Institute for Information Infrastructure Protection

Special Research

Regulatory Impacts on Cybersecurity Governance

This section will provide research on impacts by the European General Data Protection Regulation (GDPR) and other cybersecurity regulations. Our researchers examine the practical implications of privacy, data breach and general cybersecurity on governance issues. Their papers will also examine how regulatory changes may impact the creation of norms on the conduct of state and non-state activities in cyberspace.

PAPER #1:

Data protection as an emerging norm for cyberspace activities: two national approaches to balancing national security considerations with data privacy, "20190107-Housen-Couriel.Paper1-2dzbxa5 [https://www.thei3p.org/files/2019/03/20190107-Housen-Couriel.Paper1-2dzbxa5.pdf] ."

Deborah Housen-Couriel is an Israeli attorney specializing in cybersecurity and data protection issues for clients with global reach, and her practice is supported by independent cybersecurity research and teaching. She was a member of the group of experts for the Tallinn Manual 2.0 and is currently a core expert for the MILAMOS project on space and cyber law. Deborah chairs a Global Forum on Cyber Expertise [https://www.thegfce.com/] Working Group and serves as a member of the advisory board of the Hebrew University Cyber Security Research Center [https://csrcl.huji.ac.il/book/about-center].

Abstract: Data protection is emerging as an essential element of international cybersecurity and stability in cyberspace. Cybersecurity strategies, policies, and regulations increasingly include it as an inherent part of the advancement and achievement of national, regional and international cybersecurity goals. Moreover, this trend towards convergence of data protection and cybersecurity is underway in a diverse array of jurisdictions in the Western hemisphere, in Africa and in Asia. This development represents an important next phase in the governance of cyberspace at both the international and national levels, broadening the conceptual basis for government and organizational mitigation of cyberspace risks and threats. Especially given the present cyber threat landscape, partly characterized by hostile actors' intensive exploitation of data vulnerabilities, it is critical for regulators and policymakers to move ahead with the integration of data protection regimes in cyberspace – or "cyber privacy" – with cybersecurity laws and regulations. The EU and China regulatory models (respectively, the General Data Protection Regulation (GDPR) and China's Cybersecurity Law (CCL) draw global attention to the need for more robust and transparent balancing mechanisms between cybersecurity needs and privacy rights, ultimately contributing towards increased levels of cyber stability and security overall. The difficult challenge that lies ahead is the coordination at the regional and global levels of emerging cyber privacy regimes such as the GDPR and the CCL, in order to better leverage the regulatory tools that are becoming increasingly available for achieving this common aim.