13 "TANGO DOWN". SOME COMMENTS ON THE SECURITY OF CYBERSPACE OF REPUBLIC OF POLAND

13.1 Terminology

It is necessary to distinguish the meanings between two words in English language:

- safety – understood as in the context of the people and safeguard their basic needs of living (sometimes speaks about the safety of persons and property, eventually safety) and
- security – in regard to economic aspects, the managerial and technical, including IT [41, 42].

Security can thus be defined as a state in which the person has not sense of danger (subjective) or is not threatened (objectively) [41].

Issues related to the widely understood security are dealt with in a variety of sciences, ranging from - what is natural - science of safety and defense (the science of safety and the science of defense were added to the humanities sciences as two new disciplines under the Resolution of the Central Commission for Academic Degrees and Titles on January 28th, 2011 amending the resolution on the fields of science and arts, and scientific and artistic disciplines in place of the deleted military science) and police (the term "police science" works in some countries (e.g. Slovakia) [4]. In Poland, criminology is classified in law science), through the medicine (for example, disaster medicine, emergency medicine, forensic medicine, criminology (criminology deals with the psychology of crime), engineering sciences, IT sciences (e.g. cryptography, forensic informatics), to the social sciences (for example: economics of disasters).

The natural trend is trying to find common elements among the group of disciplines involved in the issues of security, which are carried out either from the perspective of extracting the self-study, or only in order to organize the nomenclature and – at least partially – research instrumentations. There are several approaches to the so-defined problem.

- Within the social sciences and management sciences should be noted the proposal to separate the name "securitology") [40, 41], which is the subject of human security and social organizations.
- Within the technical science sometimes used the term "security engineering" [1] or "safety engineering" [48]. The Author in publication [48] also identify the technical safety engineering and civil safety engineering. The first concerns the security of technical installations (given in appointed work examples concern the installation of protective reactors in nuclear power plants or marine engines), while the second deals with issues such as the removal of chemical contamination or evacuation of the population from places of disasters. In this approach the themes of the work will belong to technical safety engineering, as it concerns the security of specific technical objects, i.e. information systems.

- In informatics, although issues related to the technical aspects of security, storage, processing and transmission of information play an extremely important role (note that today the overwhelming majority of the information is in the form of electronic means: more than 90% of corporate documents is created, reviewed and stored in electronic form, with more than 70% of these information is never printed, the called digital universe in 2007 had a volume of 281 EB (exabytes). Information technology equipment also play an increasingly important role in various protective devices and monitoring, and these in turn are becoming an integral part of life: in 2007, the "shadow of the digital", that is, the amount of digital information generated about humans, exceeded the amount of information generated by themselves) [44, 52, 36, 45], there are separate names of disciplines dealing with security (probably one of the reasons is far-reaching terminological mess in informatics). In scientific sources operates dozens of compounds idiomatic defining the discipline of computer science (computer science in mathematics, geoinformatics, informatics in management, the economic data processing, computer science in law and history [43] (except - possibly - forensic informatics and judicial informacits (although it is worth mentioning about the series is sometimes truly bizarre – a proposal naming conventions for disciplines on the border of law and computer science (informatics law, cybernetics law, computer criminology, and even the computer forenscic) [54]).
- In the management science, it is referred to the management of security in the context of the continuity operations management systems [3], security management and health at work management [49, 47], risk management [37] and in the end, information security (information security management systems [38]).

The concept of "cyberspace" operates primarily in the language of the law (from a technical point of view, this is the name of at least questionable.

Neither a computer network is not a "space" nor cybernetics does not deal with computer systems. The subject of the last are the control systems and associated with them processing and transmission of information, while the subject of Informatics - technical aspects of information processing, particularly in computer systems. Sometimes used in the common language cyber-prefix is an old-fashioned word). And so the Act of August 30th 2011, amending the Act on the state of the war and the competence of the Supreme Commander of the armed forces and the basis for its reporting of the constitutional authorities of the Republic of Poland and certain other laws [58] defines it as follows: "space, processing and exchange of information created by ICT systems referred to in article 4. 3 section 3 of the Act of February 17th 2005 on the computer activities of entities realizing public tasks, together with the links between them and the relationships with the users".

While The Government's Program for the Protection of Cyberspace in Poland for 2011-2016 [46] defined it as:

- "Cyberspace – area of processing and exchange of information, created by the computer systems and networks, along with links between them and the relationship with users".

- "Cyberspace RP (CRP) – cyberspace within the territory of the Polish State and in locations outside the territory where there are representatives of the Polish Republic (diplomatic institutions, military contingents)".

