EUROPEAN E-READINESS? CYBER DIMENSION OF NATIONAL SECURITY POLICIES[1]

Uroš SVETE[2]

The majority of social processes have become very dependent on information and communication technologies (ICT) according to their quick development and increasing use. With the emergence of new technologies and growing dependence of society on ICT, threats have emerged, which experts described as new. Information security or cyber dimension of national security has thus become an increasing priority for the countries, but they face these new threats differently. This article contains a specialized in-depth analysis of the situation of ICT in Estonia, Switzerland, Sweden and the United Kingdom. The selection of the countries was based on their ICT development, experience with information threats and membership in various political and security organizations. We examined the following indicators: the incidence of threats, normative (legal) acts and actors who are responsible for assuring information security. These indicators subsequently allowed us a detailed understanding of ICT threats faced by selected countries and their responses to them.

1 INTRODUCTION

Today, the modern and technologically advanced state is undoubtedly facing the greatest structural change since the fall of the Berlin Wall and the end of the Cold War, referring to its economic, political, information and nonetheless security role. In our analysis, the latter is especially going to be emphasised, as the attitude towards the question of security has recently undergone a fundamental change, whilst the information dimension has become one of the key sources of social power.[3] Cyberpower is now fundamental fact of global life, while in political, economic, and military

[1] The article was written on the basis of a research study conducted by Primož Bizjak, Tea Bizjak, Gregor Čehovin, Matej Čerpnjak, Tjaša Karničar, Tomaž Kregar and Maša Žunič Marinič working under the author's mentorship at a postgraduate subject Information Technology and National Security.

[2] Uroš Svete is employed as an Assistant Professor at the Faculty of Social Sciences, University of Ljubljana. His main research fields are (non)military security, crisis management and conflict resolution as well security implications of the information-communication technology use. He is a member of ERGOMAS (European Research Group on Military and Society), ISA (International Sociological Association), SPSA (Slovene Political Science Association). At the moment he is an Executive Secretary of ISA Research Committee 1 (Armed Forces and Conflict Resolution).

[3] Christian Fuchs, *Internet and Society: social theory in the information age* (New York, London: Taylor & Francis, 2008), 99.

affairs, information and information technology provide and support crucial elements of operational activities.[4]

Throughout the human history, technological-technical revolutions have always been a matter of security dimensions as well. However, few had had such a profound impact on the power relations as it has been the case with the information and communication technologies (the ICT) and the related information revolution. Even though we often think that the Cold War Era was primarily marked by the nuclear arms race and the struggle for resources in the physical (real) space, more and more authors have been looking for causes of the well-known outcome of this period as well as the final domination of the Western world in the development of information technology and its influence both on weapons systems and the ways of operation of both military and non-military organizational structures.[5] In spite of differing explanations of causes and intentions that eventually led to the Internet's predecessor, the ARPANET,[6] an increasing consensus is emerging that the rise of the Internet-Protocol-based ICT and the creation of cyber space have undoubtedly changed the fundamental aspects of literally all social subsystems as well as the individual's role within them. Regardless of how we assess the events of the late 1950s and early 1960s that brought about the informatisation of the world, there is no doubt that the cyberspace and security sector have been interrelated from the beginning, both in theoretical-conceptual and empirical sense, whereby their relationship has been of inverse-deductive character.

Hence, the discourse of a new conceptualisation of security is completely understandable. It is the looks or the external image of security that has changed so much. Apart from national, state and individual security,[7] we nowadays also speak of cyber security, which is becoming more and more equivalent an agenda in the more developed states.[8] Nevertheless, information or cyber threats are still so "new" that they are still fairly unresolved, especially as concerns international law. However, the only certainty regarding them is that these threats take place in the virtual space of the critical information infrastructure (the CII) and with the assistance of the ICT. Cyber threats to security are connected with the use of modern ICT. And they refer to cybercrime, espionage, terrorism, extortion, misleading, scams and information warfare. Recently, an increase in acts of cybercrime has been detected, causing an estimated $1,000 billion of damage globally

[4] Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, ed. Franklin D. Kramer et al (Dulles: Potomac Books, 2009).

[5] Janez Škrubej, *Hladna vojna in bitka za informacijsko tehnologijo* (Ljubljana: Pasadena, 2008); see also Alexander Klimburg, ″Mobilising Cyber Power,″ *Survival,* 53, 1 (2011), 41–60.

[6] Charles Herzfeld, ARPA Director (1965–1967) argued The ARPANET was not started to create a Command and Control System that would survive a nuclear attack, as many now claim. To build such a system was, clearly, a major military need, but it was not ARPA's mission to do this; in fact, they would have been severely criticized had they tried. Rather, the ARPANET came out of our frustration that there were only a limited number of large, powerful research computers in the country, and that many research investigators, who should have access to them, were geographically separated from them (http://arpanet.co.tv/). On the other hand, however, Škrubej sees the main initiators of this network's development in the tendencies towards setting up a command and communications network that would survive even a nuclear attack.

[7] In the 1960s more complex definitions of national security appeared. According to the liberal and especially the constructivist critical security theory, the foci and security agenda had moved from the national state level towards non-state actors. But the new security understanding ("new security") did not acquire significant legitimacy until the end of the Cold War, when human beings/individuals as reference objects of security had been exposed to the collapse of the static bipolar world order and influence of the globalization (the concept of human security). See Edward Newman, ″Human security and constructivism,″ *International studies perspectives,* 2, 3 (2001), 239–251.

[8] See *Dealing with Cyber Security: Accept vulnerability.* Issue Brief 1, 2011. World Foresight Forum. Available at http://www.worldforesightforum.org/data/spaw/files/WFF/Publications/WFF_Issue_Brief_Cyber_Security_420x297_HR.pdf (15 December 2011).

every year.[9] But cyber security will include not only technical issues, but also human matters –such as insider deception as well as normal human mistakes – and the problems of governance, both national and international.[10]

Considering that, in 2010, there were approximately two billion Internet users (Internet World Stats)[11] and that the cyberspace is decentralised (the Internet and the IP protocols operate without a single central server), we can assume with certainty that cyber threats are going to be an ever increasing security as well as a general social problem.

This article provides for a comparative analysis of the development in the sphere of information security in Estonia, Sweden, Switzerland and the United Kingdom of Great Britain and Northern Ireland. These states were selected according to their informational development and experience with information threats, their membership in different political and security organisations, such as the EU and NATO, and, last but not least, due to their varying size, which is a matter of relevance. Namely, the selected states derive from differing strategic-cultural patterns and the culture has become fashionable in the mainstream international relations scholarship in the Post-Cold war era. One of the most surprising aspects of the renaissance of scholarly interest in culture has been the emerging consensus in national security policy studies that culture can affect significantly grand strategy and state behaviour.[12] According to that finding we have chosen Switzerland which has maintained its military and political neutrality for several centuries and its stability has enabled it to develop one of the best and most stable banking systems in the world. On the other hand, Estonia has gone through a period of post-Cold-War transition and it is one of the few states that have experienced an all-out cyber attack, which left almost its entire critical infrastructure paralysed for several days. Sweden is a neutral Scandinavian state with a high level of ICT use that invests a lot in innovations. Yet the United Kingdom is a state belonging to the Anglo-Saxon political and value model, showing a relatively strong transatlantic orientation. Although we are aware of the fact that different states have had different experience in the field of ICT security, we are primarily interested in the similarities between models, since analyses and experience of this kind are of great importance in terms of providing information security in other countries.

Even though it may seem that researchers have an easy access to the sphere of information security, the empirical aspects of reality show a completely different picture. It is especially difficult to get the data on the number of attacks or incidents, be it either due to the classified nature of systems or due to companies' unwillingness to disclose the aforementioned data for reasons such as their market positions or the possibility of losing their customers' trust. Hence, the relevance of information or cyber threats can be studied indirectly, including the analysis of normative acts concerning information security, as well as it is important to identify the more prominent

[9] See HM Government. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Available at http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf (18 June 2011), 29.

