Österreich Z Soziol (2019) (Suppl 1) 44:115–134
https://doi.org/10.1007/s11614-019-00350-7

ÖZS

HAUPTBEITRÄGE

Governing through cybersecurity: national policy strategies, globalized (in-)security and sociotechnical visions of the digital society

Christian Haddad · Clemens Binder

Abstract By exploring the political strategies that seek to advance and implement a "culture of cybersecurity" in Austria, we argue that the regimes of digital safety and security (DS&S) that are emerging worldwide should not be merely understood as a political reaction to the risks brought about by digitalization. Rather, cybersecurity further constitutes an active site where the incipient digital society is collectively (re-)imagined, negotiated, and created. As such, cybersecurity policies present sites of political articulation and intervention where the very contours of an emerging digital society and the socio-technical relationships of power and control deemed necessary to govern its emergence are (re-)assembled. Our research prompts a rethinking of the relationships between cybersecurity and the digital society to the extent that cybersecurity represents a new *globalizing* form and rationality of security that encodes and enables new forms of control and intervention, but also new responsibilities at the interface between the state, society, and individuals.

Keywords Cybersecurity · Digitalization · Digital safety and security · Global security · Governmentality · Sociotechnical visions · Security policy

Regieren durch Cybersicherheit: Nationale Strategien, globalisierte (Un-)Sicherheit und soziotechnische Visionen der digitalen Gesellschaft

Zusammenfassung Die konzentrierten nationalen Strategien der Schaffung und Implementierung einer „Kultur der Cybersicherheit" müssen als Ausdruck weltweit entstehender globalisierter Regime digitaler Sicherheit verstanden werden. Diese

C. Haddad
Institut für Wissenschafts- und Technikforschung, Universität Wien, Wien, Austria

C. Haddad (✉) · C. Binder (✉)
Österreichisches Institut für Internationale Politik—oiip, Berggasse 7/1, 1090 Wien, Austria
E-Mail: christian.haddad@oiip.ac.at; christian.haddad@univie.ac.at; clemens.binder@oiip.ac.at

neuen Cybersicherheitsregime stellen jedoch nicht lediglich eine Reaktion auf zahlreiche neue Risiken und Unsicherheiten im Kontext der Digitalisierung dar, sondern auch ein Artikulationsfeld entstehender digitaler Gesellschaften. Cybersicherheit ist demnach ein Artikulations- und Experimentierfeld, in dem sowohl die soziotechnischen Visionen einer wünschenswerten digitalen Gesellschaft als auch das Ensemble von Macht- und Regierungstechniken (neu) entworfen werden, die diese Gesellschaft hervorbringen und absichern sollen. Die vorliegende Untersuchung soll eine Rekonzeptualisierung des Verhältnisses zwischen Cybersicherheit und digitaler Gesellschaft dahingehend anstoßen, dass Cybersicherheit eine neue und globalisierte Form und Rationalität von Sicherheit darstellt, in der die Autoritätsverhältnisse und Verantwortlichkeiten zwischen Staat, Gesellschaft und Individuen neu geordnet werden.

Schlüsselwörter Cybersicherheit · Digitalisierung · Globale Sicherheit · Gouvernementalität · Soziotechnische Visionen · Sicherheitspolitik

1 Introduction

> Our freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security, too.—European Cybersecurity Strategy (EC 2013, p. 2)

In his inaugural speech to the European Parliament, President of the European Commission Jean-Claude Juncker stated that one of the major challenges ahead was the promotion and completion of the "Digital Single Market" (Juncker 2014). Estimating an additional economic growth of € 250 billion generated by accomplishing a digital single market, the EU's strategy strongly articulates these promissory links between prosperity and digitalization (EC 2015). Worldwide, digitalization has become part and parcel of problematizations and strategic visions to achieve economic growth, prosperity, and political inclusion, particularly through its perceived role in innovation and in promoting a knowledge-based economy. Moreover, framed as the "backbone of economic growth", digitalization is thought of as inseparable from the values that underpin a liberal free-market society—values that, in turn, call for and depend on protection through institutions and policies that allow for cyberspace to develop further in a safe and secure manner. The digital infrastructures deemed vital for this desirable future to take shape are increasingly exposed to newly emerging security threats and multiple forms of criminal activity, such as hacking, fraud, intrusion, and data and identity theft. Every week, banks, private enterprises, as well as public institutions, are subject to multiple cybercriminal attempts (Cyber Security Steering Group 2018).

Policy discourses thus articulate the need for novel regimes of (cyber-)security that protect citizens, consumers, and entrepreneurs from the multiple and inherently novel kinds of risks and threats that occur in a society increasingly interlaced with digital technology. Somewhere in these tensions between visions of a promissory

future on the one hand, and problematizations of new threats and insecurities on the other hand, digitalization has become a key challenge and a governmental obligation.

1.1 Digitalization and the need for a culture of cybersecurity

Not least because of the disruptive potential of digital technologies and the rapid pace of their evolution, visions of digitalization are imbued with notions of uncertainty and concerns over detrimental ramifications (ENISA 2018a, 2018b). For policy makers, enterprises, and citizens alike, a pressing question thus is how to prepare for the digital future: How, if at all, is it possible to shape the processes of digitalization and steer digital technologies into socially and politically desirable directions? And, given all these risks and uncertainties, how is the process of digitalization rendered safe and secure—and for who?

Because this future is perceived as simultaneously somehow both inevitable and highly volatile and elusive, and implications for society are also hard to foretell, cyber policies build on a plethora of anticipation and forecasting work resulting in risk assessment exercises and speculative scenarios that inform strategic policy visions. More often than not, in these visions, the possibility for a desirable digital future has become increasingly tied to concerns for cybersecurity that articulate the need to envision and bring into existence a veritable "culture of cybersecurity" not only composed of safe technologies and robust institutions but also of digitally prudent and skilled subjects—citizens and professionals who act competently and responsibly in cyberspace.

1.2 Situating our argument: envisioning the digital future through cybersecurity

Governments and international organizations worldwide have started to formulate specific cybersecurity strategies to tackle the emerging threats in and from cyberspace. According to an OECD (2012, p. 5) report, a "new generation of government policies" on cybersecurity has taken shape in several countries, including our case study of Austria, where a national cybersecurity strategy (Austrian Cyber Security Strategy, hereafter abbreviated as "ACSS", see BKA 2013a) was developed in 2013. These new policies are characterized by similar strategic goals and focus areas, such as the increasing reliance on public-private partnerships and international cooperation alongside significant reforms of governmental structures.

Against this background, this paper zeroes in on the ACSS as a particular site to study how visions of the digital future are articulated with concerns of security. Sensitized by research perspectives from critical studies of security as well as from Science & Technology Studies, we argue that these various interrelated efforts to build a novel regime of cybersecurity and, correspondingly, a "culture of cybersecurity" (ENISA 2018c) constitute a techno-political experimental field where the contours of the emerging digital society are collectively imagined, articulated, negotiated, and acted into existence. Our argument is based on the proposition that cybersecurity policies, which are being developed in several countries worldwide, are not to be understood as mere reactions to a technological transformation unfolding

independently from political steering and governance. Rather, we hold that cybersecurity policies are active sites where the normative and institutional coordinates that guide the emergent digital future are imagined, spelled out, and transformed into strategies.

