Routledge
Taylor & Francis Group

Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Cybersecurity and the politics of knowledge production: towards a reflexive practice

Fabio Cristiano, Xymena Kurowska, Tim Stevens, Louise Marie Hurel, Noran Shafik Fouad, Myriam Dunn Cavelty, Dennis Broeders, Tobias Liebetrau & James Shires

To cite this article: Fabio Cristiano, Xymena Kurowska, Tim Stevens, Louise Marie Hurel, Noran Shafik Fouad, Myriam Dunn Cavelty, Dennis Broeders, Tobias Liebetrau & James Shires (02 Jan 2024): Cybersecurity and the politics of knowledge production: towards a reflexive practice, Journal of Cyber Policy, DOI: 10.1080/23738871.2023.2287687

To link to this article: https://doi.org/10.1080/23738871.2023.2287687

Published online: 02 Jan 2024.

JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2023.2287687

Cybersecurity and the politics of knowledge production: towards a reflexive practice

Fabio Cristiano [a], Xymena Kurowska [b], Tim Stevens [c], Louise Marie Hurel[d], Noran Shafik Fouad[e], Myriam Dunn Cavelty[f], Dennis Broeders [g], Tobias Liebetrau[h] and James Shires [i]

[a]Centre for Conflict Studies, Utrecht University, Utrecht, The Netherlands; [b]Department of International Relations, Central European University, Vienna, Austria; [c]Department of War Studies, King's College London, London, United Kingdom; [d]Royal United Services Institute, London, United Kingdom; [e]Department of History, Politics, and Philosophy, Manchester Metropolitan University, Manchester, United Kingdom; [f]Center for Security Studies, ETH Zurich, Zurich, Switzerland; [g]Institute of Security and Global Affairs, Leiden University, The Netherlands; [h]Department of Political Science, University of Copenaghen, Copenaghen, Denmark; [i]Chatham House, London, United Kingdom

ABSTRACT

How does a reflexive scholarly practice matter for producing useful cybersecurity knowledge and policy? We argue that staking relevance without engaging in reflexivity diminishes the usefulness of knowledge produced both in academia and in policy. To advance a reflexive research agenda in cybersecurity, this forum offers a collective interrogation of the liminal positionality of the cybersecurity scholar. We examine the politics of 'the making of' cybersecurity expertise as knowledge practitioners who are located across and in between the diverse and overlapping fields of academia, diplomacy and policy. Cybersecurity expertise, and the practices of the cybersecurity epistemic community more broadly, rely heavily on the perceived applicability and actionability of knowledge outputs, on the practical dependency on policy practitioners regarding access, and thus on the continuous negotiation of hierarchies of knowledge. Participants in this forum reflect on their research practice of negotiating such dilemmas. Collectively, we draw on these contributions to identify obstacles and opportunities towards realising a reflexive research practice in cybersecurity.

ARTICLE HISTORY
Received 26 June 2023
Revised 13 October 2023
Accepted 9 November 2023

KEYWORDS
cybersecurity; knowledge production; epistemic community; reflexivity

Introduction: socio-technical knowledge production end epistemic encounters in cybersecurity

Fabio Cristiano and Xymena Kurowska

Once thought to be the exclusive epistemic domain of military strategists and computer scientists, knowledge about cybersecurity matters today to a wide and plural epistemic community. This includes policymakers, diplomats, military/intelligence, tech

CONTACT Fabio Cristiano f.cristiano@uu.nl

companies, activists, and academic scholars of different disciplines. Among these, cybersecurity has also developed into an established sub-field of international relations (IR) and security studies, with a growing number of research centres, initiatives, and educational programmes blossoming worldwide. Many participants in cybersecurity research, policy analysis and practice occupy liminal positionalities, that is, they work in between different roles, actors and communities. In this context, cybersecurity scholars are expected to produce policy-relevant and useful knowledge. Such positionality is, of course, not unique to cybersecurity scholarship. Similar debates have taken place across security studies (Aradau 2017; De Goede 2018; Kurowska 2020; Kurowska and Tallis 2013; Rychnovská 2016). Even if we move on from the rhetoric of exceptionalism that shaped the emergence of the cybersecurity discourse, the historical trajectory of cybersecurity still brands it as an applied and problem-solving technical discipline. Cybersecurity knowledge is also bounded by the distinct state-centrism that underpins IR and security studies more broadly. While the importance of non-state actors may be formally acknowledged, the primary status of the state still haunts contemporary cybersecurity. It prevents the field from integrating knowledge generated by actors marginal to the state or resisting its monopoly. As a result, relevance in cybersecurity still tends to be defined as technical expertise which is readily applicable and useful for furthering state interests. This aspect continues to influence practices of and expectations about knowledge production in the field (Dunn Cavelty 2018).

The specific historicity (defined as the historical development against the background of prevailing knowledge assumptions and world events) of cybersecurity as an applied and state-oriented field gives rise to two intertwined conditions of knowledge production: (1) a specific socio-technical divide, that is, a marked separation between technical and non-technical knowledge; and (2) the co-constitutive character of epistemic (knowledge generating) encounters with practitioners, that is, the dependence of scholarly knowledge production on immersion in practice, or, simply put, on having access to practitioners as sources of insight which should then be translated into academic outputs. These two conditions may seem to reflect the *epistemic pluralism* of cybersecurity as a field, and a sense of an 'imagined epistemic community' that engages in the production of relevant knowledge (cf. Adler 1997). Epistemic pluralism and proximity to practice are indeed core scholarly values that potentially make for the relevance of academic research (De Goede 2020). At the same time, they pose their own, oftentimes implicit, dilemmas when the biases of dominant scholarly frameworks, policy imaginaries and constraints, and technical solutionism (the belief in the decisive role of technology in resolving societal challenges) conspire and lead to segmentation, reproduction of hierarchies or even exclusion, rather than facilitate a productive exchange. What does *reflective* knowledge production in cybersecurity research and policy, understood as continuously questioning one's taken-for-granted assumptions, mean under these conditions?

This forum brings together a diverse group of IR and security scholars who use the lens of positionality – their reflected-upon location in the field of cybersecurity – to broaden the meaning of relevance as directly linked to reflective knowledge practice. We use our liminal positions that straddle involvement in different parts of the field to ask questions such as: Do existing knowledge conditions indeed foster epistemic pluralism that allows for generative multiplicity in knowledge production? What does translation

between different communities of practice look like in cybersecurity? How does interaction between different actors in the field affect knowledge production? Specifically, does it tend to reproduce existing schemes of what knowledge counts as relevant, or does it also create opportunities for innovation? The lens of positionality reveals a complex relationship between reflexivity and relevance that has not yet been sufficiently explored in cybersecurity. Reflexivity is an established conversation in IR and security studies and the Science and Technology Studies (STS) have inspired scholarship that challenges the state-centred frameworks in the broader discipline. This forum offers a granular close-up on concrete experiences of producing cybersecurity knowledge that opens new vistas on such themes. Its insights derive from first-hand familiarity with practice which is, however, also problematised. In providing such reflection, we carve out a reflexive agenda based on a more capacious understanding of usefulness in cyber research and policy. Positionality, in other words, helps to understand what makes knowledge practices relevant and, in a reflexive move, how to broaden the scope of relevance to avoid reproducing received wisdom.

From the socio-technical divide to the socio-technical opportunity for reflexivity

Making sense of computational grammar is core to practices of knowledge production in cybersecurity. For IR and security scholars, engaging with the computational element has, however, primarily meant translating 'received' technical categories into familiar concepts and frameworks of international politics through analogical reasoning (cf. Betz and Stevens 2013). Creating actionable knowledge is expected from an applied discipline (Buzan and Hansen 2009). Yet such 'epistemological adaptation' (Cristiano 2022) reproduces state-centred narratives of cyberspace as a threat – and risk-prone environment and replicates the dominance of legal and normative frameworks (Kello 2021). Critical works have now questioned the underlying socio-technical divide in cybersecurity: it brought out instead the socio-political entanglements that constitute internet technology (Cristiano 2018a; Liebetrau and Christensen 2021; Stevens 2019). Inspired by STS and critical security studies, this literature re-conceptualises cybersecurity as a 'work-in-progress, emergent along with the recursive interactions of communications technologies with their associated societal processes' (Stevens 2019, 133). Prominent recent contributions further discuss the effects of the uncritical translation and reception of technical categories that influence the research process (Egloff and Cavelty 2021; Tanczer et al. 2020), the over-emphasis on certain actors and issues to be studied (Maschmeyer, Deibert, and Lindsay 2021; Stevens 2019), the overlooking of intersectional aspects (Cristiano 2018b; Fouad 2022; Millar, Shires, and Tropina 2021), the relative poverty methodological apparatus (Stevens 2016), and the limited scope of critical engagements with the socio-technical divide (Dwyer et al. 2022; Hurel 2022a). The lens of positionality significantly expands this debate by problematising 'the making of' expertise in cybersecurity research and policy.

