Research Article

S|S|S

Social Studies of Science
2021, Vol. 51(2) 189–213
© The Author(s) 2020
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0306312720953515
journals.sagepub.com/home/sss
SAGE

Science, technology, security: Towards critical collaboration

Sam Weiss Evans[1,2]

Matthias Leese[3]

Dagmar Rychnovská[4]

Abstract

Science and technology play a central role in the contemporary governance of security, both as tools for the production of security and as objects of security concern. Scholars are increasingly seeking to not only critically reflect on the interplays between science, technology and security, but also engage with the practices of security communities that shape and are shaped by science and technology. To further help this growth of interest in security topics within science and technology studies (STS), we explore possible modes of socio-technical collaboration with security communities of practice. Bringing together literatures from STS and critical security studies, we identify several key challenges to critical social engagement of STS scholars in security-related issues. We then demonstrate how these challenges played out over the course of three case studies from our own experience in engaging security communities of practice. We use these vignettes to show that there is a rich vein of developments in both theory and practice that STS scholars can pursue by attending to the interplay of science, technology and security.

Keywords

security, engagement, collaboration, critical security studies

[1] Program on Science, Technology and Society, John F Kennedy School of Government, Harvard University, USA
[2] John A Paulson School of Engineering and Applied Sciences, Harvard University, USA
[3] Center for Security Studies, ETH Zurich, Switzerland
[4] Institute for Advanced Studies, Vienna, Austria

Correspondence to:
Sam Weiss Evans, Harvard Kennedy School, Program on Science, Technology and Society, 79 JFK St. Mailbox 38, Cambridge, MA 02138-5806, USA.
Email: samuel_evans@harvard.edu

Introduction

In the early winter of 2001, Wiebe Bijker got on stage at the Society for the Social Studies of Science Annual Meeting in Cambridge, Massachusetts to deliver his Pre-Presidential Address. He began with a call to engagement, stating that 'STS is not only crucial for understanding our technological cultures; it is equally important for developing democratic politics' (Bijker, 2003: 443). What spurred Bijker to make this comment were the terrorist attacks on the US, which made use not of the latest weapons systems, but of box cutters, airplanes and letters. His concern was that such a shaking of a heavily technological culture with the most mundane of technologies might lead to political agendas that would capitalize on security concerns to diminish democratic capabilities around the world. STS, he argued, needs to 'actively contribute to democratizing this technological culture: to show to a broad array of audiences – politicians, engineers, scientists, and the general public – that science and technology are value laden, that all aspects of modern culture are infused with science and technology, that science and technology do play key roles in keeping society together, and that they are equally central in all events that threaten its stability' (Bijker, 2003: 444).

Of course, STS researchers have been actively contributing to democratizing technological cultures for some time (Ravetz, 1971; Sismondo, 2008), but the last 20 years have seen a significant uptick in those of us who see ourselves as doing STS 'in the world', making and remaking sociotechnical systems based on – and furthering – insights from over half a century of analysis. These efforts of engaged STS span a breathtaking range of issue areas, from Dutch policy engagement to Brazilian mosquito control to Japanese disaster recovery. Curiously, interest in what might be called the security sphere has only received low-level, if fairly constant, attention (Vogel et al., 2017), despite Bijker bringing up this specific topic because of the September 11th, 2001 attacks.

STS scholarship tends to love a hard case, which acts as a grindstone upon which we can hone our analytic capabilities and advance our theories. The choice of analyzing science was itself characterized as a turn to a hard case in the early days of STS (Bloor, 1976), because of its claim to be the guardian of truth in society and the progenitor of benefits (Woolgar, 2004). But whereas many of these cases have focused on the ways of ordering knowledge systems, we need to put equal weight on cases that order social and political systems. While hard cases around science, technology and the law have looked at the ways that societies order internal to themselves (e.g. Jasanoff, 2011), looking at security as a hard case is about the ways that threats to those social orders are constructed, by whom and the role of technoscience in doing so.

Luckily, STS has a closely aligned field in this hard case. 'Critical security studies' has been analyzing the pivotal societal role of security for a good thirty years now (Booth, 1991; Krause and Williams 1997). It has seen a similar increase in interest in 'assisting security practitioners in becoming more reflexive about their practices, as well as in helping them to cope with multiple truths, theories and technical knowledge' (c.a.s.e. collective, 2006: 474). STS can benefit from the decades of research within critical security studies on how discourses of security hold so much power within societies. While critical security studies has already started to incorporate STS work more systematically in order to analyze the ways that power structures are embedded within and

reproduced through science and technology (Bourne, 2014; Hoijtink and Leese, 2019; Mayer et al., 2014; Salter, 2015), STS has, with a few notable exceptions (e.g. Masco, 2014; Rappert, 2009; Suchman et al., 2017), been more hesitant when it comes to the analysis of technoscientific security practices. We contend that the fields can benefit each other when it comes to the question of how to put an engaged program into practice vis-à-vis powerful security frames.

In this article, we consider possible modes of engagement with technoscientific security contexts. We believe that a meaningful entry into this hard case is through a methodology that considers the relationality of the STS/critical security studies researcher to her or his community of practice. We analyze how STS approaches to engagement are complicated by communities of practice where security is an active discourse and frame. We use three vignettes from our own research to illustrate how productive analysis can be achieved across a range of types of socio-technical collaboration, and conclude with thoughts on future directions for coupling STS and critical security studies together. By studying how we have attempted to study, and therein shape, discourses and practices around science, technology and security, we are able to see the forces at work in opening up and closing down what kinds of analysis are even allowable.

Socio-technical collaboration and security

The creation and application of scientific knowledge plays an important role in how societies aspire to maintain order and civility (Shapin, 1995). The production, stabilization and diffusion of scientific and technical orders are closely entangled with, and mutually constitutive of, the production of social order (Jasanoff, 1996, 2004). Technoscientific enterprises are coined by specific cultural and political imaginaries that they in turn help to realize (Jasanoff and Kim, 2009, 2015), and STS has a rich history of engaging with the politics of co-production (Jasanoff, 1990; Miller and Wyborn, 2018; Polanyi, 1962; Shapin and Schaffer, 1985). Notably, it has also sparked a reconsideration of the role that the social sciences should occupy within this constellation.

Loosely gathered under the term ‘socio-technical collaboration’ (Fisher et al., 2015), a broad body of literatures engages with ways we as scholars can work with communities we research in the production of problems, relevant knowledges and innovations (Balmer et al., 2015: 8; Downey and Zuiderent-Jerak, 2017). These literatures are not homogeneous, but consist of a variety of different approaches, including the likes of applied ethics (Leese et al., 2019; van Gorp and van der Molen, 2011), public participation (Chilvers and Kearnes, 2020; Lezaun et al., 2017), ELSI/post-ELSI (Balmer et al., 2015; Fisher, 2005), responsible innovation (Owen et al., 2012, 2013) and technology assessment (Hellström, 2003; Rip et al., 1995). A major theme throughout most of them is the aspiration to render interaction between publics, governing authorities, social scientists and techno-scientific experts productive in terms of transforming professional practices and creating responsiveness to societal values (Fisher et al., 2006; Owen et al., 2012).

Such values usually include social justice, inclusivity and democracy, and are linked with issues of power and ethics (Fisher et al., 2015: 43). More often than not, however, the values with which technoscience is supposed to correspond are not easily defined, and not easily turned into concrete instructions for development or design. Rather, they

are in themselves ambiguous and contested, and they need to be filled with meaning in specific contexts. Instead of pointing to predefined or generalizable criteria that should inform science and technology (and thereby raise questions of who should be entitled to define and impose such criteria), the literature on socio-technical collaboration tends to point to reflexivity, exchange and shared responsibilities as intrinsic values that become enacted through close cooperation between the social sciences and the natural and engineering sciences (Balmer et al., 2015; Chilvers, 2012). In the best case scenario, socio-technical collaboration would then lead to more socially responsible orderings of knowledge and society. In the words of Balmer et al. (2015: 8), 'the hope for such projects is that "working with" scientists and getting further entangled could help to produce novel and more diverse forms of objects and knowledge for all participants'.

We share these hopes. We do, however, contend that the conditions under which socio-technical collaborations are possible change when security is introduced as a contextual backdrop. Security is an essentially contested concept (Balzacq, 2015; Gallie, 1955). Moreover, as Anderson (2010) suggests, it should not be understood as a condition, but rather as a process that presupposes the continuous production of intelligence, anticipation of threat, and concomitant political and practical action. This process is coined by the definition threats (the security problems that are perceived as pressing), reference objects (the lives, material goods, communities or values that are to be protected), as well as the means that are considered adequate for its production (Buzan et al., 1998; Huysmans, 1998; Krause and Williams, 1997). The meaning of security changes in accordance with what or who is considered a threat at a particular point in time, as well as in accordance with what or who is supposed to be secured. As such, security has also been deemed a 'derivative' (Booth, 2007) or 'ambiguous' (de Lint and Virta, 2004) concept.

