Legislative Intent of the Law on Cybernetic Security – Approved by the Government on 30 MAY 12

(Executive summary)

I. Rationale

A distinctive growth in usage of information technologies leads on one hand to creation of information society, faster communication and large development of services has impact on the whole society. However, on the other hand, it deepens the dependence of the society on information technologies in all fields. Consequently, the risk of misuse of information technologies that might potentially lead to substantive damages grows significantly.

At present, the security of cyberspace is ensured by private entities without any regulations laid down by state bodies. Those entities often solve possible attacks randomly. They lack knowledge about previous attacks and have to solve them independently, which leads to inefficient increase of expenses. Furthermore, there is no single system of security standards, which would minimize potential damage arising from cybernetic attacks in the area of public governance. Finally, there is also lack of prevention system and timely warning against attacks.

Since the state power shall be executed exclusively within the state´s legal framework and private entities shall be regulated only by law, it is necessary to regulate the area of cybernetic security by law, which provides for the following:

- Division of obligations of entities, which are primarily important for the functioning of the state and others;
- Determination of roles of entities affected by the public-law regulation;
- Unification of terms used in the field of cybernetic security.

II. Basic Principles of the Proposed Legislation

The draft is based on the fact that private entities are owners of a significant part of the state´s information infrastructure, including the one of critical importance. The information services important for both state and private sector are usually provided by

private entities on commercial basis. Those private entities invest in securing their own infrastructure and are economically motivated to participate in protection of overall cybernetic security. At the same time, they are technically and legally competent to resolve cybernetic security incidents within their own infrastructure due to detailed knowledge of their own systems, direct technical control and legal relations. The state can never acquire the same rights while obeying the Constitution at the same time. Therefore, the solution of specifying one general authority of the central body (the National Security Authority of the Czech Republic – hereinafter "NSA") which cooperates closely with the private entities has been chosen. Hence, the new law has to regulate specific competences of the NSA as of the central authority responsible for cybernetic security, including decision-making, oversight and imposing of sanctions and to determine the relation of the NSA to other public governance bodies. The specific competences of the NSA shall not cover cases of committed crime. In such a case, other laws (namely the Penal Code), shall apply.

The draft legislation intends to divide the Czech cyberspace into the area of responsibility of the Governmental CERT, operated by the NSA, which shall be responsible for the information systems of the public governance and the critical part of the cyberspace (critical information infrastructure) and the rest falling within the cognizance of the National CERT (operated by a private entity on the basis of a contract made with the NSA).

The law also intends to introduce a special state of cybernetic emergency to be used in case of a large-scale cybernetic attack seriously endangering or disturbing security of the Czech Republic. The state of cybernetic emergency might be declared by the Prime Minister on the basis of proposal of the NSA Director.

The proposed legislation is based on the following basic principles:

1) Minimal impact on the rights of private entities.
2) Individual responsibility of administrators for security of their own network.
3) Respecting and strengthening of right to informational self-determination.

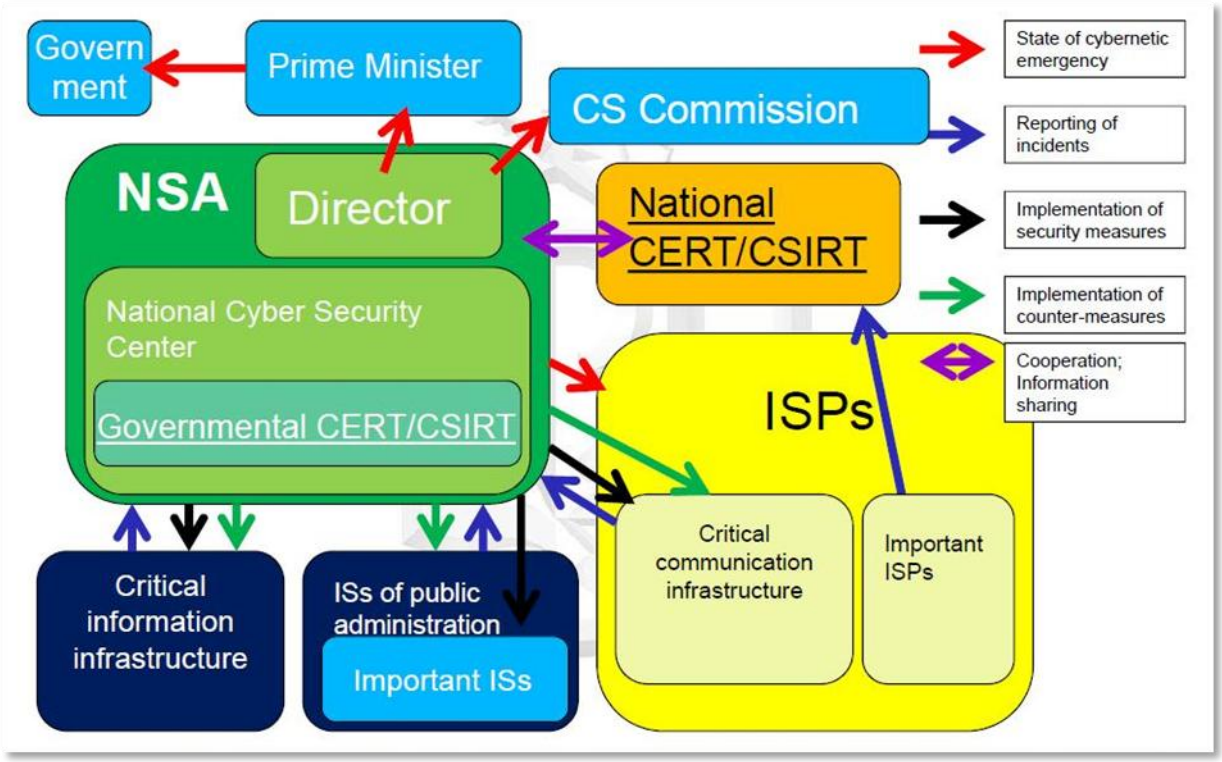
Three pillars of the proposed regulation are as follows:

1) Obligation of administrators and operators of important information systems to report contact details to either the National or Governmental CERT, as applicable

and obligation of administrators and operators of important information systems to report cybernetic security incidents.

2) Obligation of operators and administrators of critical information infrastructure to implement security measures prescribed by the NSA.

3) System of counter-measures prescribed by the NSA to be implemented in case of cybernetic attack.



III. Way Ahead

- **September 2012** – Initial operational capability of the Governmental CERT;
- **June 2013** – Presentation of the draft law to the Government;
- **July 2013** – Submission of the draft to the Parliament;
- **Beginning of 2015** - Entry into force;
- **31st December 2015** – Full operational capability of the Governmental CERT.