[10] Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, ed. Franklin D. Kramer et al (Dulles: Potomac Books, 2009).

[11] More precisely, 1,966,514,816; of this figure almost 500 million in Europe, which is an increase of 352% over the year 2000.

[12] Jeffrey S. Lantis, ″Strategic culture and national security policy,″ *International studies review*, 4, 3 (2002), 87.

policy actors and stakeholders, the perception of threats and the influence of external actors on the development of policies.

2 THE STATE OF ICT IN THE SELECTED EUROPEAN STATES

Information security and stability of the studied issue is of paramount importance for Switzerland. This state is interesting to analyse for several reasons, the most important being that it is neither a member of EU nor of NATO, yet it is a member state of the EFTA. It is one of the most developed states in terms of economy and its power is mainly drawn upon the financial sector. Switzerland has been pursuing a policy of armed neutrality for a long time and it maintains its national defence according to the principle of militia. Switzerland has a population of approximately 7.7 million, among which about 80% of those over 14 years of age use the World Wide Web services.[13] The Global Competitivness Index, annually updated by the Global Economic Forum ranked Switzerland as the first among 139 countries.[14] According to this report, the state, among other things, puts the greatest emphasis on the development of innovations and infrastructure, which includes the information and communication infrastructure.

State and public administration, traffic, vital supplies, communication and economy are heavily dependent upon the operation of information systems, which is also stressed by the umbrella document, i.e., the Report of the Federal Council to the Federal Assembly on the Security Policy of Switzerland (henceforth, the "Report").[15] In 2010, the Global Information Technology Report ranked Switzerland as the fourth among 138 countries worldwide, based on the ICT index. The only three countries ranking higher were Sweden, Singapore and Finland.[16] The reasons given above plus the obvious interweaving of different systems and information technology have stimulated the studying of this state's information security.

The second state included in our analysis is Great Britain. According to the ITU for 2010, 82.5% of its citizens use the Internet, making it one of the leading EU Member States in this respect.[17] The ever increasing e-inclusion of citizens simultaneously entails that they rely more and more on the ICT, which in turn opens greater possibilities for various cyber threats.[18] The provision of cyber security has thus constantly been gaining salience as the number of individuals who do not use the Internet has been persistently decreasing. In its document, Manifesto For a Networked Nation, the British government sets a goal claiming that, by 2012, the country is due to get as close as possible to the situation in which everyone is an Internet user.[19]

[13] See *Zum Stand der Informationsgesellschaft in der Schweiz 2010.* Bericht des Interdepartementalen Ausschusses zur Umsetzung der bundesrätlichen Strategie Informationsgesellschaft, Februar 2011. Available at http://www.bakom.admin.ch (15 December 2011), 2.

[14] See *Global Competitiveness Report 2010–2011.* Available at http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2010-11.pdf (30 June 2011).

[15] See *Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz*. SIPOL B2000, June 7, 1999. Available at http://www.sog.ch/uploads/media/SipolB2000.pdf (3 May 2011), 13.

[16] See *Global Information Technology Report 2010–2011.* Available at http://www3.weforum.org/docs/WEF_GITR_Report_2011.pdf (3 July 2011).

[17] See *Internet World Stats.* Available at http://www.internetworldstats.com (25 April 2011).

[18] HM Government. 2010a. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Available at http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf (Accessed on 18 June 2011, p. 29-47).

[19] See *Race Online 2010*. Available at http://raceonline2012.org/faqs (May 10 2011).

The British National Security Council rates cyber attacks performed either by other states or organised criminal groups and terrorists among the four threats of the highest priority for the next five years. The Council hence places cyber threats side-by-side to the international terrorism, international military crises and large-scale or natural disasters. The newest British National Security Strategy explains that United Kingdom is currently not facing military threats but that there are states that want to improve their position by using certain methods such as cyber attacks and espionage. With the use of cyberspace, the latter can be conducted from a safe distance, which further compromises the possibility of identifying the sources of such attacks and reduces political risks associated with espionage. This is but one example indicating that contemporary world calls for a consideration of more and more elements in the provision of national security, as the picture of potential threats is a far cry from the predictability of the Cold-War era.[20]

Estonia, which is a member of both EU and NATO, is among the world's most informationally developed states. Global Information Technology Report 2009-2010 places Estonia in the 23rd place regarding households' access to the Internet, whereas it is used regularly by 75.1% of the state's population. The growth rate of broadband connections is increasing and is currently at 24.6%. According to the data by World Bank, the Estonian GDP per capita is $14,060 and a quarter of the entire research and development (R&D) budget is allocated to the ICT domain, yet this budget has been decreasing.

Estonia is the first state that practically implemented e-elections in 2005 and enabled e-voting at 2007 parliamentarian elections.[21] In Estonia, 98% of all banking transactions and 82% of all tax returns are performed via the Internet. Additionally, most Estonian schools use e-learning. Personal ID cards and digital signatures have become part of everyday life both in public as well as private sectors.[22]

However, because of a rapidly developing information society, the state has become more susceptible to information systems' abuse on the part of terrorists and criminal groups. Hence, Estonia is one of the few states that have already faced an informational/cyber attack on the nation-wide scale, as many governmental web servers, banking and information services were out of service for two weeks.[23]

In terms of our research topic, Sweden is another country of great interest, as it is a member of the European Union, but not of NATO and is regarded as one of the most informationally developed states in the world. This is confirmed by the Global Information Technology Report 2010-2011 published by the World Economic Forum, which places Sweden first among all the states worldwide as regards the status of the most networked economies (i.e., the most digitally developed/connected economies). In this respect, Sweden has the most suitable environment for the development of

[20] See HM Government. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Available at http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf (18 June 2011), 14, 18, 27.

[21] See ENISA. *Estonia Country Report, 2010*. Available at http://www.enisa.europa.eu/act/sr/files/country-reports/Estonia.pdf (13 May 2011), 5.

[22] See *Cyber Security Strategy.* Ministry of Defence – Estonia. 2008. Available at http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf (13 May 2011), 12.

[23] Uroš Svete and Uroš Pinterič, *E-država: upravno – varnostni vidiki* (Nova Gorica: Fakulteta za uporabne družbene študije, 2008).

the ICT, which is contributed to by the state-of-the-art and highly developed information infrastructure plus a very good normative arrangement as well as a favourable market environment.

The data provided by the World Bank[24] indicate that Swedish economy, having $48,840 of GDP per capita, is one of the most developed European and global economies. A large portion of its economy is represented by the ICT industry, therefore it is not surprising that, already in 2003, Sweden allocated approximately one third of its entire R&D budget, which was about 1% of its whole GDP back then, to the sphere of ICT.[25]

Obviously, Sweden has been pursuing an explicitly positive policy towards the ICT and it could also be argued that it has not only been striving for developing any kind of information society, but for a modern or the most advanced one. This is confirmed by the fact that, in 2010, 92.5% of the entire Swedish population was using the Internet, which makes Sweden second only to Iceland and Norway.[26] At the same time, the state has been attempting to digitalise its operation as much as possible and to enable access to public or state services via the Internet (in the form of eHealth, eGovernemnt, ePublic Administration, etc.) and to bring them even closer to its citizens.

However, such growth in the dependency of the workings of the entire society on the ICT also brings its own pitfalls and security risks, a fact Sweden is well aware of. In the field of security or defence, Sweden once again represents a special case, since it has developed the so-called concept of “total defence”, which is evident in the provision of information security as well. Namely, the state has been pursuing a very holistic approach towards tackling these threats. In its analysis of threats and the formulation of corresponding solutions, Sweden has not limited its scope only to its own problems, but it has also paid due attention to difficulties other informationally developed countries have so far encountered. Apart from state actors, Sweden has also engaged private businesses and individuals working in the ICT domain in order to confront the threats to information security. Evidently, Sweden has, at least in part, transferred its concept of total defence into the field of information security provision, which is actually a responsibility of each and everyone connected with the ICT in some manner.

