Cyber Security
CHALLENGE FOR EU STATES

By M. Bonikowska, M. Szczygielski, A.Wierzejski

In recent years, the European Union has been commencing initiatives aimed at adapting the cyber security related regulations to a 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.

The document is to focus on protection of critical State infrastructures, aiding public administration in protecting the sensitive systems. 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 public and private sector institutions.

Development of new regulations was accelerated after Edward Snowden disclosed the PRISM affair in 2013 (acquisition of personal data on the Internet by the US 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 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 Member States the possibility to more effectively protect the critical infrastructures (including the energy sector systems, transportation and healthcare systems), and will strengthen collaboration between EU Member States and private and public sector. It shall also assure several benefits to Internet users.

Thanks to harmonisation of legal regulations throughout the EU and development of 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 Member States on certain 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.

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 European collaboration framework. 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.

With only a 1.5 million population, Estonia was one of the first countries to adopt a cyber security strategy in 2008, updated in 2014. 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 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 per cent 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 Parliament, ministries of defence and justice, political parties, and even public schools. The attacks peaked on the 9th of May (the Russian Victory Day); when hackers targeted even the private sector, and two biggest banks 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 data of, among others, critical IT systems. Another achievement is also a far-reaching PPP, which includes establishment of Cyber Defence League based on volunteers from the private sector, who in case of national security threat shall be subject to military command.

With a nearly 60 million population, the UK took a different approach to cyber security related challenges than Estonia, but is also treating these as priority. The importance of this issue to the UK administration comes from, among others, the most advanced e-commerce sector in the world.

In 2011, a new Cyber Security Strategy was adopted. 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 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 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 fall 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 government. In total, the UK government has earmarked £860 million for implementation of the goals set out by the strategy.

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. 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 ICT and ever newer solutions and possibilities provided by the market. ---INFA

(Courtesy, Centre For International Relations, Poland)