All of that said, doing work in the name of security tends to be about orchestrating the central mechanisms of power in a society (Huysmans, 1998). This is primarily because security discourses, institutions, identities and representations (whether scientific or technical) tend to be used to solidify understandings about fundamental aspects of society. Understood as processes of social ordering, they form the boundary work between normal and exceptional political states. Security, in other words, is not just about the protection of basic components of society; on the contrary, the term often arises as a way to justify violence, oppression and the maintenance of power in the hands of a few (Visvanathan and Setelvad, 2014). Through the past half-century, security logics have colonized many regulatory domains besides the traditional ones of the nation-state and the military, including migration, public health and the environment (Buzan and Hansen, 2009), thus extending questions of social ordering throughout many registers of society.

This has become problematic, as policy-makers, practitioners and the technical academic disciplines often demonstrate a tendency to bracket the social constructedness and ambiguity of security, itself a move designed to use a sense of objectivity about the concept to do political work (cf. Anderson, 2006). Security issues are instead perceived and presented as taken-for-granted problems that could, notably with the help of technoscientific tools, be resolved in a straightforward fashion. Science and technology, in this perspective, are reduced to vicarious agents that serve to realize a political agenda and are productive of power in the name of security (Bigo et al., 2014; Davidshofer et al., 2017). Critical security scholars have pushed back on this

characterization, and have pointed to the exclusionary, undemocratic and/or illiberal effects that technoscientific security tools can produce throughout various domains such as border control (Dijstelbloem and Meijer, 2011), risk analysis (Leese, 2014), biometric identity management (Epstein, 2007) and automated behavioral analytics in surveillance footage (Matzner, 2016).

To counter the colonizing tendencies of security, and to address concrete problems of 'too much' or problematic securing practices, significant work has been done on the notion of desecuritization. Rather than defining and dealing with threats in an exceptionalist fashion, scholars have suggested that security issues should be dealt with in the same ways as 'normal', non-security political issues. In doing so, security politics could be brought into standard democratic policy-making processes that entail careful deliberation, transparency and accountability (Aradau, 2004; Hansen, 2012). At the same time, Huysmans (2011) has pointed out how mundane, everyday practices of data production and processing, while in themselves not spectacular or even noteworthy, can become important sources for security operations (see also Woolgar and Neyland, 2013). Calling them 'little security nothings', Huysmans points to how security practices at times tend to fly beneath the radar of public attention. Both perspectives highlight the need for scholarly engagement with security in order to understand how it comes into being and how it can be challenged or contained.

In summary, STS takes the ontological multiplicity of science and technology as its starting point, and critical security studies does the same with the ontological multiplicity of security. There is a need to problematize what security is and what it does, how (in-) security is framed as a political problem, how security is productive of power relations, and how security policies and security practices unfold normative repercussions. Combining STS and critical security studies puts our focus on technoscientific security assemblages, i.e. those processes and tools that turn sociotechnical imaginaries (Jasanoff and Kim, 2015) into ordering practices. Like the turn towards engagement in STS, a 'critical' attitude towards security, for many scholars, presupposes scholarly interventions to address violence, discrimination, and social injustice, and to exercise a form of advocacy on behalf of those who are negatively affected by security policies and practices. In light of the potentially negative ramifications of security, scholars have however been cautious in how they approach collaboration. Entering technoscientific security contexts presents an opportunity to apply principles of socio-technical collaboration to security practices, but it comes with a set of normative challenges, to which we now turn.

Boundary work in socio-technical collaborations

Collaboration presupposes proximity, and there are long-standing concerns within STS and critical security studies about such proximity (Price, 2011). Many of these concerns center on questions of the proper role or researchers and their relationships to the sites and communities they study, thus doing boundary work of academic research. Critical security studies scholars tend to be more attuned to these concerns than many in STS, who, particularly recently, are more concerned with pushing the boundaries of how to have STS concepts travel across contexts (Downey and Zuiderent-Jerak, 2017). Coleman and Hughes (2015: 145) have, for example, pointed to the need to 'step back from and

problematize security.' For them, critical distance is paramount for scholars in order to maintain a space for reflexivity that does not become colonized by security logics, the professional habitus of practitioners, or political discourses.

Such considerations echo concerns that have been put forward in the literature on socio-technical collaboration as well. As Nordmann and Schwarz (2010) have argued, it might at times be hard to resist the seductive 'lure of the "yes"' in technoscience, as it presents presumably elegant and straightforward forms of addressing social problems. Such seduction becomes aggravated by the (institutionalized) positionality of the social sciences within technoscientific contexts, the shared forms of responsibility, and the dependencies that result from close entanglements (Leese et al., 2019). STS techniques of attuning exactly to those claims of the supposed elegance of technical solutions can help those with a stronger background in critical security studies navigate these issues of proximity and openness.

With regard to security communities of practice, the risk of co-option (Mosse, 2006) does not merely come in the form of the seduction of science and technology, but also in the form of larger political agendas. Collaboration with the intention of infusing the production of technoscientific security tools with reflexivity, shared responsibilities and democratic oversight can end up inadvertently legitimizing undesired political programs. This has been illustrated in the case of peace research. Researchers who, in order to address the roots of political violence, choose to engage with policy-makers and to contribute to international interventions and peace-making processes, have at times found that their knowledge about conflict structures may have been used to reinforce existing power structures rather than to tackle the root causes of conflict (Hynek and Chandler, 2013). This example demonstrates how collaboration can be turned into a fig leaf that conceals structural questions of power and politics while at the same time resorting to the pretense of academic impartiality and analytical rigor.

Finally, similar arguments have also been put forward with regard to the reproduction of dominant discourses. Close proximity to security communities of practice will almost by default result in a deep immersion into professional cultures, rationales and processes of meaning-making. While this is generally desirable in order to foster mutual dialogue, scholars have pointed to the danger of embracing and reinforcing particular framings and discourses in collaboration and academic analyses (Rappert, 2009). This is particularly pertinent against the backdrop of the social constructedness of threats and reference objects, and the tools that would allegedly be needed to get the job done. Huysmans (2002) has cautioned that social scientific work, even with a clear critical edge, can contribute to the entrenchment of certain threat imaginaries or terminologies (e.g. migration as a security risk, or the use of 'border management' as a euphemism for highly exclusionary security practices at border crossing points).

Security, we argue, creates a number of complications for forms of socio-technical collaboration. Some have argued that, in the light of potential co-option and reproduction of dominant narratives, there should not be any socio-technical security collaborations at all (Neocleous, 2018). Others have been more optimistic, although aware of the challenges (Austin, 2019; Burgess, 2018; Leese et al., 2019). Building on these works, we propose to pursue collaboration with security communities of practice, but to proceed with caution. Following Jasanoff (1996), there can be no such thing as impartiality or

a-politicality in research. It is then all the more important to actively shape research along the lines of reflexivity, shared responsibilities, dialogue, public involvement and democratic procedures.

In the following, we trace how forms of critical socio-technical collaboration could play out in practice. We draw on three vignettes from our previous and ongoing work. Each vignette exemplifies a different type of socio-technical collaboration defined by different positionalities and modes of engagement. For each case, we briefly introduce the specific empirical context and then focus on five aspects of our collaborations with security communities of practice: (1) The *form* of intervention, that is, the relational configuration between the researcher and the relevant community of practice. (2) The intended *goal*, that is, the normative orientation of our engagement. (3) The *mode* in which the collaboration took place and the explanations of the methodological means we chose for the engagement. (4) The *challenges* that appeared during our collaborations and how we coped with them, with what success, and how we critically reflect on this experience. Finally, each vignette will describe (5) the *impact* of the engagement, especially in comparison with the intended aims.

Vignette 1: An outside commentary on information warfare

What kind of security concern is the spread of disinformation? Many politicians, journalists, think-tanks, security experts and academics in the Czech Republic believe that information chaos and the spread of disinformation is not only a political challenge, but also a symptom of being in a new type of information warfare or hybrid warfare with Russia (Eberle and Daniel, 2019). Since the Russian annexation of Crimea in 2014, previously overlooked conspiracy websites publishing news of dubious quality and pro-Russian propaganda started to be perceived as an extended arm of Russian government seeking to destabilize Western liberal democracies. This concern even translated into an update of the Czech National Security Strategy, in which the spread of disinformation and propaganda were labelled as security issues threatening the cooperative security mechanism in the West (Ministry of Foreign Affairs, 2015). Against the backdrop of this narrative on 'Russian-led information warfare', disputes over the factual accuracy of news started to be framed by security experts and politicians as an existential clash between active opponents of Russian aggression on the one hand and supporters of Putin's regime on the other (Daniel and Eberle, 2018).

