INFO-84
Primljeno/Received: 2014-12-04
UDK: 004.521.39:004.7:001
Authors Review/ Pregledni rad

VULNERABILITIES OF NEW TECHNOLOGIES AND THE PROTECTION OF CNI

Krunoslav Antoliš [1], Petar Mišević [2], Ana Miličević

Ministry of the Interior of the Republic of Croatia, Police Academy, Police College, Zagreb, Croatia [1]; Zagreb School of Economics and Management[2], Zagreb, Croatia

Abstract

New information technologies are unavoidable factor in modern world as they are changing it both in technological and in communication aspect. Unfortunately, despite the opening of new possibilities, both aspects of changes have brought about vulnerabilities which cannot be ignored. These vulnerabilities directly affect security state in the systems where ICT is becoming dominant information and communication platform. Therefore, critical infrastructure security as the key element of national security today is to a great extent determined by ICT security as its component. Thus, ICT vulnerabilities are directly spread to critical infrastructure in which they are built and whose abuse is only a matter of time. It is not only terrorists who should be regarded as a threat when thinking about critical infrastructure security, but also organized and commercial crime, competitive companies, various hackers, even all those who due to different social and economic reason live on the margins of modern society. Of course, nobody among the mentioned is immune to committing a terrorist act so as preventive measure all of them should be spotted and prevented in accordance with security estimates.

Keywords

Information and communication technology, vulnerability, safety, security, critical infrastructure

1 Introduction[1]

Intensive development of information and communication technology (ICT) in the past few decades has greatly changed the way we used to communicate, do business or manage companies but it has also substantially changed our lifestyle. Innovations, flexibility, dynamics and high productivity rate are only some of the benefits that modern IT application has brought to modern companies. What small or big proprietary or public companies have in common is that they base their business processes on information systems. Development of wireless communication networks was a further step forward in creating an independent and flexible communication system. However, from the CNI aspect, besides numerous advantages and new possibilities, innovation in communication and information technology has faced us with new security challenges. Since all ICT vulnerabilities directly affect CNI, security of the critical national infrastructure is greatly dependent on skillful IT risk assessment as well as a quick and systematic reaction to newly detected ICT vulnerabilities.

This paper gives a short review of some of ICT vulnerabilities, their impact on CNI and possible responses to the existing security challenges at the national and international level.

[1] *All statements made in this article are solely those of the authors and in no way reflects the official positions or policies of the Republic of Croatia, Croat's Parliament, Croat's Government or Ministry of interior.*

2 CNI and the Internet

In order to better understand a Croatian CNI and all of its segments we will use its legal based definition. National Strategy for the Prevention and Suppression of Terrorism is the first strategic document in the Republic of Croatia (RH) which defines and emphasizes the importance of critical infrastructure at national and regional level. CNI of the Republic of Croatia, according to the Strategy, makes as follows: "assets, services and systems (traffic, energetics, communication, industrial, financial and administrative) which sustain economic, political and social life in the Republic of Croatia and whose importance is so vital that their whole or partial loss or threats to them can cause great loss of human lives and have serious impact on national security and economy or other serious consequences for the community as a whole or to any part of the community". /**1**/

- energetics (production, transmission, storage, transport of energy-generating products and energy, distribution systems),
- communication and information technology (electronic communications, data transmission, information systems, providing audio and audio-visual media services),
- traffic (road, rail, air, sea, inland waterways),
- health (health care, drug production, distribution and supervision),
- water management (regulatory and protective water structures and municipal water structures),
- food (food manufacturing and supply and food safety system and commodity stocks),
- finances (banking, stock exchange, investments, insurance and payment systems)
- manufacturing, storage and transport of dangerous goods (chemical, biological, radiological and nuclear materials),
- public services (ensuring public order and peace, civil protection and rescue, emergency medicine),
- national monuments and values. /**2**/

Although ICT is pointed out as a separate item in the above mentioned threat assessments to CNI of the Republic of Croatia, it is inevitable component of all other services, systems and assets since they all use the same IC technology as a basic information and communication platform. Therefore, this technology should be considered within a broader context since the abuse of ICT vulnerability can have far-reaching consequences for national security and economy of the country. Along with a number of advantages and possibilities that the ICT development and application is opening, the questions is how reliable and safe the system is with so many devices interconnected to one or several networks with high flow of information, often classified and hidden from the public. The question is hard to answer. None information system is so perfectly designed to be entirely safe. If we add to this the possibility of accidental and intentional failures and probability of human error and likely abuse, then such systems require a complex process of security risk assessment and protection. That is why it is exceptionally important to identify all defects of information and communication technology on which particular CNI is based, starting from wireless communication systems.

