PRZEGLĄD ZACHODNI
2015, nr 3

MIRON LAKOMY
Katowice

THE PARADOX OF CYBER DEVELOPMENT TWICE THE TECH, DOUBLE THE FALL?

Several decades ago cybersecurity problems were usually treated by political scientists as a curiosity, mostly a vision of the future, based less on facts and reality, and more on cyberpunk science fiction novels and stories, such as William Gibson's *Neuromancer* or Vernor Vinge's *True Names*[1]. In the 1960s and 1970s most mainstream international security specialists usually neglected the scope of challenges emanating from the digital revolution[2]. Such attitudes had an obvious influence on policymakers, who were rather uninterested in the detrimental potential of computer networks in the field of national and international security during the Cold War[3]. Instead they focused mostly on the political, economic, social and scientific benefits of the emergence of information and communication technologies (ICT).

The global view began to change at the end of the 20th century, when it became apparent that the Internet and computers could be used for a range of malicious activities, which initially were not foreseen by their creators. It was proved by, among others, the Morris worm in 1988. In just a few years, multiple cyber incidents made cybersecurity

[1] W. Gibson, *Neuromancer*, New York 1984; V. Vinge, *True Names: And the Opening of the Cyberspace Frontier*, New York 2001 .

[2] Digital or information revolution can be understood as a profound change of the methods of collection, storage, transmission, analysis and presentation of data with the use of information technologies, such as computers or their networks. For example, Nicolas Negroponte described this phenomenon as a shift from transport of atoms to the transport of bits. See M. Deegan, K. Sutherland, *Transferred Illusions. Digital Technology and the Forms of Print*, Farnham 2009, pp. 19; P.F. Drucker, *The Next Information Revolution*, "Forbes", 24.08.1998.

[3] There were, however, some outstanding exceptions. One of the most prominent politicians who understood the significance of cybersecurity in the mid-1980s was Ronald Reagan. In *National Security Decision Directive Number 145* he stressed that "As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat". See R. Reagan, *National Policy on Telecommunications and Automated Information Systems Security*, National Security Decision Directive Number 145, White House, 17.09.1984.

one of the key subjects of international debate[4]. According to global public opinion the real computer security "boom" arrived a bit later, after 2007, due to a series of grievous cyber-attacks in Estonia, Georgia, Kyrgyzstan and South Korea[5]. As a result, Erik Gartzke stressed that, nowadays, "a blitz of media, punditry, and official pronouncements raises the specter of war on the internet"[6]. At present these issues are frequently addressed by the academic community which is attempting to create a widely accepted theoretical framework for the new phenomena appearing in cyberspace[7]. Usually such attempts fail, as there is no agreement between scholars even in the simplest of cases, e.g. definitions of various cyber threats like cyberterrorism or cybercrime. The profound rupture between scientists is, however, best seen when it comes to discussions over the controversial notion of cyberwar[8]. There are three major causes of this situation. To begin with, research on cybersecurity is conducted from various scientific perspectives (political, military, computer science etc.). It requires the use of diverse methodologies, which focus largely on different, yet interconnected problems. Secondly, discussion over these issues is frequently hindered by the unique features of cyberspace itself, such as the lack of geographical boundaries, open architecture or easily achievable anonymity. Thirdly, there is still a shortage of credible data on cyber incidents. This is not only due to objective difficulties in tracing malicious activity online, but also the unwillingness of governments to share such information and cooperate with civilian experts[9].

---

[4] See T.E. Copeland, ed., *The Information Revolution and National Security*, Carlisle 2000; D.S. Alberts, J.J. Garstka, F.P. Stein, *Network Centric Warfare. Developing and Leveraging Information Superiority*, Washington, D.C. 1999; J.S. Nye, Jr., W.A. Owens, *America's Information Edge*" "Foreign Affairs", Vol. 75 (March/April 1996); R. Henry and C.E. Peartree, eds., *The Information Revolution and International Security*, Washington 1998; M.C. Libicki, *Information War, Information Peace*, "Journal of International Affairs", Vol. 51 (Spring 1998); G.R. Sullivan and A.M. Coroalles, *The Army in the Information Age*, Carlisle 1995; R.C. Molander, A.S. Riddile, P.A. Wilson, *Strategic Information Warfare: A New Face of War*, Santa Monica 1996; D.S. Alberts, D.S. Papp, eds., *The Information Age: An Anthology on Its Impact and Consequences*, Fort McNair 1997.

[5] J. Nazario, *Politically Motivated Denial of Service Attacks*, in C. Czosseck, K. Geers, eds., *The Virtual Battlefield: Perspectives on Cyber Warfare*, Amsterdam 2009.

[6] E. Gartzke, *The Myth of Cyberwar*, "International Security", vol. 38, No. 2 (Fall 2013), pp. 41.

[7] See J. Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, Sebastopol 2010; F.D. Kramer, S.H. Starr, L.K. Wentz, eds., *Cyberpower and National Security*, Washington, D.C. 2009; C. Czosseck, K. Geers, eds., *The Virtual Battlefield: Perspectives on Cyber Warfare*, Amsterdam 2009; R.J. Deibert, *Black Code: Inside the Battle for Cyberspace*, Toronto 2013; M. Dunn-Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure in Information Age*, New York 2008; S. Even, D. Simon-Tan, *Cyber Warfare: Concepts and Strategic Trends*, Tel Aviv 2012; K. Geers, *Strategic Cyber Security*, Tallin 2011; N. Arpagian, *La cybersecurité*, Paris 2010; A. Bautzmann, *Le cyberespace, nouveau champ de bataille?*, "Diplomatic. Affaires Stratégiques et Relations Internationales" (Février-Mars 2012).

[8] See T. Rid, *Cyber War Will Not Take Place*, "Journal of Strategic Studies", Vol. 35, No. 1 (February 2012); T. Rid, *Think Again: Cyberwar*, "Foreign Policy", 27.02.2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar (access: 27.11.2014); E. Gartzke, *The Myth of Cyberwar*, "International Security", vol. 38, No. 2 (Fall 2013); R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York 2010.

[9] Such tendencies were greatly depicted by Ron Deibert in the preface of his recent book *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. See R.J. Deibert, *Black Code: Surveillance,*

Therefore, despite the rising popularity of cybersecurity research, consensus between scholars in this field is non-existent.

In the wealth of books and articles concerning different aspects of cybersecurity, one basic problem is usually omitted or neglected by academics. While they focus on the accurate and extensive analysis of different types of cyber threats or features of cyberspace as a new operational domain, so far there has been little considerable attempts to clarify the very sources of these problems. This issue can be siphoned down to the question: what is the relationship between the proliferation of information and communication technologies in almost all areas of human activity and the rise of new threats for national and international security? Usually most scholars accept simple *a priori* statements that the rising popularity of ICTs is one of the major causes of cyber threats, what is a far-reaching oversimplification. Others focus only on specific aspects of this problem and, therefore, lose the overall perspective. There were, of course, some pieces of work, which reached the core of the problem. For instance, Edward Tenner in his book *Why Things Bite Back* from 1997 argued that human development often encounters unintended consequences ("revenge of unintended consequences")[10]. Gene I. Rochlin on the other hand, emphasized that mankind is making irreversible technological changes, which can be often harmful for itself[11]. In this context, it is, however, difficult to encounter an up-to-date paper, which analyzes these issues from the perspective of their strategic consequences for national and international security. Therefore, this gap in research must be plugged, as it is crucial to conduct efficient cybersecurity policy, focused not on manifestations, but the sources of these challenges.

Why the title: "the paradox of cyber development"? Paradox is usually defined as an "apparent contradiction"[12] or a "person or thing that combines contradictory features or qualities"[13]. Such an apparent contradiction sometimes occurs at the intersection of the processes of the digital revolution and national and international security. The emergence of information and communication technologies, notably computers and the Internet, opened completely new possibilities and opportunities for individuals, societies and states. Of course it is hardly an innovative statement, as many authors even in the early 1960s or 1970s highlighted that the technical revolution will open a new era of humankind's development. For example, Daniel Bell anticipated the end of the "ideology era" and Marshall MacLuhan provided a vision of a "global

---

Privacy, and the Dark Side of the Internet, Toronto 2013. See also: L. Kello, *The Meaning of the Cyber Revolution*, "International Security", vol. 38, No. 2, (Fall 2013), pp. 22-37; F. Schreier, *On Cyberwarfare*, "DCAF Horizon 2015 Working Paper", No. 7, pp. 31-93.

[10] See E. Tenner, *Why Things Bite Back: Technology and the Revenge of Unintended Consquences*, New York 1997.

[11] G.I. Rochlin, *Trapped in the Net: The Unanticipated Consequences of Computerization*, Princeton 1997.

[12] J.W. Wirsbinski, *Paradox. Systems Thinking at Its Best or at Its Worst?*, World of Systems, 12.02.2007, http://www.boardmansauser.com/downloads/SDOE775-Wirsbinski.pdf (access: 28.11.2014).

