Editorial

Current Challenges in the Field of Cybersecurity

Ioan-Cosmin MIHAI
Vice President of the Romanian Association for Information Security Assurance

The evolving of the cyber environment generates development opportunities for the information society, but also risks to its functioning. The existence of vulnerabilities of information systems, which can be exploited by organized groups, makes the security of cyberspace a major concern for all the entities involved.

Although there are numerous and better performing methods of protection, ensuring information security in the cyber environment can't be achieved only by technical measures, being mainly a human problem. Security incidents are frequently generated by an inadequate organization of security policies and less because of a security system failure. In this context, it is necessary to develop strategies on cybersecurity by defining policies in this respect and campaigns to prevent and combat cybercrime.

At European level, several steps have been taken to adopt new policies against cybercrime and to ensure the cybersecurity. The Directive on security of network and information systems (NIS Directive), adopted by the European Parliament and the Council of the European Union on July 6, 2016, entered into force in August the same year, and benefits from a 21-month period to be implemented by Member States. The objective of the NIS Directive is to ensure a high common level of networks and information systems security in the EU and it requests essentials service operators and digital service providers to adopt appropriate measures for risk management, and to report serious security incidents to the competent national authorities. providers.

At national level, conceptual separation of key action directions is important: cyber defense, cybercrime, national security, critical infrastructure and emergencies, international cyber diplomacy and Internet governance. Separation is not the ideal situation, but it is a reality due to the complexity and diversity of cybersecurity as a whole. It is necessary to clearly define the roles and responsibilities of each responsible national institution.

An area that may be of interest in the future is given by cyber-risk insurance to cover the risks of attacks that may affect cyber-related services and infrastructures. The existence of breaches in cybersecurity can affect institutions and companies on many levels, both financially and reputational. An insurance against the risks in the virtual space could protect financially against losses in case of cyber-attacks.

Another segment that needs to be developed is the professional training in the field and the realization of awareness / understanding of the field at the decision makers' level within the public organizations.

Research and education in the field of cybersecurity must be priorities of public policies. Strengthening information security research, improving education and developing trained workforce are essential to achieving the overall cybersecurity policy objectives. Research and education policies will be effective only if they include the multilateral and multidisciplinary nature of cybersecurity as a fundamental and ubiquitous element in the culture, approaches, processes, systems and technical infrastructures.

Financing research and development in the field of information security is indispensable for bringing innovation and developing new technologies. Extensive access to cybersecurity education at all levels (pre-university, university and post-graduate) is necessary for the preparation, construction and improvement of the workforce. The many possibilities for universities, teachers and students from all study cycles (bachelor, master, and doctorate) to engage in cutting edge research are important for the development of a strong scientific community.

International cooperation plays a key role in this area, as cybersecurity challenges go beyond boundaries, extending to global interconnected systems. Collaboration with European and International entities is absolutely necessary, whether it is educational establishments, research centers, private companies or government institutions. Cooperation between institutions, organizations and the cybersecurity community can be useful in finding and fixing vulnerabilities. A proven cooperation mechanism in this regard is the coordinated disclosure of vulnerabilities.

Adoption of coherent public policies at Members State level on coordinated vulnerability disclosure and coordinated cross-sectoral action/trans-sectoral cooperation mechanisms will provide the necessary ecosystem to ensure security in the community.

The opening of communication channels, the creation of working groups and public consultation, the involvement of civil society and the public-private partnership are key directions that public policies should focus on.

The importance of the domain of cybersecurity in the global context of state security is highlighted by the many directions of development of the domain. Technological evolution and automation of the various sectors of activity of a society, characterizes cybersecurity as a priority dimension of action in the development of national defense strategies of states.

Concluding, the adoption of comprehensive and up-to-date cybersecurity legislation to support the development of state defense capabilities is a national priority. Ensuring a secure cyberspace is the responsibility of both the state and the competent authorities, the private sector and civil society. For the development of the cybersecurity culture, the most important levers are education and research, public-private partnerships and cooperation mechanisms

****This editorial was taken from the conclusions of the project SPOS 2017 – Current challenges in the field of cybersecurity – the impact and Romania's contribution to the field, written by Ioan-Cosmin MIHAI, Costel CIUCHI, Gabriel-Marius PETRICĂ, coordinated by European Institute of Romania. The project is available at the address: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS_2017_Study_4_FINAL.pdf*