What harms may come?

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

Kazansky, B.

Publication date
2021

Chapter 7. Infrastructuring the future(s) of cybersecurity: Towards fully automated anticipation?[19]

19 This chapter has been submitted as an article for peer review in July, 2021

Abstract

At a time in which the practices and institutions of 'cybersecurity' are increasingly bounded and consolidated through global governance mechanisms, weaponized in the '5fth dimension of warfare', and enacted through automated, data-driven systems, this chapter aims to contribute to the questioning of the hegemonic logics embedded into contemporary configurations of cybersecurity. Through multi-sited ethnographic study based on four years of fieldwork, this chapter provides a multi-perspectival account of *security infrastructuring* amongst community organizers, technical security providers and non-profit organizations responding to the threat of digital intrusions, surveillance, and online harassment. The chapter looks at how coordination amongst heterogeneous communities of security practice leads to the refraction of anticipatory, data-driven logics of contemporary security across data infrastructures. The chapter introduces the concept of an 'anticipatory security infrastructure' – an information infrastructure which facilitates the collection, processing and analysis of data in order to anticipate harmful future security events.

Keywords: cybersecurity, digital security, data governance, automation, AI, activism, civil society, feminism

Introduction

One day in 2014, the staff of a women's and LGBTQIA+ rights[20] group based in a country formerly part of the Soviet Union were tipped off to an alarming video spreading through online social networks by a pseudonymous youtube account. The video contained a montage of sensitive photographs exfiltrated from the private Facebook accounts of the organization staff. As the photos faded in and out of the montage, the distorted voice of the video's narrator accused the organization of undermining the traditional family values of the country, part of a broader disinformation campaign that took them by surprise. Following an unsuccessful request for assistance from local authorities, the group called together several local organizations working on women's and LGBTQIA+ rights to discuss the attacks. They learned that they were all experiencing similar forms of targeting. However, they were unsure of who the perpetrators were, nor could they anticipate their next moves. In response to the attacks, they began to collectively document concerning digital security 'incidents' through an improvised infrastructure. The goal was to identify patterns in perpetrator actions, predict their future plans, and plan mitigations in response. With few resources and an urgent need to act, the group used the Facebook platform, which it already relied upon for its organizing and community building activities, to collectively track and analyse concerning security incidents through 'secret message groups'. Together they tracked suspected telecommunications surveillance, threats of violence and instances of online harassment. As the months wore on, the organizations became increasingly invested in tracking and documenting these incidents, eventually doing so in 24-hour shifts. The anticipatory labor of vigilance and incident tracking solidified within what I term an 'anticipatory security infrastructure' – an information

20 LGBTQIA+ stands for Lesbian, Gay, Bi, Trans, Queer, Intersex, and Asexual. It is used as an umbrella term used to describe a number of interrelated communities and identities related to sexuality and gender.

infrastructure which facilitates the collection, processing and analysis of data in order to anticipate harmful future security events.

Recently, scholars have explored 'anticipatory infrastructures' in the context of journalism; bitcoin; and energy grids, respectively (Ananny and Finn, 2020; Enslev et al., 2018; Ulfstjerne, 2020). This chapter brings the study of anticipatory infrastructures to the contested realms of civil society digital security and state and corporate cybersecurity, drawing conceptually on critical histories of cybersecurity, 'relational' studies of infrastructure, and studies interrogating the future-driven logics and practices of state and corporate security. The chapter introduces the concept of 'anticipatory security infrastructures' as information infrastructures which result from contestations and collaborations between diverging communities of security practice. While the infrastructure developed by the women's and LGBTQIA+ rights groups introduced above was confined to a small group of people, arose in a moment of crisis, and creatively re-appropriated the existing affordances of Facebook's commercial platform, this chapter explores attempts by digital security specialists working with civil society groups to standardise, centralise, and automate such anticipatory security infrastructures in order to facilitate efficient and 'rapid' response to 'digital threats' at global, trans-regional and local levels. Through a multi-sited ethnographic study of infrastructure (c.f. Star, 1999) based on four years of fieldwork and interviews, the chapter provides a multi-perspectival account of *security infrastructuring* amongst activists, community organizers, technical security providers and nongovernmental organizations (NGOs) responding to 'digital threats', looking at how interaction amongst heterogeneous communities of security practice leads to the refraction of anticipatory, data-driven logics of contemporary security across data infrastructures.

In providing such an account of security infrastructuring, the chapter aims to contribute to academic and practitioner efforts questioning the

hegemonic logics embedded into contemporary configurations of security. At a time in which the practices and institutions of 'cybersecurity' are increasingly bounded and consolidated through global governance mechanisms (Morgus et al., 2015; Slayton, 2020), weaponized in the '5fth dimension of warfare' (Cavelty, 2013; Dyer-Witheford and Matviyenko, 2019), and enacted through automated, data-driven systems (Amoore, 2020; Dwyer, 2019; Bellanova and de Goede, 2020) it bears reminding that security is a fundamentally open-ended and irreducible concept, practice, and goal articulated through vastly different epistemologies and moires (Fichtner; 2018; Hansen and Nissenbaum, 2009; Nissenbaum, 2005). While the international relations of cybersecurity play out in high-level policy fora, security practices, standards, and infrastructures are articulated through daily practice (Ermoshna and Musiani, 2018; Kazansky and Milan, 2021; Monsees, 2020) as well as attending cycles of infrastructure maintenance and innovation (Bellanova and de Goede, 2020; Slayton and Clarke, 2020). Scholars, activists, and community organisers have worked to 'reconfigure security' (Reconfigure Network, 2021) to take account of its hegemonic logics, pushing for practitioners and policy makers to bring cybersecurity in line with human rights frameworks, anti-racist commitments, and gendered considerations (Brown D and Pytlak, A (2020); Coding Rights, year; Hackblossom, n.d.; Kazansky, 2015; Millar, et al., 2021; Petty et al., 2018; Slupska, 2019; Tactical Tech, 2016; Tanczer et al., 2018). Towards the de-centring of state and corporate cybersecurity narratives, the chapter calls attention to the way that security standards and infrastructures arise not just from hegemonic state and corporate security actors, but through friction-full 'governance from below' (c.f. Lea and Stenson, 2007) lead by civil society actors.