In cybersecurity, the role and relevance of the (policy) researcher are still circumscribed by the juxtaposition between techno-scientific cybersecurity knowledge and non-technical policy-driven knowledge (Cristiano and van den Berg 2023). Such entrenched categories uphold the socio-technical divide and thus undermine the potential of genuine

epistemic pluralism that the variety of actors brings to the field. They diminish the productivity of their encounters by determining a priori the expectations as to what type of knowledge a given actor should provide. The liminal positionality of knowledge producers, that is, their practical ability to transcend the prescribed roles and boundaries by moving across them, opens up such entrenched categories. The contributions in this forum exemplify how cybersecurity scholars navigate the socio-technical divide and the related rigidity of 'modes' of knowledge production, specifically in terms of temporality, secrecy, and the emergent and 'unknowable' character of cyberspace. Their encounters also reveal the limits that such endeavours face. Even innovative and contextually appropriate knowledge practices are bounded by relations of power and the resulting hierarchies that shape the process and outcome of knowledge production. Such conditions weigh heavily on what is perceived as legitimacy and therefore what constitutes the researcher's epistemic (knowledge) authority, or expertise, in cybersecurity as an epistemic community.

In this forum, Tim Stevens reflects on hyper-technical understandings of time and temporality in knowledge production about cybersecurity. They dictate the research agenda – insofar as cybersecurity researchers rely on the temporality of technical 'discoveries' and policy logic in their research. At the same time, the socio-technical temporality of cybersecurity creates spaces for a 'politics of theory', thus providing opportunities for greater reflexivity through 'messing' with timing. The inherent (im-) possibility of grasping the computational grammar of cybersecurity further troubles what being an expert in cybersecurity means. Louise Marie Hurel shows how the socio-technical divide informs roles and identities in the cybersecurity community. The divide leads to the fragmentation of the cybersecurity epistemic community, wherein knowledge hierarchies are established through the politics of expertise and technological (mis-)performativity. Against this diagnosis, Hurel ponders the potential to shift from the problem-solving mode to embracing discomfort as a means to interrogate the expert's practices and positionalities. Noran Shafik Fouad unpacks how taking the socio-technical divide for granted affects practices of knowledge transfer and co-production in the classroom. Specifically, upholding technical considerations as established frameworks conceal the western-centric and state-centric historicity of cybersecurity, thus creating a potential bias also in our positionality as educators. Critical pedagogies, as Fouad discusses, offer concrete tools that help break down such epistemic exclusions.

Epistemic encounters and useful knowledge

Cybersecurity is commonly thought of as security that anticipates or responds to risks, incidents, threats and attacks (Dunn Cavelty and Wenger 2022). This 'emergent' technical character of cybersecurity dictates what constitutes the usefulness of the knowledge we produce in cybersecurity. It calls for expertise in how to deter, patch, govern, or prosecute exploits of technical vulnerabilities as issues of national security and global governance (Whiting 2020). In this context, non-technical cybersecurity researchers inhabit a peculiar liminal positionality that requires them to align technical categories to established concepts in scholarship on security, and in particular regarding security governance. This applied character of cybersecurity steers knowledge production towards policy dependency, wherein even theory work tends to be bounded by the expectations of creating

actionable models and recommendations. While this may seem to produce scholarship that matters, such scholarship matters to the extent it complies with the pre-existing ideas about relevance. It thus diminishes the potential for creativity, forcing established categories over innovation, which in turn reinforces the dilemma of responsibility for the products of knowledge that scholarly practices co-constitute (Austin, Bellanova, and Kaufmann 2019; Deibert 2018).

The second part of the forum showcases how cybersecurity scholars navigate such dilemmas across different communities, such as policy, diplomacy and military/intelligence, and how they do so against disciplinary fragmentation within academia. The lens of positionality allows them to acknowledge the situatedness of knowledge production. It brings to the fore the role of context, material conditions, ethical predicaments, and opportunities for engagement, rather than the universality or epistemic and moral superiority of established frameworks. The contributors thus reveal the actual contours of cybersecurity practice, specifically as it takes shape in encounters with practitioners. Myriam Dunn Cavelty provides an auto-ethnographic account of the relationship between policy and knowledge production, suggesting different modes of engagement between communities of practice and arguing for more collaboration beyond disciplinary boundaries. Dennis Broeders explores the limited insight into practice when the main sources of knowledge remain adopted documents that are sanitised of struggles that precede diplomatic consensus. He warns against the uncritical reproduction of geopolitical narratives that pervade the ongoing UN diplomatic process on cyber norms. Drawing on his professional background in military intelligence, Tobias Liebetrau provides a reflexive account of the practical challenges related to producing critical scholarship at the juncture between policy and scholarly research, in a context which is shrouded in confidentiality and secrecy. In his concluding piece, James Shires grapples with research identity and funding challenges in Western and non-Western settings and ponders possible shapes of principled reflexivity in both. Taken together, the contributions interrogate the liminal positionality of the cybersecurity scholar and bring to bear the granularity of the relationship between reflexivity and relevance and advance a reflexive research agenda that expands what it means to produce useful knowledge in cybersecurity research and policy.

A matter of timing: on the temporalities of cybersecurity research. Tim Stevens

It might appear arrogant for cybersecurity researchers to claim for ourselves a peculiarly frenetic field of inquiry. After all, as Barry Buzan (2000, 3) observed during the Cold War, security researchers were even then constantly trying – and often failing – to keep up with the 'hectic empiricism' of international relations. Few would argue that the world has somehow 'slowed down' since the demise of the Soviet Union and more than a few sociologists assert a twenty-first century sociotechnical acceleration that further complicates empirical research and theory-building (Hassan 2009; Rosa 2015; Rosa and Scheuerman 2009). Information technologies are inextricably bound up in these diagnostic narratives. Paradigmatically – perhaps even metonymically – this refers principally to 'the internet' as a driver and expression of hypermodernity, its ailments and opportunities being precisely the concerns of cybersecurity as a field of practice and of analysis (Stevens 2023). The

internet's billions of nodes and trillions of data packets interact at the speed of light across, below and above the surface of the Earth. Its logical topologies reconfigure at timescales beyond human sensibility. The sheer diversity of actors and agents operating in this environment, from polymorphic malware to shifting assemblages of hackers, state agencies and cybercriminals, can be bewildering. The internet and other information systems obey consistent technical rules and protocols but continuously manifest in complex and sometimes surprising ways. To even the most knowledgeable and experienced researcher, studying this environment presents significant challenges, many of which can be understood as problems of time and temporality.

Time is everywhere in cybersecurity research, even if it is not always made explicit. Issues of cyber risk, resilience, war, security and strategy are all informed by identifiable temporal assumptions, biases and propositions (Stevens 2016). We can argue about the structuring effects of digital technologies – the push and pull of informational supply and demand – but we should also accept that researchers and practitioners create, channel, encourage and shape particular temporal attitudes and arrangements, not least as ways of taming the bewilderment we often experience. For instance, internet technologies do not demand that we reach for apocalyptic metaphors to railroad cybersecurity decision-makers into particular courses of action; these are rhetorical choices that mobilise specific temporal imaginaries for distinct political effect (Lawson 2020). Similarly, lazy allusions to cyber weapons being released at the simple press of a return key do serious damage to our understanding of how offensive cyber capabilities are developed and deployed and the institutional arrangements necessary to do so (Smeets 2018a; Smeets 2022). These well-known examples illustrate that cybersecurity knowledge production is intimately related to how we understand time and temporality and to how we express this in disciplinary and political settings. Specifically, we can introduce time to our research, not as a (meta)physical object or dimension but think instead of 'timing' as a social and purposive process of organising ideas and entities. Through brief discussions of the ontology, method and politics of timing below, we can more clearly see the link between time/temporality and cybersecurity knowledge production and generate a more reflexive appreciation of the positionality and politics of our interventions. If we ignore the 'timing' of both scholarly practice and the objects of our enquiries, we are missing fundamental aspects of how cybersecurity is constructed in the world, thereby closing down opportunities for more sensitive engagements with the local, contextual and culturally specific politics of cybersecurity.

Knowledge construction is a practice of ordering. Theory-building, for instance, is a process of organising data and experience into patterns that we can use to understand, explain and, perhaps, predict (Jackson 2011). Patterning is an active temporal process, of establishing cause and effect, deliberation over the implications of change and continuity, and of understanding negative and positive feedback mechanisms. For Andrew Hom, we can better understand these practices through 'a theory of timing' that 'describes a holistic and ongoing effort to constitute change processes in the first place, establish their importance, arrange them hierarchically, and relate them to other changes to produce a new relational series that unfolds in some ways and not others' (Hom 2020, 33). A theory of timing helps to explain the emergence of particular conceptions of time and temporality and how these interact in ways important for understanding the processual dynamics of local, national and international politics, including cybersecurity. This is a

significant shift in the emerging 'temporal turn' in International Relations (IR) (Chamon 2018; Hom 2018), which attempts to examine 'time' as a political phenomenon as important to global affairs as the conventional IR concern with 'space'. As Hom (2020, 27–29) explains, we can move the grounds of debate from arguing over which ontological commitments present a 'correct' view of time, and from worrying about how to integrate the physical and the phenomenological.

