Historia i Polityka
No. 26 (33)/2018, pp. 111–121
www.hip.umk.pl
ISSN 1899-5160, e-ISSN 2391-7652
DOI: http://dx.doi.org/10.12775/HiP.2018.035

Beata STACHOWIAK
Nicolaus Copernicus University, Faculty of Political Sciences and International Studies, Toruń, Poland

The Development of Information Society *Vis-à-Vis* Threats in the Realm of Internal Security, as Construed by the Respondents from Kuyavian-Pomeranian Voivodeship

Rozwój społeczeństwa informacyjnego a zagrożenia w obszarze bezpieczeństwa wewnętrznego w opinii respondentów z województwa kujawsko-pomorskiego

• Abstrakt •

Technologie informacyjno-komunikacyjne odgrywają w życiu jednostki, grup społecznych czy też społeczeństwa znaczącą rolę. Jest to związane nie tylko z nowymi urządzeniami, ale także poszerzającą się ofertą softwarową. Obecnie e-usługi są proponowane nie tylko przez podmioty komercyjne (np. e-bankowość, platformy handlu elektronicznego), ale również przez administrację szczebla centralnego (np. mDokumenty, Regionalny System Ostrzegania) czy samorządowego (np. aplikacja BLISKO). Często korzystanie z tych programów wymaga podania danych, które nieodpowiednio zabezpieczone mogą być wykorzystane przez przestępców. Użytkownicy, zarówno indywidualni, jak i instytucjonalni, powinni zachować rozwagę podczas korzystania z technologii komunikacyjno-informacyjnych. Dlatego też tak ważne są badania diagnozujące w zakresie odczuwania zagrożeń, także w obszarze bezpieczeństwa wewnętrznego, wynikających z rozwoju technologicznego. Niski poziom odczuwania niebezpieczeństw może skutkować ryzykownymi zachowaniami. Zaniechanie lub nieprowadzenie tego typu eksploracji skutkuje zazwyczaj nie-

• Abstract •

Information and communication technologies play a vital role in the lives of individuals, social groups or society as such. This fact is related not only to new devices but also to a further- and further-reaching software offer. Nowadays, e-services are offered not only by commercial entities (eg. e-banking or electronic trade platforms) but also by central administration (eg. mDokumenty [personal documents available on electronic devices], Regionalny System Ostrzegania [Regional Warning System] or by self-governments (eg. the application BLISKO). Frequent use of these programmes requires providing data which, when improperly secured, may be taken advantage of by criminals. Users, both individual and institutional ones, should remain alert while availing themselves of information and communication technologies. That is why, diagnostic research with respect to estimating threats – also in the realm of internal security – resulting from technological development is so important. Underestimating dangers may result in risky behaviours. Negligence or simply not conducting this sort of explorations usually lead to misfired educational-informa-

trafionymi akcjami edukacyjno-informacyjnymi lub wzrostem liczby przestępstw. W artykule zostały przedstawione wyniki badań przeprowadzonych wśród mieszkańców województwa kujawsko-pomorskiego w obszarze zagrożeń bezpieczeństwa wewnętrznego związanych z rozwojem ICT.

Słowa kluczowe: społeczeństwo informacyjne; obywatel; bezpieczeństwo wewnętrzne; ICT; województwo kujawsko-pomorskie

tional actions or to the increase in the number of crimes. The present paper presents the results of the research conducted among the inhabitants of Kuyavian-Pomeranian voivodeship in the area of threats to internal security, with the threats being contingent upon the development of ICT.

