Editorial

A Regional Strategy for Cybersecurity

Over the last two decades, the Internet and more broadly cyberspace has had a very important impact on all parts of society. Our entire life, social interactions and economies as well as fundamental rights depend on information and communication technology working seamlessly.

Securing network and information systems is essential to ensure prosperity and to keep the online economy running. Network and information systems can be affected by incidents (human mistakes, natural events, technical failures or malicious attacks) that are becoming bigger, more frequent and more complex. A high level of network and information security is essential to ensure consumer confidence and to keep the online economy running[1].

Cybersecurity is - according to ITU-T X.1205 - the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Cybersecurity is one of the biggest issues currently facing governments and businesses in the European Union (EU) and globally: it is important to mention that the European Union works on several fronts to ensure cybersecurity in Europe.

The European Commission and High Representative's *2013 Cyber Security Strategy* was the first comprehensive policy document of the European Union in this area. This Strategy covered the internal market, justice and home affairs and foreign policy angles of cyberspace. The Strategy was accompanied by a legislative proposal to strengthen the security of the EU's information systems.

The Strategy outlined the priorities for the international cyberspace policy of the European Union[2]:

- Freedom and openness: the strategy outlines the vision and principles on applying core EU values and fundamental rights in cyberspace.
- The EU's laws, norms and core values apply as much in cyberspace as in the physical world: responsibility for a more secure cyberspace lies with all players within the global information society, from citizens to governments.
- Developing cyber security capacity building: the EU engages with international partners and organisations, the private sector and civil society to

[1] http://www.computerweekly.com/opinion/What-to-expect-from-European-NIS-Directive

[2] *** European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013) 1 final

support global capacity building in third countries. This includes improving access to information and to an open internet, and preventing cyber threats.

- Fostering international cooperation in cyberspace: preserving open, free and secure cyberspace is a global challenge, which the EU is addressing together with relevant international partners and organisations, the private sector and civil society.

Another important for step in the process of EU's cybersecurity assurance was the adoption by the European Parliament of a proposal for a *Network and Information Security Directive* (*NIS Directive*) in March 2014[3].

Member states are required to adopt a national strategy that sets out concrete policy and regulatory measures to maintain a level of network and information security. This includes designating a national competent authority for information security and setting up a computer emergency response team (CERT) that is responsible for handling incidents and risks.

In this European context, it could be mentioned some important *regional* meetings and initiatives in the field of *cybersecurity*.

We can mention in this regard the *Regional Cybersecurity Summit* held in May 2015 at the Parliament Palace in Bucharest, Romania.

17 Central and South-East European states, members or non-members of the EU and NATO, were invited to attend the event, to present their cybersecurity policies and to tackle issues such as cyber threats and vulnerabilities, to try to identify opportunities for international and regional collaboration as well as to exchange good practices in this domain.

The summit brought together companies and government officials, public and private sector cybersecurity specialists from Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Hungary, Latvia, Lithuania, Macedonia, Moldova, Montenegro, Poland, Serbia, Slovakia, Slovenia, Ukraine, United States of America and Romania.

Several leading politicians and international experts have expressed their points of view on strategies in the field of cybersecurity during this Summit.

The Prime Minister of Romania, Mr. Victor Ponta said that Romania represents a stronghold of security, stability, predictability in a complicated region, where difficult wars are being carried out, especially in the energy area. In what concerns cybersecurity, the Prime Minister pointed out that cyberattacks take place every minute, but there are specialists who manage to block them. "*Each minute, each second there are attacks on the data systems, on the advanced technological, communication systems, which some people, whom you never see on TV, whom the press doesn't write about, but who exist (...) and manage to block, providing us the capacity of using the internet and the television and the control system of air and railways transports*," Ponta said.

The Prime Minister underscored the importance of the partnership between Romania and the USA in ensuring the cybersecurity.

"*The opportunity we now have to collaborate and be together with the* world *leader, namely the US government, the US companies, is an enormous opportunity that we want to make the most of. I am giving guarantees to all present that together the*

[3] http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis

United States of America – Romania (...) we can build a safer world and an environment in which our security, but also economic development should not live each second under the threat, under the danger of a cyberattack," Ponta added.