We can also challenge the preponderance of Western standards of time and temporality (Hom 2010) and the implications of dominant modes of time-reckoning and historical narrative. The 'racial-epistemic hierarchies' underwriting assertions of differential cybersecurity knowledge production and claims to expertise (Mumford and Shires 2023), for instance, are themselves structured with respect to Western standards and expectations of time and history. This serves to marginalise and diminish the attempted contributions of non-Western cybersecurity experts as less 'advanced' or 'immature' relative to Western voices and therefore less able to influence cybersecurity policy that is increasingly globalised and globalising. A more productive approach is to focus on the 'timing activities' of actors and agents as empirical objects in our fields of enquiry. Thinking of time as something that is 'done' – as opposed to something that just 'happens' – allows us to render visible the politics of timing practices, shorn of some of the intellectual and cultural baggage that often impedes our understanding of world affairs, including the twin perils of extreme social and technological determinisms. This applies to cybersecurity studies as much as any other field of security studies or international politics, in which time and temporality are not metaphysical givens but dynamically constituted by what we do in practice.

Our empirical challenge is therefore to identify timing dynamics in cybersecurity practice and theory. We have already seen productive engagements with wider disciplinary currents of practice theory in IR (Lechner and Frost 2018) and with STS (McCarthy 2017; Singh, Carr, and Marlin-Bennett 2019), each of which emphasises that what is done is just as important as what is said. Emerging from diverse methodological standpoints, cybersecurity studies have engaged with ethnography and participant observation in sociological sites of cybersecurity practice (Coles-Kemp, Ashenden, and O'Hara 2018; Dwyer 2021; Shires 2018; Slupska and Duckworth 2021). Elsewhere, they have paid close attention to how human and nonhuman entities interact in the co-production of cybersecurity knowledge (Balzacq and Cavelty 2016; Fouad 2022; Liebetrau and Christensen 2021; Stevens 2019). Given this body of disciplinary expertise, we might now turn our attention to timing practices in cybersecurity, both in their realisation as granular 'micromoves' in theory and practice (Solomon and Steele 2017) and in how they inform intellectual knowledge production in the field. This will enable us to challenge dominant narratives in cybersecurity, such as the persistent construction of timelines that prioritise visible 'events' – from the Morris Worm to Y2 K, Estonia, Stuxnet, and so on – to the exclusion of the warp and weft of everyday cybersecurity practice and the 'little security nothings' (Huysmans 2011) thereby marginalised as indistinct or irrelevant. What are the disciplinary effects of timing practices like these, and when do 'active' timing practices become sedimented and normalised as 'passive' ones (Hom 2020)? While we should make no assumptions about the inevitable productivity of these lines of enquiry, it will at least cause us to ask what we overlook when we accept timing practices uncritically and what we may already have missed by doing so.

Timing is political. As Hom (2020, 50) asserts, 'timing is like theory – always for someone and some purpose.' Our temporal positionalities require continuing attention and critique, lest they 'turn imperial' (Ib.). At the macro-level, this is a persistent problem in cybersecurity scholarship, which is heavily skewed towards the Global North and the industrial time of Western societies and their military, intelligence, diplomatic and economic practices. This is a timing issue; of historical time, of course, but also of times of labour, gender, empire and race, of notions of social-technological progress, and much else. How are we to understand non-Western conceptions of digital sovereignty, for instance, if we ground our analyses of political order in seventeenth century Europe alone? How can we engage productively with indigenous cybersecurity needs and ambitions if we prioritise our industrialised temporalities over theirs? Crucially, these timing practices co-produce our theory-building and our political normativities: they exclude as much as they include. We should ask what temporal assumptions are expressed, encouraged and reproduced in our scholarly practice, including teaching, and our performance of public 'expertise'. How might we do things differently? What are the implications for the politics of cybersecurity knowledge production, if we problematise 'time' as 'timing'? Writing at the turn of the century, Patrick Morgan (2000, 66) remarked that we 'need greater respect for time, combined with a richer sense of what this means for thinking about security.' This remains so for the politics of cybersecurity, in which key variables and drivers alter over time and 'change the knowledge, understanding and consciousness that support existing practices' (Buzan and Hansen 2009, 55). Our timing decisions play constitutive roles in the practices of cybersecurity knowledge production and are therefore worthy of reflection.

From holy grails to missing pieces: discomfort and the politics of cybersecurity expertise in academia. Louise Marie Hurel

The study of cybersecurity has often revolved around at least two key concerns: the security expert and the breakdown of networked systems. On the one hand, the security expert has been associated with the development of communities of practitioners such as hackers, incident responders and other IT professionals. It has evoked images of *who* these practitioners are (hacktivists, military officers, mercenaries), *what* they do, their moral and ethical *values*, and their *capacity* to provide technical insights. On the other hand, the concern with the security of networked systems is intimately linked to the discovery/concealment of vulnerabilities, prevention of crises, responses to breakdowns and maintenance of systems. Imaginaries (Mansell 2017; Taylor 2002) about networked infrastructures are not necessarily linked to their well-and-stable functioning but concentrate precisely on when and how they might fail to operate as expected.

Both the security expert – in its embodiment as 'the hacker' being the go-to reference – and the compromise of networked systems and infrastructures – in their expected domino-effect large scale cyber-doom vision – have become the extreme representations of the imaginaries that have taken the position of the holy grails in policy and academic cybersecurity circles. 'Holy grails' are those objects that have a specific status of signification – sacred, shiny, mystical and meaningful – for a particular field. They are directly entangled with knowledge production practices in their demarcation of who gets to know about cybersecurity, what are the objects of protection, and what kinds of research count as valid.

The problem, however, is that the lure of these shiny tenets of cybersecurity research, both the agent (security expert) and the object of security (networked systems) can often conceal other kinds of expertise and thus other kinds of politics embedded in knowledge production, for instance, of those conducting academic research. In becoming objects of cybersecurity, the holy grails also become the objects of care, attention and consideration, not revealing the place and entanglement of the researcher in their creation and emergence in our contemporary security dilemmas. Expertise is not only positioned in these imaginaries about cybersecurity but also feeds into them as the performance and recognition of 'valid' knowledge. Even so, current literature on cybersecurity reflecting on expertise usually tends to focus on the former (the study of 'X'), rather than the role of academia in making expertise ('becoming' through studying and practising expertise).

I suggest that a deeper interrogation of the politics of knowledge in cybersecurity requires a critical assessment of academia's relationship with the 'holy grails' and practices of expertise-making. To do so, I suggest that we refrain from rushing to the grails, solving the crises, and running from uncertainty; rather I propose we embrace the discomfort proposed by feminist theory to interrogate our own motivations, practices and positionalities (geography, gender, race) as we conduct and navigate the policy and scholarly world. I raise three points regarding the politics of knowledge production in cybersecurity in academia: First, I position the notion of the 'holy grails' that have pervaded policy and research debates. Second, I reflect on the entanglement of scholarly expertise with crises. Finally, I conclude with some considerations for future research from a place of discomfort, one that invites reflexivity in a context where expertise is rewarded for being ready to be served.

The holy grails

Throughout the years, the practices of technical security experts have become the object of ethical and legal discussions. Since the 1980s, the image of the hacker has undergone a transformation from an underground subculture to a professional career (Goertzen and Coleman 2022) – with professionals pursuing jobs that range from bug bounty programs and penetration testing to security analysts in cyber commands. As cybersecurity gained traction across different countries' national security agendas in the mid-2000s and private companies worked to provide services that could maintain and enhance knowledge about computer security issues, the greater the impetus for these sectors to identify and seek to incorporate more systematic skills present in the 'hacker'. The professionalisation of cybersecurity through certifications, for example, came to 'solve' practical ambiguities of conducting hacking, while also demarcating the boundaries between white, black, and grey hat hackers. Such language served, at times, to delineate the spectrum of their actions, ranging from illegality to legality, from 'bad' to 'good'; and teams from 'red' to 'blue' (Tanczer 2020).

A common thread that weaves these communities together is that they are usually qualified by the technicity of their expertise, that is, how close they are to monitoring or actively engaging in an operational environment. While important, such literature often equates security expertise to technical expertise. It legitimises cybersecurity expertise as the knowledge and capability to operationally or managerially deal with cyber incidents. Recent scholarship has sought to include other actors such as cyber diplomats and

cybersecurity capacity builders as important communities of actors (Pawlak and Barmpaliou 2017).

