RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE STUDIES

Report

Cyber Space in Estonia: Greater Security, Greater Challenges

By Piret Pernik with Emmet Tuohy

August 2013

ISSN 2228-0529

Introduction

For the last five years, Estonia has been implementing its 2008-2013 Cyber Security Strategy (hereinafter referred to as, Strategy). In light of the fact that the government expects to endorse a replacement document by the end of this year, it is important at this point to assess how Estonia has performed in its efforts to foster cyber security at home and globally.

To assess the effectiveness of any cyber security strategy, some key questions should be asked: are its objectives realistic? How adequately have they been attained? And, ultimately, has the implementation of the Strategy increased the cyber security of the country? To answer these questions, at the request of the Ministry of Defence I drafted an analysis in April 2013, based on a detailed review of the objectives and outcomes of the Strategy, including 14 interviews with key government stakeholders. This short overview presents the most important findings of this analysis, along with its key policy recommendations and suggestions for the future.

Key findings

Overall, Estonia's cyber security has increased in the last five years. Although no cyber security plan can ever be one hundred percent effective, cyber defences in Estonia have grown in scope and in quality even as cyber attacks have become more frequent and more sophisticated. Moreover, there is a better understanding throughout the public sector of what is happening in the cyberspace.

It should be acknowledged that all of the Strategy's goals were not achieved, due to lack of resources, weak leadership and administrative obstacles that encumbered the implementation, as well as other reasons discussed later in this paper. Nonetheless, the most critical objectives were reached, along with some others not even envisioned by the Strategy, for example in the military domain.

Domestically, new and more sophisticated security measures have been applied in both the public and private sectors. Internationally, Estonia has become a leader in international cooperation efforts aimed at guaranteeing both cyber security and online freedoms. In regards to the other objectives, while they have not been reached in full, a majority of their set sub-goals were achieved. While the level of expertise and public awareness on cyber security in Estonian society has increased, much still needs to be done; further analysis is needed on how to improve national legislation, especially in regards to encouraging the private sector to adopt better defences.

Background

By 2007, Estonia had started to move its public services online: e-voting, e-taxes, e-banking, e-school etc. Although citizens relied heavily on online services in their daily interaction with government and private companies (for example 95% of banking transactions that year were carried out electronically), the Estonian government did not have an overarching strategy for securing its cyberspace. The main document that regulated the country's information society was a fairly broad document, known as the Estonian Information Policy Concept.[1] In 2006 the government adopted a sectoral development programme, the Estonian Information Society Development Plan 2007-2013, that mainly dealt with the question on how to promote the use of ICT in society and improve the competitiveness of the IT sector. The only document that specifically addressed information security, known as the Information Security Interoperability Framework, was adopted by Ministry of Economic Affairs and Communications in January 2007.[2] It laid out the general principles for improving information security in Estonia, and established a unified set of standards for the public and private sector with regard to ensuring information security.

The cyber attacks in April and May 2007 against government institutions, media and news portals, banks, and telecommunications infrastructure soon provided the impetus for the development of a truly comprehensive cyber security strategy. The attacks accentuated the further need to improve the protection of the critical infrastructure on which "E-stonia" depended, such as by strengthening the regulation of internet service providers.[3] Shortly after the attacks, the National Security Committee tasked the Ministry of Defence with formulating proposals for a cyber security strategy. By launching its first cyber security strategy, Estonia was at the forefront of a new and evolving policy domain – at that time, only three other countries (the United States, Germany, and Sweden) had produced specific strategies for cyber security.

[1] Estonian Information Policy Concept was adopted by the Estonian Parliament on May, 13 1998.

[2] The first version of this document was published in 2004. The last version 3.0 was adopted in December 2011. The latter versions of the document deal more thoroughly than its predecessors with protection of critical information infrastructure. The last version in English is available at http://www.riso.ee/et/koosvoime/raamistik.

[3] Most attacks were distributed denial of service (DDoS) attacks, but there were others, such as efforts to bring down the routers and domain name servers of internet service providers, as well as the defacement of websites and the bombarding of email accounts with large amounts of spam. The attacks caused temporary service disruptions, but did not paralyze domestic internet traffic. Nevertheless, some government and private sector sites remained inaccessible for long periods of time.