The US Deputy Secretary of Commerce, Mr. Bruce Andrews, said the United States sees great opportunities for collaboration in the field of cyber security. "*With so much of our lives connected to the Internet – from our critical infrastructure and national security systems to our cars and bank accounts – we know the urgency of addressing these new and growing cyber threats. Against this backdrop, there are many emerging opportunities to partner with our strong ally Romania to create a more secure cyberspace*," Andrews said.

"*Romania is on the front lines of the growing cyber conflict threat in the region. In the first half of 2014, the Romanian* National *Computer Security Incident Response Team issued 54,000 alerts – up from 44,000 alerts in all of 2013.We in the United States face this same threat, and we are eager to collaborate with you to face this emerging danger*," Andrews added.

The US Deputy Secretary of Commerce emphasized that Romania has already proven itself to be a world leader in information technology and showed that firms here are breaking new ground around the world. For example, he said, "*the Romanian company Bitdefender recently released one of the first security products made specifically for home networks: "Bitdefender Box.*"

„Your expertise in this area has not gone unnoticed *by American companies. Romanian is now the second most spoken language – after English – in Microsoft offices around the world.*

Because of the combination of technical sophistication *and language skills of your people, major U.S. companies like IBM, Hewlett-Packard, and Oracle have established regional offices here",* mentioned Andrews.

According to the US Deputy secretary of Commerce, in order to prevent future cyber-attacks, government and industry must work together to evolve and meet our shared challenges: "*On behalf of the United States Government, we greatly value our close relationship with Romania, and we are committed to strengthening bilateral commercial ties between our countries*"

"*Cybersecurity is a perfect example of a sector in which we can work together to increase national and economic security, create jobs, and provide mutual prosperity for both our economies. Together, I am confident that we can provide leadership to enhance cybersecurity capabilities across Central and Southeast Europe*" Andrews concluded.

Romania's Minister of Information Society Mr. Sorin Grindeanu mentioned that *cybersecurity* and *trust in public services* are a national priority with the Romanian Government, and in the current context, Romania is advocating the adoption of a new legislative package that regards personal data protection.

"*Romania aims to develop a dynamic information environment based on the interoperability of information society systems and services, to introduce security measures designed to increase protection of cyber infrastructure in accordance with the European and international regulations in force while also respecting the regulatory framework that regards the protection of the citizens' rights and freedoms. Cybersecurity and trust in public services are a national priority for the Romanian Government. (...) Romania is advocating the passage of a new legislative framework for personal data protection, which requires not just the consolidation and detailing of the right of the*

persons in question, but also *the obligations incumbent on those who process personal data*," said Grindeanu.

He added that the level of the European citizens' trust in online services is not encouraging, particularly because they have to reveal too much personal data.

"*Citizens' trust in online services can be consolidated by ensuring a high degree of cybersecurity, and also by improved transparency and efficiency. Yet, not be overlooked is the fact that as many as 72 per cent of Europe's Internet users are currently voicing reservations over the use of online services, especially e-commerce services, because they feel they have too much personal data to reveal, which means we should emphasize ensuring confidentiality, authenticity and availability of such data*," the minister added.

It is important to mention that Romania already coordinates a NATO-backed project aimed at helping to defend computer networks and communications systems in Ukraine, which is locked in conflict with Russia.

Romanian specialists in cybersecurity are tasked with defining the technical necessities and the architecture of a security system for protecting the country's IT&C infrastructure against cybernetic threats. Bucharest is providing project management and training for Ukrainian specialists to ensure the system yields results, too.

The Cybersecurity Summit meeting in Bucharest materialized in two important moments: the initialing of a *Joint declaration on cybersecurity cooperation in the region*, as well as the release of a pilot project for a *Centre for Cybersecurity Innovation* in Bucharest.

Now in the fourth year of publication, the *International Journal of Information Security and Cybercrime* (IJISC) will continue to analyze the cybersecurity phenomenon in all its complexity: from scientific research to policy developments in this important and actual domain.

Prof. Ioan C. BACIVAROV, PhD
President of Romanian Association for Information Security Assurance (RAISA)
Chairman Editorial Board of International Journal of Information Security and Cybercrime (IJISC)