The Internet as publicly available, global information-communication system is today rightfully included in the category of goods with double purpose. /**3**/ Invention and application of this technology has made our life more comfortable but it has also exposed its users to new and terrifying threats. Terrorist groups such as Al-Qa'ida recognized numerous advantages of the technology: its decentralized infrastructure, simple access and anonymity, global impact on making public opinion, cheap maintenances, possibility of development of various web applications, possibility of multimedia and its superiority over other traditional media, so they skillfully used them in spreading their ideology, intimidating the public and recruiting new members./**4**/, /**5**/ Due to the above mentioned properties the Internet has become frequent tool for carrying out terrorist attacks, organized and economic crime, hacking and other criminal acts which, if considered in relation to CNI, are getting quite new dimension with much more severe consequences. One of more frequent abuse of modern technology along with skillful exploitation of numerous vulnerabilities of the Internet is identity theft which caused damage to both individual and legal persons and can be calculated in millions of the US dollars. Social networks and a number of personal information on their users' profiles have made the job of the perpetrators of these criminal acts enormously easier along with their competencies in using software and hardware tools for abusing the ICT vulnerability. /**6**/

Skype is one of the examples of frequent attacks on user's privacy through which the email address and user's profile are easily accessible. Besides, Microsoft, Hotmail and Outlook user accounts have drawbacks in authentification procedure of the email service enabling the thieves to collect users' data via cookies of the web browser. Furthermore, it is interesting that the whole procedure of the privacy attack via memory stick takes only 30 seconds at most. /**7**/ Examples of stealing money from credit and debit cards, breaking into bank accounts or interception of users' data are numerous. Recently, identity theft has been closely connected with intellectual capital of successful companies. Since the intellectual capital is the biggest value of a company which in synergy with ITC provides its clients with products and services and makes profit, this very capital is becoming more often the target of identity thieves. The reason for this is that the value of intellectual capital which stands beyond any material value. /**8**/

All the above mentioned and many other ICT vulnerabilities built in the structure of information-communication systems of critical infrastructure represent the key element of national security. Apart from financial, health, traffic and other CNI sectors mentioned at the beginning of the paper, safe and reliable information-communication platform is the main goal of the intelligence service community of all countries. The countries which are not capable of developing the intelligence service systems of their own are in unenviable position. In that case, it is necessary to take many preventive measures and meet very high security standard levels. Many intentional software tool vulnerabilities such as "Zero days" and data encryptions like the "backdoor" encryption tools, can inflict irreparable damage to any CNI segment. /**9**/ The former case is about newly discovered intentional errors in software enabling perpetrators to penetrate into information system while the time of error detection and correction/debugging takes less than 24 hours. In the case of "backdoor" encryption tools, whose creators enable data decryption on the "back door", without the user's knowledge. None of the information-communication systems is immune to such vulnerabilities. That is why prevention and fighting against ICT abuse at national and international level is very important factor in security level analysis of information and communication systems and wireless communications as a great part of these systems.

3 Evolution of wireless communication vulnerabilities

Security threats to internal communication systems of a particular CNI based on wireless transmission are still a great unknown. All vulnerabilities of wireless communication systems such as GSM, GPRS, UMTS or LTE in that case will directly affect the security of a part or even of the whole system of a particular CNI. /**10**/ If we view the GSM network in this way, we should take into account the GSM network security drawbacks such as one-sided authentication, errors in A3 and A8 algorithm implementation, and weaknesses in user's anonymity, deficiencies of cryptographic algorithms, limited encryption area and in protection of message integrity. /**11**/ GPRS system, unlike GSM enables the Internet access with the WAP protocol which imposed new requirements to the GPRS system. The required security level within GPRS network is achieved by WTLS protocol within WAP. UMTS, better known as 3G mobile technology system, represents the third stage in mobile technology development eliminating security deficiencies of the two previous generations but opening the way to new forms of threats. The fourth wireless network generation or LTE is essentially different from previous generations since its entire functionality is based on TCP/IP protocol. In this manner a greater interoperability and compatibility between wired and wireless networks is achieved but on the account of security. /**12**/ Vulnerabilities of this system are related to the characteristics of radio interface. Some of the threats which can endanger security system of LTE technology are the following: unauthorized approach to network, attacks on the eNB network component, attacks on the core network including attacks on the locations of the eNB network components, threats related to DoS and DdoS attacks. /**13**/