The plan of the chapter is such: in the next section, I contextualize concerns with anticipation and security infrastructures in the literature. Following this, I explain my research methods. I then introduce efforts by civil society digital security practitioners to more rapidly respond to

digital threats. The chapter then introduces and investigates the practices of three groups and individuals engaged at the cross-sections of divergent security infrastructuring approaches, looking at the 'frictions' of security standards-setting and anticipation across an 'institutional ecology' of digital security rapid response. The chapter concludes with questions for further research.

Situating Anticipatory Security Infrastructures

This chapter studies processes which 'infrastructurally encode anticipation' (paraphrasing Ananny and Finn, 2020: 1604) at the intersection of security specialist repertoires and NGOs and grassroots groups experiencing 'digital threats'. Towards the investigation of security infrastructuring, the chapter builds on two areas of study: first, it draws on information studies literature exploring digital and data infrastructures as processual, diffuse, and heterogeneous entities built and maintained through the interaction of communities; and second, it looks to critical and historical studies of security to help contextualize the digital security practices of civil society. This section draws on the above to contextualise three main areas of concern for this chapter: anticipation, infrastructure, and digital security.

'Anticipation' refers to future-oriented modes of action which intervene against potential undesirable security outcomes (c.f. Adams et al., 2009; Anderson 2007; 2010; Kazansky 2021; Pink et al., 2018). As framed in this chapter, anticipatory security action emerges from a heterogeneous milieu of practices, drawing from data intensive and algorithmic prediction regimes as well as intuitive pattern-finding and sense-making practices. This framing builds on my findings in Chapter 4, where I explored anticipation as it is enacted through the practices of security

specialists working beyond corporate and state structures. In this chapter, I showed that 'anticipatory data practices' draw from a number of different culturally specific histories of risk, modelling, preemption, and prevention of undesirable futures. I also argued that anticipation can be understood as a thread which ties the interactional dynamic so-called 'dance of surveillance' (Marx, 2009) together. Per Clarke (2015), anticipatory modes are a kind of interstitial 'articulation work' which help give shape to sociotechnical assemblages. In this chapter, I build on Clarke's notion of anticipation as infrastructure articulation work to show how anticipatory modes serve as a driving force of the maintenance and development cycles that shape security infrastructures. These themselves arise from ongoing interaction of surveilling and intruding actors and those who build infrastructures to withstand against, recover from, or 'neutralize' (c.f. Marx, 2009; Wood and Thomson, 2018) their actions through security measures.

'Digital security', as scoped by interviewees, is a broad term used to refer to civil society repertories for safety from different forms of data exploitation, harassment and targeting, and security intrusions by states, corporations, and affiliated actors. The chapter contextualises digital security practices and infrastructures in relation to commercial and state cybersecurity, showing the porousness of these overlapping communities of practice and how civil society's digital security practices are shaped by values articulated through agonistic interactions between groups of varied institutionalization, geographic location, issue scope. As I argue across the chapters of this thesis, civil society challenges and reconfigures hegemonic notions of security while also appropriating the logics and practices of hegemonic actors (see in particular Chapter 4 and 5). The chapter studies this appropriation and reconfiguration through the lens of a porous 'institutional ecology' (Star and Grisemer, 1989) attuned to the agonistic relations of civil society organizations, security specialists, grassroots movements, and technologies brought to bear against digital threats (c.f. Mouffe, 2013; Horgan and Dourish, 2018). Looking at the

infrastructural politics of data collection, analysis, standardization, and automation, I draw upon work that studies information infrastructures as contingent and processual, bound up in continuous construction and entropy (Star, 1999; Bowker and Star, 1999).

As Bellanova and de Goede (2020) point out, 'data infrastructures are not neutral, as they materially, legally and politically support specific ways of doing security'(13). Clark-Ginsberg and Slayton (2017) point to the processural way that these 'ways of doing security' emerge, highlighting that contemporary cybersecurity infrastructures are 'the embodiment of a cacophony of overlapping and congruent standards' (2) which result from decades-long struggles at local, regional, and global levels. In this chapter, I will show that digital security infrastructures emerge through conflicting ways of doing security, and as such, may be more 'seamful'(Vertesi, 2014) than congruent. Specifically, the chapter identifies an important friction between what I identify as two overlapping yet divergent approaches to digital security rapid response and infrastructural security anticipation. The first – a 'global' approach encourages increased threat data standardization and automation across globalized, centralized data super-structures, while a second - 'local' approach encourages community-driven and 'autonomous' – not to be confused with automated – security through localized data infrastructures and practices which challenge state and corporate driven security definitions. Taking a processural and relational perspective on anticipatory security infrastructures (c.f. Star, 1999) this chapter looks at how the friction between these two identified approaches contributes towards the making and un-making of cyber and digital security standards and infrastructures, honing in on data standardization conflicts, infrastructural politics and anticipatory logics imbricated in the struggle to respond rapidly to 'digital threats'. In exploring the tension between two approaches to digital security and attending contestations, I draw on Star and Bowker's notion of imperialism (Star and Bowker, 2007) to characterize the power-laden conflicts that arise in the development of security metrics, standards, and

classification schemes. The chapter investigates what emerges from the push and pull of these two approaches, analyzing their significance amidst broader discussions of security, data, and automation.