[13] *Paradox*, Oxford Dictionaries, http://www.oxforddictionaries.com/definition/english/paradox.

village"[14]. Even Zbigniew Brzezinski wrote about the beginning of the "technetronic era" in international relations[15]. Nowadays, the multidimensional benefits drawn by mankind from ICT development, such as the rise in productivity, improved quality of life, boosts for innovations, boosts for economic growth, higher quality products, and facilitated communication[16], are well examined by decision makers, scholars and societies around the world.

This study, however, argues that the development of information and communication technology is accompanied by multiple detrimental trends. They strongly contribute to the advent of new challenges, especially for wired nations, which may have serious, strategic consequences for their security. It has to be noted that the notion of "paradox" in the context of cybersecurity was already used in the recent Microsoft Security Intelligence Report (*The Cybersecurity Risk Paradox*) prepared by David Burt, Paul Nicolas, Kevin Sulllivan and Travis Scoles. This document, focusing only on the proliferation of malware argued that "countries with a developing level of ICT may be unprepared to secure their ICT infrastructure commensurate with the increase in citizen use of computer systems, which provides greater opportunity for malware to spread unchecked", however "there appears to be a certain level of technology maturity at which countries develop enough technological sophistication that they can curb the growth of malware"[17].

This paper touches upon a similar subject while also focusing on a much broader scope of issues, important for national and international security. It argues that the rising pace of technological development in the 21st century, rooted in expected, multidimensional benefits, is also met by the widespread "folly" of being always up-to-date with the latest trends and fashions, especially in the sensitive and ever changing area of IT. Humanity is contributing and increasing the flood of technological innovations, frequently blindly assimilating all electronic devices, including some which appear to be unnecessary or even harmful. Almost no one asks: where are the boundaries and at what point do hi-tech pursuits cease to make sense? The popular answer is simple: there are none, we need everything that is advertised in the media, even TVs, automobiles and famous toasters[18] connected to the Internet. Those who have different views are usually ignored by the public, more interested in the release of the new version of the iPhone which is in itself generating popular turmoil without understandable

---

[14] A. Giddens, *The Class Structure of the Advanced Societies*, New York 1975, pp. 53-59; D. Bell, *The End of Ideology: On the Exhaustion of Political Ideas in the Fifties*, Cambridge 1960; M. McLuhan, Q. Fiore, *War and Peace in the Global Village: an inventory of some of the current spastic situations that could be eliminated by more feedforward*, New York 1968.

[15] Z. Brzezinski, *Between Two Ages. America's Role in the Technetronic Era*, New York 1970.

[16] See for example, R.D. Atkinson, A.S. McKay, *Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution*, The Information Technology & Innovation Foundation, March 2007.

[17] "The Cybersecurity Risk Paradox". See D. Burt et al., *The Cybersecurity Risk Paradox*, Microsoft Security Intelligence Report Special Edition, Microsoft Corporation 2014, p. 8.

[18] See M. Devost, B. Houghton, N. Pollard, *Information Terrorism: Can You Trust Your Toaster?*, in R.E. Neilson, ed., *Sun Tzu and Information Warfare*, Washington D.C. 1997.

reasons. In this context, recognized science-fiction writer and futurologist Stanisław Lem once said that "most technologies have luminous obverse, but life gave them the reverse - black reality"[19]. This is the very logic of the cyber development paradox. We now live in an accelerating and interconnected world of technology, being much more than MacLuhan's "global village". The pace and scope of development raises legitimate doubts, as it is outpacing the growth of deepened intellectual reflection; even the "fathers" of the information revolution, such as Bill Gates[20], were surprised by the bewildering speed of changes it brought for humankind. Unfortunately, in the digital era even the most intriguing thoughts on this topic are quickly forgotten, although they raise some serious questions.

This paper intends to contribute to the discussion over these often neglected issues. It argues that the more that ICTs are introduced without sufficient deliberation into different areas of life, the greater the challenges, resulting from their improper use, we face. Such correlation, as stated above, is visible at a glance, but so far there has been little effort to understand the very causes and strategic consequences of this profound paradox. Therefore, this study aims to: (1) analyze major sources of negative trends appearing at the intersection of ICT development and cybersecurity; (2) present practical manifestations of cyber development paradox; (3) indicate major strategic repercussions of this phenomenon for national and international security.

In order to achieve these goals, this article has been divided into three parts. The first examines the major sources of paradox of cyber development. The second, gets to the core of the problem, highlighting several distinct examples of the negative consequences of the emergence of information and communication technologies for national and international security. The final part covers what are the most important strategic consequences of this paradox.

THE ROOTS OF THE CYBER DEVELOPMENT PARADOX

At first glance, it seems that everything has already been said over the last 40 years about the positive and negative impacts of the information revolution. This is far from the truth, as the scientific community, experts and government agencies are constantly being surprised by the craftiness and creativity of malicious activities in cyberspace. 30 years ago no one would expect that programmable logic controllers (PLCs) may be used to harm critical infrastructure, as the case in Iran proved. 20 years ago no one would think that crude portable phones could be used to gather sensitive data or to empty a bank account. Today it is sadly part of daily life. Every day we are exposed to dozens of new technologies, promising us a new, better world, which are constantly being used by the criminal underground, terrorist organizations or even political re-

[19] „Stanisław Lem", *Cytaty.info*, http://www.cytaty.info/autor/stanislawlem-7.htm.

[20] For example, at the end of 1980s he stated that „we will never make a 32-bit operating system", which proved to be wrong in 1993. See T. Ferguson, *In his own words: Bill Gates' best quotes*, ZDNet, 26.07.2008, http://www.zdnet.com/article/in-his-own-words-bill-gates-best-quotes/ (access: 01.12.2014).

gimes for malicious activities, in a way and manner that was not foreseen by their inventors. It proves that, nowadays, there is a dire need to analyze ICT development as a factor contributing to the emergence of new threats to national and international security. It could not only help to grasp all the cyber challenges that exist today, but also to anticipate and counter their evolution in future. There is a need for greater awareness and understanding that every new service, device or application based on ICTs may lead to unexpected effects within society. A proper domestic and international reaction, however, requires knowledge of what their common denominator is. Specific countermeasures may differ, but efficient long-term strategy should be aimed at tackling the very root of the problems.

In this context, it should be asked what are these aforementioned detrimental trends within the digital revolution, which can contribute to the advent of new challenges for national and international security? The first, and the most obvious, trend concerns rising dependence on the reliability of ICTs. Ron Deibert aptly presented this problem in his recent book stating: "here is a dark side to all this connectivity: malicious threats that are growing from the inside out, a global disease with many symptoms that is buttressed by disparate and mutually reinforcing causes. Some of these forces are the unintended by-products of the digital universe"[21]. It is worth noting that, surprisingly, there are little to no complex studies on the relationship between individual daily life and the reliability of digital technologies, such as smartphones, computers, and the Internet. Most of the studies are carried out from a psychological perspective, which is somewhat irrelevant to security studies[22]. The remaining studies usually focus on such issues as the rising threat of (il)legal surveillance or cybercrime[23], though they typically lack hard data. Research concerning ICT dependency at society and state level is usually much more developed. There are three distinctive tendencies here. Firstly, to exaggerate existing cyber threats due to rising "ICT addiction". Some authors, politicians, journalists and blogosphere pundits argue that due to the vast scope of cyberspace, governments nowadays can be easily targeted and defeated with the use of cyberattacks[24]. Secondly, to underestimate existing challenges in cyberspace, emphasizing that the chances of critical cyber incidents are small to none existent[25].

---

[21] R.J. Deibert, *Black Code: Inside the Battle for Cyberspace*, Toronto 2013, pp. 14.

[22] See M. Choliz, E. Echeburúa, F.J. Labrador, *Technological Addictions: Are Theseׂthe New Addictions*?, "Current Psychiatry Reviews", Vol. 8, No. 4 (2012).

[23] D. Lyon, *Surveillance, Power and Everyday Life*, in C. Avgerou et al., eds., *The Oxford Handbook of Information and Communication Technologies*, Oxford 2009.

[24] J. Best, *Industrial Systems Automation and Security: an "Electronic Pearl Harbor"?*, Global Assurance Certification Paper, Version 1.4, SANS Institute 2000-2002; Secretary of Defense Leon E. Panetta, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*, U.S. Department of Defense, New York, 11.10.2012; R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York 2010.

[25] S. Lawson, *Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History*, "George Mason University Working Paper", No. 11-01 (January 2011), p. 30-31; D. Isenberg, *An Electronic Pearl Harbor? Not Likely*, in T.E. Copeland, ed., *The Information Revolution and National Security*, Carlisle 2000, pp. 92-100.

