PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BULLETIN

No. 9 (741), 22 January 2015 © PISM

NATO and the EU Should Urgently Strengthen Cyberdefence for Critical Infrastructure

Wojciech Lorenz

The cyberattack against Sony indicates the potential of cyberweapons, which could be used against critical infrastructure (CI) to undermine the stability of a country or even a whole region. To avoid such a scenario, governments and private companies have to advance coherent cybersecurity and defence standards. NATO and the EU should also take an important step towards interoperability by introducing standard operating procedures for computer emergency response teams (CERTs).

At the end of 2014, computer networks of Sony Pictures were disabled by a massive cyberattack, which was allegedly supposed to discourage the company from releasing a comedy about the assassination of North Korean leader Kim Jong Un. The attackers stole an immense volume of sensitive data (confidential documents, emails, internal memos, unreleased scripts and full length movies) and infected company networks with malware designed to wipe hard disks. It took weeks to restore networks to functionality. Sony admitted it was unprepared for the attack, branded as the most significant event of this kind on the U.S. territory.

This attack indicated the vulnerability not only of Hollywood giants, but all large networks that are the backbone of corporate activities, in general. Furthermore, many such networks ensure the proper functioning of critical infrastructure (CI), including power plants, electricity grids, refineries, pipelines, transportation, banking systems and telecommunication systems.

The Growing Threat to Critical Infrastructure. As the backbone of advanced societies, CI belongs to the most attractive cyberattack targets. Within the CI domain, electricity grids are diagnosed as those which, should they be affected, are most likely trigger a cascade of negative effects to other dependent and interdependent CI sub-sectors (telecommunications, the banking sector, automated transport systems etc.), multiplying the negative impact on the functioning of a state or even a whole region. The risk of such an attack is growing together with the development of electric networks, regional interdependencies and computer-based, remotely controlled “smart grids,” which are used to improve the efficiency of energy distribution. Although some systems, including nuclear power plants, will remain separated from the outside networks and the Internet (so called air gaps), they can also be infected with more sophisticated cyberweapons, through employees’ personal electronic devices, e.g., flash memory. Before the Sony case, the destructive potential of such targeted attacks was disclosed by computer malware Stuxnet and Shamoon. The first disrupted the operation of Iranian nuclear facilities in 2010, and the latter wiped the data from 30,000 computers of the Saudi Aramco oil producing company in 2012.

The volume of attacks on CI has been growing quickly in recent years. In 2014, Deutsche Telecom, which operates in Europe and the U.S. with almost 160 accesses, registered close to one million hacker attacks to its networks every day, three times more than a year earlier. Experts agree that majority of the attempts to hit critical infrastructure come from non-state players, who do not possess the skills and extensive funding to create sophisticated cyberweapons, but instead are able to perform a large number of different types of attacks and intrusions. Such attacks may challenge the stability of networks, rather than lead to large-scale disruptions of their functioning. However, some of the low-end hackers without sophisticated skills can use the black market of cybercrime services and “goods” such as “zero day vulnerabilities” (information on previously undisclosed security holes in software), which can be used for infiltration of CI systems and to launch more destructive attacks. It is also likely that the deteriorating security environment caused by a resurgent Russia, an increasingly assertive China, potential tensions with Iran and North Korea, and crises in the Middle East, will enhance the probability of cyberattacks instigated by state players. The attacks against Estonia in 2007, Georgia in 2008, and Ukraine in 2014 indicate that cybercapabilities have become a standard tool of demonstrating leverage and exerting pressure aimed at achieving foreign policy or economic goals. States can try hiding behind hackers and apply a whole spectrum of low-end attacks, which are difficult to attribute and offer governments plausible deniability. They can also develop sophisticated, expensive (the estimated cost of Stuxnet was $10 million) and labour-intensive cyberweapons, but are likely to use them as a last resort, so as not to disclose their capabilities and the origin of attack.

The Weak Links at the National Level. The first line of cyberdefence has to be erected by states, which are responsible for their CI, and there are a number of weak links at this level. Although over the last decade most of the EU and NATO members have adopted cyberstrategies, these documents should be subject to regular updates, based on the lessons learned by more experienced states. The already diagnosed best practices include consultation with the private sector and all relevant players at an early stage, which is required to make the strategic vision implementable, given that the vast majority of CI is privately owned and operated. New or updated strategies need to be supported with robust risk assessments and clear definitions of CI categories based on verifiable and updated criteria, which is lacking in the documents of many EU and NATO members.

The security of critical infrastructure across the transatlantic area is also compromised by a general lack of effective Public Private Partnerships (PPP)—institutionalised collaboration between governments and the private sector. Top down cooperation on different levels of decision-making is necessary to provide policymakers, CI owners and operators with platforms for regular meetings, exchange of information, and fostering a common approach to threats.

Most of the EU and NATO countries still need to advance a coherent approach to security standards among CI owners and operators. To promote higher cybersecurity standards they will have to offer incentives for operators, such as protection from compensation claims in case of successful attack, lower insurance costs and certifications supporting a company's reputation. With such incentives, companies could be encouraged to use independent audits to check their preparedness for cyberthreats.

Since the human factor remains the weakest link in the cybersecurity architecture, it should be a priority for governments and companies to invest in cybersecurity awareness campaigns and cybereducation.

Potential for EU—NATO Cooperation. Recognising the threats, NATO and the EU have put cybersecurity and defence high on their agendas. The EU has been focused mainly on cybersecurity in the civilian domain, but is also trying to improve its military cyberdefence capabilities. Member States adopted the comprehensive Cybersecurity Strategy (2013) and the EU Cyberdefence Policy Framework (November 2014), and are working on a proposal for a Directive on Network and Information Security, which will ensure basic cybersecurity standards, such as having a single national CERT (Computer Emergency Response Team), in every EU country.

NATO's primary task in this field is to defend the organisation's networks, but it also offers assistance to allies in reducing vulnerabilities in their critical infrastructure. The alliance approved an enhanced cyberdefence policy at the NATO summit in Wales in 2014, and is developing a doctrine for invoking Article 5 in response to cyberattacks. Once in place, it may allow an allied response to potential large-scale cyberattacks. Despite traditional political obstacles, both NATO and the EU advocate close cooperation in cyberdefence, with the aim of avoiding duplications of efforts and capabilities. The ongoing efforts are focused on development of the whole spectrum of civilian and military cyberdefence measures, including threat assessment and raising awareness (for example, through training, education and exercises), detection of incidents (such as through the development of advanced cyberdefence sensors), exchange of information and coordinated incident response (for example, through CERTs), identification and prosecution of aggressors (forensics gathering and harmonisation of legal procedures), and enhanced cooperation with partner countries.

Priorities for Poland. Poland should place CI cyberdefence on the agenda for the next NATO summit, to be held in Warsaw in 2016, through enhanced interoperability among EU and NATO members at operational level. Such interoperability could be accelerated by liaisons between military and civilian CERTs, and the introduction of standard operating procedures enabling cross border operations and information sharing. Should this prove to be too ambitious a task, it is in Poland's interests to promote such enhanced cooperation in the Baltic Sea region, which is developing interconnections of its critical infrastructure systems (mostly energy grids and pipelines), but is at the same time becoming more vulnerable to the full spectrum of cyberattacks, from both state and non-state players.