What harms may come?

Exploring the anticipatory dimensions of surveillance resistance in an age of datafication

Kazansky, B.

Publication date
2021

Chapter 6. Taming uncertainty into risk: Towards a critical lens on risk management practices in digital and cybersecurity[17]

17 This chapter has been submitted for peer review in July, 2021

Abstract

Amidst myriad forms of contemporary governmental and commercial digital surveillance, civil society actors grapple with a number of threats and uncertainties related to digital intrusions, online profiling, harassment, and technology-facilitated violence. This chapter explores how targeted civil society actors work with digital security specialists work to tame surveillance-related uncertainties into 'manageable' risks. The chapter investigates risk assessment as it is enacted in the context of a digital security training organized for human rights defenders to learn concrete security mitigations such as encrypted communications tools. Drawing on ethnographic data from participant observation in 12 digital security trainings organized for human rights defenders, the chapter shows that in the context of the digital security training, the transformation of uncertainty into risk occurs through the development of a shared language about danger. I term this process one of 'qualculative convergence', a critical intervention into corporate risk management language which conceives of risk as a cold and quantifiable phenomena. The chapter draws on valuation studies and studies of risk calculation in STS to enrich an interdisciplinary understanding of how people make sense of uncertainty. In exploring how targeted communities apply risk-centric logics to their work, the chapter also extends critical security studies' long-standing concerns with the ethico-political dimensions of risk beyond its focus on state and corporate security actors.

Keywords: risk assessment, risk management, risk calculation, qualculation, valuation studies, digital security, cybersecurity

Introduction

The rationalities and techniques of risk management are of central interest to studies of security, surveillance, and algorithmic, data-driven profiling (c.f. Amoore, 2013; Amoore and de Goede, 2008; de Goede, 2004; 2008; Dencik et al., 2019; Gandy, 2009; Monahan, 2010; Stachowitsch and Sachseder, 2019). Who or what is framed by institutions as risky or at risk serves to justify the development and deployment of novel forms of surveillance against different populations, entrenching inequalities and enrolling people within 'anticipatory regimes'(c.f. Adams et al., 2009) of disciplinary power. As Amoore (2013) and O'Grady (2016) argue, risk logics and practices are highly mobile, traveling across disparate social realms to inform rationalities around security, safety and emergency response. Yet the focus of much critical risk and security literature has historically been the logics of state and corporate risk regimes. This chapter instead explores the risk-centric practices of civil society actors seeking to resist and find safety from the harms of digital surveillance and 'digital threats' related to online harassment, data theft, and intrusion into digital infrastructures. The chapter investigates how surveillance and security risks are made sense of by civil society actors in the context of digital security trainings, events organized to facilitate learning about mitigation strategies against common forms of digital attacks and compromise caused by state and corporate actors antagonistic to civil society goals.

The threats and uncertainties of concern to civil society actors attending digital security trainings cover a range of different issues related to surveillance, security, and datafication; from concern over the spread of wide-scale 'smart' facial recognition infrastructures to the individual targeting of high-profile HRDs through sophisticated state-sponsored malware. The continued uncertainty over how exactly surveillance is conducted and whether an individual or group are being targeted at any

given moment contributes to a sense of overwhelm for those seeking safety, as I show in Chapter 4 of the thesis. Civil society groups therefore work to grapple with these uncertainties in a way that facilitates agency and safety. As Chapter 5 shows, this can mean turning to different forms of technological mitigations and risk management strategies to 'tame' uncertainty. Yet, per Scoones and Sterling (2020), 'uncertainty is never just a technical issue'(15). Scoones and Sterling argue that 'addressing uncertainty means confronting inequality, vulnerability, precarity and the deeply embedded inheritances of history head-on'. The authors further suggest that turning to risk management to deal with violence and danger rarely results in doing away with the risk of concern. Rather, it provides violence and danger with an aura of manageability. What does this mean for the efforts of civil society actors who apply different tools and techniques of risk management to deal with digital surveillance and insecurity? Taking inspiration from Scoones and Stirling, this chapter looks closely and critically at how dangers related to surveillance and digital insecurity are flattened into manageable contingencies and mapped to appropriate mitigations for anticipated threats through techniques of risk management. Further, the chapter proposes a critical intervention into risk management approaches through a concept aiming to de-naturalize the corporate rationalities that inform the risk-centric practices of civil society and other social realms.

