Pulaski Policy Papers
Komentarz Międzynarodowy Pułaskiego
ISSN 2080-8852 Warsaw, 24.02.2016

Author: Kamil Gapiński

Towards a system of cybersecurity – a review of the existing strategies and proposals for a new beginning

On February 23, 2016, the Ministry of Digitization published its "Assumptions of Cyber Security Strategy for Poland" document, announcing the legislative work of the Ministry of Digitization in the field of security concerning civil systems of critical ICT (information computer technology) infrastructure. This is the first project of the current government in the area of cybersecurity, although similar legislative and policy initiatives have already appeared before. It should be noted, however, that the previous documents produced by the state authorities were not legally binding. They did not give legal authority to appropriate state entities, which made their full implementation impossible ('cyberspace' is the only term introduced into Polish legislation; its definition can be found in the Law of August 27, 2002, 'on martial law and the competence of the Supreme Commander of the Armed Forces and principles of his subordination to the constitutional authorities of the Republic of Poland'). The problem of the lack of legal regulations concerning a cyber security system, as well as negligence in this area, have for years been one of the most important challenges facing the country. It led to a dilution of competence, the lack of a coordinating body, and paralyses in decision-making, as in the case of building the cyber capacity potential in the Polish Armed Forces (National Criptology Centre case). Moreover, according to experts, too many actors are involved in the protection of cyberspace in Poland, and they are not fully aware of their powers. The published document of the Ministry of Digitization also has a strategic character, but ultimately is a prelude to legislative changes fixing the protection system of cyberspace in Poland.

> *The position of the Undersecretary for Cybersecurity, announced by the Ministry of Digitalization, must be filled by a person who understands not only the issues of IT security in the technical sense, but has a broad understanding of systemic, organizational and legal problems.*

An overview of cyber strategy

Before the emergence of the Assumptions, the Cyberspace Protection Policy of the Republic of Poland was the main program document, adopted by resolution by cabinet ministers in June 2013. Therefore, it is not an act of general application: its recommendations apply only to the state administration. The Cyberspace Protection Policy was developed jointly by the Ministry of Administration and Digitization, and the Internal Security Agency, based on the experience of the Governmental Computer Security Incident Response Team (CERT.GOV.PL operating within the Internal Security Agency) and following the requests of the Standing Committee of the Council of Ministers concerning the proposals contained in the 'Government Cyberspace Protection Program of the Republic of Poland for 2009-2011- Assumptions.' The Cyberspace Protection Policy is a strategic document setting directions of legal and organizational solutions for the protection of cyberspace by the state administration. The strategic objective of the policy is to 'achieve an acceptable level of cyber security of the country.' The document concerns 'the systems of government administration, the legislative authorities, judicial authorities, local government, as well as strategic systems from the point of view of state security,' with the exception of classified ICT systems. It is also a declaration of participation of representatives of the government in ensuring security of information resources of the state and its citizens. The coordination of the implementation of the Cyberspace Protection Policy is the responsibility of the minister in charge of digitization.

The document was received with skepticism. Experts claim that the document displays a low level of knowledge, lacks sound analysis of threats and resources, and fails to make use of 'best practices' adopted internationally, including the European Union Agency for Network and Information Security (ENISA). The Cyberspace Protection Policy does not specify the issue of funding the implementation of security measures. The acceptable level of safety, which is not determined, is also enigmatic. It confirms the inadequate organizational and substantive preparation of the task force, partly resulting from under-funding of the project. Despite the obligation to implement the provisions of the policy, the process has not actually happened, as shown by the results of the control of the Supreme Audit Office in June 2015 (implementation of tasks by state authorities regarding the protection of cyberspace).

The Cybersecurity Doctrine of the Republic of Poland is an important strategic document covering similar goals to the ones outlined in the Policy. It was approved and signed in January 2015 by the President of Poland. The document developed by the National Security Bureau, like the Policy, is of strategic character, and, under the premise of the authors should be treated as a 'unified conceptual basis, providing a coherent and comprehensive approach to cyber protection and cyber defense.' The doctrine was created through consultations with the private sector and non-governmental organizations. It is also an executive document to the National Security Strategy of the Republic of Poland. Several pages long and the result of the work of the Bureau and external consultation, the document describes strategic objectives in the field of cyber security, internal and external threats, the concept of operational tasks and the role and nature of the entities involved. The doctrine is an important starting point for the implementation of strategic measures, and determines the vision of cooperation between the different actors in the field of cybersecurity. It also presents a list of major threats and challenges. The basic problem of the doctrine is that it is only of a conceptual and strategic nature. Its imperfection also shows in the absence of specific institutional recommendations, guidelines for the funding of the cybersecurity system, as well as an imprecise and inconsistent formulation of the issues of the so-called offensive capabilities and the role of the Polish Armed Forces in the system. In addition, while the doctrine mentions the public-private partnership, it does not state concrete ways of implementing such a project, focusing only on the task platform. Despite its obvious shortcomings and the too general conclusions it occasionally draws, the document is a valuable source from the point of view of the concept of the system. It is also evidence of a clear substantive progress and of greater reliability in identification and understanding of the problem of protecting cyberspace.

