THE MODERN SOCIETY DANGERS OF SHARING PERSONAL INFORMATION

Sylwester PNIAK

MILITARY UNIVERSITY OF TECHNOLOGY

Abstract. The article describes the importance of information resources as fundamental potential action. The constant technological progress brings rapidly changing situations but there is a thin line between the availability of innovation and the protection of privacy. The author shows how the use of the Internet significantly accelerates the exchange of information. Networking opportunities with global reach have been appreciated throughout the world which in turn resulted in incredible progress in the development of institutions and the acceleration of the process of globalization. Among the advantages of the presented network development outreach the author analyzes the technology widely available discussing the performance and the possibility of surveillance of users. The article also presents a security risk posed by the use of the mentioned services presenting the possibility of obtaining data and describing the risks resulting from active participation in the life of the Internet.

Keywords: information, surveillance, social networking, information flow, cybercrime.

Introduction

Without doubt one of the human qualities is the need to talk, the desire to constantly communicate, exchange information, and the imaging of one's life. However this need creates threats in the sphere of cyberspace and the information provided by the unit may adversely translate into life.

Cyberspace was created as one of the largest and informal projects of mankind whose origins are difficult to determine and the end may never come. It is quite another dimension, one can say that it is a land of utopia the subconscious dream of mankind for hundreds of years. Cyberspace is a world of advanced technology where you can go where eyes cannot reach and break what the mind does not break[1].

However among the advantages resulting from the operation of cyberspace there hides many risks. One of them is undoubtedly the danger of the information society and therefore society which is a very active way of using cyberspace to

[1] Material from the lecture, W. Żorski, *Wyzwania cyberprzestrzeni*, Wykład inauguracyjny Wydziału Cybernetyki WAT, Warszawa, 6.10.2014.

exchange information. This is certainly the fastest way to communicate combined with mass broadcasting and receiving messages.

Society is dependent on the use of the possibilities offered by cyberspace and more network with global reach. Cut-off from this service would cause disharmony, slow action and intensify lack of information in real time. The fact that the use of mass of different software applications and websites make the relationship between the functioning of the real and the virtual world indiscernible.

1. The value of information in the digital world

Access to information has always formed the foundation of all activities over the centuries changed only the manner of its acquisition and subsequent use. Information significantly affects the functioning of society moreover it plays a special role in ensuring the safety of the individual and ending with the wider security of the state.

Oscillating around the security of the information society it is necessary to draw attention to the source of today's exchange of information and its transmission routes. A multitude of devices owned by users enables continuous communication with the global network. A disturbing fact is that today there are more devices connected to the Internet than the users themselves. It makes us slaves in a sense of new technologies. The use of desktop computers, laptops, tablets, smartphones, as well as a direct link between private life with the use of software applications that condition the majority of its activities on access to technology and more importantly the Web.

The nineties of the twentieth century have opened new doors in the development of the technology by which a global network became more and more popular. The use of it can find a growing number of supporters who are successively involved in the development at the same time saving in the history their creation. An amazing flourishing network has made the Internet become part of our lives.

Public involvement in the exchange of information with the use of this technology has led to the situation that you can take to the conclusion that mankind suffers from information overload. Furthermore the problem also stems from maintaining the pace of development in relation to new technologies. While users of smartphones, tablets, laptops, etc. use the features and applications of the basic usually not going into the whole potential of the device.

This ignorance translates into the ability to dispose of the unconscious, sharing and dissemination of information which may adversely affect the unit. Thus the fact of having access to new technologies and their use does not relieve consumers of ignorance about the full capabilities of the device. It is a mistake to infer that if you do not use the feature which supplied equipment it does not need to know their application. There are many applications that share certain parameters that directly affect the use of the equipment. Therefore having the fullest possible knowledge of device capabilities increases guarantees deliberate disposal of information and databases.

Information as a foundation for action must have elements that shape its value. This value affects the quality and usefulness of the information[2]. Depending on the situation in question for each customer quality but above all the utility will be oscillated in a different spectrum.

