European Journal for Security Research (2020) 5:1–3
https://doi.org/10.1007/s41125-019-00063-8

EDITORIAL

Digitalization and Its Security Manifestations

Sabrina Ellebrecht[1] **· Stefan Kaufmann**[2]

Received: 15 August 2019 / Accepted: 25 November 2019 / Published online: 13 January 2020

Digital technologies increasingly penetrate societal life. They do so to the extent of significantly transforming public and societal security. CCTV cameras, body scanners, and sensors are as much an ordinary part of our public spaces, as satellites, digital technologies, and communication media have restructured our social relations and the public sphere. On a global scale, these transformations are further reflected in phenomena such as cyberwars or gradual information warfare, and in the growth of cybercrime. The notion of a (digitally) networked society further condenses this. As a networked society is dependent on its (digital) infrastructures, the security of those very infrastructures requires its own securing. This interplay between digitalization and vulnerability resonates in the term *critical infrastructure* and brings about new processes and forms of prevention, preparedness, and of intervention in the security sector.

Digitalization unfolds, provokes, and shapes different manifestations of security. It leaves a mark on the quality of public and societal security and affects the way it is organized, sustained, endangered, and at risk. A digital technology that is dedicated to security does not *per se* deliver, establish, or increase security. Just as is the case with security technologies in general, digital technologies are part of complex socio-technical constellations. Digital technologies and processes allow law enforcement agencies and rescue services to perform and decide on the basis of more, or rather *big data*. They allow for protection, monitoring, and control without physical interference and actual presence. Generally, digitalization accelerates, expands, and dramatizes processes. When concerned with public and societal security, these effects are given just another spin. This Special Issue is concerned with the specific characteristics and qualities digitalization adds to the provision, the service, the production, and the organization of public and societal security. It focuses on three specific aspects related to digitalization: the trend toward datafication, the concept and

✉ Sabrina Ellebrecht
sabrina.ellebrecht@css.uni-freiburg.de

[1] Centre for Security and Society, Albert-Ludwigs-Universität Freiburg, Werthmannstr. 15, 79098 Freiburg, Germany

[2] Institute of Sociology, Albert-Ludwigs-Universität Freiburg, Rempartstr. 15, 79098 Freiburg, Germany

the dealings with automated or even autonomous processes, and the deployment of digital communication media by security agents.

Datafication The generation and use of data is anything but new. Data are used to delineate our societies and their perceived problems: We count the resident and migrant population, we count criminal offenses, and we expose the probability of risks and dangers to make statements about the security conditions of our society. The technological developments of recent years, however, allow for forms of data collection, storage, and processing which—in quantitative and qualitative terms—are fundamentally beyond counting, accumulating, and taking stock. The following characteristics are part of this new datafication which is essentially driven by digitalization: First, digital technologies provide for a so-called "data voluntarism": data are deliberately generated by individuals, institutions, things, vehicles, etc.—*on purpose* for individual performance monitoring or *en passant* through network activities—and made available. Anything that occurs with, around, inside, by means of, or in front of digital technologies can be turned into data. Second, data that have been collected in very different contexts can be matched or even merged with other data. This kind of surveillance is no longer based on an observation (of behavior or patterns of behavior) but on data analytics. Surveillance turns into dataveillance. Third, data are the basis for automated recognition and comparisons, for example through pattern recognition on photographs or different kinds of data matching. Fourth, the generation and the meaning of knowledge itself have been transformed through big data science. This has provoked high expectation toward the predictability of social action. In order to prevent an all-embracing surveillance, digitalized data require new legal provisions for its collection, storage, forwarding, sharing, and processing.

Automatization and Autonomization The trend toward autonomous processes can be understood as a further qualitative level of automatization. There is no clear-cut criterion whether a machine is to be considered an automat or an autonomous thing. For the case of autonomous driving, for instance, it is debatable whether one can, in fact, attest autonomy or whether the vehicle is rather highly automated. The question of the determinateness or non-determinateness of systems serves as an ideal–typical distinction. On the one hand, automated systems fulfill clearly defined tasks. These are successively processed by machines according to defined and clearly structured sequences or steps. It is in this respect that the systems are determined. On the other hand, autonomization is based on forms of machine or deep learning. The system becomes, at least partially, the black box, whose behavior cannot be predicted at any time. The notion of determination blurs into consequence. Autonomized processes can greatly expand the operation and solution options of machine systems, but with a tendency to lose control of the system or system decisions. In the security field, such forms of artificial intelligence are particularly prevalent where rapid situational decisions are required in complex situations such as mass panic, evacuation, large rescue emergency situations, and the like. Finally, decision-support tools are based on algorithms, which means that they offer automated decision processes.

Mediatization Electronic mediatization changes the way we communicate, interact, organize, and plan things. Mediatization drives and reconfigures the interrelation between proximity and distance as well as between time and space. Equipped with digital technologies, common action no longer needs physical or analogue

presence. This is even true in the case of emergency situations, where medical assistance is organized remotely. Moreover, digital technologies add a tele-dimension to socio-technical constellations. The term "telematics" is composed of the terms "telecommunications" and "informatics" and refers to the digital linkage of at least two information systems. Telematization processes not only enable the transmission of data, images, or information, but also a multiple interaction and relationship management over a distance. The digitized networking of more and more devices and systems affects our lives in many ways. Using tele-banking, for example, account statements can be viewed or bank transfers can be made. Tele-work allows not only the independence of a particular computer or workplace, but also a fundamentally new division of labor, a redistribution of technical and human actors.

The six articles collated in this Special Issue describe and analyze the specific security manifestations that digitalization and digital technologies bring about. They do so by way of specific examples. *Hans-Jörg Albrecht* traces in how far data have become "the core of security policies." He unfolds different examples for data-driven policing, such as predictive policing, and risk control programs. Against the background of ever increasing volumes of data, he argues for a strengthening of personal data security and calls to seriously deal with data retention policies and deletion. *Christoph Hubig* systematizes the difference between automatization and autonomization. Distinguishing between operative, strategic, and moral autonomy, Hubig argues that the latter can only be a human responsibility. *Timo Rademacher* twists this claim for moral autonomy as he argues for a right to violate the law. He analyzes the legal contours of impossibility structures, i.e., of those technical mechanisms that could prevent humans from acting unlawfully. *Jo Reichertz* offers an example of digital surveillance and automated evaluation by discussing in how far intelligent camera systems are able to evaluate group dynamics in general and collective escalation processes in particular. While intelligent camera systems allow for a close-up of group emotions, the intention of tele-medical constellations allows the physician to take a distance. *Nils Ellebrecht* and *Andrea zur Nieden* discuss the implications of tele-diagnosis and tele-medicine. Drawing on the example of police officers using messenger services to share information on enforcement activities, *Stefan Jarolimek* calls for media literacy for security personnel, especially for the police.

Acknowledgements Open Access funding provided by Projekt DEAL.