Methods

The study is concerned in particular with an international 'ecology' (c.f. Star and Griesemer, 1989) of non-governmental and grassroots groups which, through collaborations and contestations, develop an ever-evolving repertoire of mitigations for digital threats. The analysis in this chapter draws from a larger multi-sited, qualitative study of civil society responses to the shifting threats of digital surveillance and datafication. In total, 50 interviews were conducted with digital security, digital rights, and Internet freedom practitioners between 2016 and 2019. Interviewees were selected at 12 international digital rights and Internet freedom meetings in Europe and Southeast Asia, where participant observation was also conducted. Interviewees came from 26 countries in different regions of the world. Their diffuse geographical representation results from the international nature of the conferences where fieldwork was conducted, which are explicitly organized to bring transnationally coordinating civil society actors from across different regions together for discussions. The transnationality at play connects directly to this chapter's interest in exploring friction-full governance from below, which emerges from overlaps and divergences on the basis of community priorities, geography, culture, and resource equity and inequity. Participant observation took place at public discussions about digital security rapid response, where digital security specialists, technical service providers, NGO workers and grassroots organisers engaged in frank discussion about emerging best practices, shortcomings of 'digital security support', and emerging priorities for the 'field'. The struggle to coordinate rapidly

against digital threats emerged as a recurring theme in inductive analysis of initial interviews and field observation, which lead to the snowball selection of further interviewees active in digital security rapid response. Interviewees included staff of established international NGOs, digital security specialists working with local grassroots groups, and cybersecurity technicians and service providers working with both civil society organizations, companies, and governments. The fieldwork and interviews as a whole allowed me to explore collaborations and contestations within an institutional ecology consisting of three kinds of digital security rapid response actors, identified in this chapter as global rapid response actors, local rapid response actors, and technical rapid response actors.

Rapid response to digital threats: from threat indicator to anticipatory infrastructure

As ‘digital threats’ have become commonplace, civil society organizations around the world have sought to develop standardized protocols and coordination mechanisms to respond rapidly in the wake of security ‘incidents’. A borrowed term from the fields of emergency medicine and humanitarianism, ‘rapid response’ is closely related to the ‘computer security emergency response’ practices of commercial and state cybersecurity (see: Morgus et al., 2015; Slayton and Clark, 2020). Within civil society’s ‘digital security ecosystem’, as it is referred to by practitioners (the Engine Room, 2018), rapid response refers to a repertoire of services providing technical support for urgent digital security issues, ranging from suspected malware attacks, website compromise, distributed denial of service attacks, data exfiltration, and data loss. The focus is on mitigating the threats faced by human rights and social justice nonprofits and grassroots social movements, a gap left

largely unaddressed by commercial and state security enterprises (Maschmeyer et al., 2020; Millar, 2021). Though 'rapid *response*' implies action taken to counter the effects of a concerning event, interviewees underline that responding rapidly requires having the correct mitigations and resources already in place beforehand.

This need for preparedness engenders a future-oriented approach to security (c.f. Amoore, 2020; Anderson 2010; Aradau and Blanke, 2017; de Goede, 2012). As an interviewed digital security specialist explained it 'being able to know what is going to happen is a way to find out where to put resources in the future' (Interview #42). Importantly, however, none of the security specialists interviewed believed it is possible to 'predict' digital threats with precision or accuracy, nor is that the goal. As another specialist explained, 'sometimes people are super worried because they don't know if the threat is going to happen and its really hard to say yeah there is 80 percent chance (Interview #41). On the other hand, a third security specialist offered: 'when you know enough about what happened in the past with threats you can probably figure out whats going to happen in the future or at least have an idea of how it will evolve' (Interview #29). In other words, preparedness becomes possible by tracking and finding patterns in data relating to past concerning events – and from this past data, extrapolating likely future threats. I argue that this 'loose' approach to prediction is best understood as a form of anticipation – a concept open ended enough to capture the messiness and heterogeneity of judgement and decision making enacted through future-oriented security, or, 'anticipatory security', defined here as a future-focused modality of security enacted through vigilance and data-driven practice.

Anticipatory security, as scoped by interviewed rapid response actors, requires continued pattern finding relating to past recorded events, scanning for emergent 'anomalies' (c.f. Aradau, 2018), and engaging in conjecture about potential future attacks. These different modes of analysis rest on the availability of threat-related information, which

includes organizational documentation of incidents pertaining to perpetrators and their 'tactics, techniques and procedures' (TTP); 'indicators of compromise' (IOCs); cybersecurity bulletins and alerts, research reports issued by anti-virus vendors and academic institutions documenting new vulnerabilities and attacks, and 'threat intelligence' collected on trends and attack patterns within specific sectors and communities at global, regional, and local levels. Interviewees highlighted that despite these many potential sources of threat information, 'actionable' and 'reliable' threat information is challenging to come by. One reason is the ephemerality of many kinds of digital attacks, which makes threat perception, identification, and data capture a difficult proposition. As one security specialist explained, 'there is no click click anymore when your phone is tapped' (Interview #12). In many cases, there may very well be residue left on devices and infrastructures that would constitute 'evidence of compromise' but recognizing and capturing it requires deep technical specialization out of reach for many NGOs and grassroots groups.