Recalling the example of social networking there are a wide range of people that do not give more attention to the information provided. This lack of interest in certain cases may lead to a situation in which third parties will use the published data against a selected unit. Stalkers, people rootkit spyware eager to use the published posts, photos and videos creating a supplementary database for anyone able to trace during the course of a day, the habits and the most visited places. In due time they have the opportunity to come out from hiding and take action adversely affecting sender. Thus safeguarding information and above all one's own private life should be the basis of awareness of users the consequences show the disregard of the functionality of new technology.

In addition, the usefulness of the published information due to the possibility of conscious adaptation of the content before it is put on the Internet. This procedure will allow the evaluation of information to customers and what is associated with it, its usefulness.

Prior to the publication, it is worth considering what it is worth and how it translates into the future life of the sender. Therefore it is worth to examine whether the published data is able to bring profit or its dissemination will result in losses.

It can be assumed that all available information "i" brings a profit "Z" however this gain may be the sender positive or negative (loss incurred).

$$\mathbf{Z}_i = \mathbf{Z}[\mathbf{i}] - \mathbf{Z}_0[\mathbf{i}]$$

where:

$\mathbf{Z}_i$ – profit possessed information **i**,

$\mathbf{Z}[\mathbf{i}]$ – profit after the release of information **i**,

$\mathbf{Z}_0[\mathbf{i}]$ – profit without sharing information **i**[3].

Making a statement of the positive and negative aspects of the usefulness of the information extracts the value of communication. However the value of certain hazards arise, we can distinguish between direct and indirect threats.

The first of these include the activities carried out consciously and with an intended purpose. Examples of such activities with the use of social networks can be an attack DDoS – distributed denial of service. To cause dysfunction of the

[2] Cf. T. Jemioło, P. Sienkiewicz, *Zagrożenia dla bezpieczeństwa informacyjnego państwa. Identyfikacja, analiza zagrożeń i ryzyka*, t. 1: *Raport z badań*, AON, Warszawa 2002, p. 172.

[3] Cf. K. Liedel, *Zarządzanie informacją w walce z terroryzmem*, TRIO, Warszawa 2010, p. 51.

institution / company whose activities are in part based around Internet domains, simply create an event on the social networking site to convene a group (supposing million people) and set the date and time of the execution of operations. Making a large number of people logging onto the website at the designated time will overload the servers of a given entity. Consequently this will result in blocking the services of this institution and the appearance of messages about technical problems. Therefore they are fully aware of, and at the same time, direct actions creating a threat in the form of technical problems and dysfunctions of the entity.

On the other hand indirect threats relate to activities carried out to some extent unconsciously by the entity as a result of ignorance of the functioning of the mentioned technology or it does not give more attention to the action taken. It often happens that we are using the same device to further the interests of private individuals and business and the applications for quick data exchange and to collect them (the so-called. Cloud) operate at the same address logging. It may also be the case that we use our address to log on other devices. Most smartphones are synchronized, among others our Internet e-mail so log in to your account from another device which results in the copying of recorded information, eg. email addresses or phone contacts to the memory of the equipment used. At this point someone may be unknowingly sharing information with an unauthorized person, which in turn could affect own reputation and negatively affect the work performed.

There are a wide range of people who proceed from the assumption that they do not need to know the full potential of each application and what is more a function of device because these services are unnecessary to function in their lives. However, they do not realize that there are applications that are directly related to each other and the use of one can cause or reaction engaging the device in another location. There are more and more tasks related to the use of technology and ignorance of how to utilize them endangers the community in digital life.

Technological progress will stop at nothing, it will be record increasing growth of new technologies. It is necessary to raise public awareness that the lack of their involvement in the adoption of new equipment will create a growing dissonance between them and the technology. In turn the growing scale of the ignorance of its proper reap will result in the escalation of threats.

What's more scientists are concerned that the community will benefit from the rapid and shallow and more knowledge of plastic rather than surrender to contemplation and own reflections. The consequence of what we become more susceptible to suggestion which creates a lack of development of their own opinion and results in repeat information heard. In addition, we become less and less inquisitive, less creative in building concepts and new ideas. Such a turn of events may result in a slowdown of technological development, interpersonal relationships and the increase in the monotony of life.