Importantly, the uncertainties of concern to civil society actors result from political instability, shifting patterns of discrimination and targeting, and ubiquitous yet opaque data processing, with well documented yet difficult to avoid harms. In the face of such ubiquitous and power-laden dynamics, the setting of the digital security training becomes a place to come up with concrete actions that can be taken on an individual and community level in order to continue human rights and social justice related work with some degree of autonomy and safety. While in Chapter 4, I traced the growing importance of civil society practices configured to grapple with and 'tame' the uncertainties that surround contemporary surveillance and

its related threats. In this chapter, I analyse the enactment of a risk assessment process at the site of a digital security training organized for human rights defenders to learn mitigations to digital surveillance and security threats from state actors antagonistic towards their political goals. Within the realm of civil society[18], digital security training events are set up as a space to 'raise awareness' of threatening technological and political developments, build literacy around the stakes of data and the digital, and develop concrete counter-strategies against ever-proliferating forms of surveillance (Daskal, 2018; Ermoshina and Musiani, 2018; Kazansky, 2015, 2016; Monsees, 2020; the Engine Room 2018). Training participants – which in this chapter are human rights defenders working on a diverse range of issues such as environmental justice, anti-corruption, and women's rights – are asked to share personal experiences with surveillance, work hands-on with digital security tools such as secure browsers and messenger apps, and coalesce around potential strategies for action in response to past or probable harm.

Digital security trainings are varied in their scope and shape. Though 'digital security' is the stated subject, the term encompasses a wide range of technology related topics including secure data storage, 'information management', communications, and censorship circumvention, as well as issues around 'data politics'(Ruppert et al., 2017), autonomy, 'technological sovereignty' (Couture and Toupin 2019; Haché, 2014; 2018), algorithms, and digital rights (Daskal, 2018). The focus is on turning unwieldy technological complexity and political uncertainty into a manageable risk, as I show in Chapter 4. But what goes into this transformation? How does it become possible for groups under threat to

18 Civil society in this chapter refers to the ream of action beyond the state and corporation. Of particular focus is an institutional ecology of transnationally coordinating non-profit organizations, security specialists, and front-line groups, which together grapple with the threats of digital surveillance and related harms around harassment, targeting, and discrimination.

think through ‘data mess’? (c.f. Pink et al., 2018). More fundamentally, why is it important for some to imagine political strife and injustice through the language of risk, and how might thinking through the language of risk change the nature of civil society work?

In this chapter, I show that in the context of the digital security training, the transformation of uncertainty into risk occurs through the work of what one digital security trainer describes as the development of a ‘shared language’ about danger, through which ‘the individual can act’ (Interview #12) in anticipatory avoidance of undesired future events. I term this process of developing a shared risk language as a process of ‘qualculative convergence’. As I will expand upon further in the next sections, the concept of qualculative convergence is a critical intervention into the concept of ‘risk convergence’, a term that is increasingly popular in corporate enterprise risk management, which means, ‘to integrate risk disciplines that are significant to an organization, such as operational risk or compliance, within a single framework’ (Enterprise Risk Management Initiative, 2008). Where risk convergence is premised on a ‘rational’, financialized, and quantitative approach to risk, my concept of qualculative convergence pushes back against such risk rationalities. I make this intervention by drawing on the notion of ‘qualculation’ (Callon and Law, 2005; Cochoy 2008), a concept which explains human judgement as the product of messy, intersubjective forms of valuation. As Callon, Law, and Cochoy argue, when people evaluate, calculate, measure, and otherwise engage in different processes of judgement, the lines between quantitative and qualitative thinking are in fact blurry. In other words, even a quantitative judgement involves complex processes of estimation, visual guessing, and other forms of incommensurable knowledge. The interwovenness of quantitative and qualitative judgement means that hard distinctions between the two occlude a granular understanding of the complex social processes that produce numbers, heuristics, standards of measurement, and infrastructures. These three

authors hence suggest the use of the term 'qualculation' in order to draw attention to the messiness of human judgement.

I apply Callon, Law, and Cochoy's concept of qualculation within my own concept of qualculative convergence in order to build an understanding how human rights defenders and digital security trainers make sense of surveillance uncertainties. The chapter explores how the process of qualculative convergence brings people together around a shared notion of security risk. In exploring qualculative convergence, I attend to the affective, temporal, and material elements of this process. In exploring how uncertainty becomes risk through qualculative means, I aim to contribute to a richer understanding of how people make sense of datafication through different forms of calculative (or rather, qualculative) logics. Furthermore, in exploring how civil society actors such as human rights defenders apply risk-centric logics to their work, my aim is to take the long-standing field of study in critical security studies around risk beyond its focus on state and corporate security actors. As I argue, attending to civil society practice can enable critical security studies and other disciplines critically concerned with risk to build a richer empirical understanding of the mobility of risk practices and risk logics, illuminating paths through which risk rationalities and security practices are not just imported into new sociopolitical contexts but also reconfigured and reimagined.

The plan of the chapter is such: I first situate my concern with risk in the context of critical studies of security and explain my conceptual intervention into cybersecurity risk management. Following, I explain my methods. I then describe three stages of ‘qualculative convergence’ in the context of a digital security training, drawing on data collected from three years of participant observation in digital security trainings.