In response to the escalating rhetoric related to this issue, one of us (Rychnovská) co-authored an academic article analyzing how this novel problematization of security (i.e. framing information disorder as information warfare or hybrid warfare) affects the politics of security expertise (Rychnovská and Kohút, 2018), and briefly after that a newspaper commentary that criticized the militarization of the public discourse (Rychnovská and Smetana, 2019). Both pieces were written from the perspective of academic researchers contributing to the national debate, without any prior experience of engaging in these specific issues or the community of practice.

The aim of the engagement was two-fold. Analytically, Rychnovská and her collaborators sought to map the newly emerged national network of actors recognized as experts

on information warfare and scrutinize what policies they suggested as a response to the spread of disinformation, and what type of knowledge and expertise they mobilized in this regard. This was in line with analyses focused on the role that STS researchers might take in addressing public reason in a 'post-truth' age (Jasanoff and Simmet, 2017). Normatively, the academic paper aimed at destabilizing the taken-for-grantedness of a specific assemblage of actors, practices and narratives making possible the rise of information warfare as a dominant security frame in the national debate.

In the escalating expert rhetoric on information warfare, the media engagement piece went further, as its aim was to desecuritize the highly polarized, and presumably militarized, public debate by moving the issue out of the sphere of exceptional politics and to stress the possibility of political choice, not 'necessity', on how to deal with disinformation. In this context, the securitized debate suggested that Russia waged a (hybrid) war against the West and that the West needed to start defending itself. As such, we, the protagonists of the critical engagement, came to the public debate with alternative values and capacities than the community of practice (see Fisher et al., 2015) and concretely, with the goal to change the narrative.

The academic article (Rychnovská and Kohút, 2018) used social network analysis to visualize the public performance of 'information warfare expertise', that is, who was able to achieve public legitimacy to speak about what and how information warfare was ongoing. The newspaper commentary, on the other hand, looked critically at the public debate on disinformation. Specifically, it claimed that the debate overlooked the ongoing sociotechnical transformations shaping the production and consumption of news and pointed out that the framing of the debate as warfare only deepened societal polarization, breed mistrust in political elites, contribute to the further propagation of conspiracy theories, and may ultimately lead to the destruction of free democratic debate. For instance, it rejected the ranking of Czech media based on the level of their alleged pro-Russian orientation, created by an influential conservative think-tank, as well as calls for the suspension of certain rights in the fight against online propaganda, and argued that fact-checking alone would not solve the spread of disinformation. Instead, the article suggested that what was at stake better understood as a structural problem of information disorder, characteristic of occasional Russian involvement, and highlighted the importance of understanding the social demand for anti-elitist and anti-system interpretations of political affairs in the first place.

The intervention was taken from the position of outside commentators, offering critical reflection based on academic expertise and taking the risk of presenting an unpopular opinion, while questioning some of the largely undisputed truths in the dominant foreign-policy and national identity narrative. Not surprisingly, the engagement triggered a heated reaction in diplomatic and expert communities and in the public debate, and its protagonists (including Rychnovská) were accused of academic isolation, of misunderstanding the 'real' security threats and the sheer size of Russian involvement in the West, and even of co-option by the pro-Russian forces undermining Western liberal democracy. The commentary was first rejected by a major liberal newspaper, whose editor argued in email correspondence that 'the commentary underestimates the threat … that Russia is waging an information WARFARE against the West' (translated from Czech, capitalization in original), while suggesting that writing such a commentary was an act

of naivety and foolishness. It was later published by a minor left progressive online magazine and was instantly widely circulated on social media and commented on by key Czech journalists, experts and publicly known military figures. They shared a very critical view of the article, expressed shock that a young generation of Czech academics took a supposedly pro-Russian stance, and some of them referred to writing the commentary as an act of 'useful idiots', allegedly sponsored by Russia or China.

The academic article (Rychnovská and Kohút, 2018) triggered similar reactions when it was published. Some contested the value of academic research that not only lacks clear policy solutions, but also goes against the dominant foreign policy and security orientation of the country. For instance, in reaction to the visualized network of information war experts, a top-level Czech diplomat argued that 'a similar mapping might be of interest to the Russian intelligence' and suggested that such research is harmful to Czech national security (Kurfürst, 2019). The negative response to the engagement confirmed the inherently political nature of expertise and the dynamic interplay between scientific facts, values, and emotions (Durnová, 2019). In this case, this was made visible when academic arguments were contested for not confirming the mainstream political discourse and allegedly undermining national security.

In order to lower the risk of positioning researchers as moral judges and to work towards some collaborative reflexivity with the community of practice (cf. Balmer et al., 2015: 20), a public seminar was organized in which the arguments were presented to interested publics, consisting mostly of foreign diplomats, security professionals, and journalists. Opening space for critical reflection enabled the authors to discuss what Balmer et al. (2015: 20) call 'unshared goals' with communities of practice. Despite disagreement on short-term measures, Rychnovská and her co-authors were able to generate shared understanding with others at the seminar that a stable, prosperous society based on positive values would be best equipped to deal with disinformation and external propaganda.

How do we assess the impact of navigating (out of) the identity of a 'useful idiot'? Both interventions were met with much criticism and suspicion from a large part of the relevant community of practice, the network of experts shaping the discourse on disinformation and information warfare in the Czech Republic. Despite this, two positive effects can be highlighted. First, the engagement helped disrupt the binary of the public debate on disinformation and opened a space for more complex understanding of the problem, which soon started to be filled by other expert voices criticizing the dominant narrative on Russian hybrid warfare (e.g. Deník, 2019; Syrovátka, 2019). Eventually, some ideas from the initial critical piece spread to broader media and expert discourse and helped disrupt the original polarized black-and-white reading of the issue. It also gave vocabulary to people who felt a certain unease with the military language and the logic of urgency and exceptionality surrounding the issue of fighting disinformation, a role that Downey and Zuiderent-Jerak (2017: 234) call 'meta-activism'. Drawing on rich conceptual vocabulary of critical security studies and STS, the main protagonists were able to translate these concepts into vocabulary understandable to a broader – albeit still rather limited – audience and offer different lenses through which to understand social and political phenomena.

Going after the dissenting voice on scientific and security matters, particularly on politically charged topics, is a common tactic, and we are not the first STS and science

policy researchers who have found themselves to be the target of the status quo. In the world of climate science, Roger Pielke Jr., Judith Curry, and others were the subject of what could be reasonably called a political witch hunt in the mid-2010s for noting the complexity of associating specific disasters to anthropogenic climate change and pointing out the limits of climate models (Curry, 2015; Pielke Jr., 2015; Tangney, 2019). As Pielke (2015) explained, he tried to correct specific parts of the climate change narrative and point out unsubstantiated causal claims made in it, yet was labelled as a climate sceptic instead, was subjected to a congressional testimony, significant public and scientific backlash, and ended up largely exiting the climate science debate.

We found ourselves in a similar position, and are also on the cusp of deciding whether to exit the disinformation debate altogether. There is another approach, however, that we, or those who come after us, might pursue next. The issue of disinformation in the Czech Republic is being presented within a security framing as a conventional national security problem that can be 'solved'. This is very much how climate change is often characterized. As Pielke and others have argued within climate science (Prins et al., 2010), the first step to dealing with disinformation may be to recognize the complexity and 'wickedness' of the problem (Rittel and Webber, 1973). Their recommendation was to take policy advice from the famed English landscape gardener Lancelot 'Capability' Brown: 'lose the object and draw nigh obliquely' (Prins et al., 2010; Prins and Rayner, 2007).[1] In other words, unpack the multiple layers and dimensions of the 'problem' and address them separately, with different types of urgency, expertise, and in a different mode of knowledge production. We could consider a security framing for disinformation, but it will take many policy areas acting from many angles on the question of what counts as legitimate knowledge to actually make movement on the security aspects of the problem. Only then might we be pleasantly surprised to find ourselves delivered into a society that has a sustainable information environment.

Vignette 2: Ethnographic research on predictive policing

The second vignette foregrounds a quite different mode of socio-technical collaboration. It highlights how unplanned critical engagement can emerge through field research encounters with security professionals. It illustrates how close proximity to a security community of practice turned from a concern into an asset, as a window of opportunity for engagement opened up through close proximity to key actors in the field. Expertise and trust could in this case be leveraged as a means of lending credibility to critical voices within a techno-scientific security context.