2. Social networking sites and Internet domain

The functionality of online networks meant that most of the programmes, devices and systems, are based on their use. Members appreciated the fact that the information is sent in real time to the recipient so that provided a continuous updating of data and insight into the development of the situation.

The means of communication outreach we can see at every step, the widespread use of social networking sites by millions of people. The data collected at sites such as Facebook, nasza-klasa.pl, Instagram, fotka.pl, etc., make it not only meet the primary function for which they were created but their development and dissemination gave rise to endless personality database although user individually decide on the sharing of personal information. In addition to publicising the photographs and short films, the awareness of the audience is usually limited or not the fully conscious. Media often publicised case use of private images by third parties for the purpose of extortion or robbery of valuables found in homes shared in photographs. Social networking sites provide a huge database, as well as insight in the history of individuals. Thus safeguarding personal information and most of all awareness of their sharing should take increasingly higher level of security.

The first level of users surveillance through social networks takes place in a very simple way. Just the knowledge of the user's name / login / initials allows to trace his profile and individualize given messages. It is easy to see that there is a wide range of people who do not pay much attention to the published information, such as places frequently visited, among friends and places of relaxation or educational internet pages, work pages, creating emotional divisions of groups and friends, creation of supplementary database on the selected person. Through such activities there arises a constantly widening gap between real privacy and the privacy apparent – artificially generated.

The second level of surveillance takes on a much higher dimension. Where necessary to carry it out is the acquired knowledge and skills as well as the appropriate equipment. The activities of hackers in today's society is not new, misappropriation of personal data using the Web can happen to anyone. Activity crackers[4] encountered not only collecting data from social networking sites or website but also from any devices that use the internet. Securing the data before departure places considerable obligations on the part of the founders of portals and websites, as well as the thoughtful engagement of all users. Bearing in mind the possibility of loss or theft of personal information you should take appropriate steps to properly secure the data which can significantly affect private life. One such measure, and at the same time the easiest, is to collect valuable information in places cut off from communication outreach. By doing so we protect data against "remote" theft but

[4] Cracker – according to the dictionary of the Polish language – a person breaking into computer networks for illegal purposes.

they are exposed to direct theft. Despite this it is one of the best forms of storing valuable information.

As some believe, the next part of web of surveillance is individual consent to the use of "cookies". Informing about the use of Internet websites of "cookies" is an obligation that was imposed in Poland on 22 March 2013. The use of "cookies" is to collect user data using the assigned IP address identification. People who care about their Internet privacy are probably concerned about interference "cookies" in online surfing. "Cookies" are small pieces of data containing unique identifiers which somehow enable the functioning of websites – in particular online stores. The concerns they bring is that through the activity on the Internet market many companies "cookies" may be available on many websites creating the risk of transmission to third parties our habits. Furthermore, files in text – Numeric allow party website to determine user preferences and thus the appearance of the monitor which is not accidental and what's more directly affect internet users. This is because, since the display data which previously looked the user or directly interacted with them "Cookies" also function as storing logins and passwords but such a solution is not necessarily the surfer every time log which on one hand is convenient but on the other poses a real risk of use of the account by an unauthorized person.

There are several ways to protect against files "cookies" i.e. manually turn off the function in your browser settings but it may help to reduce the use of certain websites. The second way is to use software for data protection i.e. Anti-virus programs which also provide protection from "cookies".

The functioning of "cookies" creates a lot of controversy among Internet users undoubtedly interfere with our privacy subconsciously influencing the decisions that we make. Such use is advantageous for companies involved in online sales but whereas these activities are recognized users aware of the range of products and also used Internet functions. Due to the fact that the concept of cookies actually began to function only after the introduction of the requirement to inform Internet users about their use – in 2013, the awareness of their actual function in the last two years has not been clearly presented to the community. Users of Personal Computers (PC), desktops, laptops / notebooks, smartphones and tablets are at every step met with vigorous activity "cookies". A multitude of devices causes constant surveillance with the only requirement to implement it is access to the Internet. It is necessary to clearly define and make users aware of the tasks they play files in text – numeric, and how to translate into the private life of Internet users.