Questioning Risk

Cybersecurity historian Rebecca Slayton has argued that 'risk management is the central approach to cybersecurity in governments and corporations around the world' (2015: 32). Risk assessment in this realm is increasingly a highly formalized process, premised on convergence around a set of 'objective' quantitative metrics. Slayton investigates how risk management strategies provide cybersecurity entities and institutions with a sense of control – its penultimate embodiment in the appeal of automation and automated risk models, through which 'analysts could 'turn the crank' to output a measure of risk, without really understanding what they were doing' (33). My own survey of cybersecurity and information security literature since the 1980s highlights that computer science departments, commercial and state cybersecurity institutions predominantly draw on rationalist and cognitive approaches to risk in support of 'objective' frameworks for risk management. A number of studies focus on the psychological and behavioural-economic aspects of 'risk perception', postulating on why degrees of risk perception vary amongst individuals and groups (Acquisti, 2007; 2010; Asgharpour et al., 2007; Blythe and Camp, 2012; Wash and Rader, 2011). What is largely missing from this literature is a critical perspective on how experiences of surveillance and digital danger, threat, and harm become thinkable as 'risk' in the first place. Instead, risk is cast as a self-evident 'natural' phenomena dealt with in either 'rational' or 'irrational' ways. The result is an emphasis on why people fail to perceive risk – or how to better quantify it.

Drawing on the work of cultural anthropologist Mary Douglas (1992), I argue that this ignores the institutions that are responsible for danger and its harms in the first place, instead placing the onus on the individual's behaviours as a moral failing (c.f. Barnard-Wills, 2012; Kazansky, 2015; 2016). In order to break beyond this limited understanding of risk, it is

useful to follow the line of scholars studying risks and threats not as givens but as the constructive result of a process of grappling with uncertainty (c.f. Amoore, 2013; Amoore and de Goede, 2008; de Goede, 2004; 2008). Scholars critically studying the logics and rationalities of risk have long observed how the concept of risk shapes the way we think about the world. As these critical scholars observe, risk is danger or uncertainty made manageable or exploitable. Examining how uncertain, dangerous, and harmful situations are cast by risk-centric framings as manageable risks and exploitable opportunities, Douglas points to its 'universalizing terminology, its abstractness its power of condensation, its scientificity, its connection with objective analysis' (15). Where sociologist of risk Ulrich Beck's concerns lie with the proliferation of globalized risks (1992), Douglas explores how the ubiquitous 'language of risk' serves to spread and shape our thinking about danger through its narrow lens (14), urging scholars to attend to the culturally specific ways that risk is framed by powerful institutions. In more contemporary literature, scholars have taken this call forward through work examining the construction of risk and management of threats within algorithmic surveillance processes; literatures on the audit society (Gandy, 2009; Power, 2007) in the critique of the war on terror (Aradau and van Munster 2008; de Goede, Simon, and Hoijtink 2014; Suchman, 2019); predictive policing (Andrejevic,2017; Massumi, 2015) and risk scoring (Dencik et al., 2019).

These scholars look at how security 'threats are rendered perceptible through algorithmic calculative devices, logics and techniques' (Dencik et al., 2018:1435) and how risk analysis serves as a 'sense-making security practice '(Stachowitsch and Sachseder, 2019: 108). The critical study of risk management, however, remains under-developed in relation to contemporary cybersecurity in state and corporate realms, with the exception of work by scholars such as Slayton (2015; 2020) and Ermoshina and Musiani (2017; 2018) in relation to practices particular to civil society. Slayton's historical work on state and corporate

cybersecurity is particularly relevant for clues on how to study this area of practice as it pertains to my study of risk management within a civil society digital security training. In exploring the history of state and corporate cybersecurity, Slayton shows that despite its scientized aura of objectivity, risk management is processual and highly contingent on the messiness of qualitative human judgement (2015). Through an intensified focus on structured, automated, and quantitative metrics, she argues that risk management provides a false sense of control which obscures 'the most valuable part of risk assessment….namely, the learning that came from the process of measuring risk rather than the final measurement' (33). This process of arriving at risk (and the intersubjective learning therein) is what my chapter is primarily concerned with. However, rather than conceiving of risk measurement as either strictly qualitative or quantitative, it explores the messy, oft un-quantifiable processes of valuation which nonetheless draw on the language of probabilistic risk to tame uncertainty. While the above work has focused on state and corporate regimes of threat construction and risk management, this chapter brings these questions to the context of civil society work, looking at how risk emerges as the product of a sociomaterial process of sensemaking concerned with the anticipation of harm.