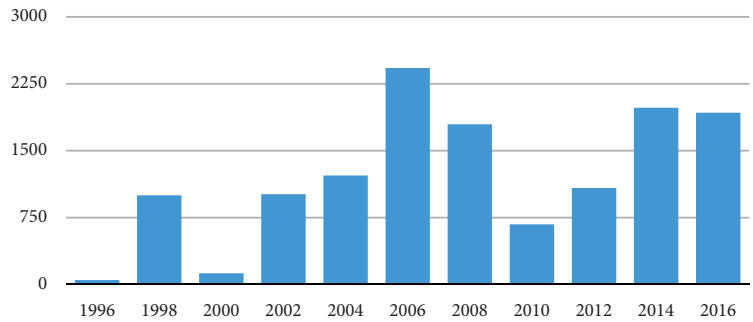
Keywords: information society; citizen; internal security; ICT; Kuyavian-Pomeranian voivodeship

Information Society *Vis-à-Vis* the Security of an Individual

In December 2019 there will have passed 25 years since I Kongres Informatyki Polskiej [The First Congress of Polish IT]. It was during this very congress that what was edited was one of the first documents that was about to pave the way to the creation and development of information society in Poland. The 1990s were full of enthusiasm; the majority of people considered ICT in terms of the possibilities they provide. Only relatively few pointed to the dangers they carry. The specialists who took heed of the latter perceived the said possible dangers in the form of – among others – informational totalitarianism, the collapse of humanism, emergence of new sorts of crimes or new types of civilizational diseases (Goban-Klas, Sienkiewicz 1999). As years went by, there were publications issued in Poland more broadly describing negative phenomena in connection with the development of ICT. Even nowadays, this problematics is raised and pertains to – among others – digital exclusion. (Stachowiak 2010, Popiołek 2016), new types of addictions (Majchrzak, Ogińska-Bulik 2010), cybercrime (Siwicki 2013, Zawisza 2017), and cyberterrorism (Marczewska-Rytko 2014, Smarzewski 2017). However, these considerations were not of purely theoretical nature. What was also initiated was the research over some negative phenomena or over the perception of some issues by the society. What can serve as an example is the research conducted by CBOS [Centre for Public Opinion Research] on representative groups of the inhabitants of Poland (CBOS 2009, CBOS 2015). As a result, for example, the respondents in 2009 regarded computer viruses as the biggest threat while using the Internet – 35% of them indicated this sort of danger. As a matter of fact, the respondents were blind to the dangers related to the development of cybercriminality. Only 5% of them admitted to having been a victim of a fraud on the Internet, while 1% of them was robbed. It appears as if a part of people were not conscious of falling prey to cybercriminals.

The beliefs held by statistical citizens are only one side of the coin since they are driven mostly by non-specialist knowledge. Yet, the research conducted by specialists gives an entirely different account: the level of danger with respect to internal security – at least in the realm of computer crimes – increases in Poland. CERT [Computer Emergency Response Team] Polska in 2016 responded to 32% of incidents more than in 2015. Figure 1 illustrates the number of incidents of this type responded to in the period of 1996-2016. The largest group among the incidents dating back to 2016 was constituted by computer fraud – 55.5% (that is identity theft, impersonating somebody else, etc.). Second most popular offence reduced to offensive and illegal content – 12.3%, with the third position being occupied by malicious software – 10.96%. However, this sort of data is accessible only to experts, and specialist reports are not adequately disseminated and are therefore not widely read.

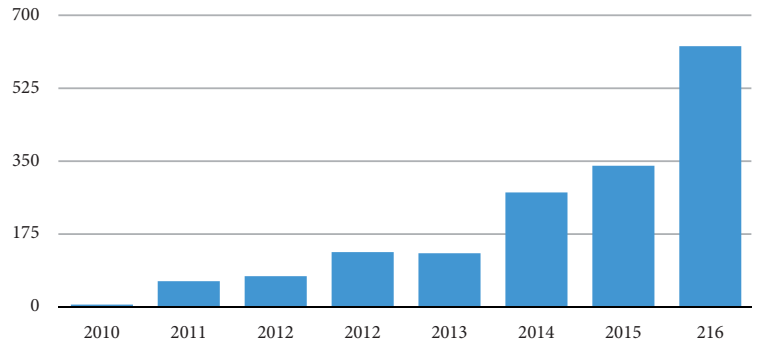
Figure 1. Number of incidents responded to manually by CERT Polska in the period of 1996–2016



Source: own study on the basis of the reports of CERT Polska (Cert 2017).