Finally, the third view tries to balance both of these tendencies, arguing that due to rising dependencies on ICTs, different types of cyber threats are becoming more and more dangerous, however the likelihood of a symbolic 'Electronic Pearl Harbor' is fairly low[26]. It seems that it is the most accurate perception, as both extreme tendencies are usually based on incorrect assumptions. On the one hand, authors exaggerating cyber threats tend to verify their theories based on unconfirmed incidents, such as cyberattacks in Brasil in 2005 and 2007, or the alleged cyber operation of the CIA against the Soviet Union in the 1980s. On the other hand, their critics frequently undervalue confirmed serious information operations, such as the famous Stuxnet worm case in Iran or cyberattacks against Estonia in 2007 and Georgia in 2008.

The problem of ICT dependence is strictly related to the increasingly popular conception of the Internet of Things (IoT). It was defined by David Lake, Ammar Rayes and Monique Morrow as "networks of sensors attached to objects and communication devices, providing data that can be analyzed and used to initiate automated actions (...) The data also generates vital intelligence for planning, management, policy and decision making"[27]. In practice, IoT manifests itself in the rising tendencies of manufacturers to include computer and network capabilities in various pieces of equipment, from automobiles through to televisions and medical equipment, and even refrigerators. This, of course, brings huge benefits, but with little effort, it also opens completely new possibilities for malicious activities, not just those specific to cybercrime but also cyberespionage or cyberwarfare. In effect, further areas of societies' and states' activities are potentially endangered by cyberattacks. This problem was accurately described by Symantec experts, who stress that: "Today the burden of preventing attacks against IoT devices falls on the user; however this is not a viable long-term strategy. Manufacturers are not prioritizing security – they need to make the right security investments now"[28]. It is a serious problem from the cybersecurity perspective, as usually random users are not skilled enough to ensure the safety of their IoT devices. This, in turn, creates security gaps, which can be exploited in many different ways. Therefore, if these tendencies will not revert, ICT development will always contribute to the creation of new challenges for national and international security.

The second detrimental tendency concerns the peculiar situation in the IT market. For several decades the accelerating technological race has been accompanied by increasing competition between the biggest corporations who manufacture both hardware and software. As a result, research & development activities are conducted under the strong pressures of time and effect. Scientists, technicians and programmers are usually expected to provide a satisfactory digital product as soon as possible, as it is one of the decisive factors in ensuring success in a highly competitive IT market.

[26] C. Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress, Washington, D.C. 29.01.2008; G. Weimann, *Cyberterrorism: The Sum of All Fears?*, "Studies in Conflict & Terrorism", Vol. 28 (2005).

[27] D. Lake, A. Rayes, M. Morrow, *The Internet of Things*, "The Internet Protocol Journal", Vol. 15, No. 3 (September 2012).

[28] *Internet Security Threat Report. 2013 Trends*, Vol. XIX (April 2014), p. 7.

The general rush to introduce new technologies has, however, led to negative impacts, as the testing phase of each product is frequently shortened to a minimum. Moreover, such evaluation is mostly focused on functionality and not on security. Consequently, merchandise may have critical vulnerabilities which can in turn be exploited by hackers. It must also be noted that growing rivalry is an important factor which sometimes forces corporations to sacrifice security concerns in order to maximize the users' convenience[29]. It is due to the fact that, as Brent Cantafio noted, "for the most part, users want an easy-to-use method to access network resources; they don't want to be riddled around with complex passwords and security schemes"[30].

The third trend concerns something that could be called a new cultural paradigm, founded on the proliferation of information and communication technologies. As previously mentioned, nowadays, almost every new popular electronic device, application or online service is indiscriminately perceived as an improvement in the overall quality of life. Sometimes these inclinations are explained as a symptom of the emerging "cyberculture"[31]. In contemporary societies around the world the ownership of various IT gadgets is considered to be a sign of wealth, prosperity and success, starting with smartphones, to smart TVs, smart refrigerators, tablets and even watches (e.g. Apple Watch). The same trend applies to various online services, such as Instagram, Facebook or Twitter. This specific way of thinking is accurately described by Robyn MacKillop, who wrote that: "if you do not have an online presence, you don't exist"[32]. On the one hand, such a global rush to be always up-to-date with technological innovations, of course, implies that there are political, social and economic benefits, which are thoroughly discussed and debated in the academic community. Yet, on the other hand, there is still a general lack of a healthy dose of skepticism towards the view that every aspect of contemporary life should be immersed and reflected in the digital world. For example, there is little public discussion over such issues as the rationality of the Internet of Things or e-voting, in the context of possible security threats[33].

---

[29] See for example: A. Arora, C. Forman, A. Nandkumar, R. Telang, *Competition and patching of security vulnerabilities: An empirical analysis*, "Information Economics and Policy", Vol. 22 (2010), pp. 164-177; S.R. Rakitin, *Balancing Time to Market and Quality*, "ASQ Software Quality Professional", No. 3 (1999); C. Edelen, *Balancing Act: Software Quality Vs. Time to Market*, Wall Street & Technology, 24.03.2014, http://www.wallstreetandtech.com/risk-management/balancing-act-software-quality-vs-time-to-market/d/d-id/1268821?.

[30] B. Cantafio, *Security vs. Convenience. Is RSA SecurID the Answer?*, Global Information Assurance Certification Paper, Version 1.4b, SANS Institute 2004, p. 4.

[31] See D. Silver, A. Massanari, S. Jones, *Critical Cyberculture Studies*, New York 2006.

[32] R. MacKillop, *If You Do Not Have an Online Presence, You Don't Exist©*, Linkedin, 31.07.2014, https://www.linkedin.com/today/post/article/20140731005316-12497773-if-you-do-not-have-an-online-presence-you-don-t-exist (access: 02.12.2014).

[33] Of course these subjects are extensively discussed by researchers, but unfortunately it does not generate greater interest in mass media or various groups (manufacturers) interested in the promotion of IoT. See e.g. R. Roman, P. Najera, J. Lopez, *Securing the Internet of Things*, "IEEE Computer", Vol. 44, No. 9 (September 2011), pp. 51-58; S. Cirani, G. Ferrari, L. Veltri, *Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview*, "Algorithms", No. 6 (2013).

Expected profits and specific fashion are the major drivers reinforcing, without hesitation, many unnecessary projects, such as the connection of TVs or automobiles to the Internet[34]. Therefore, cybersecurity problems are frequently caused by a general overestimation of the usefulness of various technologies. Unfortunately the voices of those who suggest that some of these innovations should be introduced carefully are generally ignored. One of the few exceptions was John McAfee's speech at the Def Con conference in 2014, when he emphasized that popular electronic gadgets are not always beneficial. For instance, referring to the rising scale of cyberespionage acts against smartphones he mentioned that "the most promising privacy thing is stupid phones"[35]. It was a very important statement suggesting that the lack of deliberation when it comes to ICT proliferation may have negative consequences.

The fourth and final trend lies in the rising complexity of information and communication solutions. At present, hardware and software are much more comprehensive than they were 20 or 30 years ago. Among others, this has been caused by the rising need of flexibility, utility and multi-functionality, leading to more sophisticated programming. Already in 1999 famous cybersecurity expert Bruce Schneier had written: "We've seen security bugs in almost everything: operating systems, applications programs, network hardware and software, and security products themselves. This is a direct result of the complexity of these systems. The more complex a system is – the more options it has, the more functionality it has, the more interfaces it has, the more interactions it has – the harder it is to analyze"[36]. This issue is also connected to the frequency of ordinary mistakes committed by both manufacturers and programmers. According to research carried out in 1997, experienced programmers usually made one mistake for every 10 lines of code[37]. If these tendencies have not changed, it shows the vast scale of possible security vulnerabilities in software. Nowadays popular operating systems are typically composed of tens of millions of code lines[38]. If a program contains 50 million of lines of code, it might potentially have up to 5 million mistakes. Even if 99% of them are patched, there will still be 50,000 "bugs" remaining. In short, the greater the number of code lines program has, the higher prob-

[34] See S. Rosenblatt, *Car hacking code released at Defcon*, CNET, 02.08.2013, http://www.cnet.com/news/car-hacking-code-released-at-defcon/ (access: 03.12.2014); *Reporting From Black Hat: Your Smart TV is Probably Spying on Your Family Right Now*, Digital Trends, 02.08.2013, http://www.digitaltrends.com/opinion/burn-your-smart-tv/ (access: 03.12.2014).

[35] D. Yardon, *John McAfee at Def Con: Don't Use SmartPhones*, "The Wall Street Journal", 08.08.2014, http://blogs.wsj.com/digits/2014/08/08/john-mcafee-at-def-con-dont-use-smartphones/ (access: 03.12.2014).

[36] B. Schneier, *A Plea for Simplicity. You can't secure what you don't understand*, Schneier on Security, 19.11.1999, https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html (access: 04.12.2014).

[37] S.R. Rakitin, *Balancing Time to Market and Quality*, "ASQ Software Quality Professional", No. 3 (1999), pp. 54-55.

[38] *Codebases*, Information is Beautiful, http://www.informationisbeautiful.net/visualizations/million-lines-of-code/ (access: 04.12.2014).

ability of error. Each error constitutes a potential vulnerability, which can be exploited with malicious intent.