3 THE PERCEPTION OF CYBER THREATS IN THE SELECTED STATES

Switzerland strongly stresses the perception of threats by its citizens and service users, who have the possibility of reporting irregularities to the competent state authorities. Due to its position within the international community, this state is exceptionally sovereign in its operation, which, however, does not entail that it pays no attention to developments in its close and/or distant surroundings. Among the perceived threats in 2010, the

[24] See *World Development Indicators 2011.* Washington: The World Bank, 2011. Available at http://data.worldbank.org/data-catalog/world-development-indicators, (15 May 2011).

[25] See *Sweden: ICT star.* Global Technology Forum, 2009. Available at http://globaltechforum.eiu.com/index.asp?layout=rich_story&doc_id=10697&title=Sweden%3A+ICT+star&categoryid=29&channelid=4 (18 May 2011).

[26] See *International Telecommunication Union*. Available at http://www.itu.int/en/pages/default.aspx (12 May 2011).

most important ones were attacks on the Supervisory Control and Data Acquisition (SCADA) ICT systems, inaccessibility of certain websites, which is designated as the DDoS (Deliberate Denial of Service Attack) in the international environment, computers logging into malicious networks (i.e., the Botnet), illegal acquisition of sensitive data, such as passwords, usernames, credit card numbers, etc. (phishing), permanent threats, such as computer viruses, worms, Trojans and spam, misleading e-messages, known as hoaxes, spyware and so on. There have been more and more perceived attacks on mobile telecommunication devices, such as “smart” mobile phones.[27]

These claims are corroborated by some statistical data acquired from state services entrusted with the task of providing Switzerland’s information security. These data show the percentages of specific threats reported by the inhabitants of Switzerland, as follows: spam (19.5%), hard pornography (17.8%), absence of age checking for access to such contents (14.9%). The incidence of fraught has been on the increase,[28] as it comprised 4.6% of reports over the studied period, corresponding to an 86-% increase in the numbers of this type of threats. Internet-based business crime has been on the decrease and reached “only” 3.3% of all reported perceived threats and dangers, which is 8 per cent less than the rate recorded in 2007 – 11.3%.[29]

Very important is also an awareness of political establishment, cyber threats are not coming just from individual hackers. So Swiss defence minister Maurer stressed that the danger no longer comes from single individuals, but rather from organisations or even states that seek potentially damaging information about a country and its businesses and institutions. Maurer also said that the massive amount of investment made in cyber-security in the past by Switzerland may not be enough now and added that threats could target mainly the energy, gas, transport and water sectors.[30]

A trend of increasing international cooperation for providing ICT security can be observed in Switzerland. Being a highly developed state and a member of the EFTA, it is of interest to Switzerland that it maintains and provides a high degree of security also for the CII systems, as this preserves its credibility in the international community and on international (financial) markets. Efforts for increasing information security had amounted to the first pan-European exercise in the context of critical infrastructure protection under the name of Cyber Europe, which took place on November 4, 2010 and checked the response capabilities of EU and EFTA Member States in case of a cyber attack. This exercise saw the participation of 22 states with 150 experts from 70 public services. It was led by the European Network and Information Security Agency (the ENISA) and Switzerland took part in it as well. Even though the readiness for such threats was found to be good, the ministers of participating states agreed on additional increase of information security.

[27] See *Informationssicherung. Lage in der Scwheiz und international*, 2010. Half-year report (July–December). Available at http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdIF7hGym162epYbg2c_JjKbNoKSn6A-- (12 May 2011).

[28] In our case, the category of fraud encompasses the activities associated with internet scams conducted by using the ICT.

[29] See *Koordinationsstelle zur Bekämpfung der Internet-Kriminalität KOBIK, Jahresbericht 2010*. Available at http://www.fedpol.admin.ch/content/dam/data/kriminalitaet/internetkriminalitaet/KOBIK/rechenschaftsbericht-2010-de.pdf (10 May 2011), 3.

[30] See *Switzerland »vulnerable to cyber attacks«*. The Local, 20 June 2011. Available at www.thelocal.ch/361/20110620/ (12 December 2011).

In Swiss debates over information security, experience and conceptual development of the NATO have also been taken into account. Swiss authorities carefully monitored Lisbon NATO Summit where achievements and results of Member States' exercise, dubbed the "Cyber Coalition 2010", were stressed. It is noteworthy that, in its Report, Switzerland complies with and pursues the same goals as NATO, that is, energy and information security. Switzerland has been very carefully considering foreign experience and has been attempting to implement the good practices of organisations and states in its legal order, even though it is not a member of the international organisations concerned.

As we have already found out, Sweden is one of the most informationally developed states in the world. The ICT is now embedded in literally every aspect of Swedish society. This means that the (efficient) performance of a society or a state, and consequently, of an individual, has been more and more ICT-dependent. Even though ICT allows for easier and faster execution of various (social and state) functions, the increase in this dependence also means a growing degree of vulnerability and security issues in case of errors, accidents or attacks on these systems. Considering that Sweden is among the most informationally developed states in the world, it comes as no surprise that it tops the ranks in terms of the number of incidents related to cybercrime. In the recent years, Sweden has been experiencing increases in ICT-related criminality. Its state institutions have perceived the following threats as the most frequent ones: hacking into computer systems, infections with computer viruses, information thefts, unauthorised data manipulations and hoaxes. According to the 2010 data by National Council for Crime Prevention,[31] there were 852 acts of Internet-based hoaxes and 299 acts related to Internet child pornography (19% increase over 2009), constituting criminal offences, plus 420 cases of crimes against the Law on personal computerised information, a 72-% increase over the previous year.

Phishing, which is often used in the financial sector, represents another significant problem. Since 2006, when Swedish bank Nordea suffered $1.1 million worth of damage, caused by the use of malicious software, banks have been intensively engaging this issue.[32]

An extraordinarily frequent way of attacking information systems is the DDoS, which most often affects websites of Swedish state institutions, political parties and larger companies. The number of these attacks has increased significantly since the arrest of Julian Assange in late 2010 in Great Britain, with websites of Swedish government being the primary targets. Additionally, Swedish governmental institutions claim that criminal acts performed via the Internet are becoming more and more sophisticated. There has been a growing number of carefully pre-planned cyber attacks, using a wide and branched (complex) network of hijacked or hired computers (according to certain data of the Swedish Civil Contingencies Agency, there were about 27,000 botnets in 2008 in Sweden), which makes the finding of perpetrators much more difficult.[33]

[31] *See National Council for Crime Prevention*. Available at http://www.bra.se/extra/pod/?action=pod_show&id=1&module_instance=11 (17 June 2011).

[32] Francois Paget, *Cybercrime and Hacktivisim* (Santa Clara: McAfee, 2010).

[33] See Swedish Civil Contingencies Agency. *Information security in Sweden: Situation assessment 2009*. Stockholm: Swedish Civil Contingencies Agency. Available at https://www.msb.se/Upload/Produkter_tjanster/Publikationer/MSB/0119_09_Information_security_in_Sweden.pdf (12 December 2011).

State services' report also warns Swedish government of insufficient readiness for possible attacks and malfunctions of the ICT. Network and/or computer systems errors have already crippled the operation of the governmental system, media and even health services.[34] Thus, Sweden has been encountering numerous forms of threats to information security and has developed a vast array of actors to counteract them. Apart from threats directly affecting it, Sweden constantly monitors international or global developments concerning information security (e.g. cyber attacks on Estonia and Israel/Gaza information operations). In Sweden's opinion, efficient provision of information security is only possible through continuous development of technology, formation of a unified legislative framework and monitoring of users' behaviour patterns. At the same time, Sweden sees deepened and intensified international cooperation (especially so within the EU) as a countermeasure against the information threats.[35] Sweden is actually well aware that the provision of information security is a key component of the (wider) provision of national security.