The second holy grail is the notion of continuous breakdown of systems, infrastructures and communications. Entangled with the emergence of the representation of 'the hacker' in the media and policy debates, ICTs which were mainly seen as force enablers until the 1980s, were later perceived as threat-enablers (Dunn Cavelty 2008). The expansion of digital technologies throughout the 1990s and the public debates around cyber incidents slowly introduced the idea that vulnerabilities might be exploited and that effects might lead to catastrophic results (cyberwar). Since then, the debate has significantly widened. Literature on cyber operations has proposed to conceptualise and investigate activities below the threshold of armed conflict more carefully rather than assuming escalation or cyberwar (Smeets 2018b). Others have focused on norms for responsible state behaviour in cyberspace, and critical scholarship has sought to unpack the materialities of actants in cybersecurity (Fouad 2022). While these holy grails have permeated research agendas, they still do not account for the agency of academia in both the expertise and politics of knowledge production – despite being the object of its craft and labour.

Staying with the trouble

As with every crisis, it is born with a desire for a solution. Even though it is not always achievable, there is a desire to know what is happening and for experts to provide guidance in times of trouble. While important, the desire to respond to the context of a cybersecurity crisis is entangled with the holy grails of hackers and systems that have been compromised as well as it evokes where and how scholars should perform their expert knowledge on such topics. The problem with this is that the scholar itself, embedded in the crisis, seeks to respond to it by 'staying relevant', engaging in the public debate, appearing, speaking, tweeting and the list goes on – otherwise, why would one study cybersecurity for so long if not to provide one's insights when relevant? Should one do so? Too utilitarian?

A crisis creates a space of attention, it demands knowledge that is 'fit for purpose', ready to be absorbed as part of solving the problem or making sense of the crisis (Berling and Bueger 2015). But these pressures for expertise enactment are in direct tension with some core characteristics of cyber research: secrecy; reliance on publicly available information for triangulation (which means the best incidents to be investigated are the ones with most data); temporality of analysis and methodology. Even so, social media provides a space where experts are embedded in the politics of recognition. Depending on the notoriety or virality of a tweet, that person might be spotted by a journalist and invited for an interview. At the same time, funders will seek to learn from the crisis and reach out to scholars as potential receivers of these sources of financial support.

What is the role of a scholar/cybersecurity expert in responding to crises? I suggest that the discomfort of not knowing when to perform expertise should be embraced and serve as an opportunity to question and excavate what kinds of practices scholars are willing to engage in to 'stay relevant' in this context and inquire about one's positionalities. The challenge with the practices of expertise in academia is that it can often focus on the

holy grails and staying relevant while missing the opportunity that crises create beyond solutionism (epistemic and practical): to 'stay with the trouble', to sense the uneasiness of the crisis as something that is not immediately resolvable and that can make us ask questions that had previously been unasked (cf. Bellanova, Lindskov Jacobsen, and Monsees 2020). As Donna Haraway (2016, 1) notes: 'In urgent times, many of us are tempted to address trouble in terms of making an imagined future safe' but 'staying with trouble requires learning to be truly present […] entwined in myriad unfinished configurations of places, times, matters, meanings.' It means inviting reflexivity, asking what (and where) the holy grails are, and looking into one's imbrication in political, economic and geopolitical dynamics. Discomfort, more than a thought, is our archaeological tool of trailing the dusty paths and objects that we hold dear as scholars, of asking, yet again, how we are made together and the implications that have led to our knowledge production.

Unlike the practice of expert performance that seeks to provide order to chaos (crises), to settle the unsettled, the practice of discomfort can dis/orient researchers in specific and productive ways (Chadwick 2021): dealing with epistemic uncertainty of crises, dwelling on the sensation of unsettlement with one's incentives for being rewarded for performing expertise even when not knowing what is happening, questioning feelings, elucidating a range of privileges, including embeddedness in the Global North and Western frames of reference associated with the holy grails (Hurel 2022a). Future research agendas in cybersecurity have the potential to refocus the theoretical, geographic, and gender lens that has informed the field. In this regard, new avenues for rethinking expertise need to be further explored, attending to non-Western, de-centred visions as well as accommodating alternative cybersecurity imaginaries that can support the emergence of a research agenda on cybersecurity that derives from a critical assessment of its own assumptions. Only in doing so can we move from holy grails to missing pieces.

Reflexive teaching and cybersecurity knowledge production: what do critical pedagogies mean for cybersecurity? Noran Shafik Fouad

Teaching practices are essential constitutive forces of knowledge production in the study of IR and its sub-discipline security studies (Grenier 2016). In recent years, cybersecurity has been rising significantly on research and teaching agendas in IR departments in many higher education institutions around the world and is being taught extensively either in stand-alone courses or as part of studying technology's impact on global politics and security. As such, teaching becomes an important site for interrogating positionality and thinking reflexively about cybersecurity knowledge production and its disciplinary trajectories. However, cybersecurity has arguably been evolving into a quasi-independent field that does not necessarily engage with questions, theories, concepts, and debates in other sub-fields of IR and security studies. This raises questions on how cybersecurity fits within the growing attention to critical pedagogies and calls for pluralist and inclusive classrooms when taught in IR departments. Specifically, *what does teaching cybersecurity 'critically' mean?* And, more broadly, *how can reflexive teaching influence cybersecurity knowledge production?*

Critical pedagogies in IR, advocated by postcolonial, feminist, and poststructuralist scholars, seek to advance the voices of the 'others' of politics and challenge complex

power relations and hierarchies in the discipline and classrooms (Bilgic, Dhami, and Onkal 2018). This entails teaching controversies and alternative interpretations of 'evidence' to disrupt knowledge practices and to bring discussions on race, class, gender, sexuality, ability, and intersectionality to various fields of inquiry (Kirby 2013; Malik 2013). An integral part of such pedagogical practices is decolonising the curriculum by challenging dominant Western epistemological traditions, white supremacist assumptions and Western-centric worldviews, as well as centring 'global' experiences and perspectives (Arday, Belluigi, and Thomas 2021). Adopting similar critical approaches and decolonising the curriculum in cybersecurity teaching is not an easy task, however, because such pedagogical conversations have not yet taken place in the field. Even more, while 'critique' and 'criticality' remain subjects of contestation in IR and security studies (Sjoberg 2019; Visoka 2019), such contestations have not taken up enough space in cybersecurity research (Dwyer et al. 2022).

Navigating cybersecurity classrooms through a critical lens is often challenged by three key characteristics of mainstream literature and public discourses on cybersecurity: Western-centrism, state-centrism, and negligence of the ostensibly 'mundane'. In many ways, cybersecurity has been shaped by Western-centric perspectives according to which the subject matter, referent objects, and agency in the field are defined and studied. Focusing on cybersecurity as a question of great power competition between the 'democratic West' and authoritarian governments in Russia, China, North Korea or Iran is one signification of this Western-centrism. According to this view, the Global South is often marginalised and perceived as peripheral and even as a source of cyber-threats to be addressed by capacity-building efforts supported by the Global North (Calderaro and Craig 2020). Students often come to classrooms with prior assumptions on what cybersecurity is and is not, influenced by such discourses that ground experiences of particular parts of the world and marginalise others.

Countering this Western-centrism in teaching cybersecurity requires ontological and epistemological exercises that investigate ways for the field to become more inclusive. Recent efforts to establish research centres and produce literature analysing cybersecurity policies of 'rising' or 'emerging powers' in Africa, the Middle East and South America provide the basis for diversifying the curriculum (Belli 2021; Cristiano 2022; Hurel 2022b; Shires 2021). However, more is needed than simply adding 'non-Western' experiences as 'alternatives' to the 'core' of cybersecurity. For instance, dedicating a week or multiple module design to perspectives from the Global South enables students to think beyond the West, but may contribute to modes of othering, particularly if such discussions are initiated after the field has been defined and delineated. There is also a challenge in choosing countries to include as empirical cases in teaching global perspectives. For example, while including rising cyber powers (e.g. India, Brazil, South Korea, etc.) makes sense from a strategic standpoint, using 'power' as a qualifying condition perpetuating a state-centric and/or militaristic understanding that confines cybersecurity to certain contexts and places where power lies.

Several epistemological and methodological challenges hinder such quests to decolonise cybersecurity curricula and to include perspectives from the Global South as constitutive, agential forces of the field's core subject matter. These include, for instance, the secrecy surrounding state practices in cyberspace (Buchanan 2016), uncertainties

around the implications of cyber incidents (Gomez 2021), biases in commercial cybersecurity threat reporting (Maschmeyer, Deibert, and Lindsay 2021), and the fact that most institutions producing such reports are based in the West. Consequently, cybersecurity researchers are often forced to focus on a limited number of Western countries where research-enabling data is easier to access. Added to this are constraints on academic freedoms in certain contexts that may even put cybersecurity researchers in danger. This in itself could be a point of reflexive inquiry in cybersecurity classrooms: interrogating *absences* in cybersecurity knowledge production. How, for example, are such absences influenced by global digital inequalities that dictate where cybersecurity 'power' and 'knowledge' is centred? How do colonial structures, hierarchies of power and race, influence the making and legitimacy of cybersecurity 'expertise'? How is the present state of cyber (in)security in the Global South linked to digital capitalism (Fuchs 2018) and digital colonialism (Kwet 2019)?