Still, the 'burden of proof' regarding threats and harms is placed upon the communities experiencing them, as per the case of the women's and LGBTQIA+ rights activists of the chapter's opening vignette. This kind of responsibilisation puts human rights defenders, community organizers, and NGOs to work vigilantly documenting suspicious anomalies (c.f. Kazansky, 2015). Interviewed security specialists thus promote the practices of documenting 'everything' in case it might reveal a concerning pattern of phenomena indicative of compromise. As a security specialist teaching documentation techniques to grassroots groups put it, 'it's very simple actually…. just document everything that happens' (Interview #37). Another such specialist underlined: 'whenever there is an incident we always write it down'(Interview #39). Though in commercial and state cybersecurity, threat monitoring efforts aim to obtain granular forensic data and are increasingly enacted through automated 'security sensing' devices such as network monitoring tools and intrusion detection services,

interviewed specialists working with NGOs and grassroots groups argue that documentation about potential threats can be a 'low tech or even no-tech measure' aimed at capturing experiential, circumstantial, and 'unstructured' data (Interview #12). For example, the specialists above prescribe the use of paper diaries to human rights defenders and activists in order record any kind of anomalous event occurring amidst daily life, ranging from the observation of a suddenly slowed computer to a suspicious parked car outside an office, urging also that activists and human rights defenders share this circumstantial data within trusted groups in order to tease out patterns indicative of compromise or danger.

The combined necessity to document, analyse, share and compare threat related information on a continued, anticipatory basis gives rise to information infrastructures to sort a mess of varied threat information ranging from data collected by 'high-tech' automated threat scanning platforms to the anomalous experiences recorded in the 'low-tech' diaries kept by grassroots groups. These analogue and automated forms of analysis are facilitated through a mix of structured analysis tools and the 'manual' effort to collect any and all possible indicators of potential danger and find patterns in them. Through an entanglement of so-called 'automated' and 'human' judgement, they enact what Dwyer (2019) calls a 'more-than-human sensing' of security threats (118). Multi-sited, and 'seamful' (Vertesi, 2014), these anticipatory security infrastructures may (or may not) stretch across geographic borders and communities of practice, centralized and decentralized databases, and varied forms of sensing devices. Though flexible and geographically fluid, they are also contingent and brittle, agglomerating and breaking through the social frictions and attending cycles of maintenance and innovation (Clark-Ginsberg and Slayton, 2017). As Bellanova and de Goede (2020) summarize, security infrastructures 'require encoding, standardizing, tinkering, and tailoring' (5). The next sections of this chapter focus on these processural politics of anticipatory *infrastructuring*, as enacted

through coordination between large NGOs, grassroots groups, and commercial actors trying to respond ‘rapidly’ to threats.

The geographies and institutional ecologies of anticipatory security infrastructuring

This chapter differentiates between three broad categories of actors whose agonistic politics help make and unmake anticipatory security infrastructures. First, the chapter places into one category ‘global’ rapid response actors: large NGOs with a global or trans-regional scope of work on digital rights, Internet freedom, and digital security. Predominantly based in Northwestern Europe and North America, they have historically dominated agenda-setting in the field and have presided over the majority of funds and technical resources (Brooks, 2019; Kazansky, 2021). The ‘global’ approach to rapid response has relied upon centralized forms of governance. For example, several global organizations run global emergency hot lines and ‘help desks’ to which constituents can call or send messages from any timezone and ideally be able to a representative at short notice. As explained in my interviews and hashed out at observed rapid response meetings, sometimes a global organization addresses incoming ‘support’ cases itself. However, if staff lack resources or time, the organization instead matches the constituent in search of support to the organization’s network of specialists distributed across the world. Global rapid response actors promote mechanisms for large scale threat information sharing across communities and regions, arguing that such scaled-up information sharing processes can enable civil society to collectively identify and track common threat patterns and respond with increased coordination and efficiency. As I show, the imagined ideal for such threat-information sharing processes is a birds eye view of digital threats facing civil society around the world – seen as a powerful tool to

‘proactively’ anticipate and prepare for future threats. As I further show, the desire to work at such a scale creates an imperative to automate security work – an imperative Slayton documents in the history of state and commercial security as well (2015).