To summarize, today the accelerating race between IT manufacturers is frequently fueled by universal trends, new *mode de vie*, based on the common use of not only computers or smartphones, but even printers and cars connected to cyberspace[39]. It is visible even at a government level as an increasing number of public administration sectors are deeply penetrated by increasingly comprehensive ICTS[40]. Such a global urge to introduce digital technologies in all areas of human life may, however, lead to disastrous consequences[41], as societies and states are becoming increasingly susceptible to malicious activities in computer networks. In order to understand them, it is therefore important to present several outstanding examples on how digital revolution may contribute to the creation of new challenges for national or international security.

E-BANKING

The last decade of the 20th century was the moment when humanity discovered the vast potential of the Internet as a new promising domain of economic activity. The emergence of e-business ventures in the 1990s was extremely dynamic, gaining the popular term of the "dot-com bubble". This speculative investment rush in the IT sector, illustrating the faith put into the new technologies, burst in 2000 due to the NASDAQ crash[42]. It didn't however put an end to innovative e-commerce activities, which have evolved and adapted to ever changing market conditions. One of the

---

[39] See G.E. Corazza, A. Vanelli-Coralli and R. Pedone, *Technology as a Need: Trends in the Evolving Information Society*, "Advances in Electronics and Telecommunications", Vol. 1, No. 1 (April 2010), pp. 124-132.

[40] The rising trend to digitalize all areas under the state's control is symbolized by popular concepts of e-administration or e-voting. There are hundreds of scholars around the world demanding the introduction of Internet-based popular elections, perceiving them as a remedy for many of liberal democracy's problems. See M. Chevallier, M. Warynski, A. Sandoz, *Success Factors of Geneva's e-Voting System*, "The Electronic Journal of e-Government", Vol. 4, Issue 2 (2006), pp. 55-62; M. Hajjar et al., *An E-Voting System for Lebanese Elections*, "Journal of Theoretical and Applied Information Technology", Vol. 2, No. 1 (February/March 2006); A. Rokhman, *E-Government Adoption in Developing Countries; the Case of Indonesia*, "Journal of Emerging Trends in Computing and Information Sciences", Vol. 2, No. 5 (May 2011), pp. 228-236.

[41] Of course, there are many academics stressing, sometimes even exaggerating, threats coming from the rush to include ICTs wherever possible. Unfortunately, at the same time some of these same academics simplify or trivialize the sources of these problems. Some even use the term of possible "digital Pearl Harbor" or "electronic Waterloo", which is often criticized as exaggeration. See J. Guisnel, *Cyberwars. Espionage on the Internet*, New York 1997, pp. 186-187; L. Yagil, *Terroristes et internet. La cyberguerre: essai*, Montréal 2002, pp. 53; J. Eriksson, G. Giacomello, *The Information Revolution, Security and International Relations: (IR)relevant Theory?*, "International Political Science Review", Vol. 27, No. 3 (2006), pp. 226.

[42] M. Doms, *The Boom and Bust in Information Technology Investment*, "FRBSF Economic Review" (2004), pp. 19-34.

fastest developing sectors was electronic banking[43]. At the turn of the 20th and 21st century, as Joanna Smith Bers stated, cyberspace has become an "electronic frontier in which banks can more cost effectively deploy products and services to a virtually boundless customer base"[44]. E-banking, thanks to multiple emerging "front end" and "back end" technologies and services, such as ATM cards, automatic bill payment (ABP) or electronic funds transfer (EFT), became increasingly popular, not only in the United States, but across the world. Some even called it a banking revolution, due to the scope of quality changes to financial operations[45]. Within a decade, hundreds of millions of Internet users around the world discovered the convenience of electronic banking (423,5 million in April 2012)[46]. Despite its popularity, these services were constantly evolving, providing new groundbreaking possibilities, such as mobile banking (based on smartphone applications) or online money transfers (PayPal), which ensured additional profits for the financial sector. Thus it is unsurprising that in this mutually beneficial situation, in some countries, such as Estonia, above 90% of all transactions were completed online[47].

In spite of these developments, the emergence of electronic banking services was one of the first evident signs that new, useful and widely popular technologies may be the cause of serious threats for economies. In 1987 the First National Bank of Chicago became the victim of a $70 million computer theft[48]. Over time, the hacking of banks became increasingly frequent. During the next 15-20 years, cybercriminal activities focused mostly on the financial sector. Various individuals, as well as organized crime groups, discovered huge opportunities in attacking online banking systems and their customers for financial profit.

Hackers have invented a wide range of malware, such as trojan horses and worms, designed to gain illegal access to bank accounts. One of the most successful malicious software like this was Zbot/Zeus, a trojan horse which was able to steal banking credentials. Relatively quickly it has become one of the most popular kits, sold in the criminal underground for around $3000-4000. In 2009 alone, this type of malware

[43] It has to be noted, that e-banking services were available in the 1980s and 1990s but they were rather unpopular globally until the 21st century. See *Infographic: The History of Internet Banking (1983-2012)*, The Financial Brand, 02.10.2012, http://thefinancialbrand.com/25380/yodlee-history-of-internet-banking/ (access: 05.12.2014).

[44] J. Smith Bers, *Banking and Cyberspace: The New Promised Land*, in D.S. Alberts, D.S. Papp, eds., *The Information Age: An Anthology on Its Impact and Consequences*, Fort McNair 1997, pp. 107.

[45] J.M. Hogarth, J.M. Kolodinsky, M.A. Hilgert, *The adoption of electronic banking technologies by US consumers*, "The International Journal of Bank Marketing", Vol. 22, No. 4 (2004), pp. 238-239; C.E. Anguelov, M.A. Hilgert, J.M. Hogarth, *U.S. Consumers and Electronic Banking, 1995-2003*, "Federal Reserve Bulletin" (Winter 2004), pp. 1-3.

[46] *Global online banking penetration in April 2012, by region*, Statista, April 2012, http://www.statista.com/statistics/233284/development-of-global-online-banking-penetration/ (access: 06.12.2014).

[47] *Facts about e-Estonia*, Estonian Information System's Authority, https://www.ria.ee/facts-about-e-estonia (access: 07.12.2014).

[48] R. Trigaux, *A history of hacking*, "St. Petersburg Times Online", 2000, http://www.sptimes.com/Hackers/history.hacking.html (access: 07.12.2014).

managed to gain access to 70000 bank and business accounts. Moreover, in 2010 its operators stole around $80 million from U.S. and foreign banks. Over time the software was updated and modified by various hackers, which led to the creation of the whole Zeus family, made up of: Zeus Gameover, SpyEye, Citadel or Carberp[49]. These tools were usually used in convergence with social engineering techniques (phishing). It was a reflection of the principle, that the weakest link in all security systems is always the user. Phishing was usually introduced in two ways: via e-mail messages and malicious websites designed to mimic a legitimate address[50].

Criminal groups were also able to develop some ingenious hardware, electronic devices, installed, for example, in ATMs which could scan a debit or credit card number, charge contactless payment cards or acquire personal identification numbers (PIN)[51]. All of these developments proved that the criminal underground was almost instantly able to identify and exploit security gaps in new technology. As a result, new kinds of threats in cyberspace have emerged.

The tendency to use widely beneficial banking technologies for malicious purposes is evident in the majority of the cybersecurity reports of the last decade. As the popularity of e-banking has grown throughout the years, the financial sector has become the main subject of interest for the cybercriminal underground. According to Symantec, between 2007 and 2009 more than two-thirds of all phishing attacks online were aimed at the financial sector (between 66 and 79%)[52]. Therefore, despite the rising significance and sophistication of e-banking security systems, the volume of financial losses has been growing steadily. Most current studies estimate that the Internet economy generates between $2 to 3 trillion each year. The total cost of cybercrime, most of which relates to the financial sector, extracts about 15 to 20% of the value created by the global network[53]. According to statistics provided by McAfee and the Center for Strategic and International Studies, in many countries annual losses incurred from bank hacking are counted in hundreds of millions of dollars. There are several distinct examples. In Mexico online fraud was the reason for losses estimated to be $93 million

---

[49] A. Neagu, *The Top 10 Most Dangerous Malware That Can Empty Your Bank Account*, Heimdal Security, 01.08.2014, https://heimdalsecurity.com/blog/top-financial-malware/ (access: 07.12.2014); K. Stevens, D. Jackson, *Zeus Banking Trojan Report*, Dell SecureWorks, 11.03.2010, http://www.secureworks.com/cyber-threat-intelligence/threats/zeus/ (access: 07.12.2014); *$70 Million Stolen From U.S. Banks With Zeus Trojan*, Risk Analytics, 04.10.2010, https://riskanalytics.com/2010/10/04/70-million-stolen-from-u-s-banks-with-zeus-trojan/ (access: 07.12.2014).

[50] *Symantec Internet Security Threat Report. Trends for July-December 07*, Symantec, vol. XIII (April 2008), p. 6.

