Cyber security – a problem for all of us?

Strategies of the EU Member States in the face of challenges relating to access to online data

Reports and analyses

[5]/2015

www.csm.org.pl

CENTRE FOR
INTERNATIONAL
RELATIONS

Reports and analyses

EFNI

EUROPEJSKIE
FORUM NOWYCH IDEI

This material was developed as input fore a discussion on „Cybersecurity — a problem for all of us? Strategies of the EU Member States in face of challenges relating to access to online data", to be held during the European Forum of New Ideas in Sopot on 1st of October 2015.

INTRODUCTION

Cyberspace is one of the fastest developing dimensions of threats to the modern world. It concerns not only the governments, but also the business and individual internet users. The dynamics of changes taking place on the international security arena and fast development of information technologies require that special attention be paid to digital security of nations and their strategic resources.

Poland is at the beginning of this road. Currently the Polish cyberspace security system is not adapted to the growing threats. Efforts to improve the situation will profit from using both the discussion on the European Union's forum and the experience of individual Member States, particularly the United Kingdom and Estonia.

Cyber security is often being discussed in context of scandalising incidents that concern other states, private individuals or businesses. Often these issues are viewed as something reserved for IT specialists. But cyberspace security is not something that should be dealt with only by the IT experts. Neither is it exclusively a domain of the public administration, but also of network administrators, private companies and ordinary people.

Cyber security is a perfect example of an issue that cannot be analysed or solved within a single sector. Providing digital security of state, institutions and citizens requires a dialogue and partnership between multiple parties. This concerns both the strategy, which should be developed through collaboration between the representatives of the administration creating the action plans, and the business that has the experience and proven processes for elimination of threats resulting out of being online – as well as operating procedures executed by the administrators of networks of public administration agencies and their peers in private businesses. And this dialogue may not be just a lip service. The EU and its Member States need a consistent defence system based on standards binding all entities concerned with the cyber security issues (so, in fact, all of us). Protection in the cyberspace may not be provided in isolation from the outside world.

Therefore positive conclusions needed for establishment of a consistent and effective protection system may come from both opening up of the administration to the experience and suggestions of third party service providers, providing e.g. the cloud data storage services, and from drawing on the experience and good practices of countries better prepared for threats in the cyberspace dimension. •

EFFORTS FOR
CYBER SECURITY AT THE EU FORUM

In recent years the European Union has been commencing initiatives aimed at adapting the cyber security related regulations to the new reality. Many Member States and the EU itself so far lacked legal and institutional solutions in this area. This will change with the adoption of the NIS Directive (Network and Information Security) document.

NIS Directive is to focus on the protection of critical state infrastructures, aiding the public administration in protecting the sensitive systems (it is postulated by the European Parliament, a similar point of view in Poland is presented by the Polish Chamber of Information Technology and Telecommunications and the Lewiatan Confederation). Moreover, to a lesser extent, the directive is to define the obligations of the digital industry businesses concerning among others the personal data protection. The new document will most probably be binding on both the public sector and the private sector institutions.

Development of the new regulations was accelerated after Edward Snowden disclosed the PRISM affair in 2013 (acquisition of personal data on the internet by the United States National Security Agency on claims of the threat of terrorism). In March 2014 the draft directive was passed by a vote at the European Parliament. However, the work on the final form of the NIS Directive is still going on, since the scope of its application is a subject of dispute between the Member States. This delays the adoption of the EU document, and in consequence translates to temporary lack of regulations in this area on the pan-EU level.

Enactment of the regulations shall provide the Member States with the possibility to more effectively protect the critical infrastructures (including the energy sector systems, transportation and healthcare systems), and will strengthen the collaboration between the EU Member States and the private and the public sector. Adoption of the directive shall also assure several benefits to internet users. Thanks to harmonisation of legal regulations throughout the EU and development of the Single Digital Market (treated as one of its priorities by the European Commission), the entrepreneurs shall obtain a way to more easily commence operations abroad, and businesses throughout the EU shall save — according to Commission’s own estimates — even up to €2.3 billion per year. More broadly, the adoption of the new regulations will contribute towards creation of more equal and transparent conditions for competition on the European market.