13.2 Information security management systems

Information security management systems are the subject of group of standards marked with the symbols of the ISO/IEC 27x. Now these standards are largely still in statu nascendi, and – as is the case for most of the standardization work is, the polish-language versions are translated (standards series 27xxx are the subject of the work of the Technical Committee 182 PKN) with around two-year delay compared to the standards ISO/IEC. In addition to the standards of the 27xxx series, the older standards ISO/IEC (after the part withdrawn) are operating, in particular for e.g.: GMITS (Guidelines for Management IT), the standards of ISO/IEC 13335-x series (previously designated as ISO/IEC TR 13335-x, replaced in part by the ISO/IEC 27005: 2008), also the models [51], the national standards (in particular the US standards (NIST - The National Institute of Standards and Technology)), the methodologies [2] and other standards (in particular Request for Comments documents [50]) the terminology used in which, is used – sometimes in an almost completely any way – in different studies regarding security, sometimes even in the elaborations of significant practical importance (it is worth to mentioning about the problems which are made because of use taken over information technology concepts – often without understanding – in the language of law and legal [53, 56, 55, 59]). The problematical term which should be certainly included is also mentioned earlier definition of cyberspace).

Although the standards ISO/EC 27x are relatively well known, the number of companies which decide on their implementation is very small. According to data gathered on the http://www.iso27000.pl/sites/ view/stat=2=1 in March 2012 in Poland (of course, the registration certificate on the set up page is not mandatory, so the actual number of certified systems for ISMS seems to be slightly more, however, this will not be an especially significant difference) certificate of compliance with the requirements of ISO/IEC 27001 ISMS had just 169 organization, of which only 20 of public administrations:

- The Chancellery of the Prime Minister,
- Poviat Unemployment Office in Katowice,
- District Office in Bielsko-Biała,
- District Office in Kielce,
- District Office in Limanowa,
- District Office in Żywiec,
- District Office in Tarnów,
- Marshal Office of Malopolska Voivodship,
- Marshal's Office of Mazowieckie Voivodship,
- Bydgoszcz City Office,
- Kielce City Office,
- Piotrków Trybunalski City Office,
- Płock City Office,

- Siemianowice Śląskie City Office,
- Bielsko-Biała City Office,
- Legnica City Office,
- Polanica Zdrój City Office,
- Wałbrzych City Office,
- Wrocław City Office,
- Social Insurance Institution.

As far as – by its nature – the government is, or at least should be, qualified in the field of defence and civil security, insomuch the protection the security of information systems – and the informatization activities – is for the government the relatively new task, which fulfils it in a manner unsatisfactory. Although the government take some actions related to the security of "cyberspace" (particularly the creation of February 1st 2008 the government CERT team (cert.gov.pl) and the development of two government's programs for the protection of cyberspace in Poland (respectively for the years 2009-2011 and 2011-2016), the practice shows that it is unable to provide even the elemental security of own sites.

13.3 The goverment's program for the protection of cyberspace in Poland

The Government's Program for the Protection of Cyberspace in Poland for 2011-2016 is a good example of government approach to issues related to information security.

The program was developed by the Department of State Records and Teleinformatics Ministry of the Interior and Administration in June 2010 in extremely fast mode, forced as seems by external factors. Document in version 1.1 by Under-Secretary of State in the Ministry of the Interior and Administration has been directed on September 13th 2010 to departmental arrangements. These arrangements have never been completed, and the document was put away ad acta. The timescales defined in that document have been exceeded because the planned actions have not been realized. The ensures of officials that "security is viewed as a continuous process", unfortunately are not compatible with their actions.

The strategic objective of the Government's Program for the Protection of Cyberspace in Poland is "to ensure the continued security of cyberspace". This objective, together with certain specific objectives in the document ("increase the security level of the ICT infrastructure, including critical ICT infrastructure of state, reducing the effects of violations of the security of cyberspace, define the competence of the entities responsible for the protection of cyberspace, creation and implementation of a coherent for all subjects of the public administration of the safety management system of cyberspace and lay down guidelines in this respect for the non-public entities, creation of a sustainable system of coordination and exchange of information between the entities responsible for the protection of cyberspace and entrepreneurs, supplying services in cyberspace and ICT operators of critical IT infrastructure, increasing the awareness of users on the methods and security measures in cyberspace") was to be implemented through:

- "Creating a system of coordination to prevent and respond to threats and attacks against cyberspace, including the cyber terrorist attacks;

- Widespread implementation of mechanisms for prevention and early detection of cyber-security threats and the appropriate proceedings in the case of detected incidents;
- Universal public education and special education in the protection of cyberspace in Poland" [46].