Great Britain, just as Switzerland and Sweden, also describes ICT threats as deserving the greatest possible attention. Therefore, the protection of cyberspace is one of its top national security priorities. There is a whole range of cyberspace risks, ranging from hostile attacks from other countries to people using it for terrorist purposes and, what may be the most evident one, cyber criminals. However, Internet still enables many possibilities for its every user. Such Internet-related dangers and possibilities will probably undergo a significant increase over the next five to ten years and so will the dependence on web communications and transactions. Hence, security of the use of ICT is now more important than ever before.[36]

The most prevalent threats in Great Britain are Trojans and adware, representing 33.7% and 21.1% of infections, respectively, whereas the most common Internet incidents are virus attacks (34%), phishing attacks (22%), online identity thefts (21%) and e-mail or website hoaxes (15%).[37] In the United Kingdom, there is a strong awareness of the dangers cyber attacks pose. This topic is often written about in the media, which provides for the wider public's awareness, a crucial component in the provision of information security culture.

For many years now, large numbers of attempted hacks and various cyber threats that could compromise national security have been recorded. In one of his speeches, the Chancellor of the Exchequer (i.e., the minister of HM Treasury) said, inter alia, that there were over 20,000 malicious e-mails sent into governmental networks every month. The HM Treasury Department has been the most exposed to attacks, as in 2010, hundreds of serious and pre-planned hacking attempts against its computer system were performed.[38]

[34] See *Cybercrime: An Annotated Bibliography of Select Foreign-Language Academic Literature.* Washington DC: Library of Congress, 2009. Available at www.ncjrs.gov/pdffiles1/nij/231832.pdf (22 May 2011).

[35] See Swedish Civil Contingencies Agency. *Information security in Sweden: Situation assessment 2009*. Stockholm: Swedish Civil Contingencies Agency. Available at https://www.msb.se/Upload/Produkter_tjanster/Publikationer/MSB/0119_09_Information_security_in_Sweden.pdf (12 December 2011), 27.

[36] See *GSO Annual Report 2010*. Available at http://www.getsafeonline.org/media/Get_Safe_Online_Report_2010.pdf (25 May 2011).

[37] See *GSO Annual Report 2009*. Available at http://www.getsafeonline.org/media/GSO_Report_2009.pdf (26 May 2011).

[38] See Osborne, George. *HM Treasury Press Notice 48/11: Speech by the Chancellor of the Exchequer.* Rt Hon George Osborne MP, at Google Zeitgeist 2011. Available at http://www.hmtreasury.gov.uk/press_48_11.htm (19 May 2011).

Organised criminal groups are no exception when it comes to ever more frequent use of the ICT, either.[39] In 2010, a special unit of British police forces for e-crime, in cooperation with the banking sector, exposed and foiled a criminal association of Eastern Europeans that operated in the Essex area and had managed to steal up to £20 million from current accounts of British citizens during its entire lifetime. Every month, the association was able to gain £2 million only by stealing data needed to log into the banking system, whereby criminals were using sophisticated software and the entire operation was allegedly coordinated by the gang boss using only a single laptop.[40]

3.1 Cyber attacks as a threat to national security: the case of Estonia

The Estonian cyber conflict in the spring of 2007 has attracted a great deal of interest. Some describe the case as the first official and publicly described cyber war against a country. Others point out that it was not a war but a cyber riot. Nevertheless it was the wake-up call showing the potential risks of hacktivism.[41] Although there is no hard evidence linking the Russian government to the cyber attacks launched against Estonian government websites during the week of April 27, 2007, at least one prominent Russian Nashi youth leader, Konstantin Goloskokov, has admitted his involvement along with some associates. Goloskokov turned out to be the assistant to State Duma Deputy Sergei Markov of the pro-Kremlin Unified Russia party.[42]

Attacks, which began on April 27, 2007, occurred in three waves in which 128 DoS (Denial of Service) attacks, aimed at the entire Estonian information system, were conducted. The first wave of attacks began only hours after unrest and massive demonstrations of members of Russian minority had broken out in Tallinn, due to the removal of the Red Army memorial. DDoS attacks targeted Estonian Internet service providers and governmental websites and caused a drastic sudden upsurge in incoming web traffic into Estonia, while posts appeared on Russian forums giving instructions on how to perform ICMP (Internet Control Message Protocol) attacks.

On April 30, another wave of attacks followed, this time causing overload and unavailability of the parliamentarian server for two days. It began with the publication of the list of e-mail addresses of members of Estonian parliament who had voted in favour of memorial's removal. This was followed by an appeal to spread the list through the Internet as quickly as possible. Hackers also broke into the Reform Party's website and published a forged written apology of Estonian Prime Minister concerning the removal of the memorial.

The third wave of attacks was taking place between May 3 and May 9, with the highest level of severity and frequency of assaults. The largest of them happened on May 8-9 when data traffic was at 400 times the normal levels, thus causing a 200-fold increase in network loads. About one million

[39] See *The United Kingdom Threat Assessment Of Organised Crime 2009/10*. Available at http://www.soca.gov.uk/about-soca/library/doc_download/54-the-united-kingdom-threat-assessment-of-organisedcrime.pdf (26 May 2011), 53.

[40] See Gill, Charlotte. 2010. *Hi-tech crime police quiz 19 people over internet bank scam that netted hackers up to £20m from British accounts*. Available at http://www.dailymail.co.uk/news/article1316022/Nineteen-arrested-online-bank-raid-netted-20m.html (23 May 2011).

[41] See Heickerö, Roland. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. Stockholm: Swedish Defence Research Agency, 2010. Available at www2.foi.se/rapp/foir2970.pdf (12 December 2011).

[42] Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol: O'Reilly Media Inc., 2009).

computers from all around the world (USA, Canada, Brazil and Vietnam) simultaneously sent requests at Estonian websites. During the day, additional new 58 DDoS attacks followed, forcing the two largest Estonian banks to stop all transactions for several hours, inflicting millions of dollars of damage upon them.[43]

Estonian web pages were also attacked by the SQL injection[44] and users of Estonian mobile networks were receiving false SMS messages claiming they had been sent by the Estonian government. Apart from hackers, Script kiddies[45] also played an important role.

Larger attacks finally ended on May 28 and its aftermath included a total inoperability of the parliament, a majority of ministries, political parties, larger media companies, banks and the Estonian Telecom. Electronic banking and governmental communications were broken as well. Additionally, attacks caused great surprise among the citizens as they were unable to perform most of the Internet-based services. Estonian government accused the Russian government of performing the attacks right away and Tallinn immediately activated the EU and NATO mechanisms and demanded the instant adoption of the Strategy for Preventing Cyber Attacks.[46]

4 COMPARATIVE ANALYSIS OF THE STRATEGIC IMPORTANCE OF CYBERSPACE IN NATIONAL SECURITY FRAMEWORKS

The formulation of a national security strategy is a priority of the state and, at the same time, it represents a fundamental normative stipulation that identifies the threats and directs the development of a national security policy. In its national security strategy, Great Britain defines cyber attacks on individuals, organisations and the state not as something that may happen in the future, but sees them as a threat of today, which is one of the reasons that Britain has identified the need for immediate action. Great Britain is already too dependent on cyberspace, which has become deeply woven into its society and is an element of both economy and security, to afford ignoring any of the more significant risks that obtain from such a situation. Moreover, we can expect the cyberspace-related threats to increase substantially in the next 10 years, as the country's dependence on ICT is going to further increase with the implementation of the third generation of Internet (a.k.a., the Internet of Things). On the other hand, provision of a suitable level of cyber security in all areas represents a basis for a better assertion of state's comparative advantages in the future.[47]

How implementation of elements presented by the National Security Strategy should proceed is defined by the SDSR – Strategic Defence and Security Review), which also anticipates the establishment of the Defence Cyber Operations Group. One of its tasks is to assure the

[43] Ibid.

[44] Attackers use SQL injection for stealing and manipulating confident data and for compromising the system.

[45] Persons lacking deeper computer knowledge who use hacking tools developed by others that are publicly accessible, precisely following the instructions in the process.