There is a discussion going on about the assumptions of the document, resulting from different standpoints of the Member States on certain of its provisions.

Controversies arise out of, among others, imposing the new regulations on all undertakings offering goods or services to customers in the EU, regardless of the place of incorporation of the company (so including also the leading American internet companies). Upon enactment of the NIS Directive, foreign companies wishing to disclose to third countries any information about EU citizens shall have to obtain approval of the national authorities responsible for personal data protection. Divergences include also: the level of administrative fines, imposing the regulations on the telecommunications operators and the list of entities considered parts of critical national infrastructure.

In discussions about the scope of the directive, the Polish Chamber of Information Technology and Telecommunications as well as the Lewiatan Confederation are for, among others, shortening the list of entities and resources treated as the critical infrastructure and their precise definition (creation of an exhaustive and complete list), as well as excluding the telecommunications operators from the scope of application of the regulations. Moreover, both institutions argue for adoption of the principle of maximum harmonisation, meaning identical understanding of the directive in all the EU states both concerning the requirements addressed to the market operators, as well as concerning the scope of the document. The argument brought up in favour of such approach is the intention to assure equal principles for business operations and competition. Moreover, the Polish institutions are stressing the importance of voluntary and bilateral nature of exchange of information between various entities (particularly those from the public and the private sectors).

The discussion about the NIS Directive points to an intention of comprehensive treatment of cyber security on the EU forum, as well as development of the European collaboration framework in this area. A definite plus is the stress on public-private partnership — the key condition for effective collaboration on implementation of the defined goals. The negatives are the persisting divergences resulting from tremendous complexity of the problem. A step towards their elimination is the review of two case studies of EU Member States that represent different approaches to this challenge resulting from their specifics. •

CYBER SECURITY in ESTONIA

With only a 1.5 million population, Estonia was one of the first countries that have adopted a cyber security strategy in 2008, updated in 2014. The country has mature CERT team, in 2008 the NATO Cooperative Cyber Defence Centre of Excellence was established in Tallinn, and the updated cyber security strategy for 2014-17 considers as its main goal the strengthening of the cyber defence shield.

Particular activeness of Estonia in the area of cyber security is driven by two factors. Firstly, thanks to consistent policy of its consecutive governments, expressed by the "E-stonia" name, the country become the technology leader of Europe: a place where elections are held online, the birthplace of Skype, where over 95 percent of banking transactions are made online. Secondly, in 2007, after removal of the Red Army Bronze Soldier monument from the centre of Tallinn, Estonia became a victim of a cyber attack on an unprecedented scale. It blocked the websites of the parliament, ministries of defence and justice, political parties, and even of public schools. The attacks peaked on the 9th of May (the Russian Victory Day); when hackers targeted even the private sector, and the two biggest banks, Hansapank and SEB Uhispank, had to suspend their online services and block foreign transactions.

The experiences from the cyber attack were used in developing the defence system, which went not along the line of maximising isolation and surrounding it with a virtual wall, but right the opposite – towards hosting maximum resources in the cyberspace, so that in the event of attack the country could continue to function even if derived of its territory. The specifics of this solution are reflected in the plan to create a "virtual data embassy" – a physical or virtual data centre in an allied country selected by the government, storing the data of, among others, the critical IT systems. Another achievement of the cyber security policy of Estonia is also a far-reaching public-private partnership. It included establishment of the Cyber Defence League based on volunteers from the private sector, who in case of national security threat shall be subject to military command. •

2008

↳NATO Cooperative Cyber Defence Centre of Excellence was established in Tallinn ↵