Qualculative Convergence

This chapter traces how the uncertainties of surveillance are made into a manageable problem through the collective production of a risk heuristic within a digital security training. In this section of the chapter, I explain my inspiration for developing the concept of qualculative convergence as a way to describe this process. As I argue in Chapters 4 and 5, security and risk practices and their logics have a way of 'traveling' across social realms (c.f. Amoore, 2013; O'Grady, 2016), making their way into the

practices of actors upholding values beyond the state and corporation. Risk assessment is one such mobile practice, which I focus on exploring here. While in Chapter 4, I investigated risk assessment through thin description of its mobility across different civil society contexts, in this chapter, I look at how particular assumptions of risk assessment are both appropriated and flipped on its head in the context of a civil society digital security training. I myself make a critical intervention into risk management tropes through the development of a particular concept to describe the process of how risk is tamed in a digital security training – which I call qualculative convergence. In developing the concept of qualculative convergence, I found particular inspiration from a security-focused technologist who I interviewed during my fieldwork. This technologist was charged with building an institutional risk management approach for a large human rights and development organization in the world in order to better contend with the prevalence of 'digital threats' against civil society organizations around the world (Maschmeyer et al., 2020; the Citizen Lab, 2014). Discussing the search for an appropriate institutional risk management approach, the technologist expressed frustration with existing methodologies for addressing digital security risk, explaining that the technical approaches from computer science which he had explored failed to account for the 'human' and institutional dimensions of security. Furthermore, risk focused on the individual rather than group-level concerns.

In our interview, the security specialist told me that in his research, the most useful approach he had come across for understanding risk beyond the 'individual level' came from the corporate-centric realm of enterprise risk management. Enterprise risk management is a field of practice concerned with unifying risk centric thought and action within institutional and organizational contexts (Power, 2007; 2009). Enterprise risk management literature casts the unification of risk management approaches as a central goal of contemporary corporate management cultures. A unified approach to risks (and hence its correlate of

opportunities) is seen to bring greater efficiency to organizational processes, and hence, better corporate profit bottom lines. It was in exploring literature on enterprise risk management that I came across the concept of 'risk convergence'. Risk convergence is a concept describing a multi-pronged managerially-driven effort to unify approaches to risk management across an organization. The process involves identifying and bringing together disparate risk frameworks under one unified approach (Enterprise Risk Management Initiative, 2008). Risk convergence would seem to exist in a separate realm from the civil society practices I study, but in fact, my interviews with digital security specialists at large NGOs indicate that enterprise risk management is an appealing framework for organizing thinking about dangers and hazards, because it offers a way to unify disparate concerns around security and safety – whether financial, physical, or digital. The appeal of being able to integrate or converge these various concerns speaks to the fact that nonprofit organizations are also guided and constrained by financial bottom lines. While the details of these financial aspects remain out of scope of this chapter, the important point here is that viewing danger and security through the lens of efficiency and asset management makes sense beyond the corporate realm, something I also document in Chapter 4.

For the purposes of conceptualising risk within a digital security training and developing my concept of qualculative convergence, I find risk convergence a useful term for both what it does and does not do. What the concept does is to give a name to the difficult process of arriving at a uniform lens on risk. What it does not do is challenge the corporate rationalities of risk. This chapter sees the notion of risk convergence as an instrument for dealing with uncertainty which is bound primarily to profit, and through which security threats are primarily equivocated with threats to the function of business. Exemplifying an entrenched model of corporate risk management, it is troubling for the way it conceives of and constructs risk, focusing as it does on how unwanted intruders (from both without and within) affect financial bottom lines (c.f. Power, 2007; 2009).

In doing so, this conception of risk management does not seem to match the expressed values and politics of the human rights defenders and the civil society digital security practices which are the focus of this study.

This chapter does not posit that it is possible to reform corporate approaches to risk management. As Douglas would argue, the problem of 'risk' begins elsewhere. In other words, the way risk is constructed is an artefact of an institution's values as well as its valuation practices. Rather than trying to reform corporatist approaches to risk, I make a small subversion to the concept of risk convergence in order to use it for the purposes of my analysis in this chapter. I use the concept as s a starting point from which to investigate the ambivalence of risk management as it is enacted in a rather different context than corporate security. My subversion into the concept is to flip its rationalist underpinnings. As Stachowitsch and Sachseder (2019) put it, 'risk analysis – like any form of knowledge production – is not a neutral and objective assessment of a reality outside of itself, but co-constitutive of its own subject' (108). Rather than assume the pre-existence of risk as an objective phenomena which only requires capture and convergence into a single framework, I show that it is not risk that is converged, but the imaginaries, anxieties, and experiences of danger shared by people brought together into discussion about danger. This convergence of human experience occurs through a process that entails valuating the messes of data, uncertainties of surveillance, and hazards of life within a shared space. In the context of risk assessment, convergence culminates in the flattening of human experience with uncertainty into a single, structured risk heuristic.

Instead of holding to the term 'risk convergence' to describe the flattening of unwieldy uncertainty into a unified understanding of risk, I describe the process as one of 'qualculative convergence'. Though a mouthful, the term provides an alternate way to think about how uncertainty is becomes understood through the calculative language of risk. In developing this concept, I draw on the concept of qualculation, as developed by Callon

