every day describing what happened at their place along with photos (of the house, car, business, vacation).
2. City monitoring system follows the citizen from the moment he leaves home, through shopping, work and recreation, to his return. So, not wearing a seatbelt in the car while driving or talking on the phone – that can be a fine. It is also a source of data on the biometric characteristics of many people.
3. Cell phone is strictly assigned to its user, so there is no need to install new 1000 speed cameras – it is enough to monitor the speed of movement of this device and it will be known which driver obeys the rules in a built-up area and which does not. Moreover, it shows the time spent in a specific geolocation (work, university or sports hall).
4. ATM card allows you to check the actual location of its use when withdrawing any amount of money from an ATM (date, place, time, photo).
5. Credit cards and various types of loyalty cards for stores – allow you to determine the preferences of any consumer, what they buy and how much they spend.
6. Auction portals – allow you to determine the preferences of any consumer and are a source of data about users and people closest to them.
7. Selected vehicles – already able to order spare parts and make payments over the global network.
8. Internet of things – provides a lot of information about the life of the hosts of the apartment or house.
9. What does freeware want to know about its user and what does it need access to? Beware of any apps associated with Google or shipped with your type of phone (impossible to remove/hard to disable).
10. What does Microsoft office suite collect and why does it block or uninstall software from other vendors? Why does it do that when the others are purchased and used according to their license terms? Not many people think about it.
11. Intentional use of software and tools considered at least controversial because of their use contrary to the original purpose – for example, hacking through Pegasus into the account of the author documented in February 2022, who has no information that there are any criminal proceedings against him and is also not a terrorist…
12. Under the guise of security, civil liberties are being restricted and information is being collected about individuals who have different opinions and views from those desired by the authorities.

The catalog of threats in the above area is much wider, and the most useful information for a potential opponent is found on the Internet, which always remembers and never forgets. However, it is necessary to know where and how to find, for example, the profile of a given person. This also has its connection with homeland security. A kind of fashion for "sweet-photos" or openness to electronic media caused that everything is photographed, also in places and locations considered to be particularly important. The author counts among them areas of institutions and military units responsible for national security, as well as those subordinate to the Ministry of Internal Affairs and Administration. This applies to elements of critical infrastructure, but also sharing the image of people whose work should not be exposed on a large scale. It is possible to find a lot of information that is considered especially valuable despite the fact that from a formal point of view it is not classified according to the provisions of the act on protection of classified information. The ability to collect and verify information and the ability to analyze what it is used for is a potential danger of inappropriate or unwanted use. Under the guise of caring for state security, in connection with the situation beyond Poland's eastern border and Russia's war with Ukraine, it is overlooked or forgotten that we live in a country where the right to use operational control against its own citizens should also be respected. The fact that there is no new news on this topic in the media does not mean that it does not exist.

Summary

According to the author's assessment, it is difficult to unequivocally point to the best ways of preventing the situations shown above that result in threats to the loss of information considered particularly important from the perspective of a citizen or an institution, because each of them has different expectations. The described problematic situation causes, that only after getting acquainted with potential and actual types of identified threats lurking on the side of information technology, it is possible to give an answer to the question in the introduction of the selected and propose solutions that could reduce them. The universal ones include:

1. Education system focused on the use of modern technologies, but also on creating awareness of the various threats to individual users, organizations (institutions) and the state. It should already include students of primary and secondary schools, not just university students.
2. Social campaigns that educate all citizens in the aspect of various forms of threats not only relating to various social problems, but also associated with the use of modern technologies and lack of access to resources (devices), tools and services considered today as necessary for life.
3. Broader familiarization of citizens with their responsibilities concerning state internal security in the aspect of information protection.
4. Continuous search for and application of new, more difficult to bypass or break through ways of protection.

5. Other considered important due to the multifaceted nature of the area of consideration, which have not been listed, because they will be the area of further research explorations of the author.

It should be remembered that too many safeguards may have a negative impact on the protection of transmitted information due to its poor protection or difficult to avoid improper implementation and simplification of developed procedures.

After an in-depth analysis of existing possibilities of ensuring information protection security, the following final conclusions can be indicated:

1. The weakest element of the security system is man (use of information, desire for profit, pursuit of power, designing the system or committing crimes related to hacking into information resources).
2. Information technologies cause the development of ways to secure ICT systems and networks, but also to improve the means of acquiring information.
3. Always strive to create a system that provides information security at a specified acceptable level by combining the capabilities of various measures.
4. Increase in the financial cost of information security is not a guarantee of its protection according to the category of importance.
5. The author has a number of doubts and does not know many answers about the future of homeland security in the context of the use of information technology, but its unreflective use can be fatal to institutional and individual users.

In conclusion, the problems raised in this publication are only a prelude to proper research on information technology, and the overt nature of the publication necessitates a general presentation of this area of interest in relation to homeland security.

Bibliography

Bógdal-Brzezińska A., Gawrycki M.F, Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Warszawa 2003.

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

Dictionary of the English Language, Fourth Edition copyright ©2000 by Houghton Mifflin Company. Updated in 2009. Published by Houghton Mifflin Company.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej z dnia 22 stycznia 2015 roku, BBN, wyd. Warszawa 2015.

Encyklopedia Nauki i techniki, Prószyński i spółka, Warszawa 2002, tom I.

Encyklopedia wiedzy komputerowej, 2006, Biblioteczka Komputer Świat nr 3/03 (23).

M. Frączek, Technical protection of cyberspace land force – general assumptions, ORCID: 0000-0002-2216-8053 Pomeranian Academy in Słupsk DOI: 10.26410/SF_2/21/7, Security Forum (ISSN 2544-1809), WSB University.

Frączek M, Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych, Warszawa AON 2015.

Jemioła T., Kisielnicki J., Rajchel K., Cyberterroryzm – nowe wyzwania XXI wieku, Wydział Wydawnictwa i Poligrafii Wyższej Szkoły Policji w Szczytnie, Warszawa 2009 r.

Liderman K., Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa 2008.

Liderman K., Podręcznik administratora bezpieczeństwa teleinformatycznego, Warszawa 2003.

Random House Kernerman Webster's College Dictionary, © 2010 K Dictionaries Ltd. Copyright 2005, 1997, 1991 by Random House, Inc.

Regulamin Działań Wojsk Lądowych, DWLąd Wewn. 115/2008, Warszawa 2008.

Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010.

Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U.10.18.1228).

Ustawa z dnia 17 lutego 2005 roku „O informatyzacji działalności podmiotów realizujących zadania publiczne".

Zarządzanie kryzysowe. Teoria, praktyka, konteksty, badania, J. Stawnicka, B. Wiśniewski, R. Socha (eds.), Wyższa Szkoła Policji, Szczytno 2011.

Żmigrodzki P., Słownik synonimów i antonimów, wyd. EUROPA, Wrocław 2007, wyd. 2.

About the Autor

Mariusz Frączek, habilitated doctor. Retired Colonel of the Polish Army. He is a scientific employee of the Pomeranian Academy in Słupsk. He specialises in information security research, crisis management and the use of modern technologies in security.