Program was to be implemented through: the managing risk associated with the functioning of cyberspace, the setting of priorities for the implementation of the program, and the initiating of the protection programs. The document the Government's Program for the Protection of Cyberspace in Poland for 2011-2016 included 33 page with 26 attachments. The layout of the document is shown in fig. 13.1.

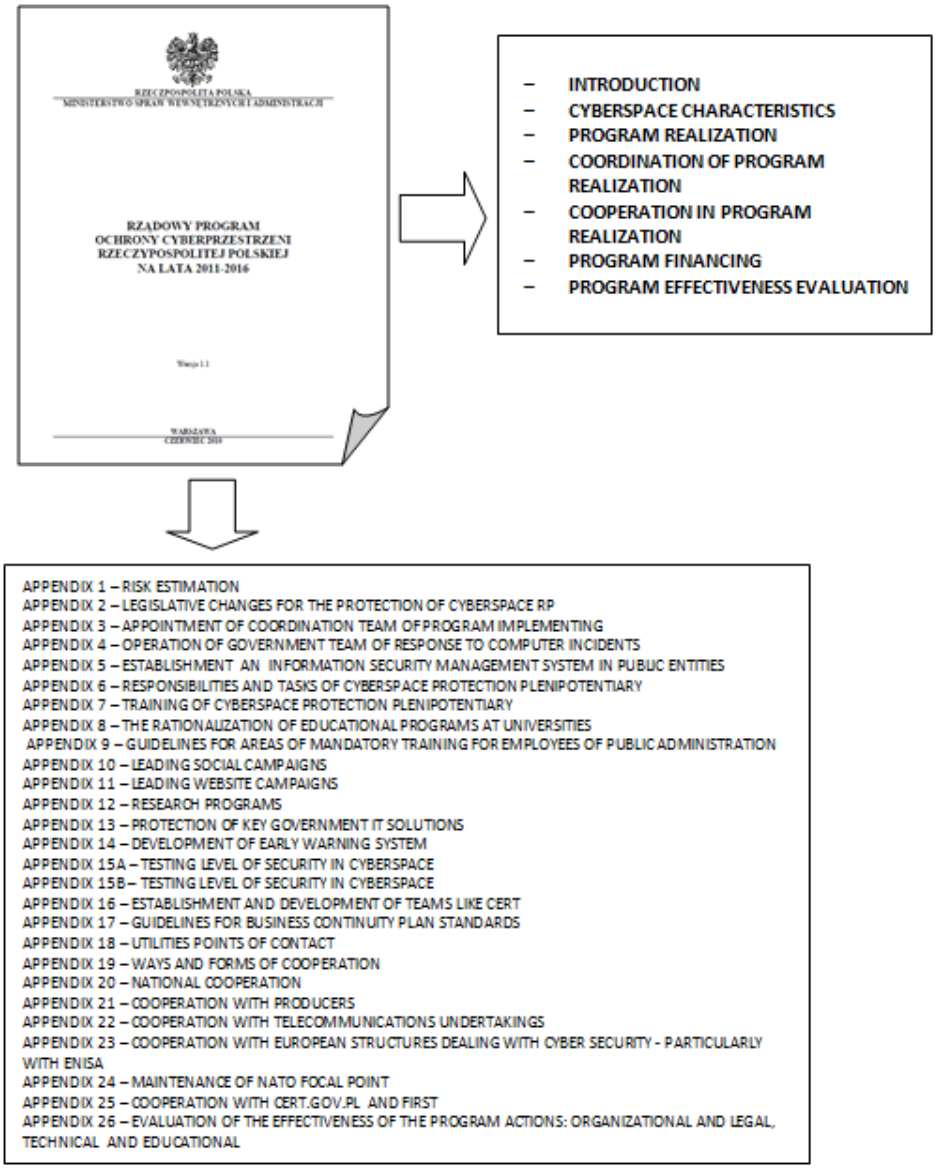

Fig. 13.1 Document layout
Source: own preparation on the basis of the Government's Program for the Protection of Cyberspace in Poland for 2011-2016

Not performing a thorough analysis of the entire document, it is worth noting a few places particularly clearly proving the quality of the elaboration.