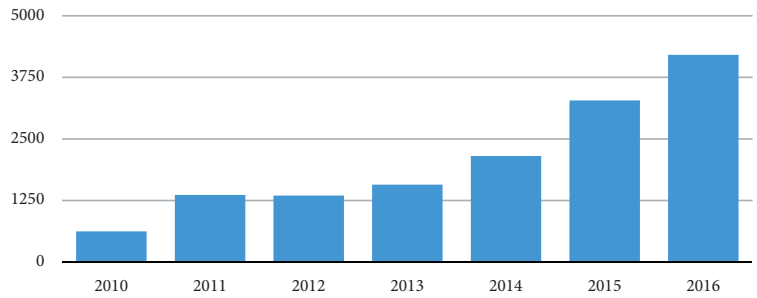
It is also police statistics that evidences growing dangers. The number of committed crimes related to ITC in some categories continuously increases. It is connected not only with the actions taken by criminal themselves, but also with the consciousness of citizens' being raised (however slowly). The data pertaining to the selected crimes; namely, computer fraud and grooming are represented in Figures 2 and 3.

Figure 2. The number of recognized crimes contrary to § 200a* of the Penal Code



Source: own study on the basis of police statistics.

Figure 3. The number of recognized crimes contrary to §287** of the Penal Code



Source: own study on the basis of police statistics.

The proportion of the phenomenon may still be much larger; Poland is still lagging with respect to technological development behind the countries excelling therein, with the countries being such as, for example, the United States and Scandinavian countries. According to the data of FTC dating back to 2011, as much as 11% of adult Americans feel prey to fraud on the Internet, having paid for services of products they did not eventually receive. In Poland, in the period of 2017–2018, the gravity of the problem may reach similar proportions – especially given that one of the features of computer crimes is the lack of awareness of being their victims.

* §200a – seducing a minor below 15 years old with the use of ICT system of telecommunications network, the punishment for the above: being subject to imprisonment for at most 3 years.

** §287 – computer fraud, with the punishment for it: being subject to imprisonment for at most 5 years.

The Description of Research

The problematics of dangers to an individual person, with the said problematics stemming from the development of information society, is crucial. Noticeable divergences in the opinions held by specialists and "plain people" encouraged the author to take up studies in this area. The research in question was conducted in 2015 in Kuyavian-Pomeranian voivodeship. 2200 questionnaires were collected. The sampling was non-random; and strictly speaking, that was the one of convenience. It was 2111 of them that proved eligible for final research. The age of the respondents ranged from 16 to 74 years old. The group was varied in a statistically significant way with respect to age, with the coefficient of variation being V=44.47%. Women constituted 54.3% of the respondents. The considerations raised in the present paper skip the respondents born before and during World War II. Eventually, the current paper shall present the opinions by 2070 people from the following generations: BB, X, Y and Z. The generational distribution, as presented in the Table 1 below, was adopted by the author to better illustrate the differences in the opinions held by the respondents. The majority were occupationally active people – 53.6%; occupationally inactive people (retirees, disability pensioners, the unemployed etc.) – 15.2%. Almost a half, that is 49% of the respondents, were still in education.

Table 1. The generational distribution of the respondents

BB	X	Y	Z
9%	23%	56%	12%

Source: own work.

The respondents, while answering the questions included in the questionnaire, estimated the level of danger stemming from the development of information society in the area of internal security, as experienced by themselves and by the remaining part of the population. The respondents specified the level of danger in the scale ranging from 0 to 5, where 0 meant the lack of dangers, 1 – negligible level of danger, 2 – low level, 3 – medium level, 4 – high level, 5 – very high level of danger. Furthermore, the respondents were allowed to select at most three out of eight variants of dangers or to independently enter their original dangers or to state the lack of opinion on that matter.