[51] See A. Sabari Rajeswaran, *Network Security: ATM PIN Unlocking and Avoid Skimming by UAN Technique*, "International Journal of Emerging Technology and Advanced Engineering", Vol. 3, No. 1 (January 2013).

[52] *Symantec Internet Security Threat Report. Trends for July-December 07*, Symantec, vol. XIII (April 2008), p. 7; *Symantec Internet Security Threat Report. Trends for 2008*, Symantec, vol. XIV (April 2009), p. 5; *Symantec Global Internet Security Threat Report. Trends for 2009*, Symantec, vol. XV (April 2010), p. 66-67.

[53] *Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II*, Center for Strategic and International Studies, McAfee (June 2014), p. 7.

annually. Japanese banks lose around $110 million each year. In 2013 one hack against a US retailer (Target) alone caused bank losses estimated to be $200 million. This data shows the grievous potential of cybercriminal activity against e-banking services. As McAfee and CSIS experts noted, "the theft of financial assets can be easiest to monetize, particularly when a criminal can transfer funds directly to an account they control. In other cases, cybercriminals must rely on an intermediary to monetize their crime"[54]. Sometimes it is possible to reduce the costs of online fraud, as recently carried out in Great Britain. Unfortunately, this must involve increased spending on cybersecurity, i.e. new, safer solutions and IT experts[55]. For example, Heartland Payment Systems, which had lost about 100 million debit and credit card numbers to hackers in 2007, had quadrupled its computer security budget over the next seven years[56].

The most significant manifestation of the cyber development paradox connected to e-banking services was, however, not related to any criminal activity but had strictly political motivations. As mentioned above, one of the most digitalized countries in this field is Estonia, where over 90% of all financial transactions are conducted via the Internet[57]. This small Baltic country in April and May 2007 became a target of one of the first of a massive series of cyberattacks, described be some analysts as the "first cyber war". The historical and political rivalry between Tallinn and Moscow resulted in serious street clashes over a monument called the "Bronze Soldier". Unexpectedly, the rioting of the Russian minority in Tallinn was also reflected in cyberspace. Hundreds of Russian hacktivists organized long-lasting cyberattacks against Estonian cyber assets. Besides the DDoS (Distributed Denial of Service) attacks aimed at government websites, they also targeted the business sector, which was mostly dependent on the reliability and performance of information technologies[58]. During more than three weeks of cyber incursions, the most prominent Estonian banks were frequently harmed. Hacktivists and script kiddies targeted, among others, Hansabank, the largest commercial bank of this country. As a result, not only were all its online services paralyzed, but so were bank cards and ATMs across Estonia[59]. Thus, the incidents of 2007 were harmful for Tallin's key financial infrastructure. These events clearly demonstrated that even the most advanced countries, which are immersed in the processes of the information revolution, may easily become the prey of relatively unsophisticated computer attacks. This was clearly a great symbol of the paradox of cyber development.

---

[54] Ibid., p. 15.

[55] B. Watkins, *The Impact of Cyber Attacks on the Private Sector*, Association for International Affairs Briefing Paper, No. 3, Prague, August 2014, p. 6.

[56] D. Yardon, *Companies Wrestle with the Cost of Cybersecurity*, "The Wall Street Journal", 25.02.2014, http://online.wsj.com/news/articles/SB10001424052702304834704579403421539734550 (access: 10.12.2014).

[57] *E-Estonia*, Estonia.eu, http://estonia.eu/about-estonia/economy-a-it/e-estonia.html (access: 10.12.2014).

[58] See K. Ruus, *Cyber War I: Estonia Attacked from Russia*, "European Affairs", No. 1-2 (2008).

[59] D. Kostadinov, *To Black Out an Entire Country - part one*, Infosec Institute, 01.10.2013, http://resources.infosecinstitute.com/estonia-to-black-out-an-entire-country-part-one/ (access: 10.12.2014).

THE EMERGENCE OF WEB 2.0: SOCIAL MEDIA AND CYBERSECURITY

The beginning of the 21st century was not only a period of rising popularity of various e-business ventures. It was also a turning point for the social nature of the Internet, highlighted by the emergence of the so called Web 2.0. It was characterized by profound changes to the previously dominant model of users' activity in the global network. In the 1980s and 1990s, it was mostly passive, based on the use of the existing tools, such as the World Wide Web (WWW) or Internet Relay Chat (IRC). Since the turn of the new century, Internet users started to shape the content of cyberspace more actively by sharing newly created tools amongst one another. The most significant manifestation of the emergence of Web 2.0 is 'social media', such as Facebook, Twitter or Youtube, which allows the user to engage in diversified forms of social, and eventually, even political interaction. The creation of social media not only facilitated communication on different levels, but also enabled data sharing on a mass scale[60].

The benefits arising from the arrival of Web 2.0 tools were quickly recognized not only by individual users, but also the private and public sector. Social media platforms proved to be useful in daily interpersonal contact and, also, in economic ventures, brand creation, public relations, political marketing and education[61]. Therefore, it is no surprise that the number of Facebook users grew dynamically from 1 million at the end of 2004 to 1.1 billion in March 2013. In other words, it has emerged as the most popular social network in the world[62], which is reflected by its estimated value of $200 billion in September 2014[63]. Within several years, social media platforms have become one of the most popular "hot spots" of cyberspace, satisfying communication needs in political, economic, cultural or strictly individual dimensions. Their rising significance was confirmed during the Arab Spring, when Facebook and Twitter appeared to be the focal points of social unrest in the Middle East, enabling the organization of civil protests and the avoidance of mass censorship[64].

While individuals and organizations adopted Web 2.0 technologies, they have become vulnerable to new kinds of inventive threats. Fernando Almeida listed three groups of threats: losses in productivity, which are irrelevant to this paper, possible

---

[60] See e.g. R. Richards, *Digital Citizenship and Web 2.0 Tools*, "MERLOT Journal of Online Learning and Teaching", Vol. 6, No. 2 (June 2010), pp. 516-522.

[61] See A.L. Harris, A. Rea, *Web 2.0 and Virtual World Technologies: A Growing Impact on IS Education*, "Journal of Information Systems Education", Vol. 20, No. 2 (June 2009), pp. 137-144; R. Szczepaniak, ed., *Media Convergence - Approaches and Experiences: Aftermath of the Media Convergence*, New York 2013.

[62] *Number of active users at Facebook over the years*, Yahoo! News, 01.05.2013, http://news.yahoo.com/number-active-users-facebook-over-230449748.html (access: 12.12.2014).

[63] C. Harrison, S. Frier, *Facebook's Value Top $200 Billion on Mobile-Ad Optimism*, Bloomberg, 09.09.2014, http://www.bloomberg.com/news/2014-09-08/facebook-s-value-tops-200-billion-on-mobile-ad-optimism.html (access: 12.12.2014).

[64] M. Lakomy, *Arab Spring and New Media*, in B. Przybylska-Maszner, ed., *The Arab Spring*, Poznań 2011, pp. 45-54.

data leaks and inherent increased security risks[65]. Data leaks were the first group of problems connected to the popularity of social networks to generate interest. It had become apparent that the users of social networks had started to share vast amounts of sensitive information, concerning not only their private life, but also their professional life. Almost instantly social networks transformed into one of the best sources of overexposed data concerning, for instance, personal contacts, internal relations in enterprises or even government activities. It became obvious that social media had quickly become one of the major targets of cyberespionage and information gathering[66]. One of the most outrageous examples took place in 2009 when the wife of MI6 chief Sir John Sawers published a huge amount of her husband's details on her Facebook wall, including his pictures and personal contact information[67]. It was an evident and popular symptom of the general lack of deliberation when using new technologies, completely ignoring the possible negative consequences.

Later on, due to their unique features, social media became to be the focus of massive criminal interest. By 2007, Symantec experts observed a new phenomenon concerning attacks against websites which were likely to be trusted by the end users, such as social networks[68]. These kinds of malicious activities have spread in 2010 as these portals became an even more convenient environment for social engineering attacks. As a rising number of high-profile individuals started to create Facebook or Twitter accounts, cybercriminals discovered a fantastic opportunity. They have quickly ceased to use primitive techniques such as infected malicious links in e-mails, in favor of much more sophisticated methods. These were mostly based on masquerading in social networks as ordinary users, in order to gain the trust of and sensitive information on the potential victim. Thanks to the general tendency to publish as much information as possible about both our professional and private lives, it has become increasingly easy to acquire knowledge about organizations' e-mail addresses or private information which is frequently used in passwords. Furthermore, social networks have proved to be a great tool for enabling the dissemination of malicious links (especially shortened URLs), due to the trend of sharing interesting information through, for example, Facebook walls or news feeds[69]. Moreover, criminals have started to exploit the varying expectations of social media users. For example, one of the most popular techniques is to inform them about the possibility to add a "dislike" button

[65] F. Almeida, *Web 2.0 Technologies and Social Networking Security Fears in Enterprises*, "International Journal of Advanced Computer Science and Applications", Vol. 3, No. 2 (2012), pp. 153.