Discussing our findings in the context of sociological literatures on digitalization, security, and governmentality, we conclude by proposing that cybersecurity can be analyzed as a new and "globalizing" political rationality that gradually gives rise to new regimes of digital safety and security (DS&S). As such, cybersecurity holds the potential to critically transform and undermine the normative orders and institutional boundaries characteristic of liberal democracies grounded in a separation between internal and external security, between a public and private sphere, and between state and (civil) society.

2 Research framework

2.1 Background, materials and methodology

The original impetus for this research came from an expert and stakeholder workshop on "*Digital Safety & Security—political and technological chances, challenges, and strategies for a digital society*", organized by the authors, at the Austrian Institute of International Affairs (oiip) in cooperation with the Austrian Federal Ministry of Defense (bmlvs). Discussing the state of Austria's cybersecurity policy, the participants broadly concurred in their assessment that a veritable "culture of digital safety and security" is desperately needed, however still lacking in Austria. However, opinion diverged considerably as to what this culture means exactly and what should be done to bring it into existence (oiip 2017).

Sensitized by these narratives, we placed at the center of our analysis the Austrian Cyber Security Strategy (BKA 2013a), which presents the central document in Austria's nascent DS&S regime. Furthermore, we traced links to a range of other national policy documents that articulate cybersecurity within broader concerns for security. These documents include the Austrian ICT security strategy (Republic of Austria 2012), the Austrian Security Strategy (BKA 2013b), and the Austrian Program for Critical Infrastructure Protection (BKA 2015). As the Austrian regime cannot be understood in isolation, we further included policy documents from inter-/supranational organizations that were frequently referenced in Austrian policy documents (OECD 2002, 2012; EC 2013, EU 2003, 2016).

Methodologically, our research is based on basic tenets of interpretive policy studies (Wagenaar 2011). The documents were analyzed using coding strategies sensitive to discursive articulation and framings (Charmaz 2006) as well as on mapping strategies drawn from situational analysis (Clarke 2005). Doing so enabled us to complete four processes: to discern the multiple meanings of cybersecurity for and in (visions of) an emerging digital society; to analyze problematizations of cybersecurity in line with the various solutions suggested to confront these problems; to examine the policy strategies articulated to bring about a "culture of cybersecurity"; and to identify the different forms of knowledge, the institutional arrangements and

policy instruments, and the forms of subjectification invoked and mobilized in the making of cybersecurity in Austria.

2.2 Theoretical perspectives: combining sociotechnical imaginaries and governmentality studies

The incipient digital society is understood as both a present reality and a projection of a societal future imbued with a range of opportunities and risks. Drawing from Science & Technology Studies, we thus approach digitalization in terms of a sociotechnical imaginary of a developing digital society. Introduced in an effort to better conceptualize the performative power of visions in the making of societal futures, the notion of sociotechnical imaginary refers to "collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology" (Jasanoff 2015, p. 5; Jasanoff and Kim 2009).

This literature suggests that (sociotechnical) visions are powerful projections to the extent that they materialize in policy documents, processes, institutions, and political programs and trickle into the strategies of a variety of social actors and public institutions. Furthermore, these visions shape normative conceptions, such as conceptions of citizenship and democracy, and help (re-)define relations between science and society, public and private, or state and market. For our purpose, conceptualizing the digital society as an overarching imaginary helps examining the various (and even partially conflicting) efforts undertaken in diverse fields by a multiplicity of actors with different, even diverging, interests that all contribute to shaping the emerging digital society in an intentional, yet highly distributed, manner. On this basis, we analyze how visions of the digital society are performed through strategies of cybersecurity and how particular notions of power, governance, and control are articulated in and through the policy concept of a "culture of cybersecurity" that needs to be established to safeguard a desirable digital future.

Our approach to sociotechnical visions of digitalization is embedded more comprehensively in a theoretical framework of governmentality studies (Dean 2010; Gottweis 2003). Understood in broad terms to include various and heterogeneous authorities and actors, governmentality studies conceptualize government as "problematizing activity" to the extent that "ideals of government are intrinsically linked to the problems around which it circulates, the failings it seeks to rectify, the ills it seeks to cure" (Rose and Miller 1992, p. 279). Conceptualizing the ACSS as a "governmental program" that articulates particular political rationalities ("policy discourses") and technologies ("policy instruments") into regimes of government (Dean 2010, pp. 30) allows us to analyze cybersecurity policies in terms of an emerging regime of digital safety and security (DS&S). Broadening the notion of policy through lenses of governmentality further helps to bring into critical perspective the performativity of policy visions that articulate a link between a present state problematized as lacking and the strategies to transform this lacking into a better future (no matter how "better" is actually defined). More concretely, these visions articulate the forms of knowledge and expertise, the relations of power and authority,

and the practices of (self-)conduct and subjectification that are (re-)assembled and articulated in the incipient regime of DS&S.

3 Problematizing cyberspace through the lenses of security

How did cyberspace become an obligation of government and a matter of political problematizations that render cyberspace a (national) security issue? The following sections start by exploring the historical genealogies of cybersecurity policy in Austria before taking a closer look at the articulation of a national cybersecurity strategy.

3.1 Securing cyberspace: historical context of Austria's cybersecurity policy

Digital threats grow with the progress of the digitalization of society and seem to be hard to tackle using conventional security practices. Both attacks and attackers appear polymorphous and volatile, permeating easily the meshes of conventional safety nets and flying below the radar of security apparatuses. Cyberattacks on critical infrastructure, the theft and making public of sensitive private information, or the deliberate tinkering with national elections from abroad span the field of numerous digital safety and security threats (Dunn Cavelty 2013; Rid and McBurney 2012). Some extreme scenarios even float the idea of a massive blackout holding the potential to unleash a regressive state of exception with dramatic implications for individuals as well as for the socio-political order as a whole (Dunn Cavelty 2013).

In Austria, cybersecurity policy emerged from a general endeavor of digitalization and its perceived opportunities. In the 2008 government agenda (BKA 2008), digitalization was seen mainly as a possibility for economic growth and prosperity; threats and insecurities were not perceived as a critical state task. However, a few years later, former Minister of the Interior Johanna Mikl-Leitner stated in the yearly intelligence report that cyberattacks constitute a growing threat to Austria's security with no signs of stopping (BMI 2011).

Around that time, a series of processes had taken shape that problematized the surging landscapes of threats and risks in cyberspace. Under the auspices of the Board of Trustees for a Secure Austria (Kuratorium Sicheres Österreich, KSÖ), a stakeholder consultation of various actors from the public and private sector preoccupied with digital safety and security, found various shortcomings and lamented the lack of an explicit cybersecurity policy as a governmental responsibility. This stakeholder process resulted in a risk matrix (KSÖ 2011) and a detailed risk report (KSÖ 2012), mapping and classifying the cyber threats in Austria (Borchert et al. 2015). These reports contributed to an understanding that the increased deployment of information and communication technologies (ICTs) exposed private, social, and economic life to various security risks. As an outcome of this deliberation, the ICT Security Strategy of 2012 (Republic of Austria 2012) marked a milestone in the making of the DS&S regime in Austria.