Achievement of strategic objectives

The Strategy called for 19 separate actions and projects in support of its five objectives: (1) applying multi-level security measures on a large scale; (2) developing a high level of expertise and awareness on cyber security; (3) enacting proportional national legislation to support the broad and secure use of information systems; (4) consolidating Estonia's position as one of the leading countries in international cooperation on cyber security; and (5) raising public awareness of cyber security.

The first and fourth objectives have essentially been met in full: more sophisticated security measures have been applied at public and private sectors, while Estonia is widely acknowledged a leading source of expertise on cyber security. With regards to the remaining three objectives, most of the associated actions and projects were nevertheless completed, even if the broader goal has not yet been attained. The first objective was a widespread application of security measures and standards. A system of graduated security measures has been implemented fairly well in most, though not all, government agencies. For the private sector, security standards are voluntary; accordingly, government has limited oversight over how (or if) they are implemented. Moreover, the government has not provided any incentives or benefits to businesses in order to persuade them to adopt voluntary standards. That said, the government has demanded that the owners of critical infrastructure draw up continuous operation risk assessments and plans.[4] Likewise, from the beginning of next year, the owners of critical infrastructure must ensure the uninterrupted continuation of their services even when they depend on information systems located abroad. For financial and banking services, specific requirements and quality levels have already been determined by law.[5] Thus, despite the fact that not all planned objectives have been attained with regards to fostering the protection of critical infrastructure, overall progress has been quite good.

In the field of training, education, and research & development, many of the planned projects envisioned by the Strategy have been launched. For example, in 2009 a joint master's degree in cyber security programme was established by the University of Tartu and Tallinn Technical University, while in 2012 the IT Academy created a program of strengthening and supporting IT education in all four levels

[4] https://www.siseministeerium.ee/public/Elutahtsa_teenuste/Toimepidevuse_plaan_EN.pdf; https://www.siseministeerium.ee/public/Elutahtsa_teenuste/Toimepidevuse_riskianalyys_EN.pdf

[5] The January 2013 amendment to the Emergency Act stipulated that authorities who organize vital services must define the requirements for vital services (such as quality indicators and levels of services). The Emergency Act is available in English at https://www.siseministeerium.ee/public/Elutahtsa_teenuste/HOS.pdf. Service requirements for financial services, meanwhile, were set forth in a decree by the president of Estonia's central bank in March 2013. The decree is avaiable in Estonian at https://www.riigiteataja.ee/akt/112032013013

of education (pre-school, basic, secondary and higher education). A cyber crime Centre of Excellence “2CENTRE Estonia” is also being set up; it already offers elementary training to law enforcement agencies, and will welcome the first students of its new English-language master’s program in 2014.[6]

The Ministry of Education and the Ministry of Defence have also provided grants to IT and cyber security research projects. Estonian experts and scientists participate actively in international collaboration within both the NATO and EU frameworks. In the short term, the growth of such activity is constrained by a lack of qualified academic personnel, especially international professors, at Estonian universities; this restricts the number of doctoral students who can receive training in cyber security. Some other activities remain to be accomplished; for example there remains a need both for providing additional training to law enforcement agencies as well as for defining competence requirements and evaluation processes for IT staff. Some actions that were envisioned in the Strategy have not yet been carried out, for example training of private sector staff.

A great number of public campaigns have been conducted in five years with the aim of raising awareness and promoting “cyber hygiene” among the general public, but the actual results are mixed. Data from public opinion surveys show that Estonians as a whole have not gained a very high standard of awareness or knowledge of cyber security issues. In 2010 Estonia ranked below the EU average in some areas of information security (e.g., in the use of antivirus programs by the population). In 2011 less than half of the population assessed that their computer protection skills were sufficient, while two-thirds of youngsters believed that their knowledge and skills for coping with the current cyber threats were inadequate. At the same time cybercrime has continued to increase; accordingly, in the future a greater emphasis should be put on education of the general public in Estonia.

In the field of national legislation a number of laws have been introduced or amended by Parliament; several directives and decrees have been drafted and approved by government and ministers as well. Most of these bills and regulations have pertained to the protection of critical infrastructure. For example providers of vital services are now obliged both to report major cyber incidents and to design risk assessment & contingency plans. These efforts are all welcome; however, some essential regulations on the protection of critical infrastructure remain to be enacted. Moreover, government officials suggested that a number of other laws (e.g. Public Information Act, Law Enforcement Act) need to be amended.

