The National Cyber Security Strategy and Action plan for the implementation of the Strategy

SUMMARY

The National Cyber Security Strategy is a document with which the Republic of Croatia intends to start planning, in a systematic and comprehensive way, the most important activities for protecting all the users of modern electronic services, both in the public and economic sectors and among the general population. The aim of the Strategy is to achieve a balanced and coordinated response of various institutions representing all the sectors of the society to the security threats in modern-day cyberspace. The Strategy recognises the values that need to be protected, the competent institutions and measures for systematic implementation of such protection. The Strategy is a statement of the cyber security stakeholders' determination to take measures in their respective areas of responsibility, cooperate with the other stakeholders and exchange the necessary information. It is a statement of their readiness to continue their own further development and adjustment, so that the Croatian cyberspace would be organised, available, open and safe to use.

The Strategy and Action plan for its implementation envisage the approach to cyberspace as the virtual dimension of the society. The goal of making the Strategy and implementing it by applying the measures elaborated in the Action plan is therefore consistent with the Cybersecurity Strategy of the European Union[1] and is directed towards achieving the maximum level of competence and coordination among all of our society's sectors, for an efficient implementation of law and protection of democratic values in the virtual dimension of today's society, that is, in cyberspace. Such a goal can only be achieved with a common, efficiently coordinated approach including a whole range of different institutions responsible for different sectors. The reason for this lies in the fact that the very complex area of cyber security covers all the segments of the society and largely exceeds the technical area from which it once arose with the rapid development of the Internet and accompanying information and communication technologies.

The fundamental issue in cyber security is therefore the issue of organisation, which is resolved in the Strategy through better and more effective connection of all the segments of the society, using as much as possible the existing bodies and their legal responsibilities. The recognised objectives in different areas of cyber security should be achieved by applying the measures elaborated in the Action plan for each individual objective of the Strategy. The description of the measures presented in the Action plan for the implementation of the Strategy shows that the Strategy will be implemented for the most part in the framework of the existing funds of the bodies competent for the activities in a particular measure and the bodies that will also be involved. The added value of these existing funds and other resources is achieved through organisational measures for the harmonisation and better coordination in various bodies' work on similar activities, a more efficient exchange of information and,

---

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, JOIN(2013) 1 final

generally, through the synergy of different institutions and society sectors that have so far not been sufficiently connected and coordinated when it comes to the activities related to cyberspace.

The intention of adopting the Strategy and Action plan and introducing a systematic and comprehensive approach to the area of cyber security is to achieve a number of objectives very important for the development of the entire society, in particular:

- Systematic approach in the application and development of the national legal framework to take into account the new, cyber dimension of the society;
- Implementing activities and measures to improve the security, resilience and reliability of cyberspace;
- Setting up a more efficient mechanism for information sharing in order to ensure a higher level of general safety in cyberspace;
- Raising the awareness of security of all cyberspace users;
- Encouraging the development of harmonised education programmes;
- Encouraging research and development, particularly in the area of e-services;
- Systematic approach to international cooperation in the area of cyber security.

The methodology of approach chosen to define the contents of the Strategy was based on determining the general goals of the Strategy, society sectors covered by the Strategy, and basic principles of approach to the implementation of the Strategy. Societal segments important for cyber security are divided into areas estimated to be of highest importance for Croatia at this level of development of the information society. The selected areas of cyber security are as follows:

- Electronic communication and information infrastructure and services, further divided into public telecommunications infrastructure, e-government infrastructure and electronic financial services;
- Critical communication and information infrastructure and cyber crisis management;
- Cybercrime.

Along with the areas of cyber security, the Strategy also recognises the interrelations among the areas of cyber security, thus ensuring coordinated planning of all joint activities and resources in the mentioned cyber security areas. The following interrelations among the areas of cyber security have been selected:

- Data protection (groups of protected information, such as classified information, personal data, trade secret);
- Technical coordination in the treatment of computer security incidents;
- International cooperation;
- Education, research, development and raising the awareness of security in cyberspace.

The Strategy is based on the existing legislation and responsibilities, but it recognises the need for certain laws to be revised through the implementation of the measures from the Action plan and harmonised with the recognised requirements of the society's virtual dimension,

which has already become an integral part of both the private and professional lives and activities of all citizens and institutions. The adoption of the Strategy cannot immediately solve all the problems that have occurred and accumulated throughout the past twenty years of rapid technological development and globalisation of the society, the problems that are now present in every facet of our society. The Strategy definitely represents the first step towards a systematic and lasting improvement of the current state in the area of cyber security and marks the beginning of introducing long-term and systematic care for all the future challenges in the society's virtual dimension, which is extremely important for the further development of the society.