PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BULLETIN

No. 68 (1139), 11 May 2018 © PISM

Editors: Sławomir Dębski • Bartosz Wiśniewski • Rafał Tarnogórski

Karolina Borońska-Hryniewiecka • Anna Maria Dyner • Aleksandra Gawlikowska-Fyk
Sebastian Płóciennik • Patrycja Sasnal • Justyna Szczudlik • Marcin Terlikowski • Tomasz Żornaczuk

Estonia as a Leader in Increasing Cybersecurity

Kinga Raś

Estonia's commitment to strengthening cybersecurity is a result of its experience as a victim of hacking. At the same time, Estonian authorities are consistently raising the country's informatisation level and lobbying for an effective digital single market in the EU. For Estonia, expertise in increasing cybersecurity has become the country's unique brand, and the application of comprehensive and effective solutions means that it can be a model partner for Poland in digitisation and combating cyberthreats.

In March, the Estonian government submitted a law on cybersecurity to parliament. It defines the principles of organising the security of network and information systems in the public and private sectors. It also transposes to Estonian law EU directive 2016/1148 of 6 July 2016, on measures for a high common level of security of network and information systems. The NIS directive, which should be implemented by 10 May, requires, among other things, that each EU country designates a body responsible for cybersecurity and develops a strategy to counter cyberthreats. The regulations will standardise network security criteria and impose an obligation to inform relevant national authorities about cyber incidents.

Modernisation of the Regulations. In Estonia, the revision of the rules and the implementation of the EU guidelines to a large extent reflect existing practice. Most of the regulations were already in force earlier on the basis of the Acts on Emergency and the Electronic Communications Law. The new document is to structure the competences and responsibilities of entities responsible for network security, in particular for preventing threats and risk management for IT systems. Therefore, the implementation of appropriate security will primarily cover email servers and document flow systems. So far, such measures have been used in systems that formally meet the database criteria. The act also defines a list of key service providers. In comparison to previous regulations, the new law will also cover the Estonian Internet Foundation, which manages the ".ee" domain, and digital service providers such as online stores, search engines and cloud data services.

Digitisation in Estonia. Estonia is a pioneer of digitisation in Europe, and offers its citizens extraordinary internet solutions, including in relation to public administration. As early as the 1990s, the X-Road digital platform system had been developed, enabling the integration of information systems and safe data transfer. Since 2001, an electronic ID card has been in force in Estonia and is already carried by 86% of citizens. The identification of people in the network made it possible to introduce internet voting in 2005. Since the parliamentary and local elections of 2009, more than more than 20% have voted online in subsequent elections. The most commonly used state e-administration service is for online tax returns, which is used by in excess of 96% of taxpayers.

Co-financing for digitisation in public administration also confirms the Estonian government's priorities in the respect. In the four-year budget perspective, in 2018, Estonia increased financing for e-services infrastructure development from €18.6 million (2017) to €52.7 million. There are also plans to increase wages for IT employees in public administration by 20% from next year.

In Estonia, it is possible to set up a company in about 15 minutes, which for a small country is an important factor for economic development. In addition, Estonia has implemented an e-residency programme a digital ID that, regardless of the place of residence, offers a streamlined and easy way to start doing business within the EU. So far, more than 37,000 people from 156 countries have submitted applications, with the vast majority of them aiming to set up a company, including in the IT sector.

Cybersecurity. Estonia's high level of reliance on information systems means the country is very vulnerable to cyberthreats. Despite hacker attacks, the country continues to make progress in informatisation, and has even intensified activities in this area, which implies the growing importance of the cybersecurity. In 2008, Estonia became the first country in the world to adopt a cybersecurity strategy (which was amended in 2014). Because of the Russian cyberattack of 2007, Estonia not only treats this sphere as a strategic aspect of security, but also effectively strives to strengthen it at EU level.

According to a report by the RIA, the institution responsible for cybersecurity, there were 2,248 cybercrime incidents in Estonia in 2016 (in Poland, according to an ABW report from 2015, this number was 8,914). Most of these were carried out using malware (30%), botnet (22%), phishing (13%) and ransomware (11%). Approximately 20-30% of cyberattacks were targeted at government institutions. In the public sector, denial of service (DOS) attacks on IT systems or supporting websites—constituting either security probes or phishing attacks—were the biggest cause of disruption. Estonian analysis also points to the growing risk of cyberattacks against local administrations. The lack of sufficient network protection also applies to non-governmental organisations.

Estonia is trying to increase its cybersecurity comprehensively, because entities providing universal services to the public are among those to have been attacked. For example, the highly-computerised Estonian healthcare system was at risk when ransomware from infected computers at one of the country's largest hospitals spread via one of its servers in 2016. In the same year, the computer network of Viru Keemia Grupp (VKG), an enterprise operating in the oil shale industry, was attacked. Network monitoring detected malware and identified a targeted attack. Server analysis indicated the activity of APT28, a group associated with Russian intelligence.

From the Estonian perspective, robust cybersecurity determines the efficient functioning of the digital single market. Estonia is a strong supporter of this, and during its presidency of the EU Council it called on EU Member States (among others) to participate in digitisation activities. Currently, it is lobbying for the implementation of key EU initiatives in this area. These concern, among other things, the protection of personal data in mobile and internet platforms, copyright laws, freedom of non-personal data transmission, and taxation of internet services. Estonia is also intensifying inter-state cooperation in the field of data exchange. Since February this year, the Estonian data platform X-Road has been connected with the Finnish Suomi.fi. Moreover, Estonian Prime Minister Jüri Ratas is in favour of extending this bilateral cooperation to the Baltic and Nordic countries.

Conclusions. In Estonia, the amendment of legislation on cybersecurity relies primarily on arranging existing regulations and their adaptation to changing conditions, and not on the implementation of completely new solutions. In this way, Estonia is trying to improve technologies for reacting to specific incidents in cyberspace.

Estonia advocates the creation of a digital single market, seeing in this measurable profit, especially for the development of the e-economy. Therefore, it promotes solutions that are conducive to security in the network and, in fact, make Estonia an attractive country for foreign investors, including those from outside the EU.

Estonia's experience in protecting e-government and IT systems makes it a model cooperation partner for Poland. In order to respond to new threats, Poland could draw on Estonian experience in providing secure e-services for public administration, including local government, to respond to emerging threats. Estonian practices in the field of personal data protection and introduction of the electronic ID system may be useful for Poland. It is also in Poland's interests to increase cybersecurity on NATO's eastern flank. Regional cooperation, including the support of NATO competence centres in Tallinn and Riga, favour this.