- For example, the statement "Moreover, Poland ratified the Convention Council of Europe on Cybercrime on November 23rd 2001"(ibid., p. 11) is incorrect, because Poland has not ratified this convention [39].
- The idea of the establishment of ISMS in all entities implementing public tasks (appendix 5 p.1: "each entity that perform tasks of the public should establish, implement, operate, monitor, review, maintain and improve the information security management systems (ISMS)". In addition, a certified ("Accredited certification organizations - the certification of ISMS and external audits of the re-certification. "[…]" Issue certificates for ISMS, which characters can be an element of promotion entity."Ibid.) is, of course, impossible to realize, not least because of too few auditors of ISO/IEC 27001 and accredited certification units, not to mention the cost of implementation of the ISMS in several thousands of organizations (the communes in Poland are 2479, hospitals – more than a thousand, the number of entities supervised by the Ministry of [30] is 682, the number of public academy – 131, etc.). Just compare this number with the number of the certificate mentioned above (169) to realize a complete lack of realism the creators of this concept. Building a complete, certified ISMS in each commune office would be also completely unnecessary and too costly.
- Implementation of postulates "introduction of the obligation for public entities and recommendations to other users of cyberspace to inform (no longer than within one day from the detection of events by staff) to the appropriate CERT of detected incidents of security related to the cyberspace RP." (appendix 2), "enter the function of cyberspace protection plenipotentiary in organizational unit in the entities of public administration and the recommendation of the creation of such function in the business units;"(ibid.) or "enter the office's investigations of breaches of security in cyberspace, which have taken place in respect of the entities of public administration, critical infrastructure"(ibid.) "it would involve additional costs (several thousand posts plenipotentiaries in communes, counties, voivodeships or ministries, the launching of the Office's investigations on the occasion, for example, the attack of the virus or Internet worm, unless the list of its objectives – often random – was a commune office or the computer in a unit of the military) and also would have a strange obligation to submit reports on incidents entities such as the Orchestra, an outbreak of an artistic or operetta [57], which may be public entities.
- For these and similar ideas, which appeared in the draft of program, for the very positive considered the fact that it is stopped in the departments consultation and nobody has attempted to implement it.

However, the program gives a good idea of the relationship of government administration to the problems of IT security. For an example of the consequences of this state has become the events connected with the countrywide protests against ACTA.

13.4 Acta – case study

Drastic example of the lack of security of government websites were the events connected with the process of signing the agreement ACTA (The Anti-Counterfeiting Trade Agreement). Below is a timeline of the most important events related to the attacks on the servers of the Government that took place on this occasion.

- ***2012-01-21-22*** – Organization Anonymous hacked the website of the President, Prime Minister, Parliament and Ministry of Culture. It had to be a protest against the plans of the signature by the Polish Government controversial act ACTA [12]. On your profile on Twitter Anonymous posted a short message - "TANGO DOWN"- sejm.gov.pl". The English term, derived from the jargon of soldiers, briefly translated as "enemy eliminated". As a result of the attack by hackers did not work, inter alia, the following government addresses: mf.gov.pl, ets.gov.pl, praca.gov.pl, mkidn.gov.pl, stat.gov.pl, mkidn.gov.pl, pip.gov.pl, mzios.gov.pl, arimr.gov.pl, uzp.gov.pl, premier.gov.pl, knf.gov.pl. Also the website of The Internal Security Agency stopped working [10, 18, 19].
- ***2012-01-22*** – the government spokesman Paweł Graś, contradicted reports of attacks by hackers on Government websites claiming that "none of the websites are not affected. It was not intrusion attempts to the servers, change the content of the pages. This phenomenon is due to the enormous interest of the government websites. We had a few million visits." After the comment, the Minister Graś concerning to lock the pages premier.gov.pl and sejm.gov.pl, a moment later, his personal website was also attacked [14, 20].
- ***2012-01-22*** – the break-in to the private laptop Vice Minister of Digitization Igor Ostrowski, a specialist from the digital media, one of the founders of the Digital Center "Project Poland" A hacker hacked into his mail, contacts, and calendar, and as a result of the attack, the Minister did not have access to any files [21, 35].
- ***2012-01-23*** – hackers from Polish Underground group attacked website of Chancellery of the Prime Minister. The server was disabled and secured, and the site www.kprm.gov.pl has been moved to another server [15].
- ***2012-01-23*** – the instance of chief the National Security Bureau Stanisław Koziej, who spoke of considering the introduction of a state of emergency in case of further attacks by hackers [17, 22].
- ***2012-01-23*** – the instance of the Minister of Administration and Digitization, Michał Boni, during which he apologized people for lack of consultation on the ACTA and drew attention to the need to return to that stage [16].
- ***2012-01-23*** – the meeting of Prime Minister Donald Tusk from the Ministers of Administration and Digitization Michał Boni and culture Bogdan Zdrojewski on the topic of international agreement ACTA about the fight against infringements of intellectual property [23].
- ***2012-01-23*** – the part of the Government websites was still not available. Did not operate the sites of the Chancellery of the Prime Minister, the Ministry of Culture and the Ministry of National Defence.