In the ICT Strategy, cyberspace was conceptualized as essentially embedded in the larger information and communication infrastructures, hence making ICT

security a primary policy objective. However, crucial to that strategy is that it links cybersecurity to the general notion of economic growth through digitalization:

> Today the general welfare of the state depends to a considerable extent on the availability and proper functioning of cyberspace. While growth rates in Internet usage, e-commerce and e-government are significant and cyber crime [...] is on the rise, the Internet and computer skills of the users have remained virtually unchanged (Republic of Austria 2012, p. 4).

Whereas these incipient concerns of the ICT strategy generally are *users* as well as *technical systems*, the Strategy further laments that "an overarching structure for cyber security management is largely lacking" on the *state level* (Republic of Austria 2012, p. 7). These structural deficits were addressed in the ensuing Austrian Cyber Security Strategy (BKA 2013a), which has moved cybersecurity into the center of Austria's general security policy. The general security strategy of 2013 explicitly turns to cybersecurity, stating that

> cyber-crime, cyber-attacks, the misuse of the internet for extremist purposes and network security are serious new challenges for all stakeholders and require wide-reaching cooperation as part of a comprehensive policy (BKA 2013b, p. 11).

This new saliency was further reflected in the work program of the 2013 elected government that set the implementation of the ACSS as one of its main security policy objectives on the premise that cyberspace is increasingly becoming a "*vital field of action* for the state, economy, science, and society" (BKA 2013c, p. 78, emphasis and transl. by authors).

With the aim of strengthening the national risk management capacities and the overall level of resilience, cybersecurity has been inscribed into the general security strategy. As the digital technologies permeate and interconnect multiple, often critical, facets of life, cyberspace is increasingly regarded as a critical infrastructure in policy discourses (see BKA 2013b, 2015). Whereas Austria's national cybersecurity strategy came relatively late compared to that in other OECD countries, its approach is described as distinctive of a new generation of cybersecurity policy initiatives that took shape in several countries around the same time (OECD 2012).

3.2 Cybersecurity as vital systems security and process of securitization

Through the lenses of critical security studies, this emergence of cybersecurity in Austria can be captured as a process of securitization of cyberspace (cf. Hansen and Nissenbaum 2009). As a concept, securitization describes a process in which an object or phenomenon is declared as a security issue by reference to existential threats, risks, and emergencies—a process that, if successful, often legitimizes "extraordinary" (counter-)measures beyond the realm of routine political processes (Buzan et al. 1998).

Hansen and Nissenbaum (2009) perceive cybersecurity as a particular sector of security emerging in a post-Cold War conjuncture of technological innovations and geo-political shifts. In relation to problematizations of critical infrastructure pro-

tection (Aradau 2010), cybersecurity amounts to what Collier and Lakoff (2015) describe as "vital systems security", that is to say, practices that aim to "[s]ecure the functioning of systems that are essential to modern life in the face of unpredictable but potentially catastrophic threats" (ibid., p. 23). Understanding cybersecurity through the notion of vital systems security renders the understanding of the digital into a critical infrastructure, which, according to Aradau (2010, p. 501), underlies specific logics of securitization, as "[s]ocities are 'grounded' in infrastructure; their functioning, continuity and survival are made possible by the protection of infrastructure."

These combined perspectives allow further exploration into the visions of an emerging digital society through the practices of cybersecurity that constitute it, and, correspondingly, the efforts to create a "culture of cybersecurity" as a process of securitization that, by framing the digital society as constantly threatened, encodes and enables new forms of control.

4 Articulating a strategy for a safe and secure digital future

The Austrian Cyber Security Strategy (ACSS) is presented as a "comprehensive and proactive concept for protecting cyber space and the people in virtual space", a safe and secure virtual space "capable of resisting risks, absorbing shocks and adjusting to a changed environment" (BKA 2013a, p. 4, 9). It sets out an ambitious agenda defining strategic measures and fields of action embedded in an overall aspiration to "enhance the security and resilience of Austrian infrastructures and services in cyber space. Most importantly, it will, however, build awareness and confidence in the Austrian society" (BKA 2013a, p. 4). Conversely, the Strategy underscores the necessity that the "Austrian population should be aware of the individual's personal responsibility in cyber space" and that "[a]ll citizens should ensure adequate protection of their online activities". To this end, the government is dedicated to the goal that "Austria is building a culture of cyber security" through a whole series of awareness measures (BKA 2013a, p. 9).

4.1 (Re-)aligning institutional frameworks: centralizing cyber forces, monitoring cyber-risks

The ACSS provisions lay out a comprehensive strategic approach in the sense that they enroll private, civic, and state actors in a revamped institutional framework to centralize cyber forces. To overcome the lack of an institutional structure with a clear distribution of responsibilities, as lamented in the preceding ICT strategy, the ACSS establishes a framework that builds on pre-existing agencies and sets up new centers and platforms.

As visualized in Fig. 1, the ACSS distinguishes between three hierarchical levels of government with different tasks and responsibilities, ranging from the political to the strategic and operational level, and involves multiple actors. Whereas institutional makeup appears intelligible at the political and strategic level, it becomes rather messy at the operational level. It encompasses technical and managerial practices

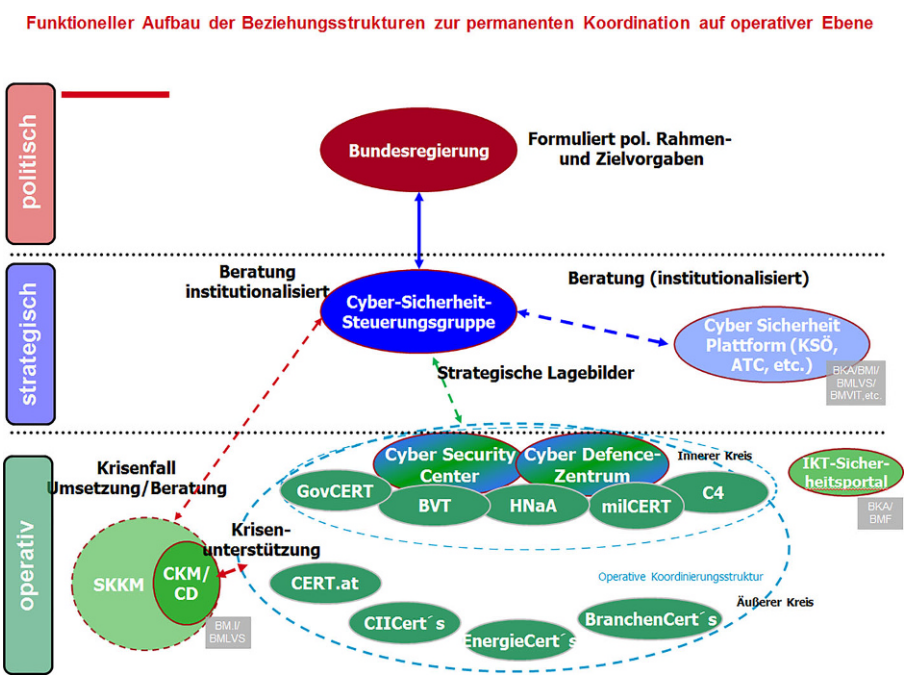

Fig. 1 Chart of the institutional cybersecurity framework. Source: https://www.cert.at/reports/report_2014_chap06/content.html

that are thought necessary and desirable for a culture of cybersecurity to take root yet retains a rather institutionalist outlook. Zeroing in on various knowledge and management practices, however, reveals that cybersecurity depends on a regime of DS&S that exceeds a discrete, narrowly understood institutional policy framework to the extent that, in order to operate, it needs to permeate almost all spheres and fields of society. Computer Emergency Response Teams (CERTs)—those units that populate the operational level of the cybersecurity architecture—are particularly crucial in this regard as they constitute branch-specific hubs that monitor, process, and report cyber incidents.