What follows are the alternatives included in the questionnaire directed at the inhabitants of Kuyavian-Pomeranian voivodeship.

1. Increase in the number of criminals due to new technologies and the possibility of remote actions.
2. Increasing threat of false alarms.
3. Susceptibility of an individual to computer crimes as a result of low level of knowledge.
4. Increasing threat of cyber attacks.
5. Sluggish reaction of law enforcement authorities and of the judiciary system to newly-emergent computer crimes.
6. Extending scope of computer crimes.
7. Too much dependence of efficient actions, also under crisis, on technical systems.
8. Violation of the "coherence of the legal system" due to new criminogenic phenomena.

The possible answers suggested to the respondents were characterized by a relatively high level of generality since the variants of answers were not addressed at specialists and too technical formulations might prove incomprehensible.

The Opinions Held by the Respondents

The respondents estimated the level of danger stemming from the development of the information society with respect to internal security. The inhabitants of Kuyavian-Pomeranian voivodeship judged the level of dangers, as experienced by themselves, respectively; and also as experienced by the rest of the population. Table 2 below includes the relevant detailed data.

Table 2. The level of danger according to the group of respondents, as estimated on the scale ranging from 0 to 5

	UMK students (2014)	Respondents without divisions into generations (2015)	Respondents from Kuyavian-Pomeranian voivodeship with a division into generations			
			BB	X	Y	Z
danger to society	3.1	3.1	3.2	3.1	3.1	2.8
personal danger	2.7	2.7	2.7	2.8	2.7	2.4

Source: own work.

The respondents estimated the level of their respective personal danger as higher than the one for the rest of the population – and this state of affairs held true for all the age groups surveyed. Furthermore, while studying the coefficient of variation for particular generations, it transpired that there is a statistically significant variety and quite a large one. With respect to the estimation of the level of danger, the coefficient of danger ranged in particular groups from 38% to 58%. When it comes to the estimation of danger to the society, the least variety was displayed in generation X, whereas as far the estimation of danger as experienced personally is concerned, the biggest variation occurred in generation Z. Such results enticed the author into searching for the factors exerting an influence on the opinions held by the respondents as well as into finding existent correlations.

Non-parametric chi-square tests for two and more independents samples proved that there are no such dependencies in the following categories: gender-level of personal danger, with chi-square being 4.223 for the critical value of chi-square being 11.07 and with alpha=0.05; frequency of using the Internet-level of personal danger, with chi-square=15.691 for the critical value of chi-square=24.996 and alpha=0.05; frequency of using the Internet – the level of danger to society, with chi-square=21.846 for the critical value of chi-square=24.996 and for alpha=0.05. It also proved that occupation status has no bearing on the estimation of the level of danger in the realm of internal security. In the case of the relation status-level of personal danger as calculated for the non-parametric test chi-square amounted to 26.456 with the critical value being 31.41 and for alpha=0.05. On the other hand, for the relation status-level of danger to society, chi-square equaled 25.489 with the critical value being 31.41.

The author also explored the correlation between the estimation of one's skills in the application of ICT and the estimation of the level of danger in two scrutinized categories: personal danger and danger to society. What was established was the coefficients of linear correlation both for the entire population of the respondents as well as for distinct age groups – even weak correlation was not observed. On the other hand, what was noticed was high correlation between the estimations of the level of personal danger and for danger to society. Pearson's correlation coefficient in this case amounted to 0.59. The present author also stated that the estimates of the level of dangers indicated by the respondents from generation Y are the same as the estimates made by the students of Nicolaus Copernicus University, the students being surveyed one year before.