and Law (2005) and Cochoy (2008). These three sociologists of knowledge characterize calculation as sociomaterial process of valuation bounded by time and space. Callon and Law work from the assumption that calculation, rather than a strictly mathematical or 'quantitative' process, is entangled with or even indistinct from different forms of qualitative judgement and valuation. Nor, they argue, do calculative processes necessarily lead to any sort of numerical output. In summary, their important move is to advance interdisciplinary understandings of of calculative rationalities by collapsing the 'distinction between the quantitative and the qualitative' (Callon and Law, 2005: 719). They emphasize that calculation 'often has nothing to do with quantification'(730), and instead argue that it is better understood as 'a process in which entities are detached from other contexts, reworked, displayed, related, manipulated, transformed, and summed in a single space' (730). What ends as a neat output in the form of a number – or not – begins as people, ideas, and assorted material elements, which through a process of valuation is flattened onto a single plane. From this: 'a result is extracted. A new entity is produced. A ranking, a sum, a decision. A judgment. A calculation' (719). In the following sections, I draw further on Callon, Law, and Cochoy's understanding of *calculation as human mess* in order to generate a critical distance from rationalist discourses of risk.

Methods

This chapter draws on data collected through ethnographic fieldwork and interviews from 2016-2019 of digital security trainings and awareness-raising events. I conducted participant observation a total of 12 workshops and trainings taking place in Europe and Southeast Asia. Specific locations and names of participants and their organizations are

anonymized in line with a research ethics protocol developed by myself together with input from the research participants. This protocol emphasized the anonymization of interviewees, the de-identification of particular events, people, and places, and a set of stringent, context-specific data security measures including encrypted data storage and communications. Some events attended were open to anyone interested in attending from within the larger civil society conferences where they took place, while two were by invitation only due to safety concerns. In addition to shorter 'open' workshops, I attended two multi-day, closed digital security trainings in 2017, each spanning five days in length. The focus of description in this chapter is on my observation of one of these events, which was geared towards addressing the particular experiences of human rights defenders and activists believed to be actively 'under threat' from state or commercial actors conducting surveillance or any number of other sources of potential harm. The training, for reasons of safety, took place away from the public, with special attention put into creating a temporary space removed from fear and trauma that accompany targeting and surveillance. Intended for people working at the 'front lines' of social movements engaged in rights-based work, attendees were brought temporarily out of urgent work environments, where they were held in suspense for a temporary period of recovery and strategy building.

The training I observed was a 'general' introductory security training for rights defenders considered 'at risk' of targeted attacks for their work. Though the training took place in Europe, it brought together participants from all over the world, many of whom had left urgent circumstances in their work to counter issues such as violence against women, indigenous land grabbing, and environmental destruction. It covered topics of information management, censorship circumvention, secure data storage, secure communication, and data politics. In addition to participant observation, I conducted semi-structured interviews with several participants as well as the trainer as time would become available during the event. In interviews, I asked the trainer featured in this chapter – as

well as in the other events I attended – how they identified threats and how they talked about risks and threats with participants. I asked participants to reflect on their motivation to attend the training and how they did (or did not) find it useful to their work. A note on issues of research access relating to my participation observation: my participation at the closed trainings I attended for my research followed only after an assessment, together with organizers and participants, to ensure that the presence of a researcher would not be disruptive or compromise the safety of anyone involved. Further, I provided back an analysis of my observations to the organizers directly following my attendance in order to gain a sense of research topics which might be a 'no-go' for safety reasons. Just as importantly, this provided the research an action-oriented outcome by immediately providing back information that might be directly useful to the group.

Steps towards qualculative convergence

This section of the chapter breaks down qualculative convergence into several processual stages taking place over the course of a digital security training. I note that I have identified these stages through inductive analysis of interviews and participant observation in 12 total workshops and trainings related to digital security. I then brought my analysis back to the particular site of the digital security training featured in this chapter. In conceptualising these stages of qualculative convergence, I found inspiration from the three-stage process of calculation put forth by Callon and Law (2005). In the **first stage** of qualitative convergence, which I call 'creating the space', the digital security trainer and human rights defenders work to establish agreements and expectations for what will happen in the training space. They also begin to discuss how they define important definitions related to security, risk, and technological threats. In the

second stage of qualculative convergence, which I call 'enumerating uncertainties', human rights defenders share – or enumerate-- stories about their experiences with surveillance. The trainer works to find threads in these stories, weaving them together to find common concerns. Finally, in the **third stage** of qualculative convergence, – which I call 'commensurating problems and solutions' – the digital security trainer brings these stories and concerns together – or, commensurates them – through a risk analysis which focuses on the situations surfaced by the human rights.

The 'product' (per the language used by Callon and Law, 2005) of this process is an intersubjective notion of risk taking the form of a risk heuristic. This risk heuristic therefore establishes a 'shared language' (Interview #12) around risk. The risk heuristic may take shape in the form of something as simple as a list on a piece of paper, a quantified, computable risk calculation, or in the grid of a visual 'risk matrix' (Jordan et al., 2016) – as I will describe in this chapter. This risk heuristic is then used help human rights defenders choose tools tactics and strategies, or so-called 'solutions'. The aim is to come out of such a training with a repertoire of strategies and tactics to mitigate the harms of surveillance, so that 'at the end of it [the training] the individual can act' (Interview #12). Thus, in the third stage, the trainer and group together apply the agreed-upon risk heuristic to choose appropriate security mitigations and make plans for how to implement and integrate them in their daily lives beyond the training space. Beyond the training space, these 'solutions' must still be transitioned back out of the artificial boundary of the training space and into the daily practices of human rights defenders and NGOs. Perhaps the most crucial stage for civil society actors, this is also where the chapter ends – and where my previous work begins. The many challenges and contestations of integrating security practices remain out of the scope of this chapter, however I have explored this issue extensively in my previous research (Kazansky, 2016). In the next sections of this chapter, I go through each stage of qualculative convergence.