CERTs are organizations that specialize in the study of IT network security risks. Increasing digitalization has strengthened the role of CERTs as integral parts of public and private organizations that specialize in the study of IT network security risks. They have also become increasingly interconnected across national and sectorial borders. In the EU, integration of CERT activities has been pursued through the evolution of the European Network and Information Security Agency (ENISA) as the competent agency in Europe. In its 2013 work program, ENISA set the goal to establish an inventory to pool and update information on the activities, initiatives, and status of CERTs in Europe (ENISA 2015, p. 6).

Closely accorded with international CERTs, the Austrian national CERT (CERT.at, established in 2008 as the first point of contact for any incident at a national level), proactively searches for potential upcoming threats. It further established the Austrian Trust Circle, an advisory network of trusted experts from

various areas of strategic information infrastructure. CERTs play an essential role in knowledge production and exchange. In the national CERT's annual reports, statistics compile information on events (discriminating between reports, incidents, investigations, and false alerts) and threats. In 2016, on average, 1300 reported incidents per month were documented (CERT.at 2016, p. 8). An incident is typically followed by an *investigation*, understood as contact being established between the CERT and the affected organizations by exchanging e-mails with all affected parties.

In an emerging control regime for cyberspace, CERTs work as intermediary organizations at the interface between politics and technology, operating at the nexus between knowledge production and interventions. Their major function is thus to document and, in a way, "process" the quantity and frequency of cyberattacks and "incidents". Making the sheer number of incidents visible and calculable not only contributes to the perception that cyber-risks are real and abundant. It thereby also creates a sense of urgency and immediacy that supports the securitization of cyberspace.

4.2 Implementing information security management systems

With the European Network and Information Security Directive (EU 2016) in force, it has become legally mandatory to implement and run effective information security management systems (ISMS) in all areas deemed critical infrastructures.

The underlying normative agenda of ISMS is to recognize information as a crucial, yet constantly endangered, *general* value for society as a whole while helping to design sector- and organization-*specific* management systems. On a technical level, ISMS demand implementation of international norms and standards in all subsectors, services, and processes deemed "critical", including energy, health, transport, finance, water, and communications. These ISO standards are articulated for the Austrian context in the Handbook on Information Security Management that provides a practical guide for ISMS implementation.

ISMS combine an epistemology of risk with management tools known as the PDCA Cycle (Plan, Do, Check, Act) to establish a protocol of constant monitoring, evaluation and assessment, practical interventions, and recalibration of governance methods. Elements of an operational ISMS should be fine-tuned with the specificities and requirements of any particular system and include management of risks and auditing programs at the systemic, process, and product-level, security analyses, and the management of regulatory guidelines. The Handbook defines a process to establish ISMS at the organization-wide level in terms of a continuous process of three intertwined phases (BKA 2016, p. 20–64).

If gradually established in all critical infrastructure sectors and in all organizations deemed security-relevant, ISMS spans a truly global network of digitally safe and secure organizations. Reaching this global web of digital safety and security requires huge efforts—a broad scale mobilization of resources to implement multiple ISMS that are adapted to each case and tailored to the specific requirements of the target organization. Moreover, implementing ISMS is not just a discrete accomplishment but sets in motion a complex process of constant monitoring, adaptation, and recalibration. This process, in turn, depends on constantly developing knowledge,

skills, and technological devices that enable state-of-the-art cybersecurity regimes to be provided.

5 Promoting digital safety and security through knowledge, skills, and innovation

5.1 Innovating DS&S through techno-scientific research and development

To a considerable extent, the vision of a safe and secure digital society is grounded in the aspiration to advance research and development (R&D) to produce safe digital technologies and secure digital infrastructures. In Austria, this emphasis on security R&D and technologies and devices that are deemed conductive to the emergence of safe and secure digital practices at all levels of society was recently reaffirmed in the Digital Roadmap (BKA 2017) as well as in the strategy of the newly elected government that aspires to render Austria as one of the main hubs of security technology development (Republic of Austria 2017, p. 32).

To pursue digital safety and security through R&D, two instruments are key in the Austrian security research sector. On a national level, the security research program KIRAS, which is mainly funded by the Federal Ministry of Transport, Innovation and Technology, represents the central framework for security research. So far, a total of 25 projects on cybersecurity have been funded under the auspices of KIRAS. At the same time, Austrian security research increasingly occurs in the context of the European Research Framework Programs, particularly Horizon 2020. Austrian agencies, enterprises, and research institutions—prominently, the Austrian Institute of Technology—are involved in both KIRAS and H2020-funded research consortia. Particularly relevant in this context is the Austrian Institute of Technology, which is the largest Austrian contributor both in KIRAS and in FP7 or H2020 (see Bigo et al. 2014). In both these funding schemes, research interests are closely matched with policy goals, such as the promotion of "secure societies", which is framed as a pressing "societal challenge" in H2020. Research results, in turn, are primarily valued in their capacity to serve a "stakeholder", such as a public agency profiting from an innovative technology or commercial technology firms that develop a prototype to market maturity in the context of a public-private partnership.

However, this focus on policy-oriented and applied R&D does not only consist of efforts to develop security technologies and devices in a narrow understanding—devices that are deemed inextricable from contemporary, highly technologized security practices (Ceyhan 2008; Amicelle et al. 2015). Rather, the broad R&D agenda increasingly focuses on integrated digital safety and security in an effort to mitigate the risks associated with "unsafe" use (EC 2017). This focus also problematizes users of technology in conjuncture with various issues of technological safety and security that stem from the import and use of unfamiliar devices. Hence, creating safer and more secure technologies is part of an effort to promote the responsible use of digital technologies and, for the entire digital society, to reduce risks that might be caused through harmful actions of a few users. R&D in this context

is, therefore, an instrument for mitigating risk and controlling insecurity; therefore, R&D assumes a central spot in the emerging control regimes for the digital society.