Another aspect of remaining in correlation with "cookies" and most of all computer networks are all sorts of applications for mobile devices (smartphones, tablets). Levied on private devices programmes it seems that they have to serve a clearly defined purpose. However, when you download the application we have to accept a number of functions with which the program will use. Often they are made available to telephone data, not flowing the proper functioning of the program. In addition, some manufacturers reserve the right that they are not responsible for the improper operation of the program, i.e. the use of a microphone and recording random content. The same applies to starting cameras built into the device. Frustration of mobile users is fully justified and leaves no doubt that privacy greatly begins to play a secondary role in relation to new technologies.

Active involvement of society, to develop proper data protection as well as access of third parties to private information must be included at ever higher levels. Security of data protection should be proportionate to the technological development. It was not until then that users are able fully and without much fear to use additional applications.

3. Data collection system Payback and system hybrid cards in the context of surveillance

The development of technology opens up new paths of humanity cognitive offering to perform tasks in a much simpler and faster way. Facilities result from successive engineers work in various fields of science and continued improvement of the existing technological achievements. However, in order to guard against partial surveillance we are faced with ambiguous choice whether to follow the spirit of the time giving part of their privacy or limit the use of new technologies.

A perfect example is the system Payback. The public eagerly reaching for technological innovations often do not realize the target operation of the system.

Daily activities include purchasing hence the idea so such a widespread operation could not be translated to the benefit of consumers, supermarkets, shopping centres, corporations, all looking for any ways to hold on to the customer. They used their technology acquisition as consumers are becoming more sophisticated. An example of such activity is a programme Payback. However what exactly is it, what is the purpose and what consequences does it bring?

The attractiveness of the programme is the accumulation of points relevant to the amount spent on purchases at the rate proposed by the managers of Loyalty Partner Poland Sp. z o.o. The offer seems to be very attractive, when accumulated on the card Payback certain number of points which we can later redeem them for prizes in kind. At this point the question arises as to what is the problem when making everyday purchases also later to receive perks?

Looked at from a broader perspective the ordinary consumer deliberately has virtually no feel of the intervention program Payback in life. However with a deeper analysis of the system we are able to see the shortcomings of what it carries. To participate in the program Payback, we have to fill out a form where we give personal details and consent to the processing of information necessary to participate in the programme. In addition we agree that our personal data is used for marketing purposes, statistical and market analysis, including but not limited to preparing and sending information about goods and services of current and future

Partners Loyalty Program[5]. Successively the third point of the Rules, entitled *Data Management*, located in the section *Principles of protection of personal data under the program Payback*, informs us that given in the application form and the personal data collected points and transactions with Partner Loyalty Program (goods / services, prices, balance points, place and date of the event) will be processed by Loyalty Partner Poland Sp. z o.o. with its base in Warsaw ("Loyalty Partner") acting as the administrator of personal data[6].

Taking a magnifying glass of the entirety of the programme Payback we come to the conclusion that by agreeing to the different points of participation in the programme we are thus expressing consent to share part of our private life. The operator has access to our personal data, he knows where we live, where we come from. Providing users with a card programme Payback, to collect additional data, which include:

- the date of purchase,
- stores where we shop,
- what items we buy, what we prefer.

Seemingly they seem to be a very insignificant things but making their connections are bornsurprising conclusions.

Having insight into what stores we shop they are able to determine in what area, place and given time that person resides. Over time the operator sees which stores we frequently visit thereby learning about our preferences in purchasing. Moreover he knows what and in what quantities we buy. The condition of gathering these data is the use of a Payback card and shopping at Partners Loyalty Program. These include a number of companies, among others: Allegro, BP, Real, LOT, Jysk, Mango Media, Multikino, Smyk, Empik, So! Coffe, Pizzaportal.pl, MediaMarkt.pl and many others. A multitude of the above-mentioned partners, illustrates to what extent programme Payback works and join more and more new players. The more shops taking part in the programme the operator has a greater insight into our privacy.

This point reveals a certain relationship the more we are active in the consumer market including greater surveillance users can make. By combining the information gathered by the programme Payback operators are able to determine what we like to buy, in which the stores, how often and in what quantities. At this stage you can start to make psychological image, as well as outline the nature of the person's preferences and desires.