- ***2012-01-23*** – ensure the Minister of National Defence Radoslaw Sikorski that ministry website is well protected "The Ministry constantly monitor the situation to ensure the security of their websites and information systems against attacks by hackers. The MNF has one of modern systems in our administration". Subsequent attacks by hackers provoked by Sikorski were finished with success and web page MNF and private Radoslaw Sikorski stopped working [11, 13, 24].
- ***2012-01-24*** – the clarification on the attacks on government websites. System of ICT security ARAKIS-GOV, which in 2010 was awarded the prize "Teraz Polska", did not protect the government websites because it was developed primarily to react to new threats, meanwhile, attacks on the government website were the simplest DDoS attacks. Also, The Governmental Computer Security Incident Response Team cert.gov.pl. has been appointed by The Internal Security Agency in 2008. Unfortunately, CERT was also the victim of the hackers attacks [26].
- ***2012-01-31*** – chief the National Security Bureau Stanisław Koziej said that currently there is no need to convene the National Security Council on safety on the internet. He also announced that probably will be ready mid-year report on national security, including cyber security [27].
- ***2012-01-31*** – Minister of Administration and Digitization, Michał Boni delivered to departments guidelines for the protection of the information portal of the public administration [28], [7]. These guidelines were adopted following consultation with task team the protections of government portals [6]. "One of the lessons learned in recent times is the lack of opportunities for real-time monitoring of load sites and thus react to the incident. It is necessary to establish permanent contacts with the Governmental Computer Security Incident Response Team CERT.GOV.PL and the obligation to implement the recommendations of the CERT.GOV.PL. The guidelines also contain information about the mandatory entries in the concluded agreements on carrying out of portals and safety procedures when using electronic mail.
- ***2012-02-03*** – at the press conference, Prime Minister Donald Tusk informed of the decision to suspended the process of ratification of ACTA [29].
- ***2012-02-08*** – the information about the attack on the website of the Ministry of Culture and National Heritage [31]. In fact, the failure of the service was due to download by visiting a page located on a single server scanned documents about ACTA in PDF format with a capacity of approximately 25 MB.
- ***2012-02-13*** – CERT.GOV.PL published a report entitled "Extract from the overall analysis of attacks on government sites during the January 21-25, 2012."[60] The report had been published two days earlier, then withdrawn and after minor amendments again restored [8]. The following chart (fig. 13.2) shows the volume of traffic during the attack on the page sejm.gov.pl. In order to implement the following statistics CERT.GOV.PL took into account the amount of visits to pages, not the number of HTTP requests.

- ***2012-03-15*** – the instance of the Director of the Internal Security Agency Kazimierz Mordaszewski at a meeting of the Parliament Commission for Innovation and Technology. By Internal Security Agency particularly dangerous hacking attacks are among others: attacks consisting of illegal obtaining the information e.g. personal data, medical information, insurance information. During the meeting, noted the basic problem with keeping up for the requirements of the regulation of computer security, the existing legal position. There is a need for continuing updates the law as a result of the emerging new forms of network services and the modern computer-related crime [34].