5.2 Forging digital subjects: training a new generation of cybersecurity experts

The focus on innovating cybersecurity through R&D is inseparable from promoting and developing a whole range of "human technologies", such as the creation of individual and institutional capacities, skills, and competencies that enable individual citizens, professionals, and organizations to act as cybersecurity experts. The ACSS states how "to ensure cyber security, technical expertise is necessary, which must be based on state-of-the-art research and development results" (BKA 2013a, p. 15). Even more dramatically, this nexus is problematized in the H2020 stream on "cybersecurity preparedness", where we read that

> [m]any organisations are unable to forecast and/or estimate the impacts of a cyber-risk. This results often in insufficient and/or irrelevant investments to ensure a more cyber secure environment. [...] In a connected EU society, there is an *urgent need for highly competent cybersecurity professionals*, and security experts need to be in a *constant learning process*, to match the quick rate of evolution of the cyber threats, attacks and vulnerabilities. *Cybersecurity skills need to be continuously advanced at all levels* (e.g. security officers, operators, developers, integrators, administrators, end users) in order to enable cybersecurity [...] within the EU Digital Single Market (EC 2017, p. 57, emphasis added).

Knowledge on risk mitigation, therefore, is not only produced through technology R&D *strictu senso*, but through educational and training practices that should assist in creating knowledge among all practitioners within the digital society.

This link between the technical and the human aspects of cybersecurity is also stressed in the Handbook for Information Security. There, the objective of building a culture of cybersecurity begins with raising individual awareness, which is essentially tied to a whole range of "technical" provisions and emphasizes the significance of norms, standards, and further educational measures for employees. An organization, the Handbook reads, "will only reach [their] security relevant goals if they have sufficiently educated and informed employees" (ibid., p. 72).

Yet, awareness does not primarily consist of a notion of risks and threats but first and foremost expresses an acknowledgement of information as having precious and critical *value* for society:

> Information security does not emerge almost automatically from Technology and Know-how, but first of all from the awareness of management and members of an organization, that information presents values that are endangered and in need of protection (BKA 2016, p. 26).

To turn the unskilled citizenry and labor force into digitally apt and prudent subjects, a range of specific programs to increase digital awareness and practical knowledge have been launched that include assistance for Small and Medium Enterprises, financial funding schemes for improving the digital structures, training courses for employees offered in cooperation with Federal Ministry of Digitaliza-

tion and Economics and the Federal Economic Chamber (WKO), or, on a local level, e.g., through regional governments, various trade fairs and showrooms devoted to the topic (WKO 2018; Stadt Wien 2015).

In the ACSS policy vision, forging digitally aware and prudent subjects is not just a matter of professional training and continuing skill development but has to extend into the education system. This extension is envisioned through basic educational institutes—the primary and, particularly, secondary schools—where teaching plans have adapted (e.g., through the Digital Competences initiative "digi.komp") and a digitalization strategy for Austrian schools, which in the Digital Roadmap (BKA 2017) articulates the process of accomplishing digitally educated citizens. Beyond that, specialized study programs are developed and implemented in the tertiary sector, namely in universities of applied sciences, in an effort to create academic career pathways and to train a new generation of cyber-experts. These curricula are not only geared towards producing and disseminating technological knowledge but also towards enhancing capabilities in risk and security management. These efforts combined are supposed to increase the number of experts who should not only possess the ability to mitigate risks and appropriately react to threats but furthermore be able to distribute their specific knowledge to their peers.

5.3 Exercising the contingency: enhancing crisis response through simulated cyberincidents

Measures of creating awareness and skills go beyond education and professional training on the firm level; they provide for settings designed to generate a practical level of preparedness by "rehearsing" the emergency (Lakoff 2008). Large-scale cyber exercises are organized by cybersecurity communities at the national and the international level. In Austria, "Cyber-Planspiele" are organized annually by the KSÖ in cooperation with the Austrian Institute of Technology, which provides the necessary software (KSÖ 2017). In these events that usually take several days, practitioners from public institutions and private enterprises, IT scientists, and members of the CERTs are required to collectively handle simulated cyberattacks.

The events aim to enhance the level of resilience by creating inter-disciplinary and inter-institutional practical expertise (BKA 2013a; Brassett and Vaughan-Williams 2015). While participants gain technical knowledge on specific risks and threats, such as hacker attacks or ransomware, they also increase their embodied knowledge of how to react individually and as an institution, as well as of their respective responsibilities, technical and legal competencies, and organizational resources in a crisis. Mutual learning and jointly shared responsibility in these simulated events should provide the basis to reduce knowledge gaps between institutions and boost the level of inter-organizational trust and the quality of cooperation and communication between the different societal actors and CERTs.

To sum up, all these efforts combined suggest that the overarching objective of the emerging DS&S regime does not lie exclusively in the forging of competent digital subjects in itself—subjects *of* digitalization that can responsibly and aptly manage their private and professional lives in a rapidly changing digital society. Rather, all these disciplinary measures, educational tactics, and technologies of self-formation

work together to accomplish a broader objective, namely, to preempt risks of and threats to the digital society. In this regard, education should provide early measures of control, as digitally savvy citizens (cf. Gates 2010) are less likely to unsafely use digital technologies. Considered potential weak points (the "incompetent user") or even aggressors (the cybercriminal, the hacker), individuals are themselves securitized and subjected to various disciplinary and control practices in the context of emerging regimes of digital safety and security.

6 Discussion

Taking the Austrian case as an example, we have explored the efforts and strategies to establish a cybersecurity strategy conducive to governing the emerging digital society in a favorable and desirable direction. Extrapolating from the case study, we will now reflect on the broader implications of this emerging form of cybersecurity for social and political theory.

From today's perspective, digitalization confronts contemporary societies as a virtual process full of opportunities *and* threats. Yet, at its embryonic stage in the 1990s, the Internet was often imagined as a truly democratizing technology that enabled radically new forms of freedom and emancipation from entrenched power structures, such as through free expression of opinion or the organization of protest movements (Saco 2002).

Once imagined as a "virtual commons", through the rise of Big Data (Cukier and Mayer-Schönberger 2013), cyberspace has increasingly grown into a medium of control (Cheney-Lippold 2011) and a site of expropriation and accumulation though dispossession (Thacker et al. 2016), as well as a space of potential instability, disorder, and disobedience. Its paramount importance for growth and competitiveness in an ever-growing innovation economy based on digital platform technologies has further propelled the perceived need for "securitizing" cyberspace, i.e., rendering the digital sphere "safe and secure" to bring about a desirable future. How can we make sense of the emerging regimes of DS&S for a broader critical understanding of contemporary societies?

6.1 Cybersecurity as "globalizing" form of security

Around the time when the OECD (2012) observed a new generation of cybersecurity policies emerging worldwide, NATO reflected on the topicality of cybersecurity ten years after the 9/11 attacks.

> Together with the Twin Towers, our traditional perceptions of threats collapsed. [...] Before 9/11, cyberspace risks and security challenges were only discussed within small groups of technical experts. But, from that day it became evident that the cyber world entails serious vulnerabilities for increasingly interdependent societies (Theiler 2011, n.p.).

As this quote illustrates, cybersecurity has become closely articulated within a broader shift in security in a new constellation of globalized threats in the af-

termath of the 9/11 terrorist attacks. In this narrative, sources of insecurity have virtually globalized. This articulation of cyberspace within an emerging landscape of generalized (in-)security and terrorism not only frames cyberspace as a new field of security interventions but also calls for a novel rationality of security and, correspondingly, a novel epistemology of threat, a revised toolbox of countermeasures, and adaption of bureaucratic institutions (Hansen and Nissenbaum 2009, Simon and de Goede 2015).