Analysing the program further, you come to surprising conclusions. By making regular purchases with the card Payback, the operator knows the changing tastes of buyers and sometimes you can tell what was the cause. For example, if during the traditional shopping, the customer begins to buy children's items it can be deduced that the family have a new baby and when the user begins to buy dog food,

[5] [online]. [access of 05.11.2016]. [in:] https://www.payback.pl/regulamin.

[6] Ibidem.

it is known that in his home there is a quadruped. On the other hand when supplies of food increases to large quantities probably someone has joined the family.

It slowly shows a sketch of the life of a person that the Operator is able to interpret in the right way. In addition when the number of partners Loyalty Program is constantly expanding and therefore broadcasters have become actors of different industries it is an insight into the lives of individual consumers beginning to take on larger dimensions. Surveillance begins to include more and broader aspects of our lives from the use of large chain stores to small local shops. In July 2013 Payback started a new project called My City Payback which includes local partners operating in categories such as catering, accommodation and travel, health and beauty, sports and other activities as well. This shows the development programme on a large scale covering most aspects of life with which almost all of us have to deal with.

Having insight into the totality of the data collected all Partners Loyalty Programme Loyalty Partner is able to create a life history of individual users. However you have to mention that the above described activities carried out under the Act on the Protection of Personal Data of 29 August 1997. Despite this the information at the disposal of a company tend to profound considerations or take advantage of the Programme which later will be rewarded with a small prize in kind of several times its actual value or limit themselves to traditional methods of use of the various services.

An interview with the head of Payback, Michał Pieprzny, implies that the possibility of a programme Payback apart from market analysis Loyalty Partner for individual Partner Loyalty Program and focusing on surveillance head of Payback speaks as follows: "Do not analyze individuals because we respect and protect privacy. However, we are in a position to fully anonymous analyze buying behavior of individual participants"[7]. Nevertheless, it is possible surveillance of individuals makes a thorough analysis of their behavior.

Recent years have shown that seemingly insignificant things can take significant dimensions especially if they relate to public persons. Thus the protection of privacy should be on getting a higher level. New technologies make the sharing of data to become very simple. You have to bear in mind that this carries implications not necessarily visible immediately but over time taking the weight. To protect your privacy we face a choice concerning the involvement in the use of new technologies or reduction. This decision is extremely difficult because our future is based on new solutions to advance the communication and exchange of information.

In such a situation it is necessary to develop an appropriate solution that will allow the use of innovation while reducing insight into our privacy. In addition user awareness not only of the strengths of data technical innovations but above all with their pros and engaging in private life.

[7] [online]. [access of 06.11.2016]. [in:] http://manager.money.pl/prosto-z-firm/artykul/payback-wiemy-o--konsumentach-rzeczy-ktorych,183,0,1806519.html.

Another solution constitutes an indispensable part of our lives are bank cards, credit and debit cards, called later in the discussion as the Charter. They are used by a large part of society and this is due to their convenience and ease of use. Thanks to them in a small place we can keep our money and find it easy to use them. They have become a great solution to measure the twentieth century when the first Charter came into general circulation. This electronic payment instrument is a remote connection between an individual's bank account and a partner with whom we can make non-cash payments for goods and services. Moreover it allows us to perform a transaction at an ATM and buy or sell at a distance using the Internet or phone.

Today's cards have three technologies in use. The first, and also the oldest, is the technology of magnetic cards. Reading data is performed through a magnetic strip that by dragging the card reader reads the data on the basis of changes in the magnetic field. However, this technology is being supplanted by electronic cards, pin, also called chip cards – smart card. The principle of operation of electronic cards, is to use the IC – chip, that store user data. In the card's microprocessors there is rewritable memory usually from 8.24 kbit capacity which allows you to control access and login process as well as data collection user. On the other hand, access to transaction completion or release contained on the grid data requires entering 4-digit pin code. The latest innovation used in the safety data technology is a proximity card – contactless. It is characterized by a built-in microprocessor memory and an antenna. Proximity card to perform data read by electromagnetic induction and thus provides wireless technology. Most cards with this solution operate at a maximum distance of 5 centimeters from the reader. Thus reducing the likelihood of obtaining data on the card. The following figure (Figure 1) shows the hybrid card containing all of the above-described technology.