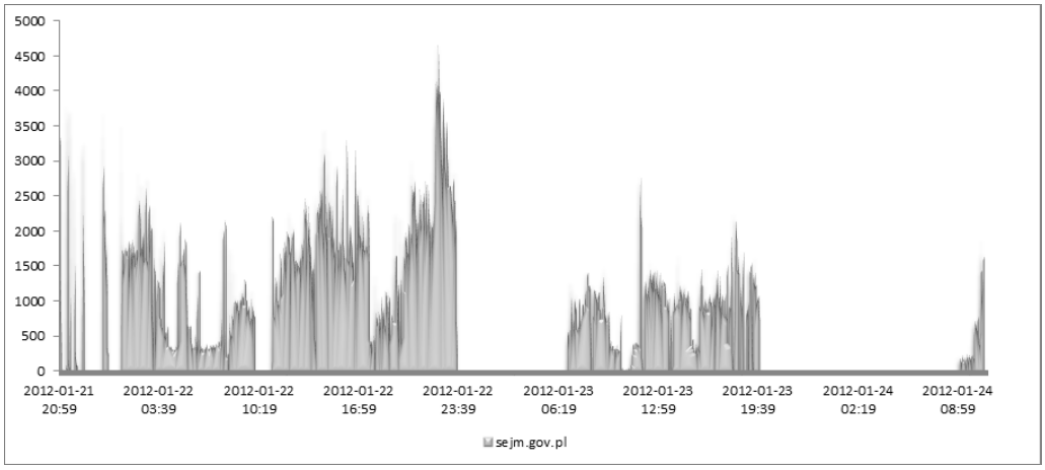

Fig. 13.2 Number of visits per minute to page sejm.gov.pl on January 21-25. 2012
Source: Extract from the overall analysis of attacks on government sites during the January 21-25. 2012

It is worth to notice the extremely unprofessional behavior of the officials of the state administration (public denying the fact of a security incident, the false assurances for the security, public considerations on the introduction of a state of emergency. You should also note that the same entries of the recast of the Act of 29th August 2002 on the state of the war and the competence of the Supreme Commander of the armed forces and the basis for its reporting of the constitutional authorities of the Republic of Poland, which provide, among others, the possibility of introducing martial law "against external threats , caused by the actions of a terrorist or actions in cyberspace" (article. 2.) does not correspond to the nature of the IT threats. Information security is maintenance of its confidentiality, integrity and availability, as well as authenticity, accountability, reliability and undeniability (see the ISO/IEC 27000: 2008-2.19), it is difficult to guess how the introduction of martial law, with its restricted civil liberties, whether the prohibition of gatherings would help maintain availability and accountability of information in "cyberspace".), the ineffectiveness of the applied methods of protection, failing to draw conclusions from the past situation (blocking the site of Ministry of Culture and National Heritage after the publication of the text of the ACTA agreement).

Unfortunately, further actions (including guidelines the Ministry of Administration and Digitization) does not lead to believe that the situation has changed for the better. In particular:

- Guidelines of the Ministry formed extremely fast, so as you might expect to run out of time on the professional identification and assessment of risks and the rational choice of proceeding with it;
- With unknown reasons, on the first position in the list of preventive measures was the systems of elimination of anonymous traffic (although the analysis report, CERT is not due to the attacks were carried out via the anonymity programs [9]);
- The guidelines recommend the introduction of (but does not specify where) filtering capabilities to specific packet types or protocols, which is in itself a legitimate but is an elementary function of any firewall including firewalls built into the operating systems in computers or routers. This recommendation is therefore de facto recommendation for implementation of something which was introduced;
- A large part of the recommendations is common sense (using a difficult-to-guess passwords (although after disclosure by the hackers that the user name and password of an administrator on the page premier.gov.pl were, respectively, the "admin" and "admin1" you can understand the rationale for inclusion of such recommendations in the Ministerial document [33]), or the anti-spam software;
- Flip the responsibility (therefore - using concepts from ISO/IEC 27005 - risk transfer) to the link suppliers or a hosting companies. This is a strange recommendation, the method of dealing with risks should be selected in process of management, after assessing its potential effects and safeguards costs, and not by apriori way of the recommendations of an expert external. Nota bene the introduction of minimum guaranteed bandwidth (Committed Information Rate, CIR) is not quite related to resistance to ddos attacks. In this case, more important is the high value of the actual bandwidth, or the scattering of resources, for example through solutions for Content Delivery Network (unless the attack ddos is consist of the clogged links) or the design of the site and the distribution of loads (load balancing) servers (unless the attack ddos consists of depletion of server resources);
- Astonishing recommendation of establishing permanent contacts with the government team CERT. Although this is, of course, the right idea, the regulations of the relations between the organs of government administration should be carried out in accordance with the relevant provisions of administrative law governing the rules of its actions (in particular, the principle of action of the Council of Ministers) and be mandatory and not take the form of appeal placed among the good advice on the use of difficult-to-guess passwords whether not-opening attachments to suspicious e-mail letters.

13.5 Conclusions

Informatization of the state administration in Poland is in a terrible condition [5]. In the report of the UNITED NATIONS in 2012 Poland took 47th place (behind the countries such as Kazakhstan and Croatia), while in 2010 - 45th place, and in 2008 – 33. It is therefore not a surprise that the management of security of information systems, which is one of the difficult aspects of the IT techniques, it also leaves much to be desired. A bad symptom, which is visible to the naked eye, is the offices indolence and even failure to coordinate the work

of the state administration, which not allows the achievement of a reasonable level of security, despite the recruitment by the relevant services and authorities sometimes high class professionals, use the appropriate hardware or software. You may fear that further spectacular a tacks on government sites are just a matter of time.