Answering these questions requires historicisation exercises that link modern-day cybersecurity challenges to the evolution of technology and colonial histories and that, as Stevens argues above, move beyond Euro-centric temporalities and conceptualisations. Answering these questions requires historicisation exercises that link modern-day cybersecurity challenges to the evolution of technology and colonial histories and that, as Stevens argues above, move beyond Euro-centric temporalities and conceptualisations. This is what Shires and Mumford, for example, establish in their work on the 'racial-epistemic hierarchies' that grant legitimacy for cybersecurity expertise in Gulf States, and how such hierarchies, which are primarily constituted by coloniality, influence perceptions of technological ability, rationality and authority (Mumford and Shires 2023). Further, we need to contextualise cybersecurity knowledge by questioning the politics of academia: who is teaching and where and under what conditions cybersecurity knowledge is developed in and outside academia. This is essential in investigating *how* to decolonise and *why* it matters to understanding power dynamics and issues of representation and diversity in the field. Yet, in a fast-moving field like cybersecurity in which academics are required to keep pace with constant developments, the value of such exercises is often obscured.

Another key challenge in teaching cybersecurity critically is countering state-centrism for students to view cybersecurity as a lived experience and to contemplate the potentially violent consequences of states' cybersecurity practices (Egloff and Shires 2023). In recent years, some contributions have started to move from a state-centric focus towards conceptualising actancy in cybersecurity as an *assemblage* in which various actors interact (for example, Egloff and Cavelty 2021; Stevens 2016; Stevens 2019) and adopting a human-centric approach to cybersecurity (Burton and Lain 2020). Reflecting this shift in teaching is not an easy task, however, particularly when global perspectives are included as discussed above. This is because the majority of research on the Global South focuses on states' official cybersecurity strategies and national policies, and not necessarily on human experiences. Hence, diversifying and decolonising the curriculum does not always coincide with a non-state centric approach to cybersecurity teaching.

In addition, including normative and ethical questions that problematise state behaviour risk leaving students with more questions than answers on what cybersecurity is and what it ought to be, thus challenging some of the established understandings and concepts in the literature. For example, is there a risk of condoning cyber intrusions for

intelligence gathering by teaching them as cyber 'defence' practices? Should the distinction between cyber offence and defence be questioned? Should the state's level of democracy/authoritarianism decide whether its cyber operations are justified? Should the lines between hacktivism and criminality be challenged? Engaging in such discussions moves classrooms away from what is pragmatic, feasible, or realistic in cybersecurity politics. Whether this is a desirable learning outcome is a judgment call for academics who may find it challenging to lay enough foundational groundwork for students to engage in such advanced discussions (Grenier 2016), particularly given the complexity and technicality of cybersecurity.

State-centrism is also closely linked to tendencies to prioritise the high-profile rather than the ostensibly 'mundane' in cybersecurity. Many literatures tend to focus on high-profile cyber operations that cause disruption or damage at scale with considerable impacts on policy circles and media discourses. The inclusion of such examples in classroom discussions is imperative in a highly empirical field like cybersecurity that can only be taught through extensive case studies. However, the challenge for a critical classroom is disrupting the state-centric understandings of many such incidents, the Western-centric frameworks according to which they are analysed, and the periodisation of 'global' cybersecurity they may convey. Moreover, moving away from the strategic to the mundane is particularly challenging in IR departments as many of the less-than-high profile topics may not necessarily fit within conventional disciplinary boundaries, for example, organisational cybersecurity.

Besides, centring everyday cybersecurity becomes a key learning design challenge for critical pedagogies that encourage students to question hierarchies of power and how they affect their everyday cyber (in)security. For example, there is a wealth of literature on cyber deterrence, cyber espionage, offensive cyber operations, cyber governance, and various strategic themes, but not as much on intersectional approaches to cybersecurity that highlight injustices and inequalities in human experiences of cybersecurity based on race, gender, sexuality, class, ability, etc. (Millar, Shires, and Tropina 2021; Slupska 2019). It thus becomes difficult to integrate cybersecurity of the everyday in course design in absence of solid scholarly foundation and data that enable students to challenge the lecturer as an authoritative voice on that matter. Here, an interdisciplinary approach to curriculum design that integrates perspectives from other adjacent disciplines to IR could help students engage in such critical discussions on the security of the everyday (Asmolov 2021; Leman-Langlois 2013; Yar and Steinmetz 2019).

To conclude, more scholarly conversations are needed to establish a strong case for the value of critique as central to understanding the politics of cybersecurity, rather than as an alternative perspective to the original story. This is a necessary starting point for designing critical pedagogies to teaching cybersecurity that contribute to critical pedagogies in IR more generally. There is opportunity for cybersecurity classrooms to be spaces where students reflect on the history and theories of IR, rather than cybersecurity appearing as an independent subject with completely separate sets of questions. To do so, more space has to be given to theoretically and conceptually oriented research that brings a necessary level of abstraction to establish such disciplinary links and to engage with pedagogical conversations in IR and other sub-fields of security studies. This, however, is a challenging research endeavour in a fast-moving, empirical field like cybersecurity, in which the production of knowledge is being increasingly conditioned by direct policy relevance.

Critical knowledge production through policy encounters in cybersecurity. Myriam Dunn Cavelty

From the moment security studies scholars began to take notice of cybersecurity, encounters with the 'policy world' have shaped the field's intellectual history – and in reverse, knowledge built up by experts influenced policy decisions. Of course, such a co-constituting co-dependency and often overlap between academics and policy practitioners is neither new nor is it restricted to cybersecurity, as the rich literature in security studies on different aspects of the relationship shows (cf. Berling and Bueger 2015; Evans, Leese, and Rychnovská 2021). However, when there is little agreement about what the security object constitutes and how it should be governed, awareness about how knowledge practices co-shape accepted versions of reality becomes particularly important (Liebetrau and Christensen 2021). After all, knowledge production is not a neutral or a-political endeavour, but a form of ontological politics that co-creates 'entities and relations in the world' (Rubio and Baert 2012, 4) by naming, categorising, producing, and presenting specific realities or 'truths' that serve as a basis for policy decisions and practices.

In what follows, I highlight two aspects of how the field of cybersecurity research has developed in the last 20 years because of encounters between the academic and the practitioner communities. First, I focus on the role policy played in the inception, maturing, and change of cybersecurity as an academic field of study, showing the impact of two incidents that unearthed the practices of previously hidden actors. My reflection is based on a subjective auto-ethnography (cf. Jackson 2015). Such a reflexive historicisation is a good starting point for understanding how the knowledge we as social scientists generate interacts with the 'reality' we describe but also how we are dependent on the 'visibility' of practices. Second, and given the close and I would argue inevitable link, between academic and practitioner communities, I think about the necessity of engagement between the two, and the further questions this raises in particular for critical scholars. Knowing just how important the interface between security experts and practitioners is, we should make sure to actively shape it.

Researching policy: from visible discourses to invisible practices

Policy and politics go hand in hand, with policy being, among other things, a 'product' arising from the political system (Knill and Tosun 2011, 373). As such, policies come in many forms, as rules, regulations and even laws, but also as goals for the future, acceptable procedures, a statement of intent, as a 'way of doing things', etc. As an output and by the nature of their function to influence the behaviour of people, policies are 'observable' (and therefore 'visible'). This visibility, I argue, had significant effects on research. When cybersecurity was first perceived as a political issue, it was discussed almost exclusively in publications from US think tanks and war colleges (such as Arquilla and Ronfeldt 1993). The literature at the time had no ambition to contribute to an academic debate but aimed to consolidate threat perceptions and to help with difficult policy decisions. In this, cybersecurity follows a pattern that is well known to security studies: The political urge and urgency to react to 'new threats' creates an immediate demand for policy-relevant and 'actionable' knowledge, which is provided by think

tanks and similar institutions. Only with time, new topics might turn into academic specialties when scholars begin to link it to ongoing academic debates (Buzan and Hansen 2009).

Due to another recurring pattern – technological innovations are always understood as massive power political game changers (cf. Goldfarb and Lindsay 2022; Lindsay 2020) – the policy debate was dominated by disaster scenarios for decades. The new threat was presented as existential and countermeasures as inadequate, with minor, mostly non-politically motivated cyber-incidents cast as harbingers of certain doom. As a reaction to what looked like a 'hype', a first wave of scholarship used security studies theory to engage with the how and why of political threat constructions and securitisation dynamics (Dunn Cavelty 2008; Eriksson 2001; Hansen and Nissenbaum 2009). This was done by focusing on congressional hearings, official statements by heads of state or other high-ranking officials etc. – in short, visible output in the form of policy. Two cyber incidents – the discovery of Stuxnet in 2010 and later the Snowden disclosures in 2013 – were instrumental in shifting the debate from the threat politics of 'what if' scenarios to the actual strategic use of cyberspace. They created moments of disruption that unearthed previously hidden characteristics about state capabilities and practices: mainly that politically relevant cyber operations did not leave easily 'visible' traces, but were conducted in secret, below the threshold of armed conflict, in the domain of intelligence agencies and semi-state actors (Georgieva 2019).