[46] See Traynor, Ian. *Russia accused of unleashing cyberwar to disable Estonia*. Available at http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (1 June 2011).

[47] See HM Government. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Available at http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf (18 June 2011), 29; see also HM Government. S*ecuring Britain in an Age of Uncertainty: The Strategic Defence and Security Review.* Available at http://www.cabinetoffice.gov.uk/content/securing-britain-age-uncertainty-strategic-defence-and-security-review (10 May 2011), 47.

interconnectedness of country's cyber and traditional military capabilities. The group is thus going to bring together experts from all the fields related to defence, so that they will be able to support Great Britain's and allies' cyber operations with a view to protecting the key networks and developing new cyber capabilities.[48]

The National Security Strategy builds upon the first cyber security strategy adopted by Great Britain in 2009 and, as far as cyberspace is concerned, it especially emphasises risk reduction, seizing the opportunities and improvements in capacities of knowledge, capabilities and decision-making.[49] Currently, a new version of cyber security strategy is being prepared and it is going to elaborate on the objectives defined by the National Security Strategy and the Strategic Defence and Security Review and will include guidelines for offensive responses of the state against potential cyber threats.[50] In the Strategic Defence and Security Review, the UK government also prepared a plan for introducing the National Cyber Security Programme intended to reduce the gap between the demands of modern economy on the one hand and ever increasing threats related to cyberspace on the other. The government is going to allocate a sum of £650 million in support of this programme during the next four years.[51]

Actors cooperating in this domain are numerous and operate in different specialised areas. The supreme body within the government responsible for network and information science is the Office of Cyber Security and Information Assurance (OCSIA), organised within the Government's Cabinet Office and is entrusted with the planning of cyber security and controlling other bodies regarding the attainment of strategic cyber objectives (http://www.cabinetoffice.gov.uk/content/cyber-security). The monitoring of health within the cyberspace is the task of the Cyber Security Operations Centre (CSOC), which also serves as a coordinating body when measures are applied in response to incidents. Department for Business, Innovation and Skills (BIS) is an advisory body offering consultations to businesses operating in the UK, informing companies of security and encouraging them to adopt security measures that would help towards establishing good practice cases of security within the UK business community. The Home Office bears the main responsibility for controlling computer crime and protecting the UK's key national infrastructure. In order to reduce the vulnerability of state infrastructure to terrorism and other threats, the Centre for the Protection of National Infrastructure (CPNI) offers security consulting to businesses and organisations that set up the national infrastructure. The national technical body, Communications-Electronics Security Group (CESG), provides information, consulting and assistance to the government and other organisations as regards important information services. The Information Assurance Policy and Program Board (IAPPB) and the Chief Information Officer (CIO) Council from the Cabinet Office are responsible for implementing the NIAS (National Information Assurance Strategy). Several organisations from the academia and industry participate in various stages

[48] See HM Government. S*ecuring Britain in an Age of Uncertainty: The Strategic Defence and Security Review.* Available at http://www.cabinetoffice.gov.uk/content/securing-britain-age-uncertainty-strategic-defence-and-security-review (10 May 2011), 27.

[49] See *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space.* Cabinet Office. 2009. Available at http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf (5 May 2011), 1–7.

[50] See Marshall, Rosalie. *UK to launch cyber offence strategy to prevent attacks*. Available at http://www.v3.co.uk/v3-uk/news/2074991/uk-set-launch-cyber-offence-strategy-prevent-attacks (31 May 2011).

[51] See HM Government. S*ecuring Britain in an Age of Uncertainty: The Strategic Defence and Security Review.* Available at http://www.cabinetoffice.gov.uk/content/securing-britain-age-uncertainty-strategic-defence-and-security-review (10 May 2011), 47.

of developing and implementing the national policy on data protection. The Information Commissioner's Office (ICO) takes care of data and privacy protection.[52] Also, the Home Office and the Metropolitan Police have established a special police unit that is specialised in e-crime, designated Police Central e-Crime Unit.[53]

Additionally, Great Britain also has many different Computer Emergency Response Teams (the CERTs), namely 2 in the government, 1 military, 11 for users, 3 research and educational plus four others,[54] which perform specific tasks.

Similarly, Switzerland adopted a consolidated document at the level of national security strategy under the name of Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz.[55] This Report was adopted in 2010 and has been the only one after 1999. Notably, 11 years had passed between the two reports, which is definitely (too) long a period for the information age.

In this Report, information is referred to as "an increasingly important good".[56] As a consequence, attacks against information and communication infrastructure are defined as a direct threat and danger to the state, as this infrastructure is the main conductor of information. Compared to the 1999 Report, the threats and dangers to information and communication infrastructure are now placed as 6th instead of 7th in the 2010 Report and are now unambiguously defined in greater detail. What is new in this report is the definition of threats and dangers to the CII that have a high probability in the next 10-15 years and would have a medium-size impact on the state. This is related to the fact that the CII is a key component of critical infrastructure's elements, which could primarily be affected by threats and dangers at electronic level.

With the intent to facilitate the operation of the Swiss CII society, the Federal Council adopted the Information Society Strategy in 1998 and then remoulded and amended it in 2006. The aim of this change was a quick, coordinated and useful introduction of ICT into the society and its organisations. State and public administration began an accelerated implementation of e-governance or e-services, such as e-health.

There are several stakeholders involved in the formulation of legal order that guarantees the provision of a suitable level of ICT security; hence the policy is formulated by different national-level actors. We are going to present only the most important ones, i.e., those that have a direct influence on the formulation of policies and play their role on a daily basis. The most important stakeholder in the development is undoubtedly the Federal Council, which, through its bodies, oversees the development of ICT policy. There are three ministries[57] of more significant importance within the Federal Council that govern the development of documents related to this area, as follows: the Ministry of Environment, Traffic, Energy and Communication

[52] See ENISA. *United Kingdom Country Report, 2010*. Available at http://www.enisa.europa.eu/act/sr/files/country-reports/UK.pdf/view (11 May 2011), 19–20.

[53] More information availabe at PCeU; http://www.met.police.uk/pceu/ (December 2011).

[54] See ENISA. *United Kingdom Country Report, 2010*. Available at http://www.enisa.europa.eu/act/sr/files/country-reports/UK.pdf/view (11 May 2011), 38–39.

[55] Report of the Federal Council to the Federal Assembly on the Security Policy of Switzerland.

[56] See *Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz.* SIPOL 19650, June 23, 2010. Available at http://www.admin.ch/ch/d/ff/2010/5133.pdf (15 September 2011), 9.

[57] In Switzerland, these are called "departments" (originally, "Departementen").

(originally, Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation – UVEK), the Ministry of Justice and Police (originally, Eidgenössisches Justiz und Polizeidepartement – EJPD) and the Ministry of Finance (originally, Eidgenössisches Finanzdepartement – EFD). Various bodies operate within these ministries, having the responsibility of providing CII security.

The department in charge is the Ministry of Finance, which established the Federal Information Council for this purpose (originally, Informatikrat Bund – IRB), bearing the strategic responsibility for ICT in the Federal Administration. The IRB hence plans the strategy, architecture and protection of the ICT and determines its mid- and long-term development. Its administrative body for plotting the course of ICT is the Federal Information Strategy Body (originally, Informatikstrategieorgan Bund – ISB).