2013

↳ the Estonian Government commenced the "virtual data embassy" initiative ↵

€16 million

i↳is the cost of implementation of the cybersecurity strategy for 2014-17 ↵

30

↳ number of minutes it takes to obtain a new electronic national ID ↵

CYBER SECURITY in the UNITED KINGDOM

With a nearly 60 million population, the UK took a different approach to cyber security related challenges than Estonia, but is also treating them as priority. The importance of this issue to the UK administration comes from, among others, the most advanced e-commerce sector in the world. It is part of the economic landscape, to a significant extent based on web-based services (e.g. the City). Acknowledging the magnitude of the problem, the National Security Strategy of 2010 has rated cyber attacks as "Tier 1" threat. In 2011, a new Cyber Security Strategy was adopted (initially it was developed in 2009). One of its goals is to make the UK one of the most secure places in the world to do business in cyberspace. The key importance attached to this aspect is the most significant differentiator between the UK and the Estonian systems, the latter being oriented primarily on assuring the security of structures of the state in case of external threats (including information warfare).

In its cyber security policy the UK authorities attach significant importance to protecting the private sector and the citizens. To increase awareness among the entrepreneurs, they have developed handbooks addressed to businesses of all sizes, containing clear and concise information on how to improve the security of key resources.

An important problem in assuring cyber security of the private sector is the reluctance of businesses to share information that they fell victim to cyber attacks, due to reputation concerns. To bypass this problem, a special CISP (Cyber Security Information Sharing Partnership) platform was created that allows anonymous real-time sharing of such information between the businesses and the government. In total the UK government has earmarked £850 million for implementation of the goals set out by the strategy. •

750

↳organisations associated in CISP (Cyber Security Information Sharing Partnership) ↵

£850m

↳funds earmarked forimplementation of Cyber Security Strategy assumptions over five years ↵

£2bn

↳forecasted value of cyber security related exports in 2016 ↵

24127 people

↳registered in the first round of the "Introduction to Cyber Security" online courses ↵

Poland has already taken certain measures concerning challenges of access to the online data by introducing to the Polish legislation, among others, the term “cyberspace” and by forming legal grounds for extraordinary responses to threats appearing therein. In June 2013, the Council of Ministers has adopted the document “The Policy of Protection of the Cyberspace of the Republic of Poland". Most of the recommendations it prescribes are still under implementation.

On the operating level Poland has two CERTs (Computer Emergency Response Teams) — CERT.GOV.PL and CERT PL. The former fulfils the role of the main CERT in the area of government administration and in the civilian space. Its prime task is to assure and keep developing the public administration’s abilities to protect it against cyber threats. In turn, CERT.PL, functioning at the Scientific and Academic Computer Network (NASK), is the first incident response team that was established in Poland. It collaborates with peer organisations throughout the world.

The above document stresses the key role of education. It points out that educational efforts should be made not only with focus on the employees of government administration accessing and using the cyberspace, but also with focus on the general public. Assuring ICT security in the modern world to a large extent depends on the knowledge and day-to-day conduct of every internet user. If introduction of ICT security as permanent element of higher education curriculum, promised in the document, shall be effectively achieved, also private businesses will profit from this situation, as they are permanently short of specialists in this domain. This is only one of the examples of benefits resulting from more close public-private partnership.

In turn, the Doctrine of Cyber Security of the Republic of Poland published by the National Security Bureau in January 2015, states that the private sector shall collaborate with the public sector on tackling the cyber threats, including on development of proposals for legal regulations. It seems that this is the area where Poland might achieve much more than at present. However, it shall require overcoming numerous stereotypes, distrust and mutual opening towards the common goal — security of all network users. It is of particular importance with respect to the critical infrastructure that is most important to the national security and more and more dependent on information and communications technology solutions. And for this very reason the cyber attacks are becoming an ever more important threat. Close collaboration of public administration with private operators is necessary also due to the fact that a growing part of critical infrastructure is privately owned.

Other challenges for the public sector entities are: defining responsibilities and coordination of collaboration between individual entities and their units as well as development of standards and good practices relating to cyberspace, including exchange of information and collaboration with the business community. A report by the Polish Supreme Audit Office (NIK) of June 2015[1] points out that the efforts by the state institutions are conducted in silos and without a common systemic vision. NIK has pointed to lack of necessary legal regulations and incoherent and ineffective policies of key institutions of the state responsible for security of Poland in the ICT space. Most worryingly, the report raises the lack of procedures for responding to crisis incidents relating to the cyberspace.