When talking about wireless network security within the CNI context, we cannot omit Wireless local area networks (WLAN). Despite numerous security disadvantages of such networks, their popularity is permanently increasing. In 2010, 50% of the Internet ADSL users in Croatia opted for WLAN. Researches have proved that a very small percentage of users (about 10%) have security protection of the highest degree (WPA2), while most users have WEP and WPA protection (about 80%). /**14**/ Disapproving fact is that less than 10% WLAN users have no protection at all. The Internet security experts does not recommend using of WEP security standard due to frequent abuse of this standard. WPA and WPA2 use randomly selected encryption key and provide better network protection. By using all above mentioned security standards it is necessary to apply concrete measures at the technical level, by selecting the appropriate security software, setting the highest security level in the operating system properties and applications, and setting their automatic update.

The awareness of the importance of such network protection is not at very high level, which makes abuser's job much easier to do. Besides, in this manner it is extremely hard to discover and follow digital traces of perpetrators. Although it is impossible to achieve absolute security, it is necessary to install adequate protection to disable frequent abuse of such networks. It is possible to provide by applying security standards which enable device authentication, user authentication and mutual strong encryption keys (TKIP or AES).

4 CNI and ICT abuse

Although the term of national critical infrastructure was first defined in the Republic of Croatia in the National Strategy for the Prevention and Suppression of Terrorism (NN 139/2008), legislation referring to critical infrastructure came into force only after accepting the EU acquis communataire into the laws and regulations of the Republic of Croatia by defining the law on critical infrastructures (NN/ 56/2013). So, the Republic of Croatia was required to create national security policy in this field. The law, accordingly, has defined national critical infrastructures and their sectors giving initial directions for managing security and security risks of these systems. Based on the definition of CNI and all related sectors mentioned in the previous chapters, we can see all complexity in the application of this law in all domains of critical national infrastructure. Added the necessity of transparency and applicability of the law in all domains of critical national infrastructure which can be state-owned or owned by local and regional self-government and private companies or societies, then the need for multidisciplinary approach to risk assessment prior to defining particular protective measures for critical infrastructure is quite clear. Creating security policy for prevention and fighting against the ICT abuse within the critical national infrastructure represents a particular challenge, not only for the Republic of Croatia but also for the countries with a long tradition in fighting against cybercrime. The EU legislation framework which enable us to do it this is The Convention on Cyber Crime of the Council of Europe and Additional Protocol which were signed and ratified by the Republic of Croatia. The first reason is that this technology has manifold application since the ICT today makes a basic information-communication platform of all companies including pharmaceutical industry, banking transactions or air traffic managing.

