In particular this includes risk mitigation strategies, more strict policies for data storage and data transfer, inclusion of digital signatures in data and software artefacts, in such a way data and software can be traced, Proofs of Retrievability for data integrity, and last but not least, third party monitoring and assessment of quality of cloud services.

Matej Myška, Pavel Koukal, Zuzana Vlachová, Ondřej Woznica:

With regard to the principle of predictability of law and legal certainty, we recommend that the United Nations push for the negotiation of an international treaty that would harmonize the basic issues of limiting the liability of information society service providers.

Niewiadomska-Szynkiewicz, Amanowicz, Wrońska, Kostkiewicz:

The Internet community growing and decreasing the age of people connecting to the global web raises enormous social risks, thus ensuring cybersecurity maintains a huge challenge for international organisations, governments, social communities and education systems.

To function effectively in an intelligent networked society and seize digital transformation opportunities, the community needs new and constantly updated digital competencies. Activities that improve digital competence and prevent cyberspace threats should be interdisciplinary and addressed to many groups of recipients with different needs, abilities, and ages. Universal information and media education is a socially signalled need and has its legislative and economic justification. Education, as well as preventive and protective activities, bring more practical benefits. They are more effective and less costly than reducing or eliminating negative individual interactions, social neglect or the effects of crime.

The critical tasks include raising public awareness of online threats, adopting legislation to the changing reality, international cooperation of government representatives and commercial companies, and investment in research and exchange of knowledge and experience.

Effective detection of network attacks requires collecting and processing as much data containing malware samples and vulnerabilities as possible. It is necessary to develop advanced algorithms and build efficient computer systems to support this process.

Particular emphasis such be put on development, and successful implementation of deep learning techniques combined with big data processing