[66] *Cyber Espionage. The harsh reality of advanced security threats*, Deloitte Center for Security & Privacy 2011, Solutions, p. 4.

[67] D. Harrison, *MI6 chief's cover is blown by wife's holiday snaps on Facebook*, "The Telegraph", 04.07.2009, http://www.telegraph.co.uk/news/uknews/law-and-order/5745124/MI6-chiefs-cover-is-blown-by-wifes-holiday-snaps-on-Facebook.html (access: 16.12.2014).

[68] *Symantec Internet Security Threat Report. Trends for July-December 07*, Symantec, vol. XIII (April 2008), p. 3.

[69] *Symantec Internet Security Threat Report. Trends for 2010*, Symantec, vol. XVI (April 2011), p. 9-11.

to their Facebook account, which is not normally provided[70]. Over time, new kinds of attacks have evolved in this environment, such as: fake offerings (an invitation to join a fake group with incentives such as free gifts in exchange for e-mail address), "likejacking" (scams involving the "like" button) or fake plug-ins and browser extensions advertised via social media[71]. Interestingly, malicious activities are carried out not only on the most popular websites, but also the emerging ones, such as Instagram, Tumblr or Pinterest.

Finally, it must be noted that social networks have become a convenient environment for new kinds of malware. The main symbol of these rising challenges is the computer worm Koobface, which was designed to be spread with the use of Facebook, MySpace, Tagged, Twitter or Friendster accounts. Once infected, computers were automatically sending malicious links to other social network friends. In such a way, cybercriminals were able to setup a vast botnet infrastructure composed of tens of thousands of computers mostly from the United States, and earn about $2 million between 2009 and 2010 alone. This situation was accurately summarized by Ron Deibert and Rafal Rohozinski, who noted that "criminal networks (...) are growing as fast as the social networking platforms upon which they parasitically feed. Koobface is just one example of an entire ecosystem that threatens to put at risk the very entity on which it depends - a free and open cyberspace"[72].

SMARTPHONES AND TABLETS

Another illustration of the cyber development paradox concerns the emergence of new, popular platforms of computing and telecommunication: smartphones and tablets. The first innovative and inventive smartphones which connected features of mobile phones with computing capabilities were already in existence in the 1980s, but they only appeared on the market in the mid-1990s. They have gained widespread popularity during the 21st century, starting in Japan, the United States and Western Europe. This is mostly due to the fact that they have become integrated devices that can successfully replace not only ordinary telephones, but also notebooks, netbooks, desktop computers, digital cameras, media players and GPS navigation units. Smartphones appear to be a flexible and capacious technology reflecting the global processes of digital convergence. Being an all-in-one solution, they were met with great global interest as they were facilitating daily life, communication, personal contacts, the acquisition of data and even financial transactions thanks to mobile payment technologies. They have also obtained unique operating systems, such as Symbian OS, Android or iOS[73]. A similar situation has occurred with tablets, which have emerged

[70] *Internet Security Threat Report. 2011 Trends*, Symantec, vol. XVII (April 2012), p. 39.

[71] *Internet Security Threat Report. 2012 Trends*, Symantec, vol. XVIII (April 2013), p. 32.

[72] See N. Villeneuve, *Koobface: Inside a Crimeware Network*, Information Warfare Monitor, JR04-2010, p. III; 4.

[73] See e.g. B. McCarty, *The History of Smartphone*, TheNextWeb, 06.12.2011, http://thenextweb.com/mobile/2011/12/06/the-history-of-the-smartphone/ (access: 14.12.2014).

as a new type of portable computers which sometimes even include the capabilities of a smartphone (phablets).

Due to their unique and convenient features, smartphones and tablets have turned into objects of popular desire. Some have even become a symbol of wealth and fashion. This was and is very much the case with Apple iPhones, as well as Blackberries before them. The global rise in smartphone sales is illustrated in the table below.

Table 1

Smartphone sales 2007-2013

Year	Smartphone sales in million units[74]	Change in %
2007	122,32	-
2008	139,29	13,8%
2009	172,38	23,7%
2010	296,65	72%
2011	472	59,1%
2012	680,11	44%
2013	976,78	43,6%

Source: Statistica 2014.

The year of 2011 was particularly noteworthy as smartphone shipments exceeded PC sales for the first time in history[75]. The advent of the smartphone era has had interesting social and economic results. Firstly, they have facilitated the availability of Internet access, consequently strengthening digital revolution processes. Secondly, they have also led to social networking; the smartphone boom accompanied and enhanced the rise of social media. Thirdly, they have significantly contributed to the change in digital media consumption habits[76]. Fourthly, they have brought vast, positive and negative social changes in multiple areas[77]. And finally, they have become a cornerstone of another phase of economic acceleration in the IT sector; the mobile industry in 2013 alone earned around $2.4 trillion globally[78]. At the same time this figure could be much higher considering the fact that there were around 1.75 billion smartphone users in the world in 2014, which illustrates the vast potential and popularity of these new technologies.

[74] *Number of smartphones sold to end users worldwide from 2007 to 2013 (in million units)*, Statistica 2014, http://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/ (access: 14.12.2014).

[75] P. Alto, *Smart phones overtake client PCs in 2011*, Canalys, 03.02.2012, http://www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011 (access: 14.12.2014).

[76] See *Digital Omnivores: How Tablets, Smartphones and Connected Devices are Changing U.S. Digital Media Consumption Habits*, comScore, October 2011.

[77] See M. Sarwar, T.R. Soomro, *Impact of Smartphone's on Society*, "European Journal of Scientific Research", Vol. 98, No. 2 (March 2013), pp. 216-226.

[78] *The Mobile Economy 2014*, GSMA 2014, p. 2-3.

It would be difficult to expect that such a surge in the IT sector would go unnoticed by various groups of cybercriminals and other malicious operators active in cyberspace. The first signs that smartphones and tablets may bring new kinds of challenges became visible relatively quickly, in August 2006 when security researcher Jesse d'Aguanno created the first ever Blackberry trojan. Much more grievous incidents took place due to the rising popularity of iPhones. In 2009 two cyber security experts exposed Apples' pivotal product critical vulnerability. They announced that that iPhones could be hacked with a simple text message. As a result, this platform proved to be the host of a series of new worms, designed, for example, to steal banking codes[79]. Since 2009 there has been a serious boom in malware exploiting new vulnerabilities in mobile devices. In 2010 alone 163 new vulnerabilities were discovered, compared to 115 in 2009 (315 in 2011 and 415 in 2012). New types of mobile worms, viruses and trojans were frequently pretending to be legal software. They have usually allowed its operators access to SMS information, browser history, bookmarks and other data held in internal phone storage[80]. These trends have intensified in the following years. Between 2010 and 2012, over 60 new types of malware designed to target mobile devices were created. 28% percent of them collected data, 25% tracked users and 24% sent unwanted content[81]. The rise of threats for smartphones between 2009 and 2013 is illustrated in table 2.

Table 2

Mobile operating systems vulnerabilities

Year	Mobile operating system vulnerabilities count[83]	Change in %
2009	115	-
2010	163	41,7%
2011	315	93,2%
2012	416	32%
2013	127	-69,4%

Source: *Internet Security Threat Reports 2010-2013*, Symantec.

[79] B. Parr, *iPhone Hack Exposed: The Key Facts*, Mashable, 30.07.2009, http://mashable.com/2009/07/30/iphone-hack/ (access: 14.12.2014); B. Reed, *Smartphone security follies: A brief history*, *Computerworld*, 19.04.2011, http://www.computerworld.co.nz/article/383681/smartphone_security_follies_brief_history/ (access: 14.12.2014).

[80] *Symantec Internet Security Threat Report. Trends for 2010*, Symantec, vol. XVI (April 2011), p. 15-16;

[81] *Internet Security Threat Report. 2011 Trends*, Symantec, vol. XVII (April 2012), p. 26-27; *Internet Security Threat Report. 2012 Trends*, Symantec, Vol. XVIII (April 2013), p. 32-35.

[82] *Internet Security Threat Report. 2011 Trends*, Symantec, vol. XVII (April 2012), p. 11; *Symantec Internet Security Threat Report. Trends for 2010*, Symantec, Vol. XVI (April 2011), p. 6; *Internet Security Threat Report. 2013 Trends*, Vol. XIX (April 2014), p. 16.

It must be highlighted that mobile devices are, additionally, a great tool for cyberespionage. Experts have developed multiple methods to gather information not only from smartphones themselves, but also those indirect proximity. Thus, it is possible to intercept direct calls, text messages or network activity, and also to track users' mobility or eavesdrop on nearby conversations, even if a phone is switched off[83]. On the one hand, such opportunities are important to the global fight against terrorism or organized crime. On the other hand, however, there is a rising danger that security services, like the U.S. National Security Agency, will abuse their capabilities to exploit mobile devices which may in turn be harmful toward the right to privacy and human rights in general, as Edward Snowden's case has proved[84]. The NSA in France in one month alone, between December 2012 and January 2013, was able to eavesdrop on approximately 70 million phone calls[85].