In the wake of 9/11, political philosopher Giorgio Agamben has pointed to the virtual end of a state of security understood in the framework of national sovereignty and suggested that now "security finds its end in globalization". Security, he argues, has gradually become the basic principle of state activity: "What used to be one among several definitive measures of public administration until the first half of the twentieth century, now becomes the sole criterium of political legitimation" (Agamben 2001, n.p.). This state of security operates on a permanent expectation of emergency: of risks to be controlled and threats to be preempted (Cooper 2006). This predicament further implies, as critical security scholars have shown (Buzan et al. 1998; C.A.S.E. Collective 2006), not only a drastic de-politicization and a de-democratization but, furthermore, a collapse of politics altogether—both in the sense of international geopolitics and in the sense of democratic public policy. In this new security logic, politics collapses into management, and *inter*-national military conflicts collapse into police actions rationalized in terms of a looming *Weltinnenpolitik* (Dauderstädt 2003).

Tying into these reshaped security discourses, cybersecurity hence presents a seemingly all-encompassing concern, as it articulates issues of national security and sovereignty with concerns for personal safety and the social and economic welfare of contemporary society (Cheyney-Lippold 2011; Thacker et al. 2016).

The Austrian experience with the (re-)imagination and conceptualization of digital safety and security regimes exemplifies how cybersecurity does not merely present a discrete agenda within security policy but rather amounts to a "globalizing" form of security animating, and animated by, an emerging sociotechnical regime of control. To secure present societies against digital threats and to achieve a prosperous digital future, huge efforts are taken that articulate through almost all domains and levels of society. As such, cybersecurity presents a testing ground where the relationships between an ever-emerging digitalizing society and their corresponding conceptions of security are problematized and reordered. From this, the following propositions follow:

- The digital society is co-produced with cybersecurity
  Cybersecurity must be understood as an active sociotechnical construction site of an emerging digital society. From this perspective, problematizations of cybersecurity do not merely emerge in reaction to progressing digital society but rather constitutes a medium in which the latter is collectively (re-)imagined, publicly pursued, and institutionally configured. The aspiration to create a culture of cybersecurity, hence, further indicates this generative and productive dimension of DS&S: The aspiration to train and educate individuals as circumspect users of digital technologies does not only seek to protect citizens against harm but simulta-

neously to forge prudent digital subjects—citizens with the necessary set of skills and capacities to capture and innovate a digital society imagined to be caught in constant "in-formation" processes.

Furthermore, as an active site of societal transformation, the seemingly technical nature of producing DS&S (in terms of innovating new cyber tech devices, governance instruments, and digital subjects) appears as a highly political endeavor. To (re-)produce sovereignty in the cyberspace domain, a plethora of control mechanisms have to be put in place and kept in operation: data sets are analyzed, algorithms redefined, incidents mapped and reported, and devices redesigned and developed. On the other hand, these control mechanisms operating at the level of protocol (Galloway 2004) are complemented by technologies of subjectification (Foucault 2004): digitally prudent and responsible subjects are forged, ones that acquire and embody appropriate behaviors, coping strategies, and practices of self-formation as digital citizens and/or digital experts.

- Cybersecurity (re-)articulates a new global form of security

  Given its globalizing (i.e., all-encompassing) dimension within society, cybersecurity must not be merely understood as a novel domain or "domain" (Hansen and Nissenbaum 2009) of security policy. Rather, it represents a security rationality that gradually colonizes the entire field of security—thereby reworking its normative and operational logics, its political epistemologies, and instruments of intervention. As such, cybersecurity amounts to a specific governmentality for and in the contemporary societies of control (Deleuze 1992). Put succinctly, in the context of a sociotechnical imaginary of the digital society, *conventional security tends to become (re-)articulated within a rationality of cybersecurity*: If society as a whole is increasingly reimagined as a digital society throughout, all security tends to become closely tied to digital security.

  To begin with, the growing interdependence and interconnectedness creates a situation in which digital vulnerabilities easily translate into a whole range of other types of vulnerability. This is most apparent in the concerns about critical infrastructure protection (Aradau 2010) but also manifests in a broad range of other domains, such as border security through databases (Jeandesboz 2016), the human body deciphered as "code" in the context of molecular biology (Dillon 2003), or global health policy and strategies of epidemic preparedness (Roberts and Elbe 2017). For instance, a digital security problem in a nuclear reactor could easily translate into a major nuclear safety concern, and a safety issue in the energy sector can easily spill over into a national crisis propelled by a massive black out—including disorder and insecurity due to riots, lootings, public health and safety issues, breakdown of transportation and communication, etc. (Cooper 2006; Lakoff 2008). In all these domains, possible sites of digital safety and security intervention, power, and control are exercised at the level of protocol (Galloway 2004), alongside more conventional technologies of power. With the growing digitalization of society, *all safety also involves digital safety, and all security involves also digital security*—hence reworking the very epistemologies of security policies.

  In this emerging rationality of digital safety and security, the conceptual distinction between, say, human safety and safe technology becomes not only blurred

but increasingly inconsequential for the operation of cybersecurity—not least due to the easy spillover effects from human failure to infrastructural vulnerabilities, from small security holes to large-scale public safety concerns.

6.2 Conclusions: from cybersecurity policy to regimes of digital safety & security

Given this predicament, we conclude by suggesting that the problematiziations that guide visions of an incipient digital future can be grasped by exploring the nexus between digitalization and society in terms of an emerging globalizing regime of *digital safety and security.*

The rationality underpinning the DS&S regime seems to encompass much more than narrow notions of cybersecurity might suggest. In policy discourses, this rationality is somewhat reflected by the notion of a "culture of cybersecurity" that focuses on reworking individual and institutional awareness, abilities, and responsibilities in a context of permanent urgency and constantly evolving threats in an ever-changing digital society. Moreover, as everyone—careless users, unaware citizens—and everything—devices, databanks, and entire "vital" infrastructures—are rendered potential sources of harm and insecurity to society *as a whole*, it is vital to critically engage with the oftentimes technical tropes and seemingly discrete measures that, tacitly or shrill, work towards the further securitization of substantive aspects of public and private life. As rationalities of cybersecurity proliferate in all fields of society, the visions of an open, inclusive, and truly innovative digital future risk becoming haunted by the demons of a fully-fledged security society.

Acknowledgements Earlier versions of this article were presented at the International Studies Association (ISA) Annual Convention 2018, San Francisco, California, and at the Congress of the Austrian Sociological Association (ÖGS) 2017, Graz, Austria. We particularly want to thank Tinja Zerzer for research assistance, as well as Christoph Musik, Saskia Stachowitsch, Julia Sachseder, and the two reviewers of this manuscript for their valuable comments and suggestions. All remaining error of fact or judgment remain clearly ours.

Funding Open access funding provided by University of Vienna.

References

Agamben, Giorgio. 2001. On security and terror. *frankfurter Allgemeine Zeitung*. https://libcom.org/library/on-security-and-terror-giorgio-agamben (Created 20 Sept 2001). Accessed 13 Apr 2018.