The Report and Analysis Service for Information Security (originally, Melde- und Analysestelle Informationssicherung – MELANI) can be regarded as the most important body in this respect. It is under the jurisdiction of the ISB and was established to fulfil the tasks of early detection and resolution of difficulties for the needs of both the Federal Administration and the armed forces. In Switzerland, MELANI has the jurisdiction and tasks of a governmental CERT. Every half a year, this service issues an utterly exhausting report on information security for the past six months. MELANI is actually intended for two distinct groups of clients, namely administrators of critical infrastructure within Switzerland and ICT users in domestic setting. The Swiss see it as the main body for protecting the CII.[58]

Under the jurisdiction of Ministry of the Environment, Transportation, Energy and Communication lies the Federal Bureau of Communication (originally, Bundesamt für Kommunikation – BAKOM). The Bureau was established in 1992 and is primarily focused upon the communication aspect of the CII, as Switzerland regards its television, radio and telecommunications component. There are also examples of public-private partnerships (the SWITCH Foundation – entrusted with the domain .ch), which are overseen by the BAKOM. SWITCH-CERT is one of the "groups for emergency computer intervention" in Switzerland. Other organisations with competences and responsibilities of the CERT in Switzerland include the CC-SEC, GovCERT.ch (MELANI), IP-Plus CERT and OS-CIRT.[59]

The Federal Office of Police, containing the Coordination Service for the Fight against Cybercrime (originally, Koordinationsstelle zur Bekämpfung der Internet-Kriminalität – KOBIK) is under the jurisdiction of the Ministry of Justice and Police. The KOBIK was established in 2002, parallel to the Federal Office of Police. It is a publicly accessible service receiving individuals' reports of suspected cases of cybercrime. Its tasks encompass the fight against Internet-based crime, including websites featuring racist, extremist and hard-porn contents; it investigates cases of unauthorised access into computer systems, illegal weapons trade, etc. When evidence has been collected, cases are submitted to competent criminal prosecution authorities at home as well as abroad.

[58] The Special Headquarters for Information Security (originally, Sonderstab Informationssicherung – SONIA) meets during the times of crisis, more precisely, when CII experiences disturbances. It is chaired by an official from the ISB and consists of representatives from the Federal Administration and economy. See *Melde- und Analysestelle Informationssicherung MELANI.* Available at http://www.isb.admin.ch/themen/sicherheit/00152/00175/index.html?lang=en (10 May 2011).

[59] See *FIRST Members*. Available at http://www.first.org/members/map (12 May 2011).

Unlike Great Britain and Switzerland, Sweden has no single document in the field of national security strategy, as objectives of information security are set down in the national strategy, which currently has an unclear status, as several versions thereof exist, mutually complementing each other. The first version of the abovementioned strategy was presented in a form of a draft act made by the government and entitled Society's Security and Preparedness, wherein we can find that, in terms of information security, Sweden's goal is to preserve a high level of information security throughout the entire society and to an extent that would enable the society to confront the obstruction of critical social functions and prevent it, whereas efforts invested into the attainment of this goal should be evenly distributed across the whole society, from state actors down to the very individual.[60]

In 2005, the government formulated a new draft act entitled Collaboration in the Event of Crises – For a more secure Society, representing an amendment to the previous draft act. This one states that the 2002 National Information Security Strategy should incorporate the capability of detection, intervention and action in relation to interferences in the IT systems important to society. Trust and security in the use of IT should increase. Sweden should strive towards increasing security and improving integrity protection.[61]

In 2006, the government authorised The National Post and Telecom Agency – PTS) to propose a strategy that would improve the Internet security in Sweden (Strategy for increased Security for Internet Infrastructure). The vision of the government is that the Internet in Sweden should become safe, fast and widely accessible within a time limit of ten years. It is also deemed important that individuals trust the services that are based on the Internet, legal, financial and social interactions and that these services operate safely, reliably and fast. In this context, the PTS had to cooperate with relevant actors in the ICT sphere in order for proposals to win greater support. The PTS states that, in case of a malfunction or a collapse that could cause a widespread interruption or an interference that would disable the use of Internet for larger groups, individual users, important companies, authorities or organisations, it is important to provide a long-term protection of the critical functions within the Internet infrastructure. A large part of the infrastructure is provided by private operators. Hence public enterprises are of essential importance, as follows from the assumption that the market cannot meet the stated objectives by itself. Later, in 2009, this strategy was improved and renamed as the Action plan for internet security.[62]

In line with the specification in the field of information security, the government prepared the Plan of Action for eGovernment in 2008, stating that authorities should encourage collaboration of different sectors with the eGovernment, enable them to access information as easily as possible and provide that this information be as useful as possible to them. Authorities should meet the technical requirements for supporting the eGovernment's operation and assure a high degree of security that stimulates trust in eGovernment among the people. Accordingly, the operational support across different sectors should be common and coordinated to the extent that unnecessary costs are avoided and overall productivity is increased.[63]

[60] See Swedish Civil Contingencies Agency. *Information security in Sweden: Situation assessment 2009*. Stockholm: Swedish Civil Contingencies Agency. Available at https://www.msb.se/Upload/Produkter_tjanster/Publikationer/MSB/0119_09_Information_security_in_Sweden.pdf (12 December 2011), 18.
[61] Ibid.
[62] Ibid., 77.
[63] Ibid., 21.

During the same year, the government authorised the MSB to prepare the Action plan for information security in Sweden. The MSB recognised the urge for formulating exhausting regulations that would concern all the offices under governmental control as the primary need and it also stated that the obligations of certain sectors in the process of IT policy implementation had to be clarified. Furthermore, the MSB emphasised the need for establishing baseline social information security, which is a precondition for protecting information assets that have become essential for economy and public sector alike. Thirdly, the MSB stated that the society had to be capable of confronting widespread IT crises and disturbances and hence proposed that a national operative coordinating office be established. Shortage of IT experts at all the levels of society was also identified and investments in educating such personnel were proposed.[64]

The fragmentation of actors in the formulation of ICT-related documents makes it evident that Sweden lacks a single governmental body that would be acknowledged as a national security agency by the actors operating within the ICT domain. Instead, numerous institutions operate in this sphere, such as: National Postal and Telecommunications Agency, overseen by the Ministry of Enterprise, Energy and Communications, Swedish Data Inspection Board, supervised by the Ministry of Justice, Swedish Emergency Management Agency, National Defence Radio Establishment, assisting the Ministry of Defence, the Swedish Defence Material Administration and the Swedish Security Service, sharing responsibilities and qualifications, as well as cooperating in order to provide information security and security of ICT infrastructure in Sweden.

Apart from cooperation among public actors in the field of internet security in Sweden, there is also a very good cooperation between public and private entities, which is corroborated by the case of SurfaLugnt, a national actor striving for a safer Internet, representing one of the most successful partnerships of IT industry and relevant public authorities. The partnership, which has been encouraging the development of professional knowledge and access to channels and which has been established as an alliance, is seen as more credible and as having more chance of winning attention on the part of target groups and the media.[65]

Differing from the rest of the states included in our research, Estonian documents and their basic characteristics can be divided into two distinct periods: the first one until 2007 and the second one from 2007 onwards. We are going to focus primarily on the second period.

Approximately six months after the cyber attacks had occurred, the government adopted a system of security measures for the information system. The regulation set up a system of security measures for information systems that are used for processing data coming from local and national databases. The system of security measures is composed of a procedure for the specification of security measures and a list of organisational and physical IT measures for protecting data. Emergency Act has also been adopted. The latter serves as a normative basis for crisis management, including the preparations for responding to emergency cases, as well as for providing uninterrupted operation of vital services. The Act also includes provisions stipulating and regulating the organisation of banking and

[64] See ENISA. *Sweden Country Report, 2010*. Available at http://www.enisa.europa.eu/act/sr/files/countryreports/Sweden.pdf (22 May 2011), 5.
[65] Ibid., 12–13.

telecommunication data protection, plus the provisions defining the critical infrastructure, which includes as follows: telephone and communication networks, cable casting networks, radio broadcasting networks and naval radio networks.[66]

Soon after the attack, the Cyber Defence League was established. It is a voluntary organisation bringing together computer scientists, programmers and software engineers from private and public sector. In case of a cyber war, its experts would be responsible for defence and would operate under a single command during wartime.[67]

Certainly the most important document, adopted in 2008, is the Strategy of Cyber Security in Estonia 2008–2013.[68] The strategy was adopted by the Cyber Security Strategy Committee, lead by the Ministry of Defence in cooperation with the Ministry of Education and Research, Ministry of Justice, Ministry of Economics Affairs and Communications, Ministry of the Interior and Ministry of Foreign Relations. This strategy defines the priorities and activities for improving the security in the country's cyberspace. It focuses on the following issues: responsibility of state and private organisations, assessments of vulnerability of critical national infrastructure, system of response, domestic and international legal instruments, international cooperation, training and informing on growing matters of contention. However, the strategy does not encompass national measures for the prevention of cybercrime, as the Ministry of Justice has already formulated punitive policies for the fight against cybercrime and Ministry of the Interior has prepared a draft list of priorities for providing Estonia's internal security until 2015.[69]

Notably, prior to the cyber attacks of 2007, threats to the information system had not been perceived as strongly as have been thereafter. Moreover, the documents and strategies that had been adopted had fallen under the scope of the Ministry of Economics Affairs and Communications. Documents had been adopted slowly, every couple of years or so. However, after 2007, an overturn happened, as the state has since responded to the attack with accelerated adoption of documents that should provide a higher degree of security within Estonia and the subject-matter has become a domain of the Ministry of the Defence instead of the Ministry of Economics Affairs and Communications.