In summary, in view of the above, Poland has made the first steps towards strengthening its digital national security, but is not well prepared for the threats in this dimension and has no defined strategic model of approach to this issue. In turn, the administration acts incoherently and in isolation from other sectors. On the other hand, one should note the positive examples of commitment of the general public in protection of the cyberspace. In mid-September this year the Polish Civil Cyber Defence (POC) was launched and its members — civilian experts, want to support national cyber security as volunteers. •

[1] *Protection of the security of cyberspace of the Republic of Poland tasks implemented by state institutions,* Supreme Audit Office, June 2015, URL <https://www.nikgov.pl/pliktid,8764,vp,10895.pdf> (in Polish).

INTENSIFYING THE DEBATE

There is no doubt that cyberspace security must be treated as a joint task for all entities that have influence on security of data in the internet. The states and the IT companies play a particular role here. What remains to be discussed are the methods and forms of collaboration between the public and the private sector in this area. Answers to the above issue will probably come with the transposition of the NIS directive to national legislations of Member States and local discussions around this topic.

While on the EU level intense debates about the final form of the NIS Directive are taking place, in Poland the cyber security is being discussed by only a handful of experts. Poland keeps away from the mainstream EU debate and the government does not see cyber security as a priority. Time has come for the Polish administration to actively join the search for optimal systemic solutions, among others, through initiating a broad public discussion. The issue of security in the cyberspace should engage more communities and institutions, both from the public and from the private sphere.

Elements of the system should include:

- education and preventive measures aimed at raising awareness and indicating desirable practices to avoid the threats coming from the internet,
- building a platform for closer collaboration between the administration and the business community on protection of the cyberspace,
- clear definition of competences (advisory, consultative and most importantly – coordinative) of a body assisting the Council of Ministers on cyber security issues on above ministerial level,
- presenting a catalogue of rules for creation of new legal solutions concerning secure access to online data.

When comparing the strategies of the UK and of Estonia to the Polish cyberspace defence strategy one may note how important it is to accelerate the efforts aimed at development of a holistic, strategic, and first and foremost – coherent policy of Poland in this domain. In this context it makes sense to consider what experiences of the UK and of Estonia could be of use to Poland, and what efforts and mechanisms could in turn become a Polish specialty.

With challenges of digital security, the traditional division between the state and the private sector is groundless, as it precludes development of effective protective solutions. In this context the key is a broad collaboration between these sectors — more so, as the issue of cyber security becomes ever more significant due to rapid development of information and communications technologies and ever newer solutions and possibilities provided by the market.

AUTHORS:

Dr Małgorzata Bonikowska

president of the Centre for International Relations and partner of THINKTANK centre

Michał Szczygielski

analyst
Centre for International Relations

Antoni Wierzejski

analyst
Centre for International Relations

CENTRE FOR INTERNATIONAL RELATIONS

The Centre for International Relations (CSM) is an independent non-governmental think-tank dedicated to the study of the Polish foreign policy and key international policy issues. The Foundation was established in 1996. CSM conducts research and educational activities, issues publications, organises conferences and meetings, takes part in international projects in collaboration with similar institutions from many countries. It establishes the forum for debates and exchange of ideas on foreign policy, relations between states and challenges for the globalised world. Activities of CSM are addressed primarily to local government officials and entrepreneurs, but also to the central administration, politicians, diplomats, politologists and the media. In 2009, CSM was recognised as one of the best think tanks of Central and Eastern Europe in the study "The Leading Public Policy Research Organizations In The World" conducted by the University of Pennsylvania.

Reports and analyses 1/2015 www.csm.org.pl

CENTRE FOR INTERNATIONAL RELATIONS, ul. Mińska 25, 03-808 Warsaw, phone: +48 22 646 52 67