THE STRATEGIC CONSEQUENCES OF THE CYBERSECURITY PARADOX

The examples which were described above constitute only several outstanding illustrations of the cyber development paradox. Over the course of the information revolution there were lots of other anomalies which have contributed to the rising scale of cyber threats. Besides e-banking services, social media and smartphones, there are multiple other pieces of proof indicating that new, beneficial technologies may sometimes strengthen the detrimental tendencies and processes perceptible in cyberspace. One can mention the arrival of programmable logic controllers (PLCs), which have brought huge profits for the whole industrial sector. At the same time, the automation of production processes made the critical infrastructure potentially vulnerable to malicious programs and techniques. This can clearly be seen in the case of the *Stuxnet* worm, which has exploited PLCs to slow down the Iranian atomic program[86]. The same situation has become apparent even in the electronic entertainment sector, as the rising popularity of massively multiplayer online games (MMOs) had not gone unnoticed by cybercriminals. As Eric J. Hayes noted "new technologies and high-speed internet connections have helped online gaming become a popular pastime on the internet. Because gamers invest large amounts of time and money in

[83] *Privacy Scandal: NSA Can Spy on Smart Phone Data*, Spiegel Online, 07.09.2013, http://www.spiegel.de/international/world/privacy-scandal-nsa-can-spy-on-smart-phone-data-a-920971.html (access: 16.12.2014).

[84] See G. Greenwald, *No Place to Hide. Edward Snowden, the NSA, and the U.S. Surveillance State*, New York 2014.

[85] J. Follorou, G. Greenwald, *Comment la NSA espionne la France*, "Le Monde", 21.10.2013, http://www.lemonde.fr/technologies/article/2013/10/21/comment-la-nsa-espionne-la-france_3499758_651865.html (access: 19.12.2014).

[86] A. Matrosov, E. Rodionov, D. Harley, J. Malcho, *Stuxnet Under the Microscope*, Rev. 1.31, ESET, September 2010.

today's sophisticated games, others see an opportunity for mischief or illicit profit"[87]. These risks involve among others: the exploitation of security vulnerabilities, viruses, trojans, worms, spyware, or even social interactions with strangers tricking random users to reveal personal information[88].

Being aware of these examples and their sources, it is therefore important to point out what the major strategic consequences of cyber development paradox in the context of national and international security are.

The first and most evident effect concerns the excessive susceptibility of developed states to various forms of malicious activities in cyberspace. As previously mentioned, societies and governments that have adopted the most advanced solutions in the field of information and communication technologies, have drawn huge political, social and economic profits from the digital revolution. According to the ICT Development Index these are countries like South Korea, Denmark, Sweden, Great Britain or the United States[89]. Such benefits carry, however, a particular price, which was symbolized by the case of Estonia. Before 2007, this country was commonly considered to be one of the most advanced European states. Rising reliability on computers and multiple online services meant, however, that there was a greater need for investment in the field of cybersecurity. This necessity was unfortunately ignored, exposing Estonia to new kinds of threats emerging in cyberspace. Repetitive attacks against Tallinn's computer infrastructure in 2007 shattered its prestige as one of the most successful states in the post-Soviet area. It was also the first time in history when the paradox of cyber development left such a clear mark on international relations[90]. This clearly demonstrates that highly developed countries which are dependent on the reliability of information and communication technologies and pay less attention to computer security problems may be easily harmed through cyberspace. Therefore, developed countries, while drawing multidimensional benefits from the digital revolution, are at the same time more exposed to malicious activities through computer networks, which may have drastic consequences for their national security. It also means that the widespread adoption of new technologies by society and the government should always be accompanied by increased cybersecurity efforts. It was confirmed by the above-mentioned Microsoft report, suggesting that at a certain level of technological sophistication, it is possible to curb malware proliferation[91].

The situation concerning underdeveloped nations is in direct contrast to what developed nations are experiencing. These underdeveloped nations are barely connected

---

[87] E.J. Hayes, *Playing it Safe: Avoiding Online Gaming Risks*, US-CERT, 2006, updated 2008, p. 1.

[88] Ibid. p. 1.

[89] See *Measuring the Information Society*, International Telecommunication Union, 2012, p. 21.

[90] See S. Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, "Journal of Strategic Security", No. 2 (2011).

[91] See D. Burt et al., *The Cybersecurity Risk Paradox*, Microsoft Security Intelligence Report Special Edition, Microsoft Corporation 2014, p. 8.

to the global network and are not dependent on the reliability of ICTs. There are many states around the globe which are almost unaffected by the processes of the information revolution. A range of countries, including many in Africa, are usually reliant on traditional, non-digital solutions, which is disadvantageous for their economy and society, as they possess extremely limited capabilities to gather, store and process data. However, at the same time, being cut off from cyberspace may have some positive strategic effects. In theory, most critical areas of governments and social activities are virtually immune to cyberattacks, as they are not accessible through computer networks. Interestingly the specificity of cyberspace allows such countries to possess advanced capabilities in cyberwarfare. Theoretically they may need only one entry point to the Internet in order to conduct a successful cyber intrusion. This correlation was perfectly symbolized by the case of North Korea. This is a state which maintains almost full control over the use of all digital technologies, such as mobile phones, through computers and Internet access, by its citizens. Moreover, at the end of the 20th century the regime in Pyongyang decided to remain mostly cut off from the Internet. Instead, to satisfy the domestic needs for increased communication, it created a nationwide intranet: *Kwangmyong*. Regardless of this situation, it has developed significant potential to harm other nations in cyberspace[92]. This problem became apparent in 2009, when the North Korean regime carried out repetitive cyber operations against South Korea and the United States. Initially massive cyberattacks against their government websites, as well as the business sector were unsuccessful, but later on they became a unique means to exert additional pressure in the international environment[93].

Both situations reveal interesting interdependences in the field of cybersecurity. Technologically advanced countries, such as the United States, France, Japan or South Korea, theoretically should have greater capabilities to act in cyberspace when compared to the states which draw less benefits from the digital revolution. Reality, however, is much more complicated. The introduction of new devices, services and applications has resulted in greater reliability and a need for an increase in cybersecurity efforts. As a result, often countries reliant on ICT constitute a convenient target in cyberspace, as most sensitive areas of their government's activities, including critical infrastructure, are ICT-dependent[94]. In this context Martin

[92] R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York 2010, p. 19; K. Coleman, *Inside DPRK's Unit 121*, Defensetech, 24.12.2007, http://defensetech.org/2007/12/24/inside-dprks-unit-121/ (20.12.2014).

[93] T. Feakin, *Playing Blind-Man's Buff: Estimating North Korea's Cyber Capabilities*, "International Journal of Korean Unification Studies", Vol. 22, No. 2 (2013).

[94] Even if the state owned networks and computers are relatively well-secured, there are numerous high-value private sector targets, which are susceptible to exploitation. This was proven, for example, by Chinese cyberattacks against corporations working on Joint Strike Fighter project. They eventually resulted in the theft of F-35 technologies, which holds strategic importance for the United States' security. And even if they are resistant to cyber-incursions, there are always individuals, using various Internet services, such as social media, on a daily basis. This constitutes another advantage, which can be exploited by hackers. See D. Alexander, *Theft of F-35 design data is helping U.S. adversaries – Pentagon*, Reuters,

C. Libicki rightly stated that "Given its conventional military power, the United States enjoys the kind of superiority that permits it to be the global cop (...) This is not the situation in cyberspace. The United States may have superior offensive capability – having invested large sums in such capabilities (...) But the United States is also quite vulnerable. Its society, and in particular, its military (...) depend heavily on information systems (...) Thus, the United States, for all its advantages, might suffer more than adversaries would if retaliation begets counterretaliation"[95]. At the same time, nations which are cut off from cyberspace, cannot be seriously harmed by computer attacks, although they may have the potential to carry out such attacks on more developed nations.

This is admittedly a sign of peculiar asymmetry in cyberwarfare between developed and underdeveloped countries, which is non-existent at such an extent in other theatres of war. While underdeveloped countries possess theoretically less capabilities to act in cyberspace, they are also more resistant to cyberattacks. Even if they suffer complete Internet infrastructure outage, it constitutes only a minor problem for their security. Plus, they can operate offensively in an environment which is constantly being enriched with potential targets, such as new Internet services, applications and IoT equipment. On the other hand, countries spear-heading the digital revolution, usually have at their disposal much more advanced offensive and defensive capabilities on the Internet, but they are also exposed in areas, which are not directly under the government's agencies protection. Plus, some developed countries, such as South Korea or Estonia, for many years did not connect technological development with the prioritization of cybersecurity, thus being even more susceptible to network intrusions. Therefore, it has to be stated that there is no equivalent to the M.A.D. system in cyberspace in such an asymmetric situation, as depicted above. An underdeveloped nation committing serious cyberattacks against technologically advanced state enjoys relative impunity on the Internet. This can be compared to a hypothetical situation where a state can attack its enemy with tanks, but at the same time, it cannot be seriously harmed by any armored vehicle. This was perfectly illustrated by the latest Sony Pictures Entertainment hack at the end of 2014. North Korean hackers were able to create popular turmoil in the United States, forcing a reaction from Barack Obama himself, whilst remaining unpunished. In response North Korea's Internet access was temporarily cut off, due to cyberattack in December 2014[96], although it constituted almost no threat to its national security. Moreover, the regime in Pyongyang potentially still held capabilities to counterstrike in cyberspace, us-

19.07.2013, http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619 (access: 05.01.2015).