There are literally vast numbers of actors responsible for providing network and information security in Estonia. They can be divided into state bodies, including the CERT, organisations from the industry and the academia, plus other bodies and organisations whose roles and responsibilities are related to the provision of information security.[70]

As far as state actors are concerned, the Ministry of Economics Affairs and Communications and the Ministry of Defence play the most important role, mutually cooperating in the domain of information security policy, which also

[66] See ENISA. *Estonia Country Report, 2010*. Available at http://www.enisa.europa.eu/act/sr/files/country-reports/Estonia.pdf (13 May 2011).

[67] See Tom Gjelten. *Volunteer Cyber Army Emerges In Estonia*. Available at http://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation (14 May 2011).

[68] See *Estonian Information Society Strategy 2013*. Available at http://www.riso.ee/en/system/files/Estonian%20Information%20Society%20Strategy%202013.pdf. (11 May 2011).

[69] See *Cyber Security Strategy*. Ministry of Defence – Estonia. 2008. Available at http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf (13 May 2011).

[70] See ENISA. *Estonia Country Report, 2010*. Available at http://www.enisa.europa.eu/act/sr/files/country-reports/Estonia.pdf (13 May 2011).

includes crisis management, cybercrime, education and training. The interior ministry has the most important role in terms of crisis management, cybercrime and critical infrastructure. It is responsible for the coordination of information security in Estonia and cooperates with the Ministry of Economics Affairs and Communications for that purpose. The detection and investigation of information crimes is the responsibility of the IT Crimes Office, Central Criminal Police.

There are still many other state bodies related to the provision of information security and their activities pertain to the control function, data protection on the Internet, coordination of actors and provision of high-quality national network infrastructure.

The Computer Emergency Response Team (CERT) has a special place reserved within the country, as it is responsible for managing security incidents in the .ee computer networks. It also serves as a contact point for international cooperation in matters of information security.

Industrial organisations have the fundamental responsibility in terms of state control over the lawfulness of personal data processing, management of databases and access to information of public character.

Organisations from the academia also play an important role, since they provide information and technology programmes for experts who develop the resources for Estonian information society and they as well train high-quality experts in information technology. The aims of the remaining organisations include the informing of users as to the safe use of the Internet, control and provision of security of information systems, plus the education and training of consumers.

5 CONCLUSION

Cyber threats have long since ceased to be a matter of future and science fiction and have become undoubtedly real. It is true that tracking or identifying the perpetrators is extremely difficult, as the removal of traces in cyberspace is much easier than in the real life, but the consequences for the operation of an increasing number of social systems, which are ever more serious, nevertheless have to be considered primarily. Even though cyberspace is a parallel virtual space, the attacks within it exert ever greater effects on the real-world life. Even a small-scale attack on the information infrastructure of a banking system that would disable its operation in entirety or even just one of the services, could disable the current operation not only of banks, but of an entire economy. Damage inflicted on the national level can have enormous consequences, transcending national borders. As a second example, we can mention hacking into centres of public warning systems to which individuals can report cases of traffic accidents, natural disasters, diseases, fires, spills, etc. A hack that would result in a temporarily disabled operation of the system would consequently render the systems we nowadays consider as taken for granted inoperative. Not to mention all possible cataclysmic events in case transportation infrastructure would be compromised.

The examples given above hence imply the fact that, in the countries we have studied, the ICT and, as a consequence, the e-services, have already become very important and deeply embedded into their workings. Thus, the attention paid to information security is a logical response of the modern state, which, in the national security sense, has had more and more trouble defining its priorities and mechanisms to achieve them.

A further indicator showing that the information security has been an ever important objective of states' policies is also an ever increasing number of public and private actors these states have been establishing for tackling this issue. The more states have implemented the Internet into their societies' workings, the greater the number of actors that should provide security to information systems and their users has been. In our analysis of states, we have also been able to notice that, in the presence of negative experience, states have been paying more attention to these new threats, which is especially evident in the case of Estonia. However, numerous information attacks, especially those that have had a large media profile, apart from causing direct and indirect damage, have also raised the level of individual awareness about the extent of threats and their consequences both for national and individual security. Therefore states have been attempting to include the end users of ICT services into their efforts to raise the level of information security (i.e., into various security schemes). For this purpose, many institutions have been devised, such as the CERT, the Swiss KOBIK and the like, enabling individuals to report different cyber incidents, whereas Sweden has made one step further and has set down in its documents that the responsibility for achieving information security should also be on the part of individuals.

The analysis of conceptual acts can help explain the relation of a state towards the security problématique. Therefore, it comes as no surprise that almost all the countries we have studied have already formulated strategies of information security and the documents are relatively recent. Only Switzerland is still in the phase of formulating such a document (it should be finished till the end of 2011), whereas Great Britain is already preparing a newer version. Maybe a bit more surprising is that all these countries have, at least to some extent, taken into account the normative arrangements of EU and/or NATO when drawing up their documents, even though not all of them are members of these two international organisations. This is a testimony to the awareness of states that threats to information security know no national borders and that this is essentially an international or a global problem that calls for a coordinated action of states at national and international levels alike. And exactly this has been more and more important a characteristic of the modern security environment. In short, states are forced to cooperate, especially in relation to technological or environmental threats. However, the analysis of conceptual frameworks in the selected states also leads us to a conclusion that Europe is currently witnessing adaptation and searching for appropriate ways of confronting this issue, which is also indicated by the continuous amending and adopting of new normative documents.

Regardless of all measures, a full security of ICT systems is impossible, therefore cyber security policies should no longer focus predominantly on protective measures, but should put more effort into restoring a state of normalcy after an attack has taken place.[71] Undoubtedly, cyberspace complexity demands a new security paradigm and a broader social consensus, but at the same time it is clear that conventional security

[71] See *Dealing with Cyber Security: Accept vulnerability.* Issue Brief 1, 2011. World Foresight Forum. Available at http://www.worldforesightforum.org/data/spaw/files/WFF/Publications/WFF_Issue_Brief_Cyber_Security_420x297_HR.pdf (15 December 2011).

instruments can also play a significant role when cyber space security is an issue. Namely, they are responsible for dealing with states of emergency and for crisis management. Unquestionably, we will be facing a tremendous social crisis if critical information infrastructure is paralysed or completely destroyed, be it intentionally or unintentionally. The last great earthquake in Japan has shown that a complex crisis is not just theory but it could also become a reality. Given the importance of ICT in modern societies, similar complex crises could arise from cyberspace. If this happens the society will have to mobilise all the adequate resources for restoring technical systems as well as ICT-based critical infrastructures.