I: Creating the space

It is the first morning of the digital security training. A group of human rights defenders, all coming from different countries and regions of the world, is seated on the floor in a circle. Many have taken red-eye flights to arrive at a place deemed temporarily 'safe enough' to gather and openly discuss matters of security. The room is lit by a panel of fluorescent lights and lined in grey carpeting. The corporate décor of the room gives it a generic placelessness. This, the participants are told by the trainer, is a space that offers a chance to recover, reflect, and strategize. Its remoteness from the every day is intentional –as are the multiple exit doors in case of emergency. The training is a place where for the next five days, the participants will discuss and test practices for how to conduct human rights work amidst continued dangers and threats and how to act when everything is uncertain. To conduct such a training requires the creation of a particular kind of space, one that is physically, psychosocially, and 'digitally' secure, a number of interviewed trainers underline. One explains that as part of his job to create security strategies, 'the first thing I have to do is to create a space for participants to be able to actually perceive or come up with their understanding of the situation at hand...'away from the trauma that they're in, or on the other hand, the flat affect that comes from trauma' (Interview #7). Only in a space free from immediate dangers and concerns, can analysis of risks take place. As the trainer leading this training in particular explains, this 'safe space' 'sets the stage' for risk assessment (Interview #9). Further:

> It's about creating and maintaining that kind of space where participants talk about 'this is my situation and these are the things that are threatening my sustainability, and no one is going to judge me; say that it was my fault that I left my door unlocked, or my phone unlocked', that's my space (Interview #9).

To construct such a space, the trainer prepares for the training by investigating the grounds for signs of physical surveillance and compromised telecommunications infrastructure. Through investigation, the trainer learns that the Internet service provider bringing wifi into the space is known to hand data over to the local national security agency for monitoring. To counter this threat, the facilitator decides to supplant the provided telecommunications infrastructure with his own, providing Internet access through his personal mobile hotspot. All of these safety preparations are done before the participants have arrived to the space. With the arrival of the participants, the 'facilitator' positions himself at the edge of the circle, marking the beginning of the digital security training, which will last five days. Expectations are established to further delimit the space as a safe space. The facilitator lays out some ground rules: no photos are to be taken of anything in the room. Harassment in all forms is prohibited. It is jarring – perhaps inappropriate – to imagine that walking through the door of a room in some remote place could suddenly wipe clean the burdens of life under threat. Yet, the trainer's practice of space-making holds resonance with notions of spaces as a conduit for free-thinking, safety, autonomy, and prefigurative politics (Boggs, 1977; Epstein, 1991; Polletta, 1999). For the interviewed trainer, the space to be created should particularly embody the values and priorities particular to civil society and 'defending our space for work' from those opposed to human rights, as described in the digital security training methodology manual titled 'Holistic Security: A Strategy Guide' (Tactical Technology Collective, 2016: 20). Not only do the authors of the manual speak of defending civil society's 'space', but they also seek to expand it by pushing for the extension of human rights in hostile spaces. Creating this space within a training symbolizes the first step for defending and expanding civil society space out in the world.

Further activities are chosen to help 'create the space'. Shared definitions around technological and security concepts must be stablished. 'What does security actually mean to you?' the facilitator asks the group,

pointing a marker at a flip chart. One person calls out ‘the military’; another, ‘violence’; a third, ‘protection’. The facilitator puts these on the flip chart in bold black letters. ‘What else can security mean?’, he provokes, noting the militaristic overtone of the definitions offered by the participants. Someone volunteers that security is also ‘family’; another, ‘love’. Skimming his hand across the growing word cloud, the facilitator motions at the proliferating definitions to argue that security can mean many different things. In a world of violent state centric security measures and proliferating security justifications, talking about security in this safe enough space means reframing what is meant by security, away from securitized discourse towards something closer to the values embodied by the human rights defenders in the room. The facilitator goes on to offer a symbolic intervention into the word ‘security’, suggesting that the word could be replaced with the phrase: ‘wellbeing in action’.

This activity above is the first of many designed to converge the group of human rights defenders around a shared language to discuss danger and uncertainty; as he solicits stories of activism and danger from the group; as he introduces the idea of ‘risk assessment’; as he introduces tools and techniques to deal with surveillance, intrusion, physical danger, and trauma, and finally, as he has the participants create ‘security plans’ to take back and advocate for at their respective organizations. The goal is to come to a common understanding of effective surveillance countermeasures by together defining problems, setting priorities, and building trust. This common language will allow their experiences to become fodder for a decision-making heuristic.