The opinions of the respondents from 2015 slightly differ from experts' estimates. The latter judge dangers as higher. It must be granted that specialists spoke of strictly defined dangers such as: dangers to Android platform, phishing with

the use of electronic mail box, etc. It was already in 2015 that Polish experts, while estimating the probability of an attack having at their disposal the scale ranging from 1 to 5, indicated that the most probable is phishing with the use of electronic mail box and www services – 4.67, with the second place being occupied by – *ex aequo* – DDoS attacks on commercial entities and the dangers to Android platform – 4.28; with the third place being leaks of data containing personal information – 4.22 (FBC 2015). On the other hand, for 2016, specialists indicated phishing e-mail and www – 4.33; and next – leaks of databases containing personal information, passwords, numbers of credit cards, etc. – 4.21 and dangers to Android platform– 4.21 and attacks on organizations by dint of spear phishing – 4.19 (FBC 2016). As can be noticed, professionals take heed of dangers more clearly and view them as more probable.

The questions included in the questionnaire were meant to create a rating of dangers. The obtained results were also divided into generation groups. The opinions held by the respondents differed from one another. First of all, a distinctive feature was a lack of opinion; in the group of "baby boomers", a lack of opinion was declared by as much as 15% of the respondents. For the sake of comparison, among X-generation respondents, this indicator amounted to 7%; whereas among Y-generation people – 4%, and among Z-generation ones – 11%. Second of all, it proved that there is a certain variation in the rating of dangers that are regarded by the respondents as prominent. The results are presented in Table 3. The date points to a definite convergence between generations X, Y and Z. Even the percentage shares in these groups approximate each other. What is also noticeable is the similarity of indications by generation-Y respondents to the answers of the 2014 study among Nicolaus Copernicus University students conducted by the author. What the respondents from generations X, Y and Z indicate as the main danger are the growing opportunities for criminals due to new technologies and the possibility of acting remotely. The percentage share of this danger exceeds 40%. And indeed, each consecutive year brings about new methods for criminal actions; for example, the use of mobile applications, new socio-technical methods, etc. The next two most important positions were occupied by: the extended scope of computer crimes and the increased threat of cyber attacks. Admittedly, in Polish Penal Code there is no separate section related to computer criminality; however, from time to time there are amendments of the Penal Code; eg. adding §200a. What the respondents also regard as a threat is the increase in the number of cyber attacks which can paralyze a part of services online, destroy data, and also exert some influence on safety, eg. that of air traffic. The opinions cherished by BB-generation respondents are slightly different. They do notice dangers but their perception thereof is dimmer.

Table 3. The rating of dangers in the realm of internal security stemming from the development of information society

	I	II	III
Baby boomers	Extended scope of computer crimes 37%	Increased threats of cyber attacks 29%	Sluggish reaction of law enforcement authorities and of the judiciary system to newly emergent computer crimes 24%
X-generation respondents	Greater opportunities for criminals due to new technologies and to possibilities of remote actions 48%	Extending scope of computer crimes 42%	Increasing threat of cyber attacks 35%
Y-generations respondents	Greater opportunities for criminals due to new technologies and to possibilities of remote actions 45%	Increasing threat of cyber attacks 41%	Extending scope of computer crimes 40%
Z-generation respondents	Greater opportunities for criminals due to new technologies and to possibilities of remote actions 41%	Increasing threat of cyber attacks 35%	Extending scope of computer crimes 34%
Students of Nicolaus Copernicus University (2014)	Greater opportunities for criminals due to new technologies and to possibilities of remote actions 43%	Extending scope of computer crimes 40%	Increasing threat of cyber attacks 37%

Source: own study.

Presumably, what exerted some influence on the respondents' opinions is the fact of having encountered (or not) the problematics of dangers stemming from the development of information society, and the circumstances under which they could have gotten acquainted with the problematics might have been different: Internet portals, books, magazines, debates on the media, etc. It proves that in all the generation groups, the declarations of the respondents who encountered this problematics do not exceed 50%; for details: see Table 4.

Table 4. Percentage share of the respondents who have ever encountered the problematics of dangers stemming from the development of information society

Generation BB	Generation X	Generation Y	Generation Z
44.1%	45.9%	49.8%	47.7%

Source: own work.