REFERENCES

[1] Anderson R., Inżynieria zabezpieczeń, WNT, Warszawa 2005.
[2] Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowo Techniczne, Warszawa 2006.
[3] British Standards Institution (BSI), BS 25999, Business Continuity Management (BCM)
[4] European Police Science and Research Bulletin, http://cepol.europa. eu/index.php ?id=science-research-bulletin.
[5] http://biznes.onet.pl/polska-e-administracja-nie-nadaza-za-swiatem,18554,5048220,1,prasa-detal, 2012.04.14
[6] http://cert.gov.pl/portal/cer/9/514/Wytyczne_w_zakresie_ochrony_portali_informacyjnych _ administracji_publicznej_wpro.html [2012-04-14],
[7] http://m.onet.pl/wiadomosci/5013538,detal.html, 2012-04-14.
[8] http://niebezpiecznik.pl/post/analiza-atakow-ddos-na-gov-pl/, 2012-04-14.
[9] http://niebezpiecznik.pl/post/analiza-atakow-ddos-na-gov-pl/, 2012-04-14.
[10] http://nt.interia.pl/internet/bezpieczenstwo/news/atak-hakerow-na-polskie-strony-rzadowe,1749608,1276, 2012-04-14.
[11] http://polska.newsweek.pl/acta-na-stronie-sikorskiego---f-acta-,87622,1,1.html, 2012-04-14.
[12] http://technologie.gazeta.pl/internet/1,104530,11010982,Tango_Down__trwa_akcja_ hakerow _ wymierzona_w_strony.html, 2012-04-14.
[13] http://wiadomosci.gazeta.pl/wiadomosci/1,114883,11020346,Sikorski___Kolejny_atak_ hakerow_zostal _odparty___Po.html, 2012-04-14.
[14] http://wiadomosci.gazeta.pl/wiadomosci/1,114884,11011548,Gras_o_zablokowaniu_ stron_sejmu_i_ premiera___Trudno.html, 2012-04-14.
[15] http://wiadomosci.gazeta.pl/wiadomosci/1,114884,11014860,Atak_hakerow_Polish_ Underground___ Baska__na_stronie.html, 2012-04-14.
[16] http://wiadomosci.gazeta.pl/wiadomosci/1,114884,11014962,ACTA__Boni_przeprasza _za_afere___ Jest_poczucie__ze.html, 2012-04-14.
[17] http://wiadomosci.gazeta.pl/wiadomosci/1,114884,11015090,Koziej__Stan_wyjatkowy __jesli_ataki_ hakerow_trwale.html, 2012-04-14.
[18] http://wiadomosci.onet.pl/acta,5004951,temat.htm, 2012-04-14.
[19] http://wiadomosci.onet.pl/acta,5004997,temat.html, 2012-04-14.
[20] http://wiadomosci.onet.pl/acta,5005017,temat.html, 2012-04-14.
[21] http://wiadomosci.onet.pl/acta,5005449,temat.html, 2012-04-14.
[22] http://wiadomosci.onet.pl/acta,5005497,temat.html, 2012-04-14.
[23] http://wiadomosci.onet.pl/acta,5005985,temat.html, 2012-04-14.
[24] http://wiadomosci.onet.pl/acta,5006286,temat.html, 2012-04-14.