A second category of actors is distinguished by their particular issue focus and/or ‘localized’ geographic scope, working in local or trans-local configurations to address the security concerns of human rights defenders and other constituent communities. Interviewees from North America, Central America, the Eastern Horn of Africa, South Asia, Southeast Asia, and Post-soviet Eurasia are represented in this study. Issue-focused communities work to end violence against women, advance LGBTQIA+ rights, sex worker rights, anti-racism, land and environmental rights, and anti-corruption, among other allied issues related to social justice, Internet freedom, digital rights, and human rights. Historically these organizations and grassroots groups have had less access to digital security related financial resources or specialised assistance, relying often on services disbursed on a voluntary basis by global non-profit rapid response actors and both nonprofit and commerical technical service providers. As my interviews and fieldwork will show, amidst a push by NGOs to centralize and standardize security knowledge and expertise, a number of local rapid response actors have pushed back against the globalised approach, choosing instead to keep their threat information confidential and ‘unstructured’. One reason for this is a distrust of ‘cybersecurity’ as defined by state and corporate actors, which in many cases plays out orthogonally to the interests of social movements through surveillance and monitoring of their activities (see: Amoore, 2020). Thus, a requirement to homogenize and share data could be considered a violent act of ‘imperialism’ as Star and Bowker (2007) characterize the violent processes of standardization undergone towards the advancement of information and classification infrastructures. Though local organizations run emergency hotlines and help desks as well, they are run at a smaller scale. In fact, a number of interviewed local actors push back on the idea

that a uniform or scaleable model for rapid response is possible, calling instead for the recognition of the legitimacy of heterogeneous security approaches.

The third category of rapid response actor involved in civil society rapid response consists of commercial and state cybersecurity teams and technical service providers who civil society organizations regularly reach out to in order to gain redress with social media platform content takedowns, recovery from Distributed Denial of Service attacks, and other common cybersecurity issues. In their practical role amidst emergencies, commercial and state actors require and request data from the digital devices of NGOs and grassroots groups to conduct their investigations, pinpoint perpetrators, and gather evidence of security compromise. Having been steeped for decades in the minutiae of technical standards and terms of art, these actors exert an influence on the standards-setting and infrastructuring now taking place across the digital security rapid response ecosystem. This influence occurs both in direct interactions in the midst of 'digital emergencies' as well as in the movements of 'experts' from commercial or state cybersecurity into civil society communities of security practice. One main connector between commercial/state and global 'civil society' actors is a shared anxiety over the 'global' and 'viral' dimensions of digital threats (c.f. Parikka, 2007). In interviews, a recurring theme in discussions for why centralization and standardization of threat information are important is the observation that different communities notice similar patterns of concern, yet lack the language or infrastructure to systematically track them due to a lack of establishment of common 'threat taxonomies' and data standards. This conundrum mirrors the lack of shared language documented by Slayton and Clark (2020) with regards to the early days of computer security incident response at the state level. Slayton and Clark trace how the desire to establish such a language served as the impetus for security standardization, centralization of security infrastructures, and emergence

of global cybersecurity governance mechanisms. This shared anxiety produces both collaborations and contestations between unlikely allies.

In the next sections, I follow the work of three individuals and constituent groups involved with civil society digital security rapid response. Following the productive frictions between their approaches to security allows us to explore controversies around whether security infrastructures should be global in scope; how data about security incidents should be classified and processed; with whom should and shouldn't this vital information be shared with; and to what extent security becomes an automated, data-driven enterprise. First, I introduce a security specialist at a large NGO involved in the development of an efficient and standardized security regime; second, I introduce a group of state cybersecurity incident responders who promote threat information sharing and try to collaborate with civil society organizations; and third, I introduce a group of feminist security practitioners who argue for an autonomous – not to be confused with 'automated' – and local approach to digital security.

Civil society security practices: towards common standards and centralized infrastructures?

M has spent several years developing codified practices and infrastructures for the service of civil society's efforts to manage digital threats. He considers himself an enthusiastic proponent of increased threat information collection, standardization, and threat information sharing. Around the time of our meeting in 2018, M was tasked with creating a 'systemic' approach to security for the global development organization he was working for at the time. The main impetus for this strategy was a

need to identify and respond to security risks more 'efficiently' in order to match the fast-moving and serious nature of digital threats (Interview #12). For M, this efficiency was an impossibility due to a lack of actionable threat information. M argued that while this information does exist 'in theory', it was, at the time, hidden in too many places; scattered throughout guides, mailing lists, and internal communications in non-standardized formats. Sitting together at a small table in the courtyard of a digital rights conference venue in 2018, M took me through the 'workflow' he was developing to create a more 'agile' and 'efficient' organisational security strategy. On his laptop, he drew my attention to a database listing hundreds of sources of information on potential past or future security 'events' obtained through investigation of potential threat actors and their motivations.

M searches for credible threat intelligence sources on a regular, continued basis, due to a continuously changing 'threat environment'. One technique he uses to obtain threat intelligence is to manually search on the Internet for 'publicly available' information including websites monitoring political situations in regions and countries, antivirus company reports, and bulletins from state cybersecurity teams from across the world. In addition to these 'public' sources of threat intelligence information, he also draws upon an enormous amount of information concerning security incidents documented *within* his organization. M copy and pastes all of these threat intelligence sources into an excel spreadsheet containing thousands of URLs, explaining that having this threat information arrayed within one spreadsheet is a starting point for data structuring and standardisation: 'the document itself adds structure'. Structuring for M involves developing a common 'threat taxonomy' through which to order different kinds of threats, threat actors, threat impacts, and potential threat mitigations. This kind of taxonomy will allow him to find patterns in the data, and will more broadly facilitate the standardization of rapid digital threat response.