This state of affairs is alarming because modern solutions entail new dangers. After all, the respondents expect the initiatives aimed at making individuals aware of the dangers stemming from the development of information society. In the case of BB generation, the indicator equals 65.4%, X – 71.6%, – Y 71.5% Z – 60.4%. The respondents realize that this problem requires top-down actions governed centrally.

Conclusions

The results of investigating the surveyed group mainly points to the need to raise the problematics of the dangers stemming from the development of information society. The respondents have certain amount of knowledge in this respect; yet, according to the present author, it is inadequate. Hence, any informational-educational actions should be directed to all the age groups and transferred through different channels. At school, during the classes on information and communication technologies, at universities during, say, the classes aimed at preparing students to obtain international certificates, such as for example ECDL. On the media – in popular-science broadcasts. Especially given the fact that the suggested business and administrative solutions (and others too) surround contemporary man. It is enough to mention what follows: electronic school registers allowing parents to have continuous control over the progress of their respective children, e-prescription having been implemented in Poland since May 2018 or burgeoning functionalities – not without issues, though – of e-administration. At this point, one additional thing should be mentioned. Ignorance of computer-crime-related issues may lead up not only to becoming a victim thereof but also to becoming a criminal oneself due to ignorance of the law.

References:

Centrum Badania Opinii Społecznej. (2009). *Zagrożenia w internecie*. Warszawa. Retrieved from: https://www.cbos.pl/SPISKOM.POL/2009/K_106_09.PDF.

Centrum Badania Opinii Społecznej. (2015). *Dzieci i młodzież w internecie – korzystanie i zagrożenia z perspektywy opiekunów*. Warszawa. Retrieved from: https://www.cbos.pl/SPISKOM.POL/2015/K_110_15.PDF.

CERT. (2016). *Krajobraz bezpieczeństwa polskiego Internetu w 2016 roku*. Retrieved from: https://www.cert.pl/PDF/Raport_CP_2016.pdf.

Fundacja Bezpieczna Cyberprzestrzeń. (2015). *Największe zagrożenia dla bezpieczeńtwa w internecie w 2015 roku. Głos polskich ekspertów*. Retrieved from: https://www.cybsecurity.org/wp-content/uploads/2015/01/Raport_FBC_Cyberzagrozenia_2015.pdf.

Fundacja Bezpieczna Cyberprzestrzeń. (2016). *Największe zagrożenia dla bezpieczeńtwa w internecie w 2016 roku. Głos polskich ekspertów*. Retrieved from: https://www.cybsecurity.org/wp-content/uploads/2016/02/Raport_FBC_Cyberzagrozenia_2016.pdf.

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

Majchrzak P., Ogińska-Bulik N. (2010). *Uzależnienie od Internetu*. Łódź: Wydawnictwo Akademii Humanistyczno-Ekonomicznej.

Marczewska-Rytko, M. (ed.). (2014). *Haktywizm: cyberterroryzm haking, protest obywatelski, cyberaktywizm, e-mobilizacja*. Lublin: Wydawnictwo UMCS.

Popiołek, M. (2016). Nierówności cyfrowe i podziały drugiego rzędu jak wyzwania dla gospodarki opartej na wiedzy. *Ekonomiczne Problemy Usług*, *122*, 113–122.

Siwicki, M. (2013). *Cyberprzestępczość*. Warszawa: Wydawnictwo C. H. Beck.

Smarzewski, M. (2017). Cyberterroryzm a cybeprzestępstwo o charakterze terrorystycznym. *Ius Novum*, *1*, 64–75.

Stachowiak, B. (2010). Poza granicami społeczeństwa informacyjnego – wykluczenie cyfrowe i co dalej? W: Z. Karpus, B. Stachowiak (ed.) *Granice i świat współczesny* (pp. 285–298). Toruń: Wydawnictwo Naukowe UMK.

Zawisza, J. (2017). Cyberprzestępczość i jej wpływ na bezpieczeństwo człowieka. *Przedsiębiorczość i Zarządzanie*, *18(5)*, part 2, 47–59.