[25] http://wiadomosci.onet.pl/acta,5006286,temat.html, 2012-04-14.
[26] http://wiadomosci.onet.pl/acta,5006946,temat.html, 2012-04-14.
[27] http://wiadomosci.onet.pl/acta,5012696,temat.html, 2012-04-14.
[28] http://wiadomosci.onet.pl/acta,5013538,temat.html, 2012-04-14.
[29] http://wiadomosci.onet.pl/acta,5017181,temat.html, 2012-04-14.
[30] http://www.administracja.wortale.net/22-Struktura-administracji-.html, 2012-04-14.
[31] http://www.gazetaprawna.pl/wiadomosci/artykuly/592142,strona_internetowa_ ministerstwa_kultury_ ponownie_zablokowana_przez_hakerow_od_acta.html, 2012-04-14.
[32] http://www.iso27000.pl/sites/view/stat=2=1, 2012-04-14.
[33] http://www.rmf24.pl/fakty/polska/news-login-admin-haslo-admin1-specjalisci-skandal-smiesznosc ,nId,430669, 2012-04-14.
[34] http://www.sejm.gov.pl/sejm7.nsf/biuletyn.xsp?documentId= 177F65CE5C2FA 827 C12579C F003BC990, 2012-04-14.
[35] http://wyborcza.pl/1,75478,11014989,Wlamanie_do_laptopa_wiceministra_ Ostrowskiego__Kim.html, 2012-04-14.
[36] IDC Whitepaper: The Diverse and Exploding Digital Universe. An Updated Forecast of Worldwide Information Growth Through 2011, www.ifap.ru/library/book268.pdf, 2012-04-14.
[37] ISO 31000:2009 Risk management -- Principles and guidelines,
[38] ISO/IEC 27000:2009 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary,
[39] Konwencja Budapesztańska – Konwencja Rady Europy o cyberprzestępczości, podpisana w Budapeszcie dnia 23 listopada 2001 r., http://conventions. coe.int/ Treaty/en/Treaties/Html/185.htm, 2012-04-14.
[40] Korzeniowski L. F., Informačna bezpečnost podnikania, Tlač_MULTIPRINT Košice, Žilina 2010.
[41] Korzeniowski L. F., Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych, EAS, Kraków 2008.
[42] Liderman K., O pomiarach bezpieczeństwa teleinformatycznego, [w:] Diagnostyka 42/006, ISSN: 641-6414, s. 113-118.
[43] Lisiak-Felicka D., Szmit M.: Czy istnieje technologia informacyjna? [w:] Multimedia w biznesie i zarządzaniu, pod red L. Kiełtyki, Difin, Warszawa 2009, s. 95-104.
[44] Lyman P., Varian H. R., Dunn J., Strygin A., Swearingen K.: How Much Information 2000? University of Berkeley Raport, 2000, http://www2 .sims.berkeley. edu/research/projects/how-much-info/ [2012-04-14].
[45] Lyman P., Varian, H.: How Much Information? http://info.berkley.edu/how-much-info, 2012-04-14.
[46] Ministerstwo Spraw Wewnętrznych i Administracji, Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, http://bip.msw. gov.pl/portal/bip/6/19057, 2011-12-28.
[47] OHSAS 18001:1999 Occupational health and safety management systems – Specification,

[48] Pihowicz W., Inżynieria bezpieczeństwa technicznego. Problematyka podstawowa, WNT, Warszawa 2008.
[49] PN-N-18001:2004 Systemy zarządzania bezpieczeństwem i higieną pracy – Wymagania.
[50] Shirey R., Internet Security Glossary, The Internet Society, 2000, http://www.rfc-editor.org/rfc/rfc2828.txt, 2012-04-14.
[51] Stokłosa J., Bilski T., Pankowski T., Bezpieczeństwo danych w systemach informatycznych, PWN, Warszawa – Poznań 2001.
[52] Swearingen K. (ed.), How Much Information 2003? University of Berkeley Raport, 2003. http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/, 2012-04-14.
[53] Szafrański B. i in., Interoperacyjność i bezpieczeństwo systemów informatycznych administracji publicznej, PTI, Katowice 2006.
[54] Szmit M. (red.), Baworowski A., Kmieciak A., Krejza P., Niemiec A.: Elementy Informatyki Sądowej, Polskie Towarzystwo Informatyczne 2011; ISBN: 978-83-60810-43–9 (książka); ISBN: 978-83-60810-44-6 (e-book).
[55] Szmit M., Politowska I., O artykule 267 Kodeksu Karnego oczami biegłego, [w:] Prawo Mediów Elektronicznych, dodatek do Monitora prawniczego nr 8 /2008 s. 34-40.
[56] Szmit M., Kilka uwag, nie tylko o dokumentach elektronicznych, [w:] Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały VII Kongresu, KSOIN, Katowice 2011, s. 193-200.
[57] Ustawa z dnia 19 grudnia 2009 roku o partnerstwie publiczno - prywatnym (Dz. U. 2009, Nr 19, Poz. 100).
[58] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. 2011 nr 222 poz. 1323, data wejścia w życie: 2 listopada 2011 r.).
[59] Ustawa z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz. U. 2008 nr 171 poz. 1056).
[60] Wyciąg z ogólnej analizy ataków na witryny administracji państwowej RP w okresie 21-25 stycznia 2012r.
[61] http://www.cert.gov.pl/portal/cer/9/518/Wyciagzogolnejanalizyatakow_na_witryny_ administracji_ panstwowej_RP_wokresie21__2.html, 2012-04-14.