One of us (Leese) was recently involved in a multi-year research project on predictive policing in Germany and Switzerland. Predictive policing tools are supposed to provide police departments with the possibility of algorithmically analyzing crime data to produce actionable estimates about crime risk. The police could then devise suitable prevention strategies to discourage or deter criminal activity within these spatio-temporal risk coordinates (Perry et al., 2013). The project was carried out in cooperation with one other academic researcher, and its aim was – through in-depth expert interviews with involved actors as well as participant observation of predictive policing practices – to reconstruct predictive policing as the formation of a sociotechnical system of knowledge construction

and ordering practices (Egbert and Leese, 2020). The research was not originally conceived as a form of socio-technical collaboration, and the research design was not set up in a way that would have facilitated ways to go beyond the traditional divide between researchers and research subjects.

The plan was to explore how algorithmic crime predictions would transform the ways in which society is policed. It was informed by a presupposition that predictive policing would turn out to be an inherently problematic techno-scientific security practice. Fostered by media reports (Stanley, 2014), NGO's civil rights analyses (Knobloch, 2018; Robinson and Koepke, 2016), as well as critical academic works (Andrejevic, 2017; Mantello, 2016), we expected that algorithmic forms of crime analysis and ensuing police tactics would produce or aggravate issues of profiling and discrimination, engender forms of over-/underpolicing, and reinforce feedback loops between reported/detected criminal activity and the databases for the production of crime risk estimates. These concerns were not completely off, as our research revealed that there are some worrying issues and tendencies in how the police aspire to mobilize techno-scientific tools for the production of knowledge and order.

For us, these assumptions meant that we would need to keep a certain distance from the police professionals that we studied, from their ways of thinking about crime and security, from their occupational cultures, and not least from the predictive policing software that was supposed to provide them with new forms of knowledge and power. After all, we wanted to make sure that even after prolonged phases of field research, we would still be able to criticize predictive policing and point out its shortcomings in terms of non-discrimination, social justice, and other issues that we had not anticipated. However, as we followed police departments through their experimentation with, and implementation of S predictive policing software, we witnessed both their grappling with technical and organizational aspects of technology implementation, and their struggling with legal, ethical and wider societal implications of algorithmic knowledge production. These struggles were particularly visible as they worked through the automation of tasks and processes that used to be carried out by human analysts, resulting in new constellations between human analysts and predictive policing software. To a certain degree, institutional efforts to stay in control of a new techno-scientific tool were to be expected from a public agency. Police departments aspired to understand the theories, models, data sources, and algorithms that constitute predictive policing software, and to implement it in ways that it would not undercut human decision-making and obscure institutional accountability.

It was, however, surprising how openly the police communicated their struggles and concerns to us, and even more surprising that they actively turned to us for advice on several occasions. One of us was, for example, invited to present findings from our ongoing research to senior police officers and senior analysts at a police department that had not yet implemented predictive policing software, but was considering doing so. What started as a formal presentation turned into a three-hour conversation during which the involved police officials were primarily interested in societal and normative questions around algorithmic modes of crime analysis. Rather than shutting down or dispelling critical findings, they very much encouraged arguments about potentially problematic security practices resulting from the use of algorithmic crime analysis software. In a similar vein, one of us was recently invited to contribute to the development of the German

national artificial intelligence strategy for policing, particularly with regard to the ethical aspects of techno-scientific knowledge tools. In fact, we found ourselves in a situation similar to Brian Rappert when he was researching biosecurity codes of conduct, where the 'roles of 'questioner', 'responder' and 'expert' [shifted] quite unexpectedly during social interactions' (Rappert 2009, 166).

Security institutions are not known for such openness. On the contrary, they usually present themselves as hard to access, shrouded by a veil of secrecy, and quite reserved when it comes to talking about their tools and practices (de Goede et al., 2019; Monahan and Fisher, 2015). Why were police departments during our research so willing to openly communicate and, more importantly, to listen to critical perspectives on predictive policing? A few factors may have contributed. First, during the period of our research, predictive policing technology was still in its infancy and there was little certainty around the specific software packages, the theories, the models, and the data that could and/or should be used for crime forecasts. Police departments set up predictive policing as 'experiments', 'field tests' or 'trials' during which they sought to figure out how to best implement the production of algorithmic crime forecasts, how to translate analytic insights into patrol and crime prevention activities, and how to evaluate the efficacy and 'success' of predictive policing methods.

This uncertainty produced a space in which socio-technical collaboration became possible. The work with social scientists was conceived by some of the involved police departments as a welcome opportunity to integrate a different analytical perspective into the process. In order to do so, they turned the relationship between researcher and research subject upside down, and rendered us interviewees for their own questions. In these questions, the police were not particularly interested in our research insights into the technical or organizational aspects of predictive policing. After all, they felt confident that they were able to figure those out by themselves. Rather, they were interested in the social science perspective, as they were to a lesser extent capable of covering topics such as critical perspectives on ethics, privacy and data protection, and social justice.

This was no doubt facilitated by our presence in the field. Having established trust through numerous formal and informal encounters, we were readily available as contacts who were equipped with the facts about predictive policing, as well as with expertise in critical data studies, ethics, and other relevant fields to reflect about possible larger societal repercussions. Taken together, this constellation opened up what could be considered a window of opportunity to gradually reconfigure parts of our research into an unanticipated and non-institutionalized form of socio-technical collaboration. An open and critical form of exchange was facilitated by the police's institutional need to figure out the potential societal repercussions of predictive policing, and to explore possible modes of actively intervening and shaping the ordering effects of algorithmic crime forecasts.

Even though there was no initial alignment of goals between the social scientists and the police (Balmer et al., 2015: 20), a shared perspective (i.e. a responsible form of predictive policing) was produced through open discussions about the expectations and concerns vis-à-vis algorithmic knowledge production and subsequent ordering practices. Proximity, initially conceived of by the researchers as a risk to be avoided throughout fieldwork, eventually lent credibility and opened up a space for reflection about how to implement algorithmic crime analysis in a responsive fashion. In structuring future

modes of policing, police departments came to appreciate social scientific input into the ongoing development and refinement of predictive policing technology. In the end, the vignette shows that while assumptions about security spaces as hard to access and obtain information might be true, it is nonetheless possible to build critical socio-technical collaborations within them.

Vignette 3: Formal involvement in the iGEM competition

Our third vignette provides yet another mode of collaboration. How might we use formal involvement in organizations involved in security governance to modify their practices and policies in line with STS insights? What are the challenges of such close proximity? This vignette addresses these questions through eight years of engagement one of us (Evans) has had with iGEM, the international Genetically Engineered Machines competition. In the past decade, iGEM has developed increasingly sophisticated safety and security oversight systems and is now considered an experimental laboratory for security governance (McNamara et al., 2014; Millett et al., 2019). I have been a part of discussions about many of the changes that iGEM has undergone in its safety and security governance, and have used my position to push for more reflexive capacity in very early stage research settings and ambiguous security determination processes.

The process of building the institution of iGEM has also been a process of building the field of synthetic biology. This includes the discourses of 'biology by design' (Smolke, 2009), the identities of the students not as biologists, but as tinkering bioengineers, and the organization of biology in building blocks (biobricks) that can be pieced together to create new life with a human-designed purpose (Frow and Calvert, 2013; Rabinow and Bennett, 2012). Early on, in the late 2000s, safety and security were understood to be peripheral components of the competition (Guan et al., 2013). Even in 2010, when there were 128 teams, there was no systematic screening process in place to understand which genetic sequences teams were using, what they were doing with them, and whether that work posed potential harm to them, others, or the environment (McNamara 2014; McNamara et al., 2014).

Today's iGEM competition involves over 6000 students in hundreds of teams from every continent except Antarctica. As the competition grew, so did arguments from biosafety and security professionals that iGEM needed a robust safety and security system. These arguments gained traction within iGEM Headquarters after a series of 'near misses' in the early 2010s, and over the subsequent years iGEM saw the security apparatus grow from simple screening just before the competition to a Safety Prize and commercial screening of biological parts (McNamara et al., 2014, 984) to a requirement that teams check in with the Safety and Security committee multiple times over the course of the year, or face automatic disqualification from the competition. No other aspect of iGEM has that kind of insight into, and authority over, the teams. iGEM hired the former deputy director of the United Nations' Biological Weapons Convention Implementation Support Unit, Piers Millett, to be its Vice President for Safety and Security, while all other committee heads are volunteers. Each year, iGEM continues to adapt its biosafety and biosecurity program (Millett et al., 2019). Clearly, iGEM now takes security and safety seriously. But in doing so it is widely seen to be enabling, rather than constraining,

the economic, academic curiosity, and other aspects of the competition. This is in no small part due to the birth of the safety and security program inside the Human Practices Committee, and the engagement of the program with a range of critical scholars.