The realisation that a focus on visible policy made academia blind towards impactful practices led cybersecurity research to diversify in the years that followed. On the one hand, researchers began to ground cybersecurity research in empirical 'reality' by creating datasets to test hypotheses (Kostyuk and Zhukov 2019), thereby linking the study of cyber operations to the larger agenda of conflict studies and IR. On the other hand, critical cybersecurity underwent a practice and a material turn. Like in other areas of security studies, participant observations and ethnographical work became the go-to methods to get closer to state and non-state actors such as specialised bureaucratic units, consultants, private companies or other experts (Stevens 2018; Stevens 2019).

Engaging policy: from passive observer to active challenger

The necessity to engage with security-relevant practices of (not easily visible) key actors raises a series of logistical and methodological questions, not least about research ethics. On the one hand, several excellent publications about methods for critical security studies are available to us (Aradau et al. 2015; De Goede and Pallister-Wilkins 2019). On the other hand, and in contrast to their more positivist-oriented colleagues, critical scholars face a persistent dilemma when they enter a closer relationship with security practitioners. Engaging with policy and security practices through (at a minimum) ethical critique is at the heart of the critical project. The aim has always been to challenge truth claims and political implications of established discourses based on normative ideas of just, inclusive, democratic processes (Collective 2007, 595; Hansen 2012). At the same time, however, many critical scholars feel uneasy about engaging more closely with the security sector because of the dangers of being co-opted or tarnished (Ish-Shalom 2015) or because they do not want to inadvertently reproduce what they set out to critique (Van Milders and Toros 2020).

However, if we are always and inescapably implicated in ontological politics through our research, and said research necessitates some form of engagement with the practitioner community, then we should attempt to actively shape, negotiate, and optimise the interface between practitioners and academia (Evans, Leese, and Rychnovská 2021, 204). What role we researchers end up playing is partially a personal choice and partially influenced by our institutional environments, some of which demand that the 'impact' of academic work is not only measured with the help of citation indexes but also by its policy relevance. There are different options from which to choose, ranging from passive to active, or even activist roles. Passive critique tends to stop at dissecting dominant discourses and at exposing the workings of power, usually in academic publications. More active modes wish to assist security practitioners 'in becoming more reflexive about their practices, as well as in helping them to cope with multiple truths, theories and technical knowledge' (Collective 2006, 474), which can be practiced through workshops and courses. Activist forms of engagement may seek to perform alternative practices of security or will outright refuse security arrangements as a form of resistance, potentially using 'hacking' techniques broadly understood (Dwyer et al. 2022).

Crosscutting these different modes are questions about models of communication. Many contemporary science communication models caution against the idea that the realm of 'science' possesses superior knowledge with which to educate 'the other' (such as policy, media, citizens) and advances interactive collaborations in the form of dialogue instead (Kappel and Holmen 2019). Indeed, constructing security practitioners as passive givers (to be used for knowledge input) or passive takers (to be educated about how the world should be) forecloses options for transdisciplinary knowledge production (Kurowska and Tallis 2013) and other critical practices of engagement (De Goede 2020). Unfortunately, I need to end with a note of caution. Beyond the dangers of being co-opted by systems of power, cybersecurity researchers can face direct threats as a reaction to their research. A benign dialogue between security experts and practitioners presupposes a democratic system in which all actors are open to a transparent exchange for 'the common good'. Such preconditions are not always given and even are an exception in many non-Western contexts. Going against the commercial and strategic interests of powerful actors who do not share values of democratic deliberations and openness may expose researchers to uncomfortable situations even if they are based in a democratic country (Basen 2021). The current geopolitical environment makes cybersecurity research harder.

This contribution looked at policy as an important input into knowledge production processes, also highlighting the limits of just studying visible outcomes, and then mentioned different modes of engagement between communities of practice. Given how complex the interaction between security policy practitioners and security experts is for the politics of knowledge production, it only scratches lightly on the surface of a multifaceted issue. Beyond what was already discussed, I want to highlight two additional issues in brief, partially pushing against a simple dichotomy between academia and policy.

First, complex technological security issues are already changing traditional research practices in IR and security studies. Because of the diversification of sources and the additional localities where important knowledge is produced like the private sector, interdisciplinary or transdisciplinary collaborations well outside our normal comfort zone are

going to become more important. Second, and related, data about cyber operations is increasingly produced by specialised private companies. Not only is this data already politicised but it is also not available for free. Access for academics who cannot pay exorbitant prices or maybe even better, large-scale 'neutral' data collection activities that will allow us to show dynamics beyond established friend-enemy patterns is going to be a key challenge in the future. Both these points only stress the necessity for more collaboration beyond disciplinary boundaries.

Text and tea leaves: cyber diplomacy and the politics of knowledge production. Dennis Broeders

Studying diplomacy is often historical and text-based research, although there are notable exceptions where scholars analyse diplomacy through ethnographic methods such as participant observation (cf. Adler-Nissen and Drieschova 2019; Neumann 2012). Knowledge production in this field tends to lean heavily on the texts that diplomatic processes create: the outcome of the international negotiation as well as the paper trail in domestic bureaucracies. De Orellana (2020, 473) maintains that while diplomacy cannot be reduced to text '(…) the text stands as the most highly useful and consistently produced evidence of diplomatic practices.' But it generally takes time. Many of the documents needed for analysis are classified and archived in the various countries involved and the passage of time adds context and insight as to how and why certain agreements proved valuable, fleeting or even destructive. Until that time of ex-post analysis, a successful diplomatic trajectory is often measured by the negotiated text or the absence thereof. The treaty or the published consensus report is often considered the holy grail of diplomacy, even though ultimately it is a means rather than an end in itself.

Cyber diplomacy at the UN – focusing on the UN's First Committee – is one of these processes that has been analysed by researchers almost in real time, and under conditions of limited access and sources. Analysing ongoing diplomatic processes is a mixture of reading texts and tea leaves. In the case of UN cyber diplomacy we saw some change in 2019 on account of the addition of a new and more transparent process – the Open Ended Working Group (OEWG) – to the existing format of the UN Group of Government Experts (UN GGE) that deliberates behind closed doors and only 'speaks' through the consensus report it produces, or fails to produce. During the 2019–2021 negotiations of the UN GGE and the OEWG I served as an academic advisor and member of the Dutch delegation. While taking part in those negotiations did not get me any academic footnotes, because of confidentiality, it did help my understanding of the limits, possibilities and oddities of the process.

Text: consensus reports

Until 2019 the UN negotiations on 'responsible state behaviour in cyberspace' have been characterised by a very limited paper trail – the accumulated consensus reports – that is, the main source for understanding the early years of cyber diplomacy at the UN. The UN convened six Groups of Governmental Experts between 2004 and 2021, of which four produced a consensus report (in 2010, 2013, 2015 and 2021). The OEWG also produced a consensus report in 2021 and currently there is a new OEWG ongoing. These five reports are

our main source on the state of the art of UN cyber diplomacy as they are consensus documents endorsed by their respective memberships. Scholars have analysed these documents in light of existing international law (Delerue 2020), normative theory (Finnemore and Hollis 2016) and of the politics of international (cyber) security (Broeders 2021; Grigsby 2017). However, the point here is not so much the content of these reports, but rather that this is *how* the 'cyber diplomatic community' speaks to us, as citizens and as researchers. The report speaks for itself and we hear very little about the negotiating process, the (initial) positions of states, the divisions, disagreements and band wagoning, or the issues that were raised but didn't make the cut of the report.

With the recent addition of the more transparent process of the OEWG, researchers suddenly have more text, public meetings, and recordings (such as those of the UN WebTV) to analyse. The formal sessions of the OEWG are conducted in public and, importantly, many UN member states provided written inputs into the process. Various drafts of the report were made publicly available and member states produced written comments on those drafts, which are publicly available.[1] Some delegations that were part of both the UN GGE and the OEWG explicitly stated that their input papers were meant for both processes. With this, cyber diplomacy for the first time produced something of a repository of 'traveaux preperatoires' for its negotiated text. These documents are now starting to make their way into the academic analysis (Broeders 2021; Broeders et al. 2022; Levinson 2021). However, we should be careful to avoid looking for our lost keys under the streetlight just because that is where the light shines. Nor should we take everything we read at face value: reading text is often like reading tea leaves.