[95] M.C. Libicki, *Cyberdeterrence and cyberwar*, Santa Monica 2009, p. 31-32.

[96] J. Lee, *North Korea Blames U.S. for Recent Internet Access Cutoff*, Bloomberg, 27.12.2014, http://www.bloomberg.com/news/articles/2014-12-27/north-korea-blames-u-s-for-recent-internet-access-cutoff (access: 05.01.2015).

ing, for example, various hotspots in China. Thus, the only way to seriously punish such cyberattacks is through the use of conventional force, as the United States has suggested multiple times. This solution, however, could be difficult to conduct, both politically and legally.

The third strategic consequence of the cybersecurity paradox concerns the accelerating pace of the development of threats for computers and their networks. Since the 1960s they have evolved at a tremendous pace, starting with traditional hacking, and leading to hacktivism, cybercrime, cyberterrorism, espionage and cyberwarfare[97]. All these forms of threats to national and international security use increasingly advanced means and techniques to harm the users of cyberspace. This transition is easy to see, for instance, 25-30 years ago creating a computer virus was perceived as the pinnacle of hacking skills. Nowadays, there are thousands of pieces of malware released every week, not only worms or trojans, but also rootkits and more complex software, which includes elements of each method[98]. At the same time, hackers frequently use inventive methods, such as SQL injection, buffer overflow, social engineering or numerous botnets. These are only a few of many examples as to how cyberattacks have evolved in recent decades. This specific "progress" is possible not only due to increasing hacking skills and the ingenuity of computer criminals, but also to the logic of digital development. It is effectively constantly opening new possibilities to harm cyberspace users, as every new and unproven piece of technology may be potentially exploited in various ways and can contribute to the creation of new types of cyber threats. Therefore, if these processes do not change in the future, fighting with cybercrime will resemble a battle with a mythical hydra: one countered threat will be replaced by two or three new ones emerging from newly introduced, untested technologies and services.

Finally, the lack of a proper reaction to the paradox of cyber development may also have serious economic and social consequences. It can eventually undermine confidence in new technologies and scientific development in general. Of course, as mentioned above, nowadays, we are witnessing excessive confidence in various technologies, but its absence will have even graver effects, plunging nations into stagnation. Additionally, this phenomenon may also slow down economic development, as losses from cybercrime will continue to rise, which will at the same time lead to a greater need for increased cybersecurity funding. Nowadays, global cybercrime costs are estimated at around $445 billion annually, compared to $114 billion in 2011. This problem was accurately summarized by the Center for Strategic and International Studies

[97] See L. Yagil, *Terroristes et internet. La cyberguerre: essai*, Montréal 2002; M. Milone, *Hacktivism: Securing the National Infrastructure*, "Knowledge, Technology & Policy", (Spring 2003); K. Geers, *Strategic Cyber Security*, Tallin 2011.

[98] See e.g. M. Kjaerland, *A taxonomy and comparison of computer security incidents from the commercial and government sectors*, "Computers & Security", No. 7 (2006).

report published in June 2014, which stated that "the cost of cybercrime will continue to increase as more business functions move online and as more companies and consumers around the world connect to the Internet"[99].

CONCLUSION

The paradox of cyber development is a phenomenon which has emerged in parallel to the information revolution. It has shown that as computers and their networks started to play an important role in different areas of life, it became apparent that the "new better world" founded on ICTs also carries "new graver threats" for security and privacy. In the 21st century this problem became even more apparent, as it was strengthened by the wanton global rush to include digital solutions wherever possible, often, without basic awareness of the fact that it brings new kinds of challenges to society. The phenomenon analyzed in this paper is about the processes that take place during the general rush to adopt new, unproven technologies by societies and states around the world. As the aforementioned examples prove, they frequently harm their own users in the least expected way, contributing to the creation of new kinds of threats to both national and international security. Only adequate cybersecurity efforts and spending may curb these negative trends. It must be noted that the majority of contemporary challenges for cybersecurity are an indirect result of this paradox. As the Korean, U.S. or Estonian cases indicated, these processes also have increasing influence on the course of events in the international environment. Different agents may use this paradox to exert pressure on governments or harm societies in order to achieve their particular goals. It is therefore important to carry out extensive research concerning these problems.

At first glance it may seem that the cost vs. benefit account is crucial when attempting to find an answer to the cyber development paradox. It is, however, not entirely accurate as it would be very difficult to conduct. It is due to the fact that such an account should take into consideration not only the financial dimension, which could be helpful only in the context of cybercrime, but also political, social and security aspects, which are much harder to measure. Therefore, the proper reaction to this paradox should be based on the choice between two priorities: security *versus* political, economic and social benefits. It has to be noted that not all technologies, services and applications that are introduced nowadays, have to be treated *a priori* as profitable. Some, such as "smart watches" for instance, are rather multi-functional gadgets, created more in response to the need for additional revenue, rather than being a genuine necessity. At the same time, they generate dilemmas for the security and privacy of their users. On the state level, this is the case with such ideas as aforementioned, such

[99] *Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II*, Center for Strategic and International Studies, June 2014, p. 3, 6; *Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually*, Symantec, 07.09.2011, http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 (access: 06.01.2015).

as, e-voting, which may potentially destroy the credibility of democratic elections, although this view is completely ignored by many intellectuals. Therefore, it is all about the choice to adopt only the technologies, which are necessary, useful, and secure, both in areas under and beyond the control of the government.

Therefore, understanding the cyber development paradox may be an important factor when tackling the information revolution in such a way that would prevent most of its negative consequences. Otherwise, sooner or later, safe progress will be much harder to achieve, as manufacturers and users of ICTs will repeat the same mistakes over and over again. This paradox must be accepted and understood by policymakers, or else national and international efforts to combat cybercrime or cyberterrorism will be as inefficient as they are at present. It is due to the fact that the, usually unaware, political elites tend to deal with the results, not with the causes of these problems. And the causes lie, among others, in the lack of deliberation during the process of implementation of new technologies among societies. It also must be understood by the societies, which are adopting various, sometimes unnecessary gadgets or services, unknowingly exposing itself on cyber threats.

Finally, it must be stressed, that this paper is not against the digital revolution. There can be no doubt that it improves the quality of life, accelerates economic development and opens new possibilities for political and social activities. Unfortunately, today there is not enough reflection concerning all aspects of these processes. The popular fashion of adopting technology in every aspect of live leads to more harm than good, as there is no essential balance in relations between societies and governments on the one hand, and technology on the other. The information revolution is too serious a thing to be treated without due consideration, which is sadly only visible within a part of the academic community. The political and intellectual elite, decision-makers, and societies themselves should realize that every innovation may not only bring benefits, but also new challenges for the security of nations and the privacy of technology users. If contemporary tendencies are to be strengthened, the community of computer security experts will have to deal with graver threats year after year. Therefore, there is a rising need to slow this, sometimes mindless, rush for technology regardless of price down, by instead following the famous saying of "slow and steady wins the race". The sooner this happens, the sooner the paradox of cyber development will cease to have the far-reaching effect on national and international security that it has today.

Dr Miron Lakomy, Instytut Nauk Politycznych i Dziennikarstwa, Wydział Nauk Społecznych, Uniwersytet Śląski w Katowicach (miron-lakomy@wp.pl)

Słowa kluczowe: cyberbezpieczeństwo, rewolucja cyfrowa, międzynarodowe bezpieczeństwo, ICT, paradoks cyberrozwoju, cyberwojna

Keywords: cybersecurity, digital revolution, international security, ICT, paradox of cyber development, cyberwarfare

ABSTRACT

The rising pace of technological development in the 21st century is frequently met by widespread "folly", to be always up-to-date with the latest trends and fashions, especially in the sensitive and ever changing area of IT. Humanity is contributing and increasing the flood of technological innovations, blindly assimilating all electronic devices, including some which appear to be completely unnecessary. Almost no one asks: where are the boundaries and at what point do hi-tech pursuits cease to make sense? The pace and scope of development raises legitimate doubts, as it is outpacing the growth of deepened intellectual reflection. Therefore, this paper argues that the more that ICTs are introduced thoughtlessly into different areas of life, the greater the challenges, resulting from their improper use, we face. Such correlation is visible at a glance, but so far there has been little effort to understand the causes and strategic consequences of this profound paradox of digital revolution.