II. Enumerating threat uncertainties and potential solutions

Having ‘created a space’, established expectations, and introduced a language through which to discuss security matters, the work of maintaining this space continues as a training progresses. ‘Creating the space isn’t something that I do once and then it’s always there and then we do something else’, one interviewed trainer reminds (Interview #9). Instead, he argues, it is necessary to ‘maintain a realm in which it is possible to understand your surroundings and then do something about it’. To maintain such a realm, the facilitator aims to ‘interrogate the surroundings together’ through an exploratory process designed to draw out stories about concerning security incidents. Participants are asked to make a diary chronicling the technologies they use throughout a typical day. Each person writes down what they do in the morning, afternoon and evening, punctuating the day’s events with descriptions of the use of platforms and devices (Facebook, Instagram, phones and laptops) as well as how they feel at different moments – whether fear, anxiety, happiness or excitement. Now the trainer asks participants to go down this list one more time and take stock of where their technological use creates vulnerabilities or exposes them to danger.

Following this activity, the facilitator asks if people would like to share anything from their diaries. This question is used as a springboard to talk about the different (and similar) threats faced across this international group of people. The goal is to surface stories, perceptions, shared definitions pinpoint common threads, and fuse this together within a comprehensive picture of threats at hand and potential threats in the future. Hong calls this a process of engaging in ‘cobbling what we know and suspect into a picture of a sensible, working world’ (2015: 73). The participants share their direct experiences with different forms of intrusive monitoring, data breaches, data theft, data loss, and harassment. They

speculate about potential adversaries, including the local police; jealous colleagues; controlling partners; and security agencies. From the trainer, participants seek clarification about suspicious phenomena and 'mystery problems' that might indicate potential security compromise, including suddenly slow computers and bizarrely blinking screens. This enumeration of uncertainties is the first step towards corroborating or dispelling concern about anomalous phenomena. The facilitator, in turn, seeks to find a middle ground between conjecture and 'known' threats, discussing the potential capabilities of 'adversaries', pointing out where worries shared by the participants might be merited or not, and offering known information about new surveillance technologies and worrying political developments. As participants share their stories, the whiteboard becomes a repository of different incidents and indicators. As the activities above bring together personal experience and 'factual knowledge' of surveillance and insecurity into one frame of understanding, an ad-hoc taxonomy of digital concern emerges. This activity concludes the first day of the training.

III. Commensurating problems and solutions: (Enter the risk matrix)

The next morning, the group of participants comes back together to continue the training. At this point, the group is beginning to converge around a set of common concerns. The trainer hence introduces a range of potential 'solutions' to these concerns, consisting of commonly recommended digital security mitigations. Over the course of a morning and afternoon, he goes through a slide show discussing email encryption, two-factor authentication, password managers and password management techniques, as well as strategies for safety and anonymity while participating in social media platforms. The goal is to 'raise awareness' of possible mitigations, but which of these will be applied, by whom, and for

what kind of particular scenario, is left undetermined. This activity takes the totality of day two. On the morning of the third day, the trainer takes a marker to a long sheet of paper hung from one of the walls of the conference room, drawing a basic grid. It is time to map problems to appropriate solutions. This grid will become what is called a risk matrix. As Jordan et al., (2016) describe, risk matrices 'depict risks within a Cartesian coordinate system' (46)...'classifying risks along two axes, the probability of the risk's occurrence and the severity of its consequences, its potential 'impact'(41). The trainer tells the participants that 'what you need to build is three dimensions of what you can do, what you cannot do or influence, and what you can definitely not do but you can seek help for'. These categories, he explains to me in an interview later, represent 'shades of grey' intended to help people discern the degree of control possible in a given situation, which he underlines can change at any time: 'things are dynamic so they move from one dimension to another' (Interview #9). Still, the matrix' boxes help compartmentalize unwieldy concerns. 'The aim is to eventually have more and more domains under your control or to understand what needs to be done to enable that to happen' (Interview #9).

Writing about the history of the risk matrix, Jordan et al. (2016) note that 'appearing only since the 1980s, risk matrices have quickly pervaded diverse practice fields and have become the most popular technology of risk presentation in practice'(50). Risk matrices 'act as mediating, inter-discursive instruments that translate complex themes into everyday discourse' (41). As such, they are a 'technology of normality' which: 'set borders between normal and abnormal, or...between tolerable and intolerable'(pp. 41). This space of action 'between the tolerable and intolerable' is what the trainer seeks to map out on a sheet of butcher paper. The trainer makes an addition to the classic risk matrix format, however. In addition to creating a cartesian axis which plots out potential future security events by varying degrees of impact and probability, he teases out, together with the human rights defenders, what actions can and

cannot be taken in response to identified risks at an individual, organizational and community level. As part of the exercise of filling out the grid, the trainer asks the group of human rights defenders to imagine what kinds of institutional support and structural change must happen for risks currently unaddressable to become risks that can be acted upon. In adding this criteria to classic impact and severity schema of the risk matrix genre, the trainer intervenes into tropes of risk management which serve to make tackling risk entirely the responsibility of the subject *at risk*. The risks that can't be tackled by individuals, organizations, and communities are just as important to represent as the ones that can be tackled, the trainer explains in our interview later.