Tea leaves: interpreting texts and actors

Even though the OEWG documents crack open the black box of diplomacy, we do not and cannot know how much of the deliberations we get to see. The public formal sessions and input papers – while new and valuable – should also keep analysts on their toes. In terms of text we have to read between the lines and connect written contributions with the larger picture: which information we can take at face value? Which information is strategic or even misleading? Just as important: which information is missing? Some states will refrain from submitting a written contribution as a negotiation strategy, to avoid binding their hands, to allow themselves time to think, or to keep options open and have room to manoeuvre.

Making diplomatic text is also an opaque process, even when you are in the room. During the UN negotiations I had some 'skin in the game' as I originally coined the idea of a norm calling for the protection of the public core of the internet in 2015, which was now one of the priorities of the Dutch delegation in the process (Broeders 2015). Following up close how a layered, complex idea and norm proposal – refined and elaborated on by many others since 2015 – was 'translated' into a few lines in the reports was both a clarifying and a sobering experience. Diplomacy is often the art of what is possible and is reliant on context, political (un)will and tenacity. Being on the inside makes it clear how much is hidden behind the text.

In addition to differences in strategy, diplomatic capacity varies wildly between states – not in the least in the relatively young field of cyber diplomacy – and it shows. Opening cyber diplomacy up to all UN member states in the OEWG does not mean all will come,

speak and contribute in equal measures. States with more resources and a diplomatic track record on these issues are more likely to put their contributions on paper, while less experienced states may make up their minds as the process unfolds without submitting a written contribution. That also means that the paper trail may show inflated support for some proposals and underestimate the support for others (Broeders 2021, 291). Just because there is text, does not mean we are not still reading tea leaves sometimes.

As De Orellana (2020, 472) puts it: 'Diplomacy is, however, far more than text.' For knowledge production beyond text, the interview is the classic tool, but access to diplomats is often a problem, especially for junior scholars and those new to the field. Moreover, diplomacy and secrecy go hand in hand, as diplomacy is one aspect of statecraft that is generally – and legitimately – considered to function better if it is shielded from public scrutiny. However, the digital age has not been kind to state secrecy, making it easier for states to gather information (and compile more secrets), yet harder to keep secrets safe as a result of hacks and leaks (Broeders 2016). Information tends to come out into the open faster than it used to, a phenomenon that Swire (2015) has dubbed 'the declining half-life of secrets', adding new information for analysts. But diplomats contribute to that themselves too.

The digital age, amplified by the online leap that COVID-19 provided, has added new sources of knowledge production (Eggeling and Adler-Nissen 2021). Online conferencing, amplified by the pandemic, meant that some, mostly Western, cyber diplomats could increasingly be found online. Conferences, panels, round tables and other discussions were live streamed and recorded, and diplomats also engaged in other digital forms of communication, such as Twitter and podcasts, to engage and spread the word. In terms of knowledge production it pays to dig into this digital material as well. While some diplomats are so 'on message' they sound like a broken record, some genuinely engage and give sneak peeks into the diplomatic process and the negotiating rooms. Podcasts now land in the footnotes of my academic writing.[2]

Analysing contestation

In terms of the politics of knowledge production, we are in dire need of new frameworks and sources. The study of cyber diplomacy is heavily skewed towards the like-minded countries. Furthermore, the dominant frame for analysis of cyber diplomacy is the rivalry between the (western) like-minded countries and authoritarian countries like Russia and China. Although this frame captures a substantial part of reality, it also paints the world with too broad a brush. With the OEWG all UN members were invited into the tent of cyber diplomacy. With that interests, stakes and opinions have multiplied – even if that does not necessarily surface in diplomatic speech and text yet. For example, many countries are more interested in discussing the global digital divide than the application of international law in cyberspace. Some countries are also balking at the process itself, which they consider to be dominated by the West and founded on a model in which the West diffuses 'good' liberal norms to the rest of the world (Kurowska 2019). In the coming years 'norms diffusion' will have to give way to more productive forms of 'norms contestation' in cyber diplomacy or the process is likely to stall. That process is (also) part of wider academic and multi-stakeholder deliberations and proposals, but the translation into the diplomatic context will be the diplomat's

task. For analysts of diplomacy it means we will need better frameworks and better sources to capture the dynamics of that process as it unfolds.

Practising reflexivity when researching military and intelligence cybersecurity. Tobias Liebetrau

The study of military and intelligence cybersecurity continues to be dominated by realist and strategic studies. To encourage future scholarship to engage, question, and move beyond the theoretical and methodological assumptions of this research, I build a case for reflecting on the role of the researcher in producing (knowledge about) military and intelligence cybersecurity. In this way, I strive to make a double move by exhibiting ways to practise reflexivity and supporting reflexivity-as-critique (Amoureux and Steele 2015).

I demonstrate how a practice of reflexivity can help cybersecurity researchers foreground, reflect on, and examine the ways in which knowledge production conditions what cybersecurity is and what it can become. I draw out five features that condition reflexive military and intelligence cybersecurity knowledge production: secrecy, technology, relationality, enactments of security and the political nature of knowledge production. These features demonstrate how practising reflexivity allows for continuous questioning of what cybersecurity is, where it is located, for whom, and how. Increased reflexive sensitivity thereby facilitates critical engagement with otherwise often elusive aspects of knowledge making processes in cybersecurity research. The goal of the intervention, however, is not to help reach a superior formulation of the reality of cybersecurity, or of the ways in which cybersecurity is real (or not), but to interfere with the idea of apparently singular and stable subjects and objects that dominates the current research on military and intelligence cybersecurity.

Researching military and intelligence cybersecurity: five features of practising reflexivity and critique

Secrecy is a basic condition in the study of security (De Goede and Pallister-Wilkins 2019). In the study of military and intelligence cybersecurity, documents are usually classified, information is confidential, and doors are hermetically sealed (Liebetrau 2022). A starting point for reflexivity is then to acknowledge that secrecy mediates our research practices. Secrecy is produced and generates political effects. This encourages scholars to reflect on secrecy not only as a problem generating given but as performed and performative. The performativity of secrecy must itself become subject to reflexivity. One way to foster such reflexivity is to give thought to how the production and effects of secrecy relates to absent, ignored or marginalised forms of knowledge.

In addition, military and intelligence cybersecurity exemplify how technology is both a tool to produce security and an object of security concern. Researching it is infused with technical practices, terms and expressions. Knowledge making vis-a-vis cybersecurity practices is not simply a question of accomplishments of human intent and relations. It is also the outcome of socio-technical relations and more-than-human computational processes. A reflexive approach emphasises the co-constitutive dynamic of technology and materiality and pays attention to the role of the researcher

in inquiring on the self and the research process in relation to the dynamic socio-technical relations. It requires researchers to recognise how their research process apprehends these relations.

This implies that knowledge production does not happen in a vacuum. As researchers, we must continuously navigate, assess, and decide what we want to study, how we do it, what we reveal, how we do that, and why we do it, while keeping in mind that 'all observation is embedded and embodied' (Leander 2016, 464). Knowledge-making processes in cybersecurity research are relational, dynamic and uncertain. The relationship between researcher-research-researched is never fully given or determined. Nurturing reflexive sensitivity to the conditions of secrecy and sociotechnical relations, can help us distance ourselves from both the totalising and the relativist vision/position that Donna Haraway has deemed the god trick 'promising vision from everywhere and nowhere equally and fully' (Haraway 1991, 191). Acknowledging that knowledge production is a situated and partial practice co-constituted in researcher-research-researched relations, implies recognising that no theory or method will allow us to convey the essence of military and intelligence cybersecurity.

A central discussion in critical security studies revolves around the normative dilemma of studying security. It confronts the researcher with 'how to write or speak about security when the security knowledge risks the production of what one tries to avoid, what one criticizes' (Huysmans 2002, 43). While there is no way of completely circumventing this dilemma when researching military and intelligence cybersecurity, reflexively engaging with it encourages researchers to develop thinking tools and strategies to deal with potential pitfalls of reproduction and cooptation and to expose how academic knowledge-making practices co-constitute what military and intelligence is and is not. Reflecting on how we craft our research objects and subjects is hence core to critically minded cybersecurity research.

It is, however, 'also limited, insofar as it leaves the objectifying subject, that is, the researcher themselves and the conditions of possibility of their research practices, untouched' (Jeandesboz 2018, 24). This disposition is problematic since it overlooks how security is co-created between the researcher and the researched in a dynamic process (Austin, Bellanova, and Kaufmann 2019; Evans, Leese, and Rychnovská 2021; Kurowska and Tallis 2013). It is important to reflect on how this process plays out and to what implications make reflexivity a significant concern in, and an integral part of, the research process. It is central that the study of military and intelligence cybersecurity – as practice, discourse, relation, mode of governance or political ordering – is accompanied with an effort from scholars to be reflexive about and examine their own knowledge-producing practices. Not with the goal to automatically thrash security and reveal the truth with capital T, but rather to display how knowledge-making practices are both shaped by and shape research objects and subjects.