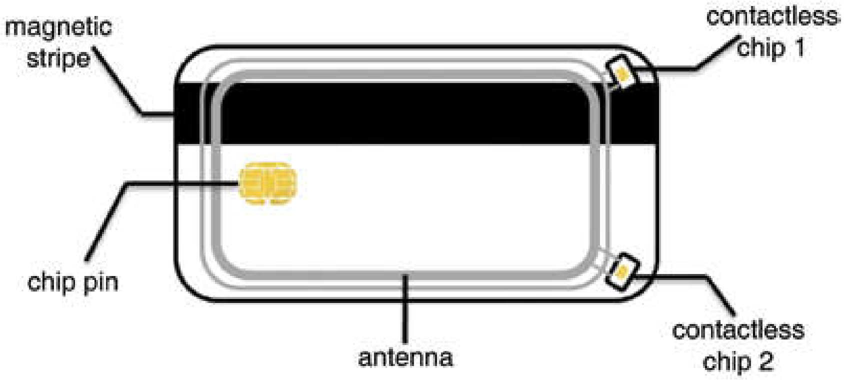

Fig. 1. Hybrid card

Based on: http://www.drukarkifargo.pl/?strona=3&podstrona=5, [access of 06.11.2016]

Cards found many supporters not only among the banking community but also in the use by corporations and rapidly growing businesses as identifiers and passes. However the most important role to play is as a form of cashless payment for services rendered.

Given the rapidly growing consumer market the use of cards is becoming a standard in everyday life. Readers allow decoding of data stored on the cards can already be found in local stores, small businesses, public transport to make payments for tickets entitling to travel, and above all shopping centers and supermarkets. A multitude of entities to exploit this technology is extremely large and still growing.

Each bank card is individually assigned to a user including the verification of the person using these services and banks do not make much of a problem. Given the user the operator is able to obtain information about executed transactions. It has therefore insight to where, when and in what amount is made of cashless payments. Moreover it is able to determine what services are being provided.

This data collection makes it possible to create the outline of the personality of the individual. Again it can be stated that the information seemingly insignificant enables the creation of the characteristics of the selected person's tastes, interests and habits. We are able to determine whether an individual attends a luxury restaurant or rather prefers local bistros. The situation is similar with the performance of shopping, some make them in supermarkets, chain stores, while others remain at the residential shops. Thus by collecting such data sets it is possible not only the control unit expenditure but to monitor the area in which the person is. Access to such information allows you to quickly track down the user and determine the position relative to the last of transactions.

Continuous infiltration of users with cards with hybrid technology and Payback cardholders raises questions about actual privacy. Undoubtedly the use of these technologies significantly facilitates everyday life however possible surveillance by the consumer may incur posing a real challenge for cardholders. Question arises whether it is reasonable to fully use the possibilities of the mentioned solutions or be subjected to strict selection entities of who will use them.

4. The specificity of action cybercrime

Today's technological development significantly improves the daily lives and saves a lot of time. Use of the network with global reach definitely speeds up the process of communication and exchange of data. This sensation has been recognized around the world translated into an incredible development of institutions and the acceleration of the globalization process. Assuming that nowadays information is the most important component of the action taken the use of the Internet is the fastest solution to the world of data exchange. In addition, more and more players use the internet or extranet[8] not only to the flow of information but also to remotely control the various systems. Operation and management of devices from

[8] Extranet – based on Internet protocols closed computer network used to exchange data.

a distance carries risks. A poorly protected link may become a target of crackers which in consequence will result in disruption of normal functioning.