Through his continuous engagement with the categorization and structuring of these sources of information, M begins to see emergent patterns in the data, attempting to identify concerning patterns in information from public sources and confidential organizational files. The goal is to identify 'flags' of concern and to extrapolate a set of 'indicators' which will serve as a triggers for action in the event of probable threats: 'we are trying to determine likelihood. If its likely its going to happen, we will have to mitigate it...what are the swaths of indicators that allow me to make a decision?' By combining this global threat intelligence with the information 'local' to his organization, M tries to obtain a comprehensive view of emerging threat patterns that can enable him to anticipate probable threats. Yet, for a truly comprehensive view, M explains that he needs to find a way to confirm this pattern is more than just his conjecture alone. In his work to standardize security practice, M wants to correlate the data points he collects with that of other organizations across civil society. In cybersecurity terms of art, M wants to engage in 'threat information sharing' with other communities conducting similar threat intelligence efforts, pointing to the threat intelligence platforms and communities established by states and corporations as inspiration. Furthermore, M wants to automate and synchronize all the different parts: 'everything needs to be a dial that you can tweak and where it cascades, so that if an indicator changes you know what else to change across the board.'

Yet to engage in this kind of information sharing in a civil society context – and beyond his own organization – requires three conditions: first, a desire by other organizations and groups to share their own information; second, a common platform on which to do so; and third, a standardized form through which to record and share it on this platform. The following section introduces an effort by one group of state cybersecurity actors to develop a threat intelligence platform which they hope can facilitate the kind of broad information sharing practices M aspires towards within civil society. As I will show, the shared interests, infrastructural meeting

points, and divergent epistemes which collide through this effort help shape the course of security standardization and rapid response coordination.

Commercial and state cybersecurity threat intelligence: overlaps and divergences

In 2012, a state-organized team of security incident responders convened a meeting to discuss the state of cybersecurity coordination and threat intelligence at a global scale. As explained by one interviewed member, 'we had a meeting with other threat intelligence teams to discuss weird stuff we were seeing' (Interview #29). One of the main outcomes of the meeting was that 'we noticed how often threats seemingly particular to one sector are in fact common across others'. However, though 'every team was working on something really similar...we didn't really want to share our data', with the result that the teams were altogether 'just sitting on piles of data'. To make this data actionable, 'the community really wanted to automate the process as much as possible'. The desire to foster information sharing and automate data sharing across teams 'was a tipping point' for the team's security work, following decades of development of common security standards, threat information taxonomies, platforms through which to comprehensively track threats, and techniques to automate all of these processes. As Slayton (2015) documents through historical analysis, by the mid-1980s, automation was viewed as a key priority in computer security. With work on automation also came the prospect of finally operationalizing 'real-time' automated threat monitoring and prediction, a goal first articulated in information security in 1967, at which time the RAND institute had laid out this aim at a prominent conference (24). Nearly 40 years later, techniques of automation had advanced through the availability of big data and new

forms of predictive analytics, yet reliable and comprehensive threat information has remained a persistent challenge.

In an effort to understand how to encourage more threat information sharing, the state cybersecurity team 'started to build a small interface to have a way to store indicators of compromise, and give access to people to it to synchronize it' (Interview #29). Each 'user' would create their own 'instance' – or personal area – on the threat intelligence platform. There, they could maintain a collection (called a 'galaxy') of threat information which could be shared controlling how 'far' the information spread share made public, shared with particular communities, or kept confidential. The hope was that the granular information controls provided to imagined threat information sharers would engender trust and confidence in sharing 'sensitive' data, and thus encourage as many different sectors and communities participate as possible – all towards a desired global view of trends in vulnerabilities and attacks. By 2017, the team's small threat intelligence interface had grown into a large online platform designed to allow any motivated security professional or targeted actor to submit threat information in a standardized format and find correlations in the data. The kind of information stored included lists of common domain names associated with malware and forensic digital evidence related to attacks, including files containing executable malware and records of abusive messages sent via email and other communications. Part of the developer team's strategy was to include civil society threat information within their platform. They underlined that at least some of the more 'common kinds of threats pertaining to malware were similar:

> All the NGOs and civil society orgs really receive the same kind of ransomeware that everyone receives...the finance departments at NGOs get the same kind of stuff all kinds of finance departments do. (Interview #29)

If the digital threats faced civil society were similar to those facing banks or commercial institutions, it followed that giving access to civil society

could allow the team – and any user of the platform – to identify common attack patterns, contributing to the broader aim of continuous threat monitoring at a global level. Yet, the inclusion of civil society into the platform was far from seamless. In our interview in 2017, one developer of the platform shared his frustration that despite the invitation they made to different civil society organizations to participate in the platform, very few had actually recorded or shared information. Why? Through discussions with civil society digital security practitioners, he and the other developers learned that the lack of participation could be attributed to two issues: first, the continued source of friction around 'trust' again appeared to place a wedge between these overlapping yet divergent communities of security practice. In particular, the developers noted a distrust by civil society organizations towards the idea of sharing security-related information about their organizations and constituents with agnostic security actors operating at the cross-section of several communities of security practice (again, the platform was intended to cater just as much to banks, other corporations, and state institutions, and was configured by a team of security professionals aiming to equally address threats from every sector).