Another document worth mentioning here is the Doctrine of Information Security of the Republic of Poland, which has been created by the National Security Bureau, and indirectly complements the Cybersecurity Doctrine of the Republic of Poland. The draft of this document was published in July 2015, and is a response to the challenges of hybrid threats and information warfare. Given the structural changes in the National Security Bureau, its eventual completion is open to question. It is possible, however, that the newly created cybersecurity team will benefit from the experience of predecessors in this area.

The Law vs. Cybersecurity

An efficient cybersecurity system depends on the proper functioning of critical infrastructure (CI). The Law of April 26, 2007 on crisis management is significant in this context. It clearly defines the CI and its sub-systems (including energy supply and fuel, financial system, supply of food and water, health, transport and communication, rescue, ensuring the continuity of public administration). Thus, it is clear that all the ICT systems providing the continuity of critical infrastructure constitute the ultimate object of protection under a cybersecurity system. As showed by numerous campaigns aimed, inter alia, at the energy sector (e.g. power plants) and transport (e.g. computer systems at airports), the protection of CI systems is a key challenge to the security of the country. Negligence in this area may lead to disastrous consequences, both financial and material. The Law of July 18, 2002, on electronic services and the Law of August 5, 2010 on the protection of classified information provide a substantial input regarding cyberspace. These documents define 'computer system' in relation to: e-commerce services and classification, protection and processing 'of information, the unauthorized disclosure of which would or could cause harm to Poland, or would be adverse to its interests.'

Expert opinions and reports

Analyzing the issue of cyber security in Poland, it is worth paying attention to independent reports. These are usually a set of best practices, recommendations and proposals for change. The most obvious place to start would be the Kosciuszko Institute's 'The Security of Critical Infrastructure - ICT dimension' and the Research and Academic Computer Network's 'Cyber Security System of Poland', prepared for the Ministry of Administration and Digitization. The Supreme Audit Office's aforementioned 'Implementation of tasks by state authorities regarding the protection of cyberspace' should not be underestimated either. It assesses the state administration's risk management of hazards in cyberspace. Annual reports by CERT.GOV.PL ('Report on the State of Cyber security of Poland') are useful for a more thorough analysis of the current challenges and trends of the ICT security. 'Legal Analysis of Activities in Cyberspace' prepared by the Casimir Pulaski Foundation is also an important contribution to the discussion on international cooperation in the field of cyber security.

Conclusions and recommendations

1. Cybersecurity program for the coming years should assume the creation of a law regulating the system of protection of cyberspace in Poland.

2. The law must precisely define: a) the institutional framework, b) the division of competence of involved parties, and c) coordinating units. It is worth including the conclusions from the 'Cyber Security System of Poland' report. Given the structural constraints of state administration, it seems most appropriate to use a centralized model. A similar model has been proposed in the 'Guidelines', where the Ministry of Digitalization is a coordination body on the strategic and operational level.

3. The issue of public-private partnership should be expanded. The tasks and possibilities of cooperation of the public sector with business have been developed in strategic documents. Now is the time to create and legitimize a special contact group to foster this cooperation.

4. It is important that actions in the civil sphere do not fall within the competence of the tasks of the Minister of Defense. However, the exchange of experiences and information is necessary. The recommendation to establish a National Center for Cybersecurity prepared by the Ministry of Digitization seems rational here.

5. The position of the Undersecretary for Cybersecurity, announced by the Ministry of Digitalization, must be filled by a person who understands not only the issues of IT security in the technical sense, but has a broad understanding of systemic, organizational and legal problems. The ideal candidate for this position would seem to be an independent expert cooperating with both the state administration and the private sector and non-governmental organizations.

Author: *Kamil Gapiński, Casimir Pulaski Foundation, Cyber Security Program Coordinator*

The Casimir Pulaski Foundation is an independent, non-partisan think-tank specializing in foreign policy and international security. The Pulaski Foundation provides analyses that describe and explain international developments, identify trends in international environment, and contain possible recommendations and solutions for government decision makers and private sector managers to implement.

The Foundation concentrates its research on two subjects: transatlantic relations and Russia and the post-Soviet sphere. It focuses primarily on security, both in traditional and non-military dimensions, as well as political changes and economic trends that may have consequences for Poland and the European Union. The Casimir Pulaski Foundation is composed of over 40 experts from various fields. It publishes the Pulaski Policy Papers, the Pulaski Report, and the Pulaski Viewpoint. The Foundation also publishes "Informator Pułaskiego," a summary of upcoming conferences and seminars on international policy. The Foundation experts cooperate with media on a regular basis.

Once a year, the Casimir Pulaski Foundation gives the Knight of Freedom Award to an outstanding person who has promoted the values represented by General Casimir Pulaski: freedom, justice, and democracy. Prizewinners include: Professor Władysław Bartoszewski, Professor Norman Davies, Alaksandar Milinkiewicz, President Lech Wałęsa, President Aleksander Kwaśniewski, President Valdas Adamkus, Bernard Kouchner, and Richard Lugar.

The Casimir Pulaski Foundation has a partnership status with the Council of Europe and is a member of the Group Abroad, an association of Polish non-governmental organizations involved in international cooperation.

www.pulaski.pl