Several institutional characteristics of iGEM have made it amenable to critical engagement. First, as a professionally-led student competition, the stakes for making changes to the structure of the institution are significantly lower than are similar changes made at, say, a university or a government body. Second, the yearly nature of iGEM provides an in-built iteration cycle for experimenting on governance structures. Third, iGEM is a small organization 'on the books', with around a dozen staff, but it has a massive volunteer community: ozens of professionals sit on its committees pro bono; all of the teams have to pay to compete and provide their own funding to attend the annual Giant Jamboree in Boston; and nearly 200 professionals also pay their own way to Boston to judge the four-day competition. This structure has flourished due to a certain laissez-faire approach from the management, where the Committees in particular are given significant autonomy to innovate on how iGEM as an institution addresses local concerns, from measurement to 'human practices' to security.

I became engaged in iGEM in 2012 as a judge, and later as part of the organization through my roles as a member of the Safety and Security Committee and a member and then Co-Chair of the Human Practices Committee. While my expertise was on security issues as well as STS, I initially chose to join the Human Practices Committee, which was focused on the ways to get teams working on the social, political, economic, and other ways of understanding synthetic biology and its possible roles in the world. This was a purposeful move, as I believed that getting students to think about security issues was really only one example of getting them most of whom were being trained in traditional scientific departments that had yet to integrate any insights from STS to think about anything 'beyond the bench'. I joined the Safety and Security Committee to stay abreast of the security developments in the field, and discovered an opportunity to modulate (Fisher et al., 2006) the connections between safety, security and the concerns of the Human Practice Committee.

Having myself, the Director of Human Practices Megan Palmer, and other members of the Human Practices Committee sit on the Safety and Security Committee has allowed us to pick up not only potential safety and security issues, but also opportunities to have conversations with teams about how things that look like just a safety concern (say, environmental containment of a project) may also have significant issues around indigenous rights (the release of organisms on native lands), politics (transboundary transfer of specimens) and the structure of science (a belief that isolation of variables is the most desirable way to conduct investigations) (Evans and Frow, 2015).

The engagement work, therefore, has had two main goals, the first of which is making sure the teams are conducting their work safely and that known or novel security concerns are addressed early in the teams' work. While most teams are undergraduates, they routinely take up techniques invented only a few years earlier, and therefore they are likely to test existing regulatory and oversight capabilities – including on security issues – of their home institutions and countries. As a result, the Safety and Security Committee often finds itself at the vanguard of novel security issues in the field, and is able to experiment with novel ways of addressing those issues. As an example, two years after

an early publication on the possibility of producing a 'gene drive' capable of altering entire wild populations of organisms (Esvelt et al., 2014), one iGEM team from Minnesota tried to build a gene drive for their project (iGEM, 2016). This was the subject of much discussion within the Safety and Security Committee during the iGEM Giant Jamboree.

After that year's competition, I worked with Piers Millett to produce the first draft of iGEM's policy on gene drives, which was the first such policy developed in the world. We happened to both be at the University of Cambridge for a conference on catastrophic risk, and we drafted the policy between his presentation and mine; I then presented it as part of my talk on 'Words of caution in making objects of security concern'. A key component in the drafting was trying to balance the safety and security concerns with the desire for iGEM to remain a place that fostered, rather than sequestered, student excitement about synthetic biology. That draft then went back to the Safety and Security Committee for further revision and was finalized by February 2017 (iGEM, 2017). Was the gene drive system that the Minnesota team tried to build even completed, and in either case, a security concern? The ambiguous answers to these questions within iGEM actually became a resource for fostering proactive engagement with potential security issues, to keep security from becoming a dominant frame for future projects. That is, the gene drive policy that was developed speaks as much to the need to reinscribe the values of the community as it does to the need to ensure oversight of potentially harmful research.

The second goal of engagement has been that I and the others on the Human Practices Committee never wanted safety and security to be the only way that teams think beyond the bench, and it has only been through our active engagement with the institutional structure of iGEM and experimenting year-on-year on how to shape that institution to be more open to STS, ethics, and other broader aspects of the research that change has occurred. This has involved many meetings with iGEM Headquarters (the permanent staff) on the nature of the competition, what counts as things 'going wrong', and how to mitigate those concerns while also reinscribing the values that iGEM espouses (iGEM, 2014). Of course, in doing so, I have several times had heated debates on what those values should be, and how they should be balanced in practice, encountering the 'deeply entrenched pervasive assumptions, framings, and narratives about … the supposed separation between science and society' (Marris and Calvert, 2020: 34–35). These moments are ones of reflection for me on the value of remaining involved in iGEM at all, if I am actually doing more to reinscribe the very narratives I am seeking to question.

Reflecting on this experience, I was concerned when safety and security moved into center stage in the organization. This included Millett becoming Vice President of Safety and Security (a title held by none of the other Committee chairs), and the lack of safety/security compliance becoming one of the few means to disqualify teams. The Safety Check-in forms also became iGEM team's primary reporting mechanism, and thus an organizational sight line for iGEM headquarters (cf. Scott, 1998). That concern was assuaged, however, through the relationships between the Committees, through iGEM headquarters' continuing to be open to supporting Committee-led initiatives to use these opportunities to create more open channels for broader concerns to bubble up, and through the commitment of iGEM to ensuring that safety and security oversight enable team learning and exploration, not constrain it.

Towards critical collaboration

Critical security studies have pointed to how security is framed as a special type of politics, and that engagement with security brings additional challenges, as it is often a matter of sidetrack deliberation among closed circles of experts (Bigo, 2014), clouded either by secrecy (Masco 2018; Rappert, 2009) or by the proprietary characteristics of the technoscientific tools that are mobilized in its production (de Goede et al., 2019). Such traits are in many respects similar in the workings of science and technology. Combined with security they become amplified and tend to build multiple barriers of access not only to decision-making on techno-security at the political level, but also to the legitimate performance of expertise. If STS turned to science to address the hard case of the construction of a 'natural reality', the turn we are making to security is to address the hard case of the construction of 'political reality' – recognizing, of course, that the social and the natural are co-produced (Jasanoff, 2004). Both provide similar claims to be able to speak for the way the world really is, and through that, what ought to be done.

There are many spaces, however, that are not fully securitized or linked with national security where security framings also gain momentum. These 'edges of security' deserve as much attention as traditional security domains. They also may be easier to access and engage, as there are de facto already competing framings to security in these cases. STS scholars might consider the relationship between science, technology and security to be a mysterious and inaccessible sphere, but it need not be. Based on our experiences described in the vignettes, we argue against the myth of security as a special space that cannot be entered and shaped by a critical researcher working towards the democratization of science, technology and politics. Instead, we encourage critical researchers to find their way to the communities of security practice and to take on responsibility for the practice of security in the given area.

Our three vignettes provide illustrations of possible modes of critical collaboration with security communities of practice. Table 1 shows an overview of the challenges we encountered and the strategies we applied to tackle these challenges. The shared challenge that we all faced was how to move towards more awareness and critical reflection in the relevant community, while at the same time balancing security concerns with other values relevant for the community or society more broadly.

The first point to note is that the vignettes illustrate the dilemma of engagement. Rychnovská describes the risk of too much distance to the community of practice and the related accusation of co-option by the 'enemy'. Her experience shows that transparency about the goals of engagement and openness regarding the strengths and limits of one's engagement can help mitigate this critique, though never fully. Leese and Evans, in contrast, were concerned with the risks and opportunities resulting from close proximity. Close proximity, for them, provided an opportunity to better understand the practices of security knowledge production and the empirical context, but as each case shows, proximity could also lead to a role in shaping these practices and thus be a part of the production of (in)security.

In reflecting on the strategies used for dealing with these challenges in our research, all vignettes highlight the importance, as well as limitations, of opening spaces for dialogue, and show diverse ways to bridge the spheres of social scientific and practical expertise and

Table 1. Challenges and strategies for critical collaboration.

Vignette (mode of engagement)	Challenges encountered	Strategies devised
Information warfare (external commentator)	distance; alleged capture by 'the enemy'	transparency about the goals of engagement; openness about its limits
Predictive Policing (ethnography)	align unshared goals; leverage expertise and credibility into active involvement in shaping of predictive policing	creating a sense of shared responsibility; opening spaces for dialogue; framing critique in a constructive and productive way
iGEM (action research)	proximity; co-option; reproduction of dominant discourses; ambiguity	positioning as internal advisor to practitioners who championed and rearticulated STS ideas; maintained professional critique within STS community of ongoing engagement

create platforms for deliberation between diverse actors. Rychnovská stresses the role of developing a conceptual vocabulary to make the critique of dominant security narratives understandable for broader audiences and the importance of being prepared to take the risk of espousing an unpopular opinion. Leese and Evans both explain how they eventually became engaged in shaping the practices of security expertise and thus took on responsibility for the practice of security in the relevant area. As such, we used our proximity to create a sense of shared responsibility, to open up spaces for dialogue, and to practice collaborative reflexivity and collective experimentation (Balmer et al., 2015).