This points to how research practices are more than (epistemological) interpretations and representations of the world. They are (ontological) enactments of it, and performative interventions in it. Whatever knowledge-producing practice a researcher engages in, it is never solely describing and interpreting the world; it is simultaneously bringing it into being (Liebetrau and Christensen 2021). Producing knowledge about military and intelligence cybersecurity thereby opens spaces for political intervention. Defining what cybersecurity politics is (and what is not) is itself a political intervention. Consequently, as Law

(2002, 11) has put it, 'the hands of the storyteller are never clean.' I revisit below my experience of becoming a storyteller.

Practising reflexivity: becoming a military and intelligence cybersecurity researcher

I illustrate the value of practising reflexivity by telling a story of my emergent reflexive practices concerned with becoming a researcher and knowledge creator in the field of military and intelligence cybersecurity. This story is meant as an invitation for researchers to actively reflect on and ask questions about our role in producing (knowledge about) military and intelligence cybersecurity.

In 2015, I wrote a PhD application with the goal to study US and European cybersecurity governance. At the time, I was working with cybersecurity at the Danish Defence Intelligence Service. Writing the application, I asked myself a bunch of questions concerning positionality: How to make my experience as a practitioner relevant for the University of Copenhagen? How to make use of my experience in framing the project/research without compromising colleagues and classified knowledge? How to distinguish between classified and non-classified information? How to be (accepted as) a critical security studies scholar when having been a 'professional manager of unease' (Bigo 2002)? How to be a critical security studies scholar and sustain my connection to my former colleagues?

These initial questions demonstrate the quandaries about becoming an analyst that a reflexive approach motivates. They were crucial in developing my research practice and engaging with the politics of researching cybersecurity. The relevance, wording, and character of questions such as these will differ across scholars, contexts and conditions. However, identifying them is a way to activate reflexivity and initiate a process of formulating strategies and thinking tools for addressing dilemmas of situatedness, positionality and the politics of knowledge creation.

The job gave me privileged access to what would later become my field of research. I experienced the quotidian and tacit processes of cybersecurity intelligence knowledge production, as well as the negotiations and translations between technical, military, legal and policy practitioners. This raised questions of how to navigate congruent, overlapping, and conflicting practices of and claims to what military and intelligence cybersecurity is. I mobilised these insights when conducting postdoctoral research in 2019 on the issue of cyberconflict, short of war. My former employment and experience with the different practices and truth claims at play in the practice of military and intelligence cybersecurity, helped me to prepare the research, gain access, and navigate interview situations. The practice of reflexivity cultivated engagement with military and intelligence cybersecurity on the premise of the coexistence of different ways of framing concerns, handling problems, and enacting reality, as well as the security politics this produces.

By translating and navigating between the technical, legal and policy departments in writing up incident reports on attacks on critical infrastructure, instructions for better protection of critical computational systems and political speeches, I was enmeshed in how various rationales and human and non-human elements came together to produce (conditions of possibility for) military and intelligence cybersecurity practices. This experience as practitioner and analyst gave me in-depth understanding of the

formation of sociotechnical relations, hypothesis, questions, analysis, classifications, controversies and regulations it took for cybersecurity to become known, for it to stabilise, and singularise.

Yet, these experiences also gave me blind spots. They steered my gaze, made me prone to reproducing certain discourses, and disposed of cooptation. The enmeshment, however, also made me less inclined to impose the vision from everywhere and nowhere that Haraway (1991) warns about. Today, my experiences continue to foster reflection on the challenges, opportunities and limitations of exercising critique from within (or perhaps more precisely from inside-out and outside-in). The distinctions between information and knowledge, technical and social, legal and illegal, and public and secret are not set in stone, but entails dynamic negotiation, translation and contestation in which research practices play an active part. The conditioning effects of my experiences are dynamic rather than static. They are relational, situated and contextual. My vantage point changes in dialogue with a vibrant research field and academic career. Hence, there is even more reason to sustain a practice of reflexivity in the pursuit of giving thought to what that which we do does.

Half-truths and home truths: instrumentalization, suppression, and manipulation in cybersecurity research. James Shires

This final contribution interrogates my experiences of cybersecurity knowledge production practices, especially regarding the extent to which such practices can be instrumentalised for commercial or political ends. The instrumentalisation of research is at once a 'taken-for-granted' aspect of highly policy-relevant fields such as cybersecurity, and one that is rarely mentioned in formal settings. Knowledge is rarely, if ever a static thing to be gained or possessed, and instead emerges through performance, enactment and practice (Bueger 2015; Schatzki, Knorr-Cetina, and Von Savigny 2000). Consequently, the practices of knowledge production concern the identities, habits, rituals and routines of the knowers/producers – both human and machine (Hayles 1999; Latour 2007).

As a personal reflection on the practice of knowledge production, this article engages in autoethnography in two ways (Adams, Ellis, and Jones 2017): first, as a study of a group in which the author is a member (i.e. academic cybersecurity researchers); and second, as ethnographic study of oneself. Despite critiques of 'retreat' into the 'narcissistic substitution of auto-ethnography for research' (Delamont 2009, 51–61), the reflexive and relational practice exemplified by autoethnography is essential to ethical, rigorous research (Denshire 2014). I combine what Anderson calls 'analytic autoethnography', which is 'focused on improving theoretical understandings of … social phenomena' (Anderson 2006, 375), with the critical purpose of many ethnographers: to 'speak against, or provide alternatives to, dominant, taken-for-granted, and harmful … scripts, stories, and stereotypes (Adams, Ellis, and Jones 2017, 3).

Positionality is central to (auto)ethnography. My identity as a White, heterosexual man, associated with prestigious Western universities with problematic colonial ties, has influenced my research (Shires 2018). I conducted much research in a region with a long and complicated quasi-colonial history, including even its designation as the 'Middle East' (Lockman 2009). I thus acknowledge the significant limits of my autoethnographic practice, *and* that simply making such an acknowledgment does little to address

global inequalities and power balances in cybersecurity, or to open it to a more diverse, intersectional, range of voices (Slupska 2019).

The clearest form of instrumentalisation is commodification. Budding researchers climb a rickety career ladder, passing from financial precarity, geographical mobility and intellectual self-doubt, to relative financial stability, disciplinary comfort and bureaucratic immersion. While the traditional mode of academic knowledge production is peer-reviewed publications, these are by far the minority of most cybersecurity researchers' output – whether measured by words, venues or number of readers. Cybersecurity researchers write in blogs, policy papers, media commentary, course materials and of course, social media posts. Although they do some of this work for 'free' (reputational pay-off notwithstanding), there is usually a financial incentive. In short, and to nobody's surprise, researchers are paid to do research.

The obvious question, then, is how funding sources affect research *content*. Academic institutions have well-established protocols to insulate researchers from undue influence (although, as Fouad shows in this issue, they introduce significant constraints on (re)conceptualising cybersecurity). For example, I was unaware that my post-doctoral position on cybersecurity in the Middle East was funded by a Gulf government until near the end of that position. Indeed, during the position, I had written articles critically examining cyber operations in and by Gulf states that were not highlighted in the final funder's report (Shires 2019). However, funding structures are rarely so helpfully opaque, and such opacity is often due to bureaucratic impenetrability rather than any more lofty ideal. In my experience, the influence of a company or government on a particular piece of research or research position is usually more subtle than direct pressures on content, concerning more which kinds of projects go ahead and which are left unpursued.

In cybersecurity, where individuals working for corporations produce as much, if not more, research than academics, questions arise around which kinds of instrumentalisation are considered acceptable and therefore naturalised in the expert community. For example, I co-authored an intervention with a US think tank in the highly charged policy debate around export control of offensive cyber capabilities (DeSombre et al. 2021). The (unpaid) think-tank authors included journalists, academics, cybersecurity researchers with corporate connections and former government officials. After the report was published, among the criticisms was the suggestion that the authors were guns-for-hire, implying that the content of the report, and especially its policy recommendations, were at least partly dictated by the think tank itself or their donors. This suggestion came from individuals working in the industry developing offensive cyber capabilities for corporate gain. Here, a clear conflict of interest (exporters criticising a report recommending export control) went unnoticed, while a mistakenly perceived conflict of interest (payment for a think tank report) became a subject of debate. Accusations of instrumental research come from surprising places.

Moving beyond financial gain, and as my colleagues have observed above, the symbiotic relationship between cybersecurity academics and their corporate or governmental counterparts creates significant anxiety about knowledge production: what if my interlocutors disagree with my conclusions? What if I represent them incorrectly or unjustly in my work? Fear of exclusion or repercussion may influence knowledge production practices as much as financial incentives. I have noticed such issues in work with a European NGO researching cyber conflict. The NGO's work has prompted considerable reflection

about its European identity: is its purpose external, to define European views *against* US, Asian or other regions? Or is it internal, to identify among disparate European states a common approach or set of values underlying cyber policy? Of course, the answer is a bit of both; but this question has been thrown into sharp relief by Russia's horrendous war in Ukraine and the human rights violations involved (Kaminska, Shires, and Smeets 2022). Practices of knowledge