Amicelle, Anthony, Claudia Aradau, and Julien Jeandesboz. 2015. Questioning security devices: Performativity, resistance, politics. *Security Dialogue* 46(4):293–306. https://doi.org/10.1177/0967010615586964.

Aradau, Claudia. 2010. Security that matters: critical infrastructure and objects of protection. *Security Dialogue* 41(5):491–514. https://doi.org/10.1177/0967010610382687.

Bigo, Didier, Julien Jeandesboz, Médérci Martin-Maze, and Francesco Ragazzi. 2014. Review of Security Measures in the 7th Research Framework Programme FP7 2007–2013. Study for the LIBE

Committee. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509979/IPOL-LIBE_ET(2014)509979_EN.pdf. Accessed 10 July 2018.
BKA. 2008. Regierungsprogramm 2008–2013. Gemeinsam für Österreich. http://www.konvent.gv.at/K/DE/INST-K/INST-K_00179/imfname_164994.pdf. Accessed 11 May 2018.
BKA. 2013a. Austrian cyber security strategy. http://archiv.bundeskanzleramt.at/DocView.axd?CobId=52251. Accessed 3 Mar 2018.
BKA. 2013b. Austrian security strategy. Security in a new decade—shaping security. http://archiv.bundeskanzleramt.at/DocView.axd?CobId=52251. Accessed 3 Mar 2018.
BKA. 2013c. Arbeitsprogramm der österreichischen Bundesregierung 2013–2018. Erfolgreich. Österreich. https://www.justiz.gv.at/web2013/file/2c94848642ec5e0d0142fac7f7b9019a.de.0/regprogramm.pdf. Accessed 11 May 2018.
BKA. 2015. Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP). http://archiv.bundeskanzleramt.at/DocView.axd?CobId=58907. Accessed 20 May 2018.
BKA. 2016. Österreichisches Informationssicherheitshandbuch. https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf. Accessed 21 Mar 2018.
BKA. 2017. Digital Roadmap 2017. https://www.digitalroadmap.gv.at/fileadmin/downloads/digital_road_map_broschuere.pdf. Accessed 10 May 2018.
BMI. 2011. Verfassungsschutzbericht 2011. http://bvt.bmi.gv.at/401/files/Verfassungsschutzbericht2011Berichtszeitraum2010.pdf. Accessed 13 May 2018.
Borchert, Heiko, Wolfgang Rosenkranz, and Wolfgang Ebner. 2015. Cybersicherheit in Österreich – Erfahrungsbericht zum Aufbau der Öffentlich-Privaten Sicherheitszusammenarbeit im Cyberspace. In *Cyber-Sicherheit*, ed. Hans-Jürgen Lange, Astrid Bötticher, 121–146. Wiesbaden: Springer VS.
Brassett, James, and Nick Vaughan-Williams. 2015. Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness. *Security Dialogue* 46(1):32–50. https://doi.org/10.1177/0967010614555943.
Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security. A new framework for analysis*. London: Lynne Rienner.
C.A.S.E. Collective. 2006. Critical approaches to security in europe. A networked manifesto. *Security Dialogue* 37(4):443–487. https://doi.org/10.1177/0967010606073085.
CERT.at. 2016. *Bericht Internet Sicherheit Österreich 2016. Gesamtausgabe.* Wien: Computer Emergency Response Team Austria.
Ceyhan, Ayse. 2008. Technologization of security. Management of uncertainty and risk in the age of biometrics. *Surveillance & Society* 5(2):102–123.
Charmaz, Kathy. 2006. *Constructing grounded theory. A practical guide through qualitative analysis*. London: SAGE.
Cheney-Lippold, John. 2011. A new algorithmic identity: Soft biopolitics and the modulation of control. *Theory, Culture & Society* 28(6):164–181. https://doi.org/10.1177/0263276411424420.
Clarke, Adele. 2005. *Situational analysis: grounded theory after the postmodern turn*. Thousand Oaks: SAGE.
Collier, Stephen, and Andrew Lakoff. 2015. Vital systems security: reflexive biopolitics and the government of emergency. *Theory, Culture and Society* 32(2):19–51. https://doi.org/10.1177/0263276413510050.
Cooper, Melinda. 2006. Pre-empting emergence: the biological turn in the war on terror. *Theory, Culture & Society* 23(4):113–135. https://doi.org/10.1177/0263276406065121.
Cukier, Kenneth, and Viktor Mayer-Schönberger. 2013. *Big data: a revolution that Will transform how we live, work and think*. London: John Murray Publishers.
Cyber Security Steering Group. 2018. Bericht Cyber Sicherheit 2018. https://www.bundeskanzleramt.gv.at/documents/131008/780563/Cybersicherheit_Bericht2018/769cb7b7-614c-49d8-8055-068d2f36009c. Accessed 12 Mar 2018.
Dauderstädt, Michael. 2003. *Weltinnenpolitik angesichts globaler Ungleichheit: zur (sicherheits-)politischen Ökonomie asymmetrischer Bedrohungen*. Bonn: FES Library.
Dean, Mitchell. 2010. *Governmentality. Power and rule in modern society*. London: SAGE.
Deleuze, Gilles. 1990. Post-script on the societies of control. *October* 59:3–7.
Dillon, Michael. 2003. Virtual Security: A Life Science of (Dis)order. *Millennium. Journal of International Studies* 32(3):531–558. https://doi.org/10.1177/03058298030320030901.
Dunn Cavelty, Myriam. 2013. From cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse. *International Studies Review* 15(1):105–122. https://doi.org/10.1111/misr.12023.