The second issue developers observed was a misalignment around what constitutes a security-related 'indicator' and how 'threat information' should be structured. As introduced earlier in the chapter, for digital security practitioners in civil society, a security-related 'indicator' may constitute any experiential data collected from immediate life and interactions with technologies therein; for example, the perception of 'slow' computers, signs of wiretapping such as clicks; or perceptions of potential physical surveillance, such as being followed by a suspicious car, were considered useful forms of data to track through diaries or secret Facebook groups (per the opening vignette of the chapter). In contrast, the developers were accustomed to working with 'highly structured' data about cybersecurity 'events' classified according to a taxonomy established by cybersecurity governance bodies. This taxonomy of threats

predominately concerned ‘indicators of compromise’(IOC), a term to describe structured data about malware, ransomeware, and DDOS attacks, while omitting the kind of experiential data mentioned above. Following this classification scheme, IOCs took the form of suspicious domain names, malware samples, and other forms of ‘forensic data’ extracted from computing processes. This misalignment around what constitutes a security-related indicator, and subsequent inability to participate according to the constraints of the platform, seemed to make data standardization an impossibility, threatening also to preclude its sharing through a centralized platform and frustrating the goal of a global, anticipatory view of cybersecurity threats.

In an effort to resolve the impasses outlined above, the state-led cybersecurity body sought to include a wider breadth of qualitative ‘unstructured’ data that does not abide by established cybersecurity threat taxonomies. This could be added to a new ‘metadata’ form adjacent to the main database where users were to record threat information. Further, the cybersecurity team shifted how it would use the infrastructure it had built in support of civil society. Rather than encouraging ‘civil society’ – in the broadest sense of the term – to use the platform, the team shifted to primarily collaborating with other technical service providers in contact more directly with NGOs and grassroots groups, who both had ready access to threat information due to their provision of services to NGOs and grassroots groups, and were already accustomed to structuring (in other words, ‘translating’) threat-related information in accordance with cybersecurity standards. Beyond the constraints of this platform, however, are more radical visions to be explored, bringing us to the next section of this chapter. While the state cybersecurity team viewed the misalignments between the different imagined users of the threat intelligence platform as an obstacle to ‘effective’, anticipatory security, they can also be understood as a productive friction; an act of principled defiance, and an impetus for the development of *other* kinds of security infrastructures and approaches to threat information, which are explored next.

Feminist counter-practices and local, autonomous security stewardship

In 2018, members from five feminist, women's and LGBTQIA+ rights groups from different countries and regions of the world converged for a trans-regional discussion of how to document and describe digitally related threats and harms in a way that would do justice to survivors of violence, both 'online' and 'offline' (field notes, 2018). In a discussion held at a large digital rights conference in 2018, they explained to the audience that 'mainstream cybersecurity' had yet to account for the concerns of their communities; particularly that contemporary cybersecurity practice predominately omits the 'gendered' concerns and embodied nature of 'digital' harm faced by women and non-binary individuals. This problem extended to the language used to describe threats not just by security specialists but by constituents trying to describe what they were experiencing. As an example, one person who participated in this discussion explained, in our interview after, that it was common for people calling the hotline she ran to try to describe what they were experiencing through the stilted language of 'hacking':

> a lot of people would call in to a helpline and say…oh I've been hacked, and we were like, you are not being hacked, this is blackmailing. Maybe it was through accessing your Facebook account that they got your images that they are using now (Interview #39).

The interviewee argued that 'hacking', along with terms like 'surveillance' and 'compromise', were much too vague and apolitical to describe phenomena such as the targeted attack which this woman had experienced. Vague, apolitical cybersecurity language had practical ramifications for information sharing and data infrastructuring: how could threat information be discussed and shared if the categories created to describe and capture threats did not recognize or describe the nature of the

threats they were contending with? Though mainstream threat taxonomies do also contain much more granular descriptors for threats and security-related indicators, the interviewee argued that it was focused predominantly on 'traditional' cybersecurity issues, while barely touching areas related to violence against women (a problem also identified in recent scholarship on tech abuse, e.g: Slupska, 2019; Tanczer, 2018). Just as omission from mainstream threat taxonomies was issue, so were the 'terms of inclusion'(Hoffman, 2020) – in, particular the requirement to conform to state-centric problem definitions. Many interviewees, for example, object to the relatively recent ubiquity of the term 'cybersecurity' due to its militaristic overtones. For this reason, throughout texts, guides, and interventions produced by feminist practitioner organisations produced over a number of years now, pleasure and embodiment are centred as elements of digital security, while fear-driven and patriarchal notions of safety and security are challenged and reframed (Coding rights, n.d.; Cyberseguras, n.d.; Kazansky, 2021; Radloff 2013; 2018; Tactical Technology collective, 2015; 2016).

Hence, the five groups pushed one another to 'dig deeper' and find language that could capture the political context of security threats; embodied experiences of danger; and motivations and end goals of attackers. One interviewed security specialist who participated in the development of the typology explained that to do so, 'we needed to come up with our own terms' (Interview #39). The group who met laid out its primary aims for the typology: first, it should give proper weight to the gendered violence perpetrated through digital platforms against women, women's rights defenders, and LGBTQIA+ communities. To do so would require accounting for the fact that attacks perpetrated 'online' – and resulting harms are rarely confined to the online realm:

> The common message is, this is violence, the same violence that we live, because people use to say 'this is not violence, I did not used to see it like violence', or ' online violence is not real'. So now, the message is, this is the same violence that we

> live in the streets, in our houses, in our beds. This is the same one (Interview #39).