Throughout the vignettes, we have shown how participation and socio-technical collaboration became subject to reimagining and remaking – and ultimately subject of ongoing experimentation and collaborative reflexivity. This is in line with the post-ELSI turn in STS (Balmer et al., 2015; Chilvers, 2012). In all cases, the relations to the community of practice and the goals of our contribution were dynamically shaped in the process of engagement, which highlights the importance of reflecting on the construction and negotiation of roles of social scientists involved in socio-technical collaborations (cf. Balmer et al., 2015). Like Chilvers and Kearnes (2020), we believe that diverse, emergent, and co-productionist approaches to socio-technical collaborations foster deeper critical, yet still constructive, engagement with science and technology.

Collective experimentation and reflexivity, together with the willingness of both parties to open up about their goals and take risks, encourage both social scientists and security communities of practice to engage with each other's perspectives. Critical collaboration can help to explicate concerns about the roles of science and technology in security, not only on the side of practitioners who are encouraged to explicate and reflect on what they do and why, but also for social scientists who might reconsider and revise their (static) positions and knowledge claims vis-à-vis practical contexts (cf. Kurowska and Tallis, 2013; Mosse, 2006).

The very possibility of critical collaboration should not be taken for granted, however. Being aware of the highly asymmetrical power relations that can structure and define

scholarly engagement with security practitioners is important. As Rychnovská argues in her vignette, entering debates in the first place might be difficult – if not impossible – especially if there is no dedicated space for collaboration and deliberation. Sometimes, as Leese's vignette shows, such spaces can emerge in an unplanned and unstructured fashion, but such opportunities should not be counted on. Conceptually, security tends to foreclose open and reflexive debate, as threats are often framed as only understandable to domain experts who are in turn considered the only ones entitled to deal with them (Bigo, 2002). The prospects of being seen as a legitimate actor with relevant expertise in the debate on security might be further complicated by other aspects, such as gender and age, which need to be taken into account when reflecting one's positionality and experience with engaging the field of practice.

Finally, we must raise the question of whether we could possibly define the success (or failure) of critical collaboration. Rather than trying to define measurement criteria such as policy-making or behavioral change in organizations, we propose a processual understanding of success when it comes to the engagement with security communities of practice (Balmer et al., 2015; Leese et al., 2019). We suggest focusing on collaborative forms of action, reflection and resulting shared responsibility. These might not always take on tangible forms, but they might come in the form of critical reflection among security practitioners, greater awareness of the consequences of doing security, or a politicization of the ways in which security is discussed and performed in a given context. The creation of a space for discussing alternative framings of the problem (and thus potentially desecuritizing the issue) can in and of itself already be considered a positive effect of critical engagement, given the initial conditions and the structure of power relations in which the engagement takes place.

Conclusions

Security is a hard case, as it is concerned with questions of who is allowed to define threats to a social order, how, and in what contexts. The workings of security are deeply ingrained in the production of knowledge and power. In this capacity, security is characterized by an intimidating aura of gravity that aspires to shut down critical voices. Both critical security studies and STS share the ambition to overcome the alleged boundary between academia and sites and communities of (in)security production. Critical forms of socio-technical collaboration, as we have put forward here, can be seen as viable ways to open deliberative and constructive spaces for more inclusive framings of policy problems and solutions around the interplays of science, technology, and security. Our vignettes show that, although there are different strategies to engage the communities of security practice, they share the ambition to shape the discourses, practices and institutions that give meaning to what is legitimate and thinkable in a specific techno-security area.

We have, in some respects, come a long way from Bijker's call in the early 2000s for engaging with the communities we research in order to open up the processes through which political power is embedded within scientific and technical systems. We now have a rapidly developing tradition within STS of 'making and doing' through a broad range of socio-technical collaborations. We have suggested that the hesitation of STS researchers to engage with security is explained in part by concerns of being co-opted into the

political. Security, as an area of critical research, might also be avoided because deconstructing and destabilizing the practices through which our societies seek to protect their survival, key values and identities may simply sound too risky and dangerous from a normative perspective. We believe the risk of not engaging in this research is greater still, precisely because security practices form the basis for institutionalized power structures, drawing the lines around who and what is allowed and forbidden.

The vignettes illustrate the fruitfulness that can come from combining critical security studies' analytic capacity for understanding political and organizational work being done in the name of security with STS's current advances in engagement methodology and its long-standing skillset in analyzing the social within the technical and scientific. We close this article with a call to action. STS scholars (Balmer et al., 2015; Downey and Zuiderent-Jerak, 2017; Lezaun et al., 2017) as well as critical security studies researchers (Berling and Bueger 2017) and social scientists more broadly (Fassin and Harcourt, 2019) can take on various roles when engaging with political practice and can experiment with numerous models of participation. Engagement with security topics brings additional challenges and obstacles, especially for researchers embracing critical approaches to dominant discourses and practices of security. That is all the more reason that this is a vital and fruitful area of development in theory and practice for STS.

Acknowledgements

The authors would like to thank the editor, two anonymous reviewers and the participants of the EWIS 2019 workshop 'Global reconfigurations of science, technology, and security' for their helpful comments on the article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Sam Weiss Evans received funding from Schmidt Futures as part of the grant on 'Ethics in the lab: A novel collaboration for technology governance'. Research by Dagmar Rychnovská has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 799805.

ORCID iD

Sam Weiss Evans https://orcid.org/0000-0001-8547-3314

Note

1. Prins and Rayner (2007: 38) note that the statement, while attributed to Brown's work, was actually coined by William Shenstone: 'When a building or other object has been once viewed from its proper point, the foot should never travel to it by the same path, which the eye has travelled over before. Lose the object, and draw nigh, obliquely' (Shenstone, 1764).

References

Anderson B (2010) Security and the future: Anticipating the event of terror. *Geoforum* 41(2): 227–235.

Anderson B (2006) Census, map, and museum. In: *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. London: Verso, 167–190.

Andrejevic M (2017) To preempt a thief. *International Journal of Communication* 11: 879–896.
Aradau C (2004) Security and the democratic scene: Desecuritization and emancipation. *Journal of International Relations and Development* 7(4): 388–413.
Austin JL (2019) Towards an international political ergonomics. *European Journal of International Relations* 25(4): 979–1006.
Balmer AS, Calvert J, Marris C, et al. (2015) Taking roles in interdisciplinary collaborations: Reflections on working in post-ELSI spaces in the UK synthetic biology community. *Science & Technology Studies* 28(3): 3–25.
Balzacq T (2015) *Contesting Security: Strategies and Logics*. Milton Park/New York: Routledge.
Berling TV and Bueger C (2017) Expertise in the age of post-factual politics: An outline of reflexive strategies. *Geoforum* 84(August): 332–341.
Bigo D (2002) Security and immigration: Toward a critique of the governmentality of unease. *Alternatives: Global, Local, Political* 27(1): 63–92.
Bigo D (2014) The (in)securitization practices of the three universes of EU border control: Military/navy – border guards/police – database analysts. *Security Dialogue* 45(3): 209-225.
Bigo D, Jeandesboz J, Martin-Mazé M and Ragazzi F (2014) *Review of Security Measures in the 7th Research Framework Programme FP7 2007-2013*. Brussels: European Parliament.
Bijker WE (2003) The need for public intellectuals: A space for STS. *Science, Technology & Human Values* 28(4): 443–450.
Bloor D (1976) *Knowledge and Social Imagery*. London: Routledge & Kegan Paul.
Booth K (1991) Security and emancipation. *Review of International Studies* 17(4): 313–326.
Booth K (2007) *Theory of World Security*. Cambridge: Cambridge University Press.
Bourne M (2014) *Understanding Security*. Houndmills, Basingstoke: Palgrave Macmillan.
Burgess JP (2018) Danger, innovation, responsibility. In: Burgess JP, Reniers G, Ponnet K, et al. (eds): *Socially Responsible Innovation in Security: Critical Reflections*. New York: Routledge, 12–21.
Buzan B and Hansen L (2009) *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.
Buzan B, Wæver O and de Wilde J (1998) *Security: A New Framework for Analysis*. Boulder: Rienner.
c.a.s.e. collective (2006) Critical approaches to security in Europe: A networked manifesto. *Security Dialogue* 37(4): 443–487.
Chilvers J (2012) Reflexive engagement? Actors, learning, and reflexivity in public dialogue on science and technology. *Science Communication* 35(3): 283–310.
Chilvers J and Kearnes M (2020) Remaking participation in science and democracy. *Science, Technology, & Human Values* 45(3): 347–380.
Coleman LM and Hughes H (2015) Distance. In: Aradau C, Huysmans J, Neal AW, et al. (eds) *Critical Security Methods: New Frameworks for Analysis*. New York: Routledge, 142–158.
Curry J (2015) A new low in science: Criminalizing climate change skeptics. Available at: https://www.foxnews.com/opinion/a-new-low-in-science-criminalizing-climate-change-skeptics (accessed 25 February 2020).
Daniel J and Eberle J (2018) Hybrid warriors : Transforming Czech security through the 'Russian hybrid warfare' assemblage. *Sociologický časopis. Czech Sociological Review* 54(6): 907–931.
Davidshofer S, Jeandesboz J and Ragazzi F (2017) Technology and security practices: Situating the technological imperative. In: Basaran T, Bigo D, Guittet E-P, et al. (eds) *International Political Sociology: Transversal Lines*. New York: Routledge, 205–227.
de Goede M, Bosma E and Pallister-Wilkins P (eds) 2019. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, London: Routledge.

