# VI FEASIBILITY STUDY FOR IMPLEMENTATION OF THE NATIONAL CERT PROCEDURES AND INCIDENT MANAGEMENT REPORTING SYSTEM

## INTRODUCTION

The aim of the study is to direct Management of the National CERT to establish in the following steps functional organizations and operating procedures, primarily regarding identification, classification, and defining of (potential) incident priorities, incident and event tracking systems, methods of data exchange with other equal entities and competent authorities as well as dissemination of the relevant information and increase of awareness of information security and potential threats.

Additionally, the Study provides suggestions for the improvement, i.e. recommendations for the preparation of formal frameworks for the regulation of certain areas of constituent information security, namely the ICT system of particular importance in Serbia.

The importance of a timely and adequate response to incidents and identification of vulnerabilities which can be subject to misuse is also intuitively clear: this allows quicker and better implementation of the adequate measures aiming at reduction of potential damage. Regardless of whether the issue involves impaired secrecy, integrity, or availability of information goods, in general case (e.g. independent ICT system operators) consequences can be expressed as losses in terms of quantitative (financial) and reputational aspects. At the national level, incidents may indicate cyber attacks the scale of which can significantly impair operation of the ICT system of particular importance on the national level and they may even represent an element of attack of a foreign country on the Republic of Serbia. Moreover, the attacks may be potentially orchestrated in such a way to have a negative impact on more than one country.

The so-called Advanced Persistent Threats (APT) may pose a specific problem, since they are characterized by focus, sophistication, and highly probable prolonged presence in an ICT system before being discovered; such situations require a specific approach as well as urgent elimination of primary cause, identification of its range, and dealing with the consequences of such incident, which is primarily the responsibility of the attacked ICT system, although it may call for additional co-ordination of the National CERT Team with other relevant authorities.

To enable a timely and adequate response, it is crucial to have the right information at the right time. Constant shortening of such response time frame keeps raising awareness of the significance of the constant:

- monitoring of the events through ICT systems;
- exchange of information and co-operation with other institutions;
- research and analysis of the available information;
- issuance of preventive warnings, as needed;
- implementation of educative and awareness-raising activities involving information on potential threats and risks.

Without an adequate co-ordination and dedication to the above mentioned activities, it is impossible to adequately respond to potential threats.

## CONCLUSION

Adopting the Law on Information Security in the Republic of Serbia makes the first step in ensuring that adequate technical and organizational action for the management of risks to their Internet and information systems crucial for regular work operations is taken by the key service providers. The Law stipulates that the Regulatory Agency for Electronic Communications and Postal Services (RATEL) is authorized to co-ordinate and perform tasks of the National Centre for the Prevention of Security Risks in ICT Systems (National CERT).

As a part of this scientific research and preparation of a Feasibility Study for Implementation of the National CERT Procedures and Incident Management Reporting System, it has been procedurally regulated how the National CERT obtains information on an incident, how it treats such information and analyses the obtained data, how it stores the processed information and informs the general public or individuals on the manner in which it manages and handles risks or incidents. The process that involves receiving, processing, and reacting to information on incidents has been analyzed and appropriate draft procedures have been provided in order to regulate the process.

As a part of this study, we have also suggested the following classifications:

- Classification of information on risks and incidents;
- Classification of information on risks and incidents relating to the secrecy of information;
- Classification of the seriousness of incidents and risks;
- Categorization of attacks according to their impact on business operations;
- Classification of incident and risk seriousness level.

Implementation of the following suggested operating models, presented as separate documents and provided within the section “Annexes,” namely:

- Information Classification Policy,
- Incident Management Procedure, and
- Framework for Business Continuity Plan for CERT Platform,

would enable uniform operation of all community sectors that must unite and make a joint effort to prevent and fight against compromising the operation of information and communication systems.