EC. 2013. Cybersecurity strategy of the European union: an open, safe and secure cyberspace. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. Accessed 8 Mar 2018.
EC. 2017. Horizon 2020 work programme. Secure societies. http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf. Accessed 5 May 2018.
EC. 2015. A Digital Single Market Strategy for Europe. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN. Accessed 8 Mar 2018.
ENISA. 2015. European network and information security agency. Inventory of CERT activities in europe. https://www.enisa.europa.eu/publications/inventory-of-cert-activities-in-europe/. Accessed 2 Apr 2018.
ENISA. 2018a. ENISA threat landscape report 2017. 15 top cyber-threats and trends. https://www.enisa.europa.eu/news/enisa-news/enisa-report-the-2017-cyber-threat-landscape. Accessed 6 Aug 2018.
ENISA. 2018b. Looking into the crystal ball: A report on emerging technologies and security challenges. https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball. Accessed 6 Aug 2018.
ENISA. 2018c. Cyber Security Culture in organisations. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations. Accessed 23 July 2018.
EU. 2003. Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security. https://publications.europa.eu/en/publication-detail/-/publication/99d9a4b4-f6f9-4716-816e-83cee56fad11/language-en. Accessed 15 May 2018.
EU. 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systemsacross the Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN. Accessed 21 Mar 2018.
Foucault, Michel. 2004. *Security, territory and population. Lectures at the Collège de France 1978*. New York: Palgrave McMillan.
Galloway, Alexander. 2004. *Protocol. How control exists after decentralization*. Cambridge, MA: MIT Press.
Gates, Kelly. 2010. *Our biometric future: facial recognition technology and the culture of surveillance*. New York: NYU Press.
Gottweis, Herbert. 2003. Theoretical strategies of poststructuralist policy analysis: towards an analytics of government. In *Deliberative policy analysis: Understanding governance in the network society*, ed. Maarten Hajer, Hendrik Wagenaar, 247–265. Edinburgh: Cambridge University Press.
Hansen, Lene, and Helen Nissenbaum. 2009. Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly* 53(4):1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x.
Jasanoff, Sheila. 2015. Future imperfect: science, technology, and the imaginations of modernity. In *Dreamscapes of modernity. Sociotechnical imaginaries and the fabrication of power*, ed. Sheila Jasanoff, Sang-Hyun Kim, 1–33. Chicago: University of Chicago Press.
Jasanoff, Sheila, and Sang-Hyun Kim. 2009. Containing the atom: Sociotechnical Imaginaries and nuclear power in the United States and South Korea. *Minerva* 47(2):119–146. https://doi.org/10.1007/s11024-009-9124-4.
Jeandesboz, Julien. 2016. Smartening border security in the European Union: An associational inquiry. *Security Dialogue* 47(4):292–309. https://doi.org/10.1177/0967010616650226.
Juncker, Jean-Claude. 2014. A new start for Europe Opening statement in the European Parliament plenary session Strasbourg. http://europa.eu/rapid/press-release_SPEECH-14-567_en.htm (Created 15 July 2014). Accessed 15 July 2018.
KSÖ. 2011. Cyber-Risikomatrix 2011. https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/KSO_Cyber_Risikomatrix.pdf. Accessed 3 May 2018.
KSÖ. 2012. Cybersicherheit in Österreich. Risikopotenziale und Handlungserfordernisse am Beispiel ausgewählter Infrastruktursektoren. https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/Cyberrisikoanalyse.pdf. Accessed 3 May 2018.
KSÖ. 2017. KSÖ Cybersecurity Planspiel – Praxistest für EU-Richtlinie. https://kuratorium-sicheres-oesterreich.at/allgemein/ksoe-cybersecurity-planspiel-praxistest-fuer-eu-richtlinie/. Accessed 12 May 2018.
Lakoff, Andrew. 2008. The Generic Biothreat or How We Became Unprepared. *Cultural Anthropology* 23(3):399–428. https://doi.org/10.1111/j.1548-1360.2008.00013.x.
OECD. 2002. *Implementation plan for the OECD guidelines for the security of information systems and networks: towards a culture of security*. Paris: OECD Publishing.

OECD. 2012. *Cybersecurity policy making at a turning point:Analysing a new generation of national Cybersecurity. Strategies for the Internet economy*. OECD Digital Economy Papers, Vol. 211. Paris: OECD Publishing.

oiip. 2017. *Digital Safety & Security: politische und technische Potentiale, Herausforderungen und Strategien für eine Gesellschaft 4.0. Workshop Summary*. Wien: Österreichisches Institut für Internationale Politik.

Republic of Austria. 2012. National ICT Security Strategy Austria. https://www.digitales.oesterreich.gv.at/documents/22124/30428/National_ICT_Security_Strategy_Austria_2012_print.pdf. Accessed 15 Mar 2018.

Republic of Austria. 2017. Zusammen. Für unser Österreich. Regierungsprogramm 2017–2022. https://www.bundeskanzleramt.gv.at/documents/131008/569203/Regierungsprogramm_2017%E2%80%932022.pdf/b2fe3f65-5a04-47b6-913d-2fe512ff4ce6. Accessed 11 May 2018.

Rid, Thomas, and Peter McBurney. 2012. Cyber-Weapons. *The RUSI Journal* 157(1):6–13. https://doi.org/10.1080/03071847.2012.664354.

Roberts, Stephen, and Stefan Elbe. 2017. Catching the flu: syndromic surveillance, algorithmic governmentality and global health security. *Security Dialogue* 48(1):46–62. https://doi.org/10.1177/0967010616666443.

Rose, Nikolas, and Peter Miller. 1992. Political power beyond the state: Problematics of government. *The British Journal of Sociology* 61:271–303. https://doi.org/10.1111/j.1468-4446.2009.01247.x.

Saco, Diana. 2002. *Cybering democracy. Public space and the Internet*. Minneapolis: University of Minnesota Press.

Simon, Stephanie, and Marieke de Goede. 2015. Cybersecurity, bureaucratic vitalism and European emergency. *Theory, Culture and Society* 32(2):79–106. https://doi.org/10.1177/0263276414560415.

Stadt Wien. 2015. Digitale Agenda Wien. https://www.digitaleagenda.wien/download-file.php?id=4&f=digitale-agenda-wien.pdf. Accessed 20 May 2018.

Thacker, Jim, David O'Sullivan, and Dillon Mahmoudi. 2016. Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning* 34(6):990–1006. https://doi.org/10.1177/0263775816633195.

Theiler, Olaf. 2011. New threats: the cyber-dimension. *NATO Review Magazine*. https://www.nato.int/docu/review/2011/11-september/cyber-threads/en/index.htm (Created 11 Sept 2011). Accessed 11 May 2018.

Wagenaar, Hendrik. 2011. *Meaning in action. Interpretation and dialogue in policy analysis*. London: Routledge.

WKO. 2018. KMU Digital. https://www.wko.at/Content.Node/kampagnen/KMU-digital/index.html. Accessed 28 May 2018.

Christian Haddad Dr. phil., is a Research Fellow at the Austrian Institute for International Affairs (oiip) and a Lecturer at the University of Vienna. At the oiip he coordinates the research area Global Politics of Innovation. Current research revolves around sociotechnical visions of innovation in the MENA region and the innovation of (in-)security in global health governance. Christian Haddad, Dr. phil., ist wissenschaftlicher Mitarbeiter am oiip und Lehrbeauftragter an der Universität Wien (Institut für Politikwissenschaft, Institut für Wissenschafts- und Technikforschung). Am oiip koordiniert Haddad den Forschungsbereich Globale Innovationspolitiken und forscht derzeit zu soziotechnischen Visionen der Innovationsgesellschaft in der MENA-Region sowie zur Innovation von (Un-)Sicherheit im Feld der Globalen Gesundheitspolitik.

Clemens Binder MA, is a researcher at the Austrian Institute for International Affairs (oiip) and doctoral candidate at the Department of Political Science at the University of Vienna (Political Science, Science & Technology Studies). His research is situated at the intersections of Critical Security Studies and Science and Technology Studies; his PhD-project deals with the connections between border security and Research and Development of security technologies in the European Union. Clemens Binder, MA, ist wissenschaftlicher Mitarbeiter am Österreichischen Institut für Internationale Politik (oiip) und Doktorand am Institut für Politikwissenschaft an der Universität Wien. Seine Forschung ist an der Schnittstelle zwischen kritischer Sicherheitsforschung und Wissenschafts- und Technologieforschung verortet. In seiner Dissertation behandelt er die Zusammenhänge von Grenzsicherheit und der Forschung & Entwicklung von Sicherheitstechnologien in der Europäischen Union.