[6] http://www.2centre.eu/network, as of July, 30 2013.

In terms of international law, Estonia has actively contributed to its development. Estonia hosts the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, which in 2009 invited international experts to prepare a comprehensive manual on the international law applicable to cyber warfare. Published this year, the "Tallinn Manual" has broken ground by definitively setting forth the rules governing cyber conflicts; drafting of the second volume, devoted to cyber incidents below the threshold of war, is already underway.

On cyber security, Estonia has proved that size really does not matter in terms of exercising influence in international relations; it has been one of the leading countries in promoting initiatives to foster cyber security in NATO, EU, United Nations, Council of Europe, OSCE, ITU and other international organizations. In the Strategy, the concrete objectives in international cooperation included sharing Estonian knowledge and experience, raising global awareness of cyber security, and supporting prevention and protection measures—all of which have been reached. Estonia has participated actively in international exercises by both NATO and the EU, organized international conferences, co-drafted international reports.[7] Estonia contributes some €10,000 annually to a Council of Europe project on fighting cybercrime; it has also effectively promoted the Council's Convention against Cyber Crime. Moreover, in 2012-14 Estonia holds the Presidency of the Convention Committee on Cyber Crime.

Estonia has benefited and will continue to benefit from its strongly positive image in the field of cyber security, and should continue to focus on increasing its influence in international settings.[8] As Estonia is a small state with limited human and financial resources, leveraging these resources in international cooperation to achieve larger overall gains would be prudent. As indicated above, the most significant progress can be found in two areas: protection of critical infrastructure and international cooperation, while the greatest challenges remain in the field of developing legislation and regulation. As for the development of international legal framework, most of the set goals have been reached, even if one of the sub-goals proved to be unrealistic. While the Strategy envisioned the emergence of a worldwide moral condemnation of cyber attacks, reaching consensus in this respect has proved to be challenging.[9] Finally, in the

[7] Report A/65/210 of 30 July 2010 and report A/68/98 24 of June 2013 of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,
http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201;
http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

[8] This view was echoed privately by numerous government officials in interviews with the author.

[9] The failure of countries to reach agreement on a universal treaty on internet governance at the World Conference on International Telecommunications (WCIT) in December 2012 highlights the sharp divide between democratic countries that believe that the internet should be open and free, on the one hand, and authoritarian regimes that advocate greater state control on the other.

domain of training, education, and research & development, results have been strong but also less impressive than were expected.

Estonian Strategy in a wider context

The first Strategy cannot be considered comprehensive because it did not incorporate two pivotal domains of activity: (1) cyber threats from criminal activity motivated primarily by financial gain, and (2) politically-motivated attacks against security and military infrastructure, including attacks by state and non-state actors. Similarly, intelligence and counter-intelligence, cyber diplomacy, and crisis management are all elements missing from the first Strategy. In today's cyber environment, where cyber sabotage and espionage are widespread and growing, - and where attacks motivated by both monetary and political objectives occur on a daily basis - official strategies need to make preventing and responding to these kinds of activities a priority.

Despite the weaknesses in implementation highlighted in this paper, it should be noted that the Strategy's drafting process in and of itself was beneficial, as it fostered cooperation within government and between the public and private sectors. This strengthened the already close links between government and private companies rendered possible by the small size of Estonian population.[10] It is also useful that providers of vital services such as telecom companies are represented in a top-level advisory and supervisory body, the Cyber Security Council, that reports directly to the National Security Council. Another example of good public-private partnership is a Committee on the Protection of Critical Infrastructure set up in 2011, which includes public and private sector IT managers and risk specialists. In the military domain, citizen participation in protecting Estonian cyberspace is embodied in the Cyber Defence Unit of the National Defence League, a voluntary defence organization. The unit is comprised of volunteer IT experts and experts from other fields related to cyber security such as lawyers, economists, etc.

Two years ago, the Estonian Information Systems Authority (EISA) was established to coordinate the development and administration of the government's information systems. It also advises and supervises providers of vital and internet services and executes supervision over them. The activities of EISA have been indispensable for strengthening national cyber security.