Thus, discussions between organizations focused on how to bring more legitimacy to the idea that online abuse or 'violence against women online' is violence regardless of whether it manifests digitally or in 'meat space'. Rather than simply add new categories of threat to the fixed classification systems of global cybersecurity actors such as the developers of the threat intelligence platform discussed in the previous section, these groups aimed to create a community-centred and relational terminology – referred to as a 'typology of violence'. In addition to coming up with terms that better matched the nature of community-centric threats, the groups involved made a conscious effort to connect different techniques of cybersecurity threat to the intention behind them, which would more explicitly link techniques of violence (intrusion into personal devices; use of sensitive data without consent; misogynist discourse) to the broader motivations of perpetrators (disinformation campaigns; intimidation; extortion; bodily harm; gaslighting). This relational terminology, they believed, would advance their own efforts to better document and track threats particular to women's, LGBTQIA+ and feminist groups – but it was not intended for inclusion in globalized cybersecurity infrastructures. The effort by these groups to reframe and redefine security is ongoing, and in the case above, only captures one moment in time in a decades-long struggle. It is, however, paradigmatic of a number of other efforts to decentre, reframe and reconfigure security technologies and governance.

In this section, I highlight one more example illustrative of the productive frictions of a broad and diverse field of security, going to a meeting I observed on the future of rapid response, where the tensions around the global and local dimensions of security work and its appropriate governance came to a head. At the 2018 edition of the same digital rights conference where the women's, LGBTQIA+ and feminist groups met, a

small Southeast Asian organization was asked to present on its experience with responding to the digital support requests of its constituent community. The organization recounted that during its years of reliance on a global organization for security infrastructure support, it had often seen requests for assistance unmet by global rapid response actors due to their lack of capacity and expertise in regional and local issues (field notes, 2018). As a result, the Southeast Asian organization went on to build up its own autonomous approach to digital security rapid response, moving away from centralized information sharing platforms with global data flows and instead building a rapid response helpline intended only for constituents and activists in-country. Because of its demonstrated need for an autonomous and localized approach to rapid response, this organisation and others in attendance expressed a wish for more control over the stewardship of the rapid response ecosystem and how its resources were distributed.

Notably, this request was acknowledged by global rapid response actors present, who responded with a proposal for a new model of governance and coordination. In particular, one high level staffer of a large global NGO proposed moving from a centralized to a 'federated' model of rapid response. Federation would involve delegating more security support tasks to smaller, local actors. To do so, the global organization would 'package [its] learnings' gained from its years as a central rapid response institution into digestible formats and 'push down' well-defined security tasks to locally operating organizations. While the open discussion was welcomed, the proposal was received with controversy. The notion of resource-rich organizations from North America and Western Europe 'pushing down' knowledge to the so-called periphery was called out for its neocolonial overtones. Instead, attendees called for substantive resource redistribution and lateral, community-centric knowledge sharing. This example illustrates that the institutional ecology of rapid response is shifting from a centralised, global model to something other. Towards a re-configuration of the rapid response ecology, large organizations have

provided increased support to regional and local infrastructures, viewing this as a positive and necessary development amidst an ever-growing influx of requests for assistance. But who decides what this new configuration will look like, and what are its implications for civil society? This remains an open question at the time of writing.

Conclusion

Through multi-sited ethnographic study of security infrastructure (c.f. Star, 1999), this chapter has provided an account of anticipatory *security infrastructuring* by digital security and cybersecurity practitioners engaged in rapid response. The chapter has shown security infrastructuring to be a contingent and fractious process which results in the challenging of hegemonic security problem definitions, standards, and forms of coordination. The chapter identified a friction between what I identified as two overlapping yet divergent approaches to rapid response and infrastructural threat anticipation, looking at how the friction between these two approaches contributed towards the making and un-making of security standards and infrastructures. This chapter thus shows that cybersecurity governance is not just the domain of state and corporate actors, but is negotiated through continued contestation amongst communities of practice ranging from the state and corporation to civil society, which have overlapping and oft-conflicting goals. In an effort to de-centre state and corporate-centric narratives of cybersecurity, the chapter illuminated the importance of feminist counter-practices and local forms of infrastructuring which resist globalized operationalizations of infrastructured anticipation.

In the time since the fieldwork for this chapter came to a close, many changes have come to bear on rapid response priorities and infrastructural

configurations. Despite efforts made to move away from centralized models cyber and digital security, the pull of the idealized, 'global', anticipatory view of security threats continues to exert a force on the practices and infrastructures of civil society digital security rapid response. In a virtual webinar hosted during the first months of the COVID-19 pandemic in 2020, one global NGO involved in coordinating rapid response efforts at a transnational level invited in a commercial cybersecurity company to give a presentation on how NGOs can benefit from its automated, predictive threat intelligence services. The selling point: where anticipating threats is an eternally difficult proposition, why not let artificial intelligence do the work? At a moment of heightened datafication and 'totalitarian zoomification' (Gürses and Rocha, 2021), we can see that the eternal promises of automation continue to illuminate particular futures of cybersecurity. On the one hand, automation seems to offer a way to lessen the unjust burdens of security placed on communities in harms way. On the other, critical debates about AI and datafication show that automated systems can also be productive of insecurity and harm. To what extent civil society approaches to digital security will converge with commercial and state models of automated, AI-driven security is left open to future research. For now, this chapter makes clear that alternate approaches to security and anticipation are important to consider further within broader discussions of security, data, automation, and human agency. As the article shows, even if people 'internalise [hegemonic] regimes of anticipation through technical practices' (Mackenzie, 2013: 391), people can also disrupt these regimes by pushing back against the way particular organizations, institutions, and sectors configure security.