The second reason is intensive development of this technology which requires a "real time" following and recognizing security risks at all levels of information systems. That is why it is very important to have multidimensional approach to the ICT security issue which demands meeting specific security requirements at all segments of information-communication infrastructure: technical equipment, software support, electronic communication networks, data transmission within the same or different communication networks and data storage. In that case, law can define the areas under special protection as well as bodies to perform, monitor and give instructions in executing security measures and achieving standards. But, concrete measures that should be executed on living systems is possible to define after a detailed and systematic analysis and risk assessment of all ICT segments of the concrete CNI. Since CNI is both in public and private ownership, there are divergent approaches to security policy regulated by the state and internal security procedures of private companies. Mutual cooperation of public and private owners of the CNI in the ICT security protection domain might open new possibilities in the development of economy where innovations and knowledge of young scientists and experts would find their place in solving concrete security issues being of high importance for the state security. In this manner industry and private companies in the Republic of Croatia would ask for professional assistance of young scientists from the Program of Croatian Innovation and Technology Development (HITRA), National CERT with very important support of intelligence system, namely, the Office of the National Security Council (UVNS) and the Department of the Information System Security (ZSIS) as the central bodies of the Republic of Croatia for security issues. By giving expertise, efficient assessment of security threats and international cooperation in the cyber security domain, the mentioned bodies are authorized to take concrete measures for ICT protection in a particular CNI domain. These measures and legally prescribed solutions are applicable not only to the Republic of Croatia but of all the former socialist countries (in South-East Europe and beyond). The measures would be directly and continuously taken maintaining security risks at a satisfactory level in all segments of the IT systems in accordance with technology development. The emphasize would be on the security of all segments of the information system because it is not only important to be on the alert and respond quickly to the threat, it is also important for all technical equipment and software support to be tested, reliable and safe before they are applied within the CNI information and technology platform. However, despite all protective measures taken, threats are always present and most of them come through the use of the Internet. Therefore, the strength of encryption algorithms on which the safe transmission data is dependent is very important as well as setting up monitoring and control over the use of the Internet. Motivated by current issues and more frequent abuse of the ICT vulnerability, in 2011, the USA passed an important international strategic document called International Strategy for Cyberspace: Prosperity, security and Openness in a Networked World“. The main goal of this document is international cooperation and support to the open and interoperable, safe and reliable information and communication infrastructure which endorse international trade, business and reinforce security of information space, encourage freedom of speech and innovation. The way to achieve this goal is defined as a combination of diplomacy, defense and development which tend to strengthen prosperity, security and openness of network technology. /**15**/ On the list of priority activities to be taken, apart from protection of the economy, computer networks in the USA, strengthening the rule of law, technology development and free Internet, multi-shareholder managing the Internet was pointed out as a significant strategic step. This manner of managing the Internet would enable further sustainable development of interoperable, safe and easily available global network to everyone. One of the approaches to this type of property includes a possibility of participation of industrial sector, academic institutions, technical experts and civil society representatives in managing the Internet. This would secure the openness if the Internet interoperability provided by equal and safe technical standards and possibility of undisturbed further development of safer use. In the 2013 annual report named Liberty and Security in a Changing World, the USA one again clearly pointed out its view which supports multi-stakeholder property, but is strongly opposed to the Internet localization: "As part of the overall discussion of US policy concerning communications technology, we believe that the US Government should reaffirm that Internet governance must not be limited to governments, but should include all appropriate stakeholders. Inclusion of such stakeholders—including civil society, industry, and technical experts—is important to ensure that the process benefits from a wide range of information and to reduce the risk of bias or partiality.“ /**16**/

The idea of localization was initiated by several countries which demanded local storage of email and other ways of the Internet communication as well as disabling data transmission across the state borders. Russia, together with a group of countries hold that the Internet as a multi-shareholder organization should be under protection of the UN and the International Telecommunication Union (ITU).

In the second half of 2013, the EU Parliament voted for demands for limiting international data transmission which tend to localize the Internet. /**17**/ This manner of establishing the Internet ownership would enable the state authorities to control the Internet traffic within a state which would certainly decrease cybercrime rate and numerous ICT abuse and increase the ICT safety level. Yet, despite the concepts of localization and limiting the Internet, more frequent use of cloud-computing option, the development of network technology leads to the opposite directions. Independence on physical machines, possibility of the access to the required networks, applications and services offered at any time and place, would move the model of modern business from office-based computer to the clouds. This model of the Internet development of fast communication and weak clients is contrary to the concept of the Internet localization and limiting the data transfer. The question is if it is possible to oppose the fierce waves of virtualization at all? Obviously, entire development of the Internet and network technologies tend to develop a higher degree of independence and flexibility. Limiting the existing or further development along with creating new security standards is the next decision in fighting security challenges which ICT development is bringing. The fact that development of virtual technology has the tendency of permanent and intensive growth, the application of this technology to CNI is a matter of time. In that case security risk assessment and entire information security will focus their attention to commination protection towards and inside the cloud. Apart from the above mentioned, it is clear that protection of the entire critical national infrastructure is possible to provide only by a creating high quality and professionally implemented security measures starting from the lowest level of information system of a particular CNI to the cooperation and fighting against all ICT abuse at the international level, regardless of servers, whether local or cloud server in the world.

5 Conclusion

Critical national infrastructure represents the key segment of national security and it is recognized as strategic target of terrorist organizations and intelligence agencies whose countries support terrorism. Intensive development of ICT introduced numerous benefits within the CNI system, but also opened the door to a number new ways of threats to national security. Therefore, CNI protection is a complex and continuous process implying preventive measures and fighting against the ICT abuse at national and international level. Precisely defined legislation frameworks, concrete and targeted strategy of national security as well as professional and competent human resources are the main weapons in fighting against information and communication threats at national level. Since cybercrime and everything that comes out of it do not know national borders, international cooperation has become the key factor for prevention and fighting against the ICT vulnerability and abuse and definition of high security standards for CNI protection.

Notes

/1/ Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies Liberty and security in a changing world, SAD 2013.