[10] While the informal cooperation model allows for flexibility and agility, the downside is a lack of institutionalization that may not be sustainable in the long run.

A further positive aspect of the Estonian approach to ensuring its national cyber security is that cyber issues are addressed as part of the overall crisis management process, not in parallel to it.

Lastly, in recent years innovations in Estonia have been used as models by other countries developing their own cyber security strategies. In terms of public-private cooperation the most widely-admired project is the above-mentioned National Defence League's Cyber Defence Unit, while in the defence field one can point to the Cyber Range Project that prepares the military for detecting, preventing, and thwarting cyber attacks in a real-world setting.

Difficulties in implementing the Strategy

As with any strategy, success ultimately depends on the effectiveness of its implementation. In the case of the Cyber Security Strategy, there were two action plans for implementation: one for the period of 2009-2011, and another for the period of 2012-2013. The first action plan was not implemented fully due wide-ranging state budget cuts in 2009. Adopted in May 2008, the Strategy was based on optimistic assumptions about continuous future economic growth. Unfortunately, the impact of the global financial crisis and of the Estonian real estate market crash in 2008 resulted in a negative GDP growth rate of nearly 15% of per capita in 2009.[11] The state budget cuts that year had a negative impact on the implementation of the first action plan, causing some planned activities to be postponed (e.g. testing and improving the security of critical information infrastructure companies' servers, communications devices, etc. against radio frequency and electromagnetic interference). Nevertheless, despite the dramatic cuts across the state budget, the government decided wisely to limit any further impact on protection of critical IT infrastructure in this period. As a result, years later Estonia continues to maintain a remarkable lead over many EU countries in this area. Regarding the second action plan, about two-thirds of its activities had been fully or partially completed by April 2013, with more to follow before the scheduled end of the plan in October of this year.[12]

Apart from the financial constraints, the implementation process faced other obstacles. First, the envisioned actions were not allocated specific funding. The concerned ministries plan their activities according to their own internal documents such as development plans, which often did not take the Strategy

[11] GDP at market prices in 2007 was 7,2; in 2008 -3,6 and in 2009 -14,1. *Statistical Yearbook of Estonia 2010*. http://www.stat.ee/38050 as of 29 July 2013.

[12] Estonian Ministry of Defence will present the final report of the action plan and the Strategy to the government by July 1, 2014.

into account. The Strategy's own financial cost projection for the period of 2008-2013 was about 303 million Estonian kroons (€19.4 million) but it is not known how much of this has actually been spent due to lack of record-keeping.

Some other difficulties are related to weak leadership, management, review, and amendment mechanisms of the Strategy. The work of the Cyber Security Council, the interagency advisory, supervisory and coordination group, was impeded by organizational deficiencies; in practice, it did not play a supervisory role. There was also insufficient interest and support from political leaders (National Security Council and Cabinet never discussed the implementation of the Strategy) to ensure that cyber policy received as much attention (and funding) as it needed. Moreover, as is frequently the case in the public sector, there was some confusion regarding which individuals or agencies were responsible for which tasks, confusion exacerbated by a lack of an efficient monitoring mechanism for the implementation of the action plans. Additionally, at times government agencies lacked a legal mandate to carry out the tasks assigned them by the Strategy.

Policy recommendations

As Estonia prepares to draft its next Cyber Security Strategy, the following recommendations, drawn from the present analysis of the first Strategy period, should be considered. The government should:

- Draw key political leaders (the government as well as the relevant individual ministers) into the implementation and supervision processes, in order to create a sense of "ownership"; furthermore, discuss the next draft Strategy in the relevant parliamentary committees, so as to secure broad political support;
- Base the guiding principles, strategic objectives and corresponding lines of action on a prudent analysis of the current situation. Such analysis should include threat and risk assessment over a five to ten-year period;
- Set realistic (i.e. objectives that have sufficient funds) and measurable objectives, and develop clear indicators (performance metrics) and timeframes that allow for tracking progress toward achieving them;
- State clearly who is responsible for what;
- Delineate a clear description of leadership, coordination, monitoring, amendment and oversight structures, procedures and mechanisms, and define adequately the roles and responsibilities of key agencies;
- Provide a clear description of anticipated costs and link them to ministries' budgets, while also introducing a mechanism for keeping better track of spent finances;