There is another particularity of the risk matrix constructed by this trainer: unlike many other calculative risk schemas, this risk matrix does not contain any numerical elements and offers no quantitative product or end result. Instead, the cartesian coordinate system drawn up by the trainer is smattered with ideas for security practices such as 'encrypting communications'; purchasing distributed denial of service (DDOS) defence services'; setting up a data back up system; and 'coordinating with other local organizations'. Jordan et al., (2016) confirm the appeal of flexibility between qualitative and quantitative schemas of risk calculation: 'unlike the notion of a 'calculative' risk', they write, 'mathematically correct and precise measurement is not presented as highly important' (45). The use of the risk matrix transports the mess of life into the realm of numbers, metrics, and formal comparison. But though it draws on the language of probability to outline the normal, abnormal; tolerable and intolerable, it fails to adhere to conventional ideas of calculative and statistical reasoning, demonstrating that the social process of making phenomena comparative and equivalent does not always result in a numbered product, even if the aura of numbers is utilized to make up a shared idea of risk. The risk matrix does, however, produce a 'calculation grammar' (Ballestero, 2015) – a common language of valuation, which stands at abstract remove of the 'mess' of information

and data brought into the training space. This calculation grammar is used to for further decision making within the remaining time in the training and beyond.

For the remainder of the training, the participating human rights defenders are asked to spend time installing the security mitigations that the trainer has introduced. Furthermore, they are asked by the trainer to create an individual 'security plan' which should incorporate relevant and appropriate mitigations into the rhythms particular to their life beyond the training. This integration becomes the link between the temporarily safe space of the training and the uncertain world beyond. However, it is unclear to the extent that this integration will be feasible. After a long fourth day spent learning different encryption tools, one human rights defender confides in an interview with me that though she has now taken part in several security trainings, she has not yet succeeded in integrating most of the mitigations she had been introduced to back into her work. As my prior work shows, the application and integration of security mitigations back into daily life beyond the training space is exceedingly difficult for a number of reasons, from the brittle nature of the software meant to serve as mitigations; to the time and attention necessary to keep them updated and configured 'correctly'; to the expectations and demands of colleagues back home. If there is funding for it, the trainer will continue to stay in touch with the participants – but often, there is not. For now, it is time to head back out into an uncertain world. As the participating human rights defenders do so, they leave having converged with the other participants and the trainer around a particular language through which to think through the dangers and harms which may come. Whether this language is useful is yet to be determined.

Conclusion

This chapter has explored calculative convergence as a way to understand the processual, intersubjective dimensions of risk assessment in the context of a digital security training. I drew on Callon, Law, and Cochoy's concept of qualculation to develop my own concept of qualculative convergence. I used this concept to build an understanding of how human rights defenders and digital security trainers make sense of surveillance uncertainties and 'tame' them. In describing a digital security training, I showed how the human rights defender participants engage in the valuation of their experiences with surveillance through a myriad tactics which, drawing on the language of numbers and statistics, aimed to make manageable 'risks' out of uncertain circumstances. I explored how this process was enacted across several stages of discussion and practice between a digital security trainer and human rights defender participants. I described these stages as: I. 'Creating the space; II. 'Enumerating threat uncertainties and potential solutions; and III. 'Commensurating problems and solutions'. In the first stage, a safe space was constructed by the trainer, who also established a set of common definitions among participants, useful to discuss and break down uncertainty. In the second stage, personal experiences with danger and uncertainty were surfaced, discussed, and weighed against 'known' information about threats and dangers. In the third stage, concerns were mapped to potential solutions, and henceforth commensurated within a common risk heuristic designed to facilitate decision making.

I show that the push towards a common notion of risk infuses the social process of the digital security training with the promise of order, within an arena otherwise felt to be arbitrary, violent, and messy. On the other hand, I also show that the practice of risk judgement and risk-based decision making is itself messy; spilling over narrow frames of 'rationality' and 'accuracy' and refusing to conform to a corporatist notion of risks out

there in the world. In demonstrating the messy transformation of uncertainty into risk, I contribute empirical richness to Callon, Cochoy, and Law's theoretical re-conceptualization of calculation. Furthermore, I augment their theory by bringing qualculation to the realm of security practice. In exploring how uncertainty becomes risk through qualculative means, this chapter also contributes to the advancement of a richer understanding of how people make sense of datafication through different forms of calculative (or rather, qualculative) logics. Finally, in exploring how targeted communities such as human rights defenders apply risk-centric logics to their work, the chapter brings long-standing concerns around risk and security practices within critical security studies into the study of civil society approaches to security risk.