TATuP Call

ZEITSCHRIFT FÜR TECHNIKFOLGENABSCHÄTZUNG IN THEORIE UND PRAXIS

Call for Abstracts:

"Cybersecurity"

TATuP special topic in issue 1/2020

Information and communication technology (ICT) has permeated almost all social practices and shapes our way of thinking, our interactions with others and with organisations and institutions; it changes our roles as citizens, workers or consumers. ICT as a complex and networked basic technology of the 21st century makes our world a richer, more efficient and highly interactive place – ICT can facilitate or even enable communication and interaction between people across borders, between countries and cultures. At the same time, however, complexity and a high level of networking make ICT susceptible to technical failure and criminal, terrorist or even warlike attacks, making it increasingly difficult to maintain the functionality of industries or supply infrastructures as complexity and networking increase. Modern societies whose ability to function is based on ICT are thus – to quote Ulrich Beck (1992) – "societies at risk". One of the great challenges of our time is to transform these societies into "risk societies", i.e. societies that organize themselves adequately against corresponding risks and find a socially acceptable and accepted balance between security and other values. This transformation is the starting point of the TATuP theme "Cybersecurity".

In 2014, the annual cost of cybercrime worldwide was more than $400 billion; at the same time, the market for all available security products grew by 14.3% between 2011 and 2014 (CSIS 2014). From a social perspective, not only the direct costs (e.g. repair costs, fraud-related losses), but also indirect costs (e.g. costs of preventive measures) and implicit costs (e.g. lower productivity increases due to lower trust in digital transactions) are attributable to cybersecurity violations (Bauer and van Eeten 2009). Given such figures, it is not surprising that current cybersecurity debates are characterized by an emphasis on ever larger and more diverse threats ranging from cybercrime and cyberespionage to cyberterror and cyberwar (Dunn Cavelty 2014). Cybersecurity has thus also become a matter for state actors; expenditure on defense-related aspects of cybersecurity is rising (Brito and Watkins 2011; Boulanin 2013).

This brief overview already points to the danger of thematically narrowing down discourses on cybersecurity: The more societies rely on functioning ICTs, the more they tend to place security above all other values on which our societies are built. As a result, boundaries that have constituted our social, institutional, legal, and moral world so far are questioned, compromised, or relativized. Traditional differentiations and demarcations of separate social spheres such as family and friendship, labor, politics, education, commercial activity and production, healthcare, research, etc., each determined by contextual norms and rules, are threatened by ICT. Concepts such as informed consent, personal data or anonymity as well as the underlying values such as autonomy, fairness, privacy and responsibility are affected. These values can be overridden by the value of security if cyberthreats are seen as a fundamental disruption of the current way of life. How much security is needed is controversial. The existing repertoire of policies and rules may already be sufficient since societies are used to taking risks and acting when needed (Odlytzko 2019). Creating cybersecurity

therefore not only means overcoming technological barriers, but also a deeper understanding of the changes resulting from the digitalisation of modern life. It requires a multi-stakeholder perspective in which experts from different scientific disciplines as well as from different professions must be involved.

References

Bauer, Johannes; van Eeten, Michel (2009): Cybersecurity. Stakeholder incentives, externalities, and policy options. In: Telecommunications Policy 33(10–11), S. 706–719.

Beck, Ulrich (1992): Risk Society, Towards a New Modernity. London: Sage.

Boulanin, Vincent (2013): Cybersecurity and the arms industry. In: SIPRI Yearbook 2013: Armaments, disarmament and international security, S. 218–226.

Brito, Jerry; Watkins, Tate (2011): Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. Mercatus Center Georg Mason University, Working Paper No. 11-24. Online verfügbar unter: https://www.mercatus.org/system/files/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy_0a.pdf, zuletzt geprüft am 12.04.2019.

Dunn Caveltry, Miriam (2014): Breaking the cyber-security dilemma. Aligning security needs and removing vulnerabilities. In: Science and Engineering Ethics 20(3), S. 701–715.

Odlyzko, Andrew (2019): Cybersecurity is not very important. Working Paper. Online verfügbar unter: http://www.dtc.umn.edu/~odlyzko/doc/cyberinsecurity.pdf, zuletzt geprüft am 15.04.2019.

Contributions requested

For the TATuP issue "Cyber Security", contributions are sought that address the subjects outlined above from the point of view of technology assessment and evaluation and cover, for example, technological developments in cybersecurity, the connection between cybersecurity and critical infrastructures, attack scenarios and their possible (social) effects, processes of social change, aspects of cybersecurity discourse at national, European and/or global level, political discourses and reactions, as well as considerations on weighing cybersecurity against other (moral) values. In doing so, the attempt should always be made to consider different stakeholder perspectives. The above list of subjects is not exhaustive; therefore, the editors of the TATuP issue would like to encourage potential authors to submit abstracts with related but not explicitly mentioned topics. This applies in particular to submissions that are concerned with whether disruptive changes are to be expected in the area of cybersecurity (e.g. with regard to availability, confidentiality, integrity) as a result of new technological, organisational and/or legislative developmentals, or whether continuous lines of development can be assumed.

Editors of this TATuP special topic

Karsten Weber (OTH Regensburg), Markus Christen (Universität Zürich) and Dominik Herrmann (Universität Bamberg)

TA TuP Call

ZEITSCHRIFT FÜR TECHNIKFOLGENABSCHÄTZUNG IN THEORIE UND PRAXIS

Submissions

Please send your abstract via email to redaktion@tatup.de by **June 06th 2019** at the very latest. Please respect the following directions:

- max. 3000 characters incl. blanks;
- the editorial office will correspond with the author submitting the abstract;
- name all authors with full names, email addresses and institutional affiliations.

Schedule

June 06th 2019: deadline for submitting your abstract.

end of June 2019: decisions on inviting authors to submit a full manuscript.

September 23rd 2019: deadline for submitting your full manuscript.

as of mid-november 2019: feedback from the reviewers followed by authors' revisions.

end of March 2020: publication.