- Monitor implementation by setting up a regular and timely reporting and oversight system, and by providing more substantial reports to political and administrative leaders;
- Ensure that ministries and government agencies charged with different aspects of cyber security treat the Strategy as their main political guidance in this area, while verifying that their budgets and development plans take into account the objectives and actions of the Strategy;[13]
- Include activities by law enforcement and military in coping with challenges posed by cyber crime and cyber attacks;
- Improve civilian and military situational awareness capabilities; and
- Engage more voluntary and non-governmental organizations in the drafting and implementation processes.

Suggestions for the next Strategy period

This analysis of the Estonia's activities in the past five years shows that Estonia's contribution to fostering European and global cyber security has been greater than one could expect from such a small country. Estonia's focus on protecting critical infrastructure that is vital for its digital way of life has in hindsight proved to be a prudent approach. Nonetheless, today a narrow focus only on the protection of critical infrastructure and the government's own systems is not enough. Advanced technology such as cloud computing, smart meters, and smart phones will also become possible targets. Likewise, the continuing growth of cyber crime calls for greater efforts to prevent and respond to malicious attacks directed towards financial gain as well as political or ideological objectives. What is more, foreign intelligence and security agencies repeatedly warn that threat from cyber attacks is high and is expected to rise further. According to the UK Security Service "foreign states…currently pose the principal cyber threat to national security" and many countries use also private groups to carry out state-sponsored attacks.

This myriad of multifaceted cyber threats has propelled governments all over the word to invest into defensive and proactive measures in cyberspace. As pointed by General Keith Alexander, Director of the National Security Agency and Commander of the United States Cyber Command, the key to success is more training and education. In Estonia, there is clearly a need for both, whether high-level training for experts or basic cyber education for non-specialist civilian and military leaders.

[13] Ministry of Defence, Ministry of Communications and Economic Affairs, Ministry of Interior, Ministry of Foreign Affairs, Ministry of Justice, Ministry of Finance, Ministry of Education and Science, and State Chancellery.

While positive steps have been taken with regard to education of operational- and senior-level personnel (cyber security module was introduced at the Baltic Defence College in 2012), such courses should be extended to trainees and junior-level staff as well, such as at the Estonian National Defence Academy.[14] Further improvements to the curricula and teaching methods of these courses are necessary as well. In addition, competence levels, assessment and evaluation processes for the government IT and cyber security experts should be clearly set out, as should standards for recruitment and hiring.

All government agencies involved with implementing the Strategy should participate in international exercises; greater participation of Estonian businesses and non-profit organizations should be encouraged as well. Throughout the cyber security community, a consistent emphasis needs to be placed on analyzing lessons learned and adjusting procedures and structures as necessary. Furthermore, to ensure readiness, government agencies should practice carrying out incident-response tasks in their areas of responsibility through means of annual exercises.

In the military domain, cyber defence and cyber operations doctrine needs to be further developed. In this process closer inter-agency coordination and cooperation between the military and civilian bodies such as law enforcement agencies would be advisable.

For better situational awareness, a real-time or near real-time information and intelligence sharing system between the government and critical infrastructure operators should be created. For instance, annual reports on major cyber incidents could be regularly distributed between the government agencies and with the key industries. Risk assessment procedures should be improved by developing data and metrics to measure and estimate cyber risks. The government could also offer greater support and funding to NGOs by providing grants for conducting awareness campaigns, training and education projects, and other initiatives. Finally, all ministries involved in drafting and implementing the next Strategy could profit from internal analysis on how well the previous Strategy has already been incorporated into their relevant working policies and procedures.

Last but not least, international cooperation with like-minded nations (whether bilaterally or in existing cooperation formats) and further exchanges of best practices will help to maintain Estonia’s influence and prominence in cyberspace in the future.

[14] Baltic Defence College’s Joint Command and General Staff Course has a cyber security module.

International Centre for Defence Studies
Toom-Rüütli 12-6, 10130 Tallinn, Estonia
info@icds.ee, www.icds.ee
Tel.: +372 6949 340
Fax: +372 6949 342