Cyber attacks are aimed among other individuals using different web portals, corporations and smaller companies, government agencies, banks, and the critical infrastructure of the country. This multiple number of potential victims creates increased activity crackers while they were in a relatively anonymous form can achieve their goals. Irving Lachs and Courtney Richardson present the five characteristics that position cybercrime as an ideal tool for crackers and even criminal organizations. First, using the Internet issued a message in a short time and in a few seconds will be the recipient so the transfer is in real time. Secondly, the Internet is a relatively cheap means of communication through which cyber criminals have the ability to duplication of functions required by today's actors, companies and the media, and government institutions. Thirdly, the general accessibility to the Internet means that even a small group of criminals and even terrorists may use a global reach and therefore have the opportunity to compete with the dominant criminal groups and terrorist organizations. What's more they have the ability to generate their own Internet domains which to the public is a wide range of people. Fourth, the escalation of cyber-attacks gave impetus to the transformation of software that helps criminal groups to develop and disseminate information. Fifth, the Internet activity of criminals gives you the opportunity to stay almost completely anonymous which is valued in carrying out illegal activities[9].

Internet attacks show that those who are specialists in this range have a wide field of activities. One of the forms of their activity can be "gentle" aggression which, among other things, blocking websites by DDoS or "brutal" attacks methods which may include the use of so-called viruses or programmes causing unwanted technical faults or illegal sharing of data sets. In addition it is necessary to note that in these processes there are not limited fields in the area of operations they can cause serious economic, political and social problems. The problem oscillates around areas such as identity theft, fraud, access passwords (Phishing), illegal Internet drug trafficking, arms trafficking, as well as endangered species. Sequentially publishing illegal pornography, glorification of violence, and incitement to terrorist acts[10]. Summing up the overall risks presents a huge range of options which negatively affects the progress of civilization which in turn translates into difficulties in social development.

Appreciating the significance of threats to cyber-attacks, it should be made only after realizing the entity that carries consequences. The introduction of new technological innovations using Internet network makes more and more devices interact with others. Therefore it is necessary to bear in mind that the distortion

[9] Cf. I. Lachow, C. Richardson, *Terrorist use of the internet. The real story*, p. 100, [online]. [access of 14.04.2015]. [in:] http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD =ADA518156.

[10] See: *Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady oraz Komitetu Regionów. W kierunku ogólnej strategii zwalczania cyberprzestępczości*, Bruksela, 22 maja 2007, KOM(2007)267.

of the functionality of one of the components of the system it can escalate the collapse of the entire system. It takes a special importance when it comes to state-owned entities and individuals directly linked to them. Proper protection, as well as limit the interaction and dependencies between systems, will allow for adequate security and reduce the possibility of a situation that has the characteristics of the crisis.

Summary

Modern technology development has enabled the creation of new solutions which radically affected the functioning of today's society. The efficiency of information flow appreciated by many corporations, businesses, and most of all individuals for communication and exchange of goods and services from other entities. The functionality of the network with global reach made the esteem in relation to the flow of data constantly growing. With the increased use of the Internet and the appearance of threat forced a greater involvement in the development of security systems.

Considering the fact that in the world every day are sent approximately 12 billion text messages are part of the concerns of private information it is necessary to develop a routine including an analysis of transmitted content. However a large group of users focusing on the quantity not the quality of transmitted information. Thus they lost in routine needs continuous conversation which may result in hasty sending data contributing to changing the image of the unit by the recipient.

A perfect example of careless sharing of information are social portals. The Information society publishes everything up to date covering the events of their lives. Such a turn of events allows outsiders insight are shared posts, photos, videos. The situation takes on special significance when we consider the possibility in which the user does not restrict in their profile against the possibility of access by strangers. At this point they not only expose themselves to the possibility of nefarious use of the content but also the person whose initials or names who were included in the message.

Problems on the challenges posed by new technologies stimulates the search for new solutions. Especially bearing in mind that Internet addiction is a social disease and thus everything becomes digital, even life.

Modern society not without reason is referred to as the information society. Information and information systems are determined not only about the welfare of the citizens of modern states, the comfort of their lives and access to knowledge but also about safety no matter what aspect is dealt with; offensive – which allows you to gather knowledge about the enemy and its activities; or defensive – which allows you to protect your own resources before someone else's interference and manipulation[11].

[11] K. Liedel, *Zarządzanie informacją...*, op. cit., p. 142.