de Lint W and Virta S (2004) Security in ambiguity: Towards a radical security politics. *Theoretical Criminology* 8(4): 465–489.

Deník N (2019) Rusko s námi hybridní válku nevede, říkají experti. Na válku jsou potřeba dva [Russia does not wage a hybrid war against us, experts say. You need two for a war]. Available at: https://denikn.cz/76245/rusko-s-nami-hybridni-valku-nevede-rikaji-experti-na-valku-jsou-potreba-dva/ (accessed 13 December 2019).

Dijstelbloem H and Meijer A (eds) (2011) *Migration and the New Technological Borders of Europe*, Basingstoke: Palgrave Macmillan.

Downey GL and Zuiderent-Jerak T (2017) Making and doing: Engagement and reflexive learning in STS. In: Felt U, Smith-Doerr L, Miller CA, et al. (eds) *Handbook of Science and Technology Studies*, 4th ed. Cambridge: MIT Press, 223–251.

Durnová A (2019) *Understanding Emotions in Post-Factual Politics: Negotiating Truth*. Edward Elgar Publishing.

Eberle J and Daniel J (2019) 'Putin, you suck': Affective sticking points in the Czech narrative on 'Russian Hybrid warfare'. *Political Psychology* 40(6): 1267–1281.

Egbert S and Leese M (2020) *Criminal Futures: Predictive Policing and Everyday Police Work*. New York: Routledge.

Epstein C (2007) Guilty bodies, productive bodies, destructive bodies: Crossing the biometric borders. *International Political Sociology* 1(2): 149–164.

Esvelt KM, Smidler AL, Catteruccia F, et al. (2014) Concerning RNA-guided gene drives for the alteration of wild populations. *eLife* e03401.

Evans SW and Frow EK (2015) 'Taking care' in synthetic biology. In: Rappert B and Balmer B (eds) *Absence in Science, Security and Policy: From Research Agendas to Global Strategy*. Basingstoke: Palgrave Macmillan, 132–153.

Fassin D and Harcourt BE (eds) (2019) *A Time for Critique*. Columbia University Press.

Fisher E (2005) Lessons learned from the Ethical, Legal and Social Implications program (ELSI): Planning societal implications research for the National Nanotechnology Program. *Technology in Society* 27(3): 321–328.

Fisher E, Mahajan RL and Mitcham C (2006) Midstream modulation of technology: Governance from within. *Bulletin of Science, Technology & Society* 26(6): 485–496.

Fisher E, O'Rourke M, Evans R, et al. (2015) Mapping the integrative field: Taking stock of socio-technical collaborations. *Journal of Responsible Innovation* 2(1): 39–61.

Frow E and Calvert J (2013) 'Can simple biological systems be built from standardized interchangeable parts?' Negotiating biology and engineering in a synthetic biology competition. *Engineering Studies* 5(1): 42–58.

Gallie WB (1955) Essentially contested concepts. *Proceedings of the Aristotelian Society* 56: 167–98.

Guan Z, Schmidt M, Pei L, et al. (2013) Biosafety considerations of synthetic biology in the international Genetically Engineered Machine (iGEM) competition. *BioScience* 63(1): 25–34.

Hansen L (2012) Reconstructing desecuritisation: The normative-political in the Copenhagen School and directions for how to apply it. *Review of International Studies* 38(3): 525–546.

Hellström T (2003) Systemic innovation and risk: Technology assessment and the challenge of responsible innovation. *Technology in Society* 25(3): 369–384.

Hoijtink M and Leese M (2019) *Technology and Agency in International Relations*. London/New York: Routledge.

Huysmans J (1998) Security! What do you mean? From concept to thick signifier. *European Journal of International Relations* 4(2): 226–255.

Huysmans J (2002) Defining social constructivism in security studies: The normative dilemma of writing security. *Alternatives: Global, Local, Political* 27(1): 41–62.

Huysmans J (2011) What's in an act? On security speech acts and little security nothings. *Security Dialogue* 42(4–5): 371–383.
Hynek N and Chandler D (2013) No emancipatory alternative, no critical security studies. *Critical Studies on Security* 1(1): 46–63.
iGEM (2014) Values. Available at: https://igem.org/Values (accessed 23 July 2020).
iGEM (2016) Minnesota. Available at: http://2016.igem.org/Team:Minnesota (accessed 23 July 2020).
iGEM (2017) Safety policies. Available at: http://2017.igem.org/Safety/Policies (accessed 23 July 2020).
Jasanoff S (1990) *The Fifth Branch: Science Advisers as Policymakers*. Cambridge: Harvard University Press.
Jasanoff S (1996) Beyond epistemology: Relativism and engagement in the politics of science. *Social Studies of Science* 26(2): 393–418.
Jasanoff S (2004) *States of Knowledge: The Co-Production of Science and Social Order*. New York: Routledge.
Jasanoff S (2015) Future imperfect: Science, technology, and the imaginations of modernity. In: Jasanoff S and Kim S-H (eds) *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. University of Chicago Press, 1–33.
Jasanoff S and Kim S-H (2009) Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea. *Minerva* 47(2): 119–146.
Jasanoff S (ed.) (2011) *Reframing Rights: Bioconstitutionalism in the Genetic Age*. Cambridge: MIT Press.
Jasanoff S and Kim S-H (2015) *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. Chicago: University of Chicago Press.
Jasanoff S and Simmet HR (2017) No funeral bells: Public reason in a 'post-truth' age. *Social Studies of Science* 47(5): 751–770.
Knobloch T (2018) *Vor die Lage kommen: Predictive Policing in Deutschland*. Stiftung Neue Verantwortung/Bertelsmann Stiftung.
Krause K and Williams MC (1997) *Critical Security Studies: Concepts and Cases*. London: Routledge.
Kurfürst J (2019) Jak badatelé ÚMV odhalili „české hybridní válečníky' a utekla jim podstata [How IIR researchers revealed 'Czech hybrid warriors' and missed the essence]. *Mezinárodní politika*, Summer. Available at: https://iir.cz/article/jak-badatele-umv-odhalili-ceske-hybridni-valecniky-a-utekla-jim-podstata (accessed 08 August 2020).
Kurowska X and Tallis BC (2013) Chiasmatic crossings: A reflexive revisit of a research encounter in European security. *Security Dialogue* 44(1): 73–89.
Leese M (2014) The New Profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue* 45(5): 494–511.
Leese M, Lidén K and Nikolova B (2019) Putting critique to work: Ethics in EU security research. *Security Dialogue* 50(1): 59–76.
Lezaun J, Marres N and Tironi M (2017) Experiments in participation. In: Felt U, Fouché R, Miller CA, et al. (eds) *The Handbook of Science and Technology Studies*. Cambridge: MIT Press, 195–221.
Mantello P (2016) The machine that ate bad people: The ontopolitics of the precrime assemblage. *Big Data & Society* 3(2): 2053951716682538.
Marris C and Calvert J (2020) Science and Technology Studies in policy: The UK Synthetic Biology Roadmap. *Science, Technology, & Human Values* 45(1): 34–61.
Masco JP (2014) *The Theater of Operations: National security from the Cold War to the War on Terror*. Durham: Duke University Press

Masco J P (2018) The secrecy/threat matrix. In: Maguire M, Rao U and Zurawski N (eds) *Bodies as Evidence: Security, Knowledge, and Power*. Durham: Duke University Press, 175–200.