/2/ Joshua Sinai, Hsinchun Chen, Edna Reid, Andrew Silke, Boaz Ganor: Terrorism Informatics: Knowledge Management and Data Mining for Homeland: http://www.google.hr/books?hl=hr&lr=&id=feoqhcd8bnkC&oi=fnd&pg=PR15&dq=maclean,+b.+(2007).+terrorism+and+internet+use&ots=PtaEEQma-Ma&sig=TX5KBW2tw1727tf7qAtJopr4D8g&redir_esc=y#v=onepage&q&f=false , 2008.

/3/ Antoliš, K. Ideological prerequisites in Combating Terrorism. CT WG conference, PfP Consortium, Oberamergau, Germany, 2004.

/4/ Ibid.

/5/ International strategy for Cyberspace: Prosperity, Security and Openness in a Networked World, SAD, 2011.

/6/ The Convention on Cybercrime (NN, International Agreements No.: 4/2002), 2002.

/7/ Ibid.

/8/ Antoliš, K. ICT and Identity theft, Informatologija, 46, 2013., 4, 353-360, UDK:681.3:340:001, Authors Review/Pregledni rad, ISSN [5] Antoliš, K. Intellectual capital and critical national infrastructure, pg. 7-15. CIP: 853091, ISBN 978-953-161-276-0, Zagreb, Croatia, 2013.

/9/ Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies Liberty and security in a changing world, SAD 2013.

/10/ National Strategy for Prevention and suppression of terrorism (NN 139/2008), Croatia, 2008.

/11/ Bilogrevic, I.; Jadliwala, M.; Hubaux, J.P. (2010.) Security Issues in Next Generation Mobile Networks: LTE and Femtocells: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.167.223&rep=rep1&type=pdf

/12/ Filković Dujmović, K. Graduate-thesis: Safety of mobile communication, Polytechnic of Zagreb, Zagreb, 2012.

/13/ Bikos, Anastasios N.; Sklavos, N. LTE SAE security issues on 4G wireless networks, 2013.

/14/ National Strategy for Prevention and suppression of terrorism (NN 139/2008), Croatia, 2008.

/15/ Antoliš, K. Cyber threats to critical national infrastructure, Corporate security in dynamic global environment – challenges and risks, str 61.-73., ISBN 978-961-92860-3-6, march, Ljubljana, 2012.

/16/ Antoliš, K. Risk assessment of terrorist abuse of ICT in the CNI, Proceedings of the International conference on "The War on Terror after 10 Years, Zagreb, 2012.

/17/ Ibid.

RANJIVOSTI NOVIH TEHNOLOGIJA I ZAŠTITA KRITIČNE NACIONALNE INFRASTRUKTURE

Krunoslav Antoliš [1], *Petar Mišević* [2], *Ana Miličević*

Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska akademija, Zagreb, Hrvatska [1]; *Zagrebačka škola ekonomije i menadžmenta, Zagreb, Hrvatska*[2]

Sažetak

Nove informacijske tehnologije nezaobilazan čimbenik u modernom svijetu koji se mijenja u svom tehnološkom ali i komunikologijskom aspektu. Nažalost, unatoč otvaranju novih mogućnosti, oba aspekta promjena dovela su i do novih ranjivosti, koje se ne može zanemariti u smislu sigurnosnih rizika. Ove ranjivosti izravno utječu na stanje sigurnosti u sustavima u kojima ICT postaje dominantna informacijsko komunikacijska platforma. Tako je sa stajališta nacionalne sigurnosti ključni element sigurnost kritične infrastrukture, a koja je u velikoj mjeri određena sigurnošću ICT kao njezine važne sastavnice. Dakle, ICT ranjivost izravno utječe na ranjivost kritične infrastrukture u koju je ugrađena i čija je zlouporaba samo pitanje vremena. Danas prijetnje nisu samo terorističke naravi već su to i organizirani i gospodarski kriminal, konkurentne tvrtke, razni hakeri, čak i one fizičke osobe koje zbog neprimjerenih socijalnih i ekonomskih razloga žive na marginama suvremenog društva. Naravno, nitko među spomenutima nije imun na počinjenje terorističkog akta, tako da ih sve preventivno treba uočiti i spriječiti u njegovu počinjenju sukladno sigurnosnim procjenama u danom trenutku.

Ključne riječi

Informacijska i komunikacijska tehnologija, ranjivost, zaštita, sigurnost, kritična infrastruktura