Therefore we can agree with Brotby[72] that the road to information security goes through corporate governance. No one can solve cyber security challenges by delegating them to government officials. Although information security is often viewed as a technical issue, it is also a governance challenge that involves risk management, reporting and accountability. As such, it requires the active engagement of executive management. Today's economic environment demands that enterprises in both the public and private sectors reach beyond traditional boundaries. Citizens, customers, educators, suppliers, investors and other partners are all demanding more access to strategic resources. As enterprises reinvent themselves to meet this demand, traditional boundaries are disappearing and the premium on information security is rising. Heightened concerns about critical infrastructure protection and some other security initiatives are accelerating this trend. Therefore, there is no doubt cyber security can be reached only through participation of all users and by reaching consensus on the definition of threats and on methods of dealing with them. This amounts to a lot of work for traditional as well as newborn security actors.

REFERENCES

Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz. SIPOL B2000, June 7, 1999. Available at http://www.sog.ch/uploads/media/SipolB2000.pdf (3 May 2011).

Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz. SIPOL 19650, June 23, 2010. Available at http://www.admin.ch/ch/d/ff/2010/5133.pdf (15 September 2011).

Brotby, W. Krag. *Information security governance: a practical development and implementation approach*. Hoboken, New Jersey: John Wiley & Sons, 2007.

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol: O'Reilly Media Inc, 2009.

Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space. Cabinet Office. 2009. Available at http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf (5 May 2011).

Cyber Security Strategy. Ministry of Defence – Estonia. 2008. Available at http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf (13 May 2011).

Cybercrime: An Annotated Bibliography of Select Foreign-Language Academic Literature. Washington DC: Library of Congress, 2009. Available at www.ncjrs.gov/pdffiles1/nij/231832.pdf (22 May 2011).

Dealing with Cyber Security: Accept vulnerability. Issue Brief 1, 2011. World Foresight Forum. Available at http://www.worldforesightforum.org/data/sp

[72] See Krag W. Brotby, *Information security governance: a practical development and implementation approach* (Hoboken, New Jersey: John Wiley & Sons, 2007).

aw/files/WFF/Publications/WFF_Issue_Brief_Cyber_Security_420x297_HR.pdf (15 December 2011).

ENISA. *Estonia Country Report, 2010*. Available at http://www.enisa.europa.eu/act/sr/files/country-reports/Estonia.pdf (13 May 2011).

ENISA. *Sweden Country Report, 2010*. Available at http://www.enisa.europa.eu/act/sr/files/country-reports/Sweden.pdf (22 May 2011).

ENISA. *United Kingdom Country Report, 2010*. Available at http://www.enisa.europa.eu/act/sr/files/country-reports/UK.pdf/view (11 May 2011).

Estonian Information Society Strategy 2013. Available at http://www.riso.ee/en/system/files/Estonian%20Information%20Society%20Strategy%202013.pdf. (11 May 2011).

FIRST Members. Available at http://www.first.org/members/map (12 May 2011).

Fuchs, Christian. *Internet and Society: social theory in the information age.* New York, London: Taylor & Francis, 2008.

Gill, Charlotte. 2010. *Hi-tech crime police quiz 19 people over internet bank scam that netted hackers up to £20m from British accounts*. Available at http://www.dailymail.co.uk/news/article-1316022/Nineteen-arrested-online-bank-raid-netted-20m.html (23 May 2011).

Gjelten, Tom. *Volunteer Cyber Army Emerges In Estonia*. Available at http://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation (14 May 2011).

Global Competitiveness Report 2010–2011. Available at http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2010-11.pdf (30 June 2011).

Global Information Technology Report 2010–2011. Available at http://www3.weforum.org/docs/WEF_GITR_Report_2011.pdf (3 July 2011).

GSO Annual Report 2009. Available at http://www.getsafeonline.org/media/GSO_Report_2009.pdf (26 May 2011).

GSO Annual Report 2010. Available at http://www.getsafeonline.org/media/Get_Safe_Online_Report_2010.pdf (25 May 2011).

Heickerö, Roland. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. Stockholm: Swedish Defence Research Agency, 2010. Available at www2.foi.se/rapp/foir2970.pdf (12 December 2011).

HM Government. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Available at http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf (18 June 2011).

HM Government. *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review.* Available at http://www.cabinetoffice.gov.uk/content/securing-britain-age-uncertainty-strategic-defence-and-security-review (10 May 2011).

Informationssicherung. Lage in der Scwheiz und international, 2010. Half-year report (July–December). Available at http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdIF7hGym162epYbg2c_JjKbNoKSn6A-- (12 May 2011).

International Telecommunication Union. Available at http://www.itu.int/en/pages/default.aspx (12 May 2011).

Internet World Stats. Available at http://www.internetworldstats.com (25 April 2011).

Klimburg, Alexander. ″Mobilising Cyber Power.″ *Survival,* 53, 1 (2011): 41–60.

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität KOBIK, Jahresbericht 2010. Available at http://www.fedpol.admin.ch/content/dam

/data/kriminalitaet/internetkriminalitaet/KOBIK/rechenschaftsbericht-2010-de.pdf (10 May 2011).

Kramer, D. Franklin. “Cyberpower and National Security: Policy Recommendations for a Strategic Framework.” In *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz. Dulles: Potomac Books, 2009.

Lantis, S. Jeffrey. ″Strategic culture and national security policy.″ *International studies review*, 4, 3 (2002): 87–113.

Marshall, Rosalie. *UK to launch cyber offence strategy to prevent attacks*. Available at http://www.v3.co.uk/v3-uk/news/2074991/uk-set-launch-cyber-offence-strategy-prevent-attacks (31 May 2011).

Melde- und Analysestelle Informationssicherung MELANI. Available at http://www.isb.admin.ch/themen/sicherheit/00152/00175/index.html?lang=en (10 May 2011).

Newman, Edward. ″Human security and constructivism.″ *International studies perspectives,* 2, 3 (2001): 239–251.

National Council for Crime Prevention. Available at http://www.bra.se/extra/pod/?action=pod_show&id=1&module_instance=11 (17 June 2011).

Osborne, George. *HM Treasury Press Notice 48/11: Speech by the Chancellor of the Exchequer.* Rt Hon George Osborne MP, at Google Zeitgeist 2011. Available at http://www.hm-treasury.gov.uk/press_48_11.htm (19 May 2011).

Paget, Francois. 2010. *Cybercrime and Hacktivisim*. Santa Clara: McAfee, 2010.

Race Online 2010. Available at http://raceonline2012.org/faqs (May 10 2011).

Svete, Uroš and Uroš Pinterič. *E-država: upravno – varnostni vidiki*. Nova Gorica: Fakulteta za uporabne družbene študije, 2008.

Sweden: ICT star. Global Technology Forum, 2009. Available at http://globaltechforum.eiu.com/index.asp?layout=rich_story&doc_id=10697&title=Sweden%3A+ICT+star&categoryid=29&channelid=4 (18 May 2011).

Swedish Civil Contingencies Agency. *Information security in Sweden: Situation assessment 2009*. Stockholm: Swedish Civil Contingencies Agency. Available at https://www.msb.se/Upload/Produkter_tjanster/Publikationer/MSB/0119_09_Information_security_in_Sweden.pdf (12 December 2011).

Switzerland »vulnerable to cyber attacks«. The Local, 20 June 2011. Available at www.thelocal.ch/361/20110620/ (12 December 2011).

Škrubej, Janez. *Hladna vojna in bitka za informacijsko tehnologijo*. Ljubljana: Pasadena, 2008.

The United Kingdom Threat Assessment Of Organised Crime 2009/10. Available at http://www.soca.gov.uk/about-soca/library/doc_download/54-the-united-kingdom-threat-assessment-of-organised-crime.pdf (26 May 2011).

Traynor, Ian. *Russia accused of unleashing cyberwar to disable Estonia*. Available at http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (1 June 2011).

World Development Indicators 2011. Washington: The World Bank, 2011. Available at http://data.worldbank.org/data-catalog/world-development-indicators, (15 May 2011).

Zum Stand der Informationsgesellschaft in der Schweiz 2010. Bericht des Interdepartementalen Ausschusses zur Umsetzung der bundesrätlichen Strategie Informationsgesellschaft, Februar 2011. Available at http://www.bakom.admin.ch (15 December 2011).