REPUBLIC OF SERBIA

“Developments in the field of information and telecommunications in the context of international security“- Resolution 70/237

General appreciation of the issues of information security

Recognizing the great importance of assuring and developing information security, Republic of Serbia has set this issue as one of the strategic priorities in information society field. Use of information and communication technologies brings our society many advantages, efficient work processes, availability of information, e-government services, broader communication possibilities and other. Due to the increase of ICT usage and rapid development of technologies, the information security risks are raising, and the threats for the national and global security become higher. Cyber-attacks can harm the state security, disrupt critical infrastructure services, make severe financial damage, endanger privacy and personal data, etc.

In the interconnected cyber world, possibility of being attacked is high, and the range of cyber-attacks can be very wide, so many of the incidents could have global impact. Cyber security became a very important topic among the international subjects, and safe cyber space cannot be reached without the active involvement of different actors. States and other stakeholders have to cooperate and take appropriate steps to ensure an adequate level of information security, to be prepared for the attacks and raise citizen’s awareness of possible risks.

Efforts on the national level to strengthen information security and to promote international cooperation in this field

The National Assembly of the Republic of Serbia adopted the Law on Information Security in January 2016. This law is the basic foundation for the development of national cyber security system, with the goal to make important ICT systems safe and prepared, and to make all society subjects aware of the cyber risks. The Law predicts the established of the competent authority for information security. This authority has different tasks, such as preparing regulations that are in compliance with the national and international standards, cooperate with competent authorities of other countries, and conduct inspection on the law enforcement.

The Law defined the ICT systems of special importance in Serbia, which means that operators have to undertake the adequate technical and organizational measures in order to ensure the security of the ICT systems. These systems are: 1) ICT systems of public bodies, 2) ICT systems where the sensitive personal data is handled, 3) ICT systems in the areas of public interest (energy, transport, gas, banking, health care and other). They are recognized as
important, because they are used by operators to provide vital services, perform business activities and store personal data. The operators have to undertake the protection measures defined in the law and by-laws, in accordance with the national and international standards. The operators of ICT systems of special importance are obliged to inform competent authority on incidents which may have significant impact on violation of information security.

The Law established the National CERT within the Regulatory Agency for Electronic Communications and Postal Services. National CERT monitors the status of incidents on national level, provides early warnings, alerts and announcements, and reacts on incidents by providing the information on affected entities and persons, makes risk assessments and raises awareness on information security issues. It is regulated that the National CERT will cooperate with the similar organizations in other countries. The Law also regulates the crypto security and the protection against the compromising electromagnetic emanation.

In March 2016, Ministry of Trade, Tourism and Telecommunications formed the special workgroup for creating Cyber Security Strategy. The document will determine further plans and priorities in cyber security area. The same Ministry is starting a campaign “Smart and Safe”, which promotes the advantages of Internet and ICT usage in education, business and communications, and informs on potential risks and dangers. The campaign is made for the population between 10 to 19 years, their teachers, and citizens in general.

Ministry of Interior has recognized the importance of dealing with information security and in 2015 changed its organizational units to form a special Department for Information Security and a CERT. Now, with the Department for High-Tech Crimes the Ministry completed the preconditions for dealing with the issues of information security.

By the Law on Information Security Ministry of Defence has been given a status of being the independent operation of the ICT systems. One of the main responsibilities of the Ministry of Defence in the area of information security is the approval of the cryptographic products, distribution of crypto materials and the protection from compromising electromagnetic emanations.

The Office of the National Security Council and Classified Information Protection of the Republic of Serbia is responsible for coordinating the implementation of the national security policy and EU security policy on the national level (NSA), also the Office is responsible for adoption and implementation of the information security measures of classified information in state bodies.

Ministry of Trade, Tourism and Telecommunication, Ministry of Interior and the EU Commission are partners of the web portal “Net patrola”, where all the illegal or harmful content on the Internet can be reported. “Net patrola” is primarily designed for prevention of spreading pictures and video materials which contains sexual abusing of children and physical and psychological attacks on children. “Net patrol” is member of International Association of Internet hotlines (INHOPE).
Possible measures that could be taken by the international community to strengthen information security at the global level

In order to strengthen the security of global information and telecommunications systems, states should cooperate, especially by maintaining effective and responsive mechanisms for information exchange, alerts and announcements on cyber security incidents. For that purpose, states should appoint focal points and made contact information easy available. The special focus should be on the protection of critical infrastructure, especially if the incidents affects the territory of more than one state. The states should also cooperate on exchange of knowledge and education in this area.

Taking into account increased risks and characteristics of cyber-attacks in the interconnected world, international community should encourage the states to cooperate and make dialogues, to promote building of mutual cyber security capacities and give a support to international organizations who are designed for cooperation in the field of information security. Joint and effective cooperation will contribute to making of the global ICT environment safer and protected, where the states and citizens are secured from various risks in cyber world.
EXECUTIVE SUMMARY

Understanding the great importance of assuring and developing information security, this area is recognized in the Republic of Serbia as one of the strategic priorities in information society field.

The National Assembly of the Republic of Serbia adopted the Law on Information Security in January 2016. The Law established the competent authority for information security, with tasks to prepare regulations in accordance with national and international standards, cooperate with competent authorities of other countries, and conduct inspection on the law enforcement. The Law defined the ICT systems of special importance in Serbia, which operators will have to undertake the adequate technical and organizational measures in order to ensure the information security. These systems are: 1) ICT systems of public bodies, 2) ICT systems where the sensitive personal data are handled, 3) ICT systems in the areas of public interest (energy, transport, gas, banking, health care and other).

The competent authority conducts the international cooperation, and especially provides alerts on risks and incidents which have one of these characteristics: 1) are growing rapidly or have a tendency to become high risks, 2) exceed national capacities, 3) may have impact on more than one country.

The Law establish National CERT within the Regulatory Agency for Electronic Communications and Postal Services, which will, among the other duties, cooperate with the similar organization in other countries.

The Law also regulates the crypto security and the protection against the compromising electromagnetic emanation.

In order to strengthen the security of global information and telecommunications systems, states should cooperate, especially by maintaining effective and responsive mechanisms for information exchange, alerts and announcements on cyber security incidents. For that purpose, states should appoint focal points and made contact information easy available. The special focus should be on the protection of critical infrastructure, especially if the incidents affects the territory of more than one state. The states should also cooperate on exchange of knowledge and education in this area.

Taking into account increased risks and characteristics of cyber-attacks in the interconnected world, international community should encourage the states to cooperate and make dialogues, to promote building of mutual cyber security capacities and give a support to international organizations who are designed for cooperation in the field of information security. Joint and effective cooperation will contribute to making of the global ICT environment safer and protected, where the states and citizens are secured from various risks in cyber world.