BIBLIOGRAPHY

Books:

[1] Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa 2006.

[2] Czekaj J., *Metody zarządzania informacją w przedsiębiorstwie*, AE, Kraków 2000.

[3] Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.

[4] Jabłoński W., *Kreowanie informacji. Media relations*, PWN, Warszawa 2006.

[5] Jemioło T., Sienkiewicz P., *Zagrożenia dla bezpieczeństwa informacyjnego państwa. Identyfikacja, analiza zagrożeń i ryzyka*, t. 1: *Raport z badań*, AON, Warszawa 2002.

[6] Kałużny P., *Techniki inwigilacji. Co nam grozi i jak się bronić?*, PWN, Warszawa 2008.

[7] Liedel K., *Zarządzanie informacją w walce z terroryzmem*, TRIO, Warszawa 2010.

[8] Verton D., *Black Ice. Niewidzialna groźba cyberterroryzmu*, tłum. K. Masłowski, Helion, Warszawa 2004.

[9] Wierzbołowski J., *Aksjologiczne i społeczne skutki przekształcenia informacji w zasób*, Warszawa 1997.

[10] Wnuk-Lipiński E., *Socjologia życia publicznego*, Scholar, Warszawa 2005.

[11] Zacher L., *Transformacje społeczeństw od informacji do wiedzy*, C.H. Beck, Warszawa 2007.

Materials from the conference:

[1] Own materials, *Wyzwania cyberprzestrzeni*, Wykład inauguracyjny Wydziału Cybernetyki WAT, prowadzący dr inż. Witold Żorski, Warszawa, 6.10.2014.

[2] Own materials, Oranowska A., *Najsłabsze ogniwa ochrony prywatności w nowych technologiach*, Ogólnopolska konferencja *Ochrona prywatności w nowych technologiach*, Wrocław, 6.04.2014.

Internet sources:

[1] Lachow I., Richardson C., *Terrorist use of the internet. The real story*, [w:] http://www.dtic.mil/cgibin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA51816 [access of 14.04.2015 r.].

[2] http://manager.money.pl/ [access of 6.11.2016 r.].

[3] http://marketingdlaludzi.pl/ [access of 28.10.2016 r.].

[4] http://www.drukarkifargo.pl/ [access of 6.11.2016 r.].

[5] https://www.payback.pl/ [access of 5.11.2016 r.].

[6] http://trybawaryjny.pl/ [access of 30.10.2016 r.].

[7] http://wszystkoociasteczkach.pl/ [access of 12.11.2016 r.].

Other sources:

[1] *Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady oraz Komitetu Regionów. W kierunku ogólnej strategii zwalczania cyberprzestępczości*, Bruksela, 22 maja 2007 r., KOM(2007)267.

NIEBEZPIECZEŃSTWA W UDOSTĘPNIANIU DANYCH OSOBOWYCH WSPÓŁCZESNEGO SPOŁECZEŃSTWA

Streszczenie. Artykuł opisuje znaczenie zasobów informacyjnych jako fundamentalnego potencjału podejmowania działań. Nieustanny postęp technologiczny niesie ze sobą niezwykłe udogodnienia, jednakże tworzy cienką linię pomiędzy dostępnością innowacji a ochroną prywatności użytkowników. Autor pokazuje, jak wykorzystanie sieci internetowej znacząco przyspiesza proces wymiany informacji. Możliwości sieci o globalnym zasięgu zostały docenione na całym świecie, co kolejno przełożyło się na niewiarygodny progres w rozwoju instytucji i przyspieszenie procesu globalizacji. Pośród prezentowanych atutów rozwoju sieci o szerokim zasięgu autor poddaje analizie technologie powszechnie dostępne, omawiając ich działanie oraz możliwość inwigilacji użytkowników. Ponadto przedstawia zagrożenia bezpieczeństwa, jakie niesie korzystanie z przywołanych rozwiązań, prezentując możliwości pozyskania danych oraz opisując zagrożenia wynikające z aktywnego uczestnictwa w życiu internetowym.

Słowa kluczowe: informacja, inwigilacja, portale społecznościowe, przepływ informacji, cyberprzestępczość.