Matzner T (2016) The model gap: Cognitive systems in security applications and their ethical Implications. *AI & Society* 31(1): 95–102.

Mayer M, Carpes M and Knoblich R (2014) The global politics of science and technology: An introduction. In: Mayer M, Carpes M and Knoblich R (eds) *The Global Politics of Science and Technology - Vol. 1: Concepts from International Relations and Other Disciplines*. Dordrecht: Springer, 1–35.

McNamara JH (2014) Bridging gaps in synthetic biology oversight: iGEM as a testbed for proactive, adaptive risk management. Thesis, Massachusetts Institute of Technology. Available at: https://dspace.mit.edu/handle/1721.1/90057 (accessed 19 February 2020).

McNamara J, Lightfoot SB-Y, Drinkwater K, et al. (2014) Designing safety policies to meet evolving needs: iGEM as a testbed for proactive and adaptive risk management. *ACS Synthetic Biology* 3(12): 983–985.

Miller CA and Wyborn C (2018) Co-production in global sustainability: Histories and theories. *Environmental Science & Policy*. Epub ahead of print 4 February 2018. DOI: 10.1016/j.envsci.2018.01.016.

Millett P, Binz T, Evans S W, et al. (2019) Developing a comprehensive, adaptive, and international biosafety and biosecurity program for advanced biotechnology: The iGEM experience. *Applied Biosafety* 24(2): 64–71.

Ministry of Foreign Affairs (2015) Security strategy of the Czech Republic 2015. Available at: http://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf.

Monahan T and Fisher JA (2015) Strategies for obtaining access to secretive or guarded organizations. *Journal of Contemporary Ethnography* 44(6): 709–736.

Mosse D (2006) Anti-social anthropology? Objectivity, objection, and the ethnography of public policy and professional communities. *Journal of the Royal Anthropological Institute* 12(4): 935–956.

Neocleous M (2018) The bleak rituals of progress; Or, if somebody offers you a socially responsible innovation in security, just say no. In: Burgess JP, Reniers G, Ponnet K, et al. (eds) *Socially Responsible Innovation in Security: Critical Reflections*. New York: Routledge, 129–140.

Nordmann A and Schwarz A (2010) Lure of the 'yes': The seductive power of technoscience. In: Kaiser M, Kurath M, Maasen S, et al. (eds) *Governing Future Technologies: Nanotechnology and the Rise of an Assessment Regime*. Dordrecht: Springer, 255–277.

Owen R, Macnaghten P and Stilgoe J (2012) Responsible research and innovation: From science in society to science for society, with society. *Science and Public Policy* 39(6): 751–760.

Owen R, Bessant J and Heintz M (2013) *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*. Chichester: Wiley.

Perry WL, McInnis B, Price CC, et al. (2013) *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND Corporation.

Pielke RA, Jr (2015) I am under 'investigation'. In: *The Climate Fix*. Available at: https://theclimatefix.wordpress.com/2015/02/25/i-am-under-investigation/ (accessed 25 February 2020).

Polanyi M (1962) The republic of science: Its political and economic theory. *Minerva* 1(1): 54–74.

Price DH (2011) *Weaponizing Anthropology: Social Science in Service of the Militarized State*. Reprint edition. Oakland, CA: AK Press.

Prins G and Rayner S (2007) *The Wrong Trousers: Radically Rethinking Climate Policy*. A Joint Discussion Paper of the James Martin Institute for Science and Civilization, University of Oxford and the MacKinder Centre for the Study of Long-Wave Events, London School of Economics.

Prins G, Galiana I, Green C, et al. (2010) *The Hartwell Paper: A New Direction for Climate Policy after the Crash of 2009*. Institute for Science, Innovation, and Society, University of Oxford.

Rabinow P and Bennett G (2012) *Designing Human Practices: An Experiment with Synthetic Biology*. University of Chicago Press.

Rappert B (2009) *Experimental Secrets: International Security, Codes, and the Future of Research*. Lanham: University Press of America.

Ravetz JR (1971) *Scientific Knowledge and Its Social Problems*. Oxford: Clarendon Press.

Rip A, Misa TJ and Schot J (1995) Constructive technology assessment: a new paradigm for managing technology in society. In: Rip A, Misa TJ and Schot J (eds) *Managing Technology In Society: The Approach of Constructive Technology Assessment*. New York: Pinter, 1–14.

Rittel HWJ and Webber MM (1973) Dilemmas in a general theory of planning. *Policy Sciences* 4(2): 155–169.

Robinson D and Koepke L (2016) *Stuck in a Pattern: Early Evidence on 'Predictive Policing' and Civil Rights*. Upturn. Available at: https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf (accessed 8 August 2020).

Rychnovská D and Kohút M (2018) The battle for truth: mapping the network of information war experts in the czech republic. *New Perspectives. Interdisciplinary Journal of Central & East European Politics and International Relations* 26(3): 57–87.

Rychnovská D and Smetana M (2019) A proti trollům povstali elfové … [And the elves rose up against the trolls …]. Available at: http://a2larm.cz/2019/01/a-proti-trollum-povstali-elfove/ (accessed 08 Aug 2020).

Salter MB (2015) *Making Things International 1: Circuits and Motion*. Minneapolis: University of Minnesota Press.

Scott JC (1998) *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven: Yale University Press.

Shapin S (1995) *A Social History of Truth*. Chicago: University of Chicago Press.

Shapin S and Schaffer S (1985) *Leviathan and the Air-Pump: Hobbes, Boyle, and the Experimental Life*. Princeton: Princeton University Press.

Sismondo S (2008) Science and technology studies and an engaged program. In: Hackett EJ, Amsterdamska O, Lynch M, et al. (eds) *The Handbook of Science and Technology Studies*. 3rd ed. Cambridge: MIT Press, 13–31.

Smolke CD (2009) Building outside of the box: iGEM and the BioBricks Foundation. *Nature Biotechnology* 27(12): 1099–1102.

Stanley J (2014) *Chicago Police 'Heat List' Renews Old Fears About Government Flagging and Tagging*. ACLU, February 25. Available at https://www.aclu.org/blog/privacy-technology/chicago-police-heat-list-renews-old-fears-about-government-flagging-and (accessed 30 November 2017).

Suchman L, Follis K and Weber J (2017) Tracking and targeting: Sociotechnologies of (in)security. *Science, Technology, & Human Values* 42(6): 983–1002.

Syrovátka J (2019) Dobře hozená rukavice [Well Thrown Gauntlet]. Available at: http://blog.aktualne.cz/blogy/jonas-syrovatka.php?itemid=33158f (accessed 8 August 2020).

Tangney P (2019) Between conflation and denial: The politics of climate expertise in Australia. *Australian Journal of Political Science* 54(1): 131–149.

van Gorp A and van der Molen S (2011) Parallel, embedded or just part of the team: ethicists cooperating within a European security research project. *Science and Engineering Ethics* 17(1): 31–43.

Visvanathan S and Setelvad T (2014) Narratives of vulnerability and violence: Retelling the Gujarat riots. In: Hommels A, Mesman J and Bijker WE (eds) *Vulnerability in Technological Cultures: New Directions in Research and Governance*. Cambridge: MIT Press, 109–130.

Vogel KM, Balmer B, Evans SW, et al. (2017) Knowledge and Security. In Felt U, Fouché R, Miller C A and Smith-Doerr L (eds.) *The Handbook of Science and Technology Studies*. Cambridge: MIT Press, 973–1002.

Woolgar S (2004) What happened to provocation in science and technology studies? *History and Technology* 20(4): 339–349.

Woolgar S and Neyland D (2013) Mundane terror. In: *Mundane Governance: Ontology and Accountability*. Oxford: Oxford University Press, 194–219.

Author biographies

Sam Weiss Evans is a Fellow in the Program on Science, Technology and Society at Harvard University's John F Kennedy School of Government and a Research Associate at Harvard's John A Paulson School of Engineering and Applied Sciences. Sam's research covers historical and contemporary efforts to remake the ways objects and practices of security concern are constructed and governed. Sam's drive is to find ways to make security objects and practices more democratically accountable.

Matthias Leese is a Senior Researcher at the Center for Security Studies (CSS), ETH Zurich. His research is primarily interested in the social effects produced at the intersections of security and technology, and pays specific attention to the normative repercussions of new security technologies across society, both in intended and unintended forms.

Dagmar Rychnovská is a fellow at the Institute for Advanced Studies in Vienna. She specializes in international relations and security studies and her current work focuses on the politics of security infrastructures and security expertise in the governance of science and technology.