

Cyberspace and information security

Abstract

The dissertation deals with information security in cyberspace and cybersecurity. Within the academic community the topic is rather neglected, even though cybersecurity may be seen as a pillar-stone for the undisturbed performance of public administration.

The thesis deals with the topic in broader theoretical and practical contexts. Technological changes in society have major influence on legal regulation and practice. Because of that, the first part of the thesis focuses on the key social changes related to digital revolution and globalization, on the values of the information society and on the principles of cybersecurity regulation, as well as on the issues regarding the applicability of law within cyberspace.

The second part of the thesis discusses the role of public power in safeguarding the information security in cyberspace. The concepts of cyber defence and cybersecurity are discussed. The concept of information security is presented through the confidentiality, integrity and availability components. The international element is addressed with the perspective of selected rules of the second version of Tallinn Manual. In particular, the problems of attribution of cyber operations, reverse hacking (hack-back) or circumstances precluding wrongfulness of cyber operations are dealt with.

The third part of the thesis focuses on the Czech Cybersecurity Act (Act N. 181/2014 Coll. on the cybersecurity and on related changes). It mainly deals with the system of ensuring cybersecurity through administrative measures, which are the preventive security measures and the specific measures called warning, reactive measures and protective measures. The administrative measures issued so far by the Czech central administrative body, National Cyber and Information Security Agency, are analysed, as well as their impact in the Czech Republic. The thesis also deals with related topics, such as the legal obligation to hand over data, operational data and information, the remedy measures, the computer security incident response teams, or the parliamentary control over the National Cyber and Information Security Agency.

The examples of information security violations, conflicts of jurisdiction, international responsibility of states for cyber operations, and other related topics are discussed. Despite the specific features of cyberspace, the law is defended as a suitable instrument of regulation. The thesis also emphasises that the constitutional principle according to which state power has to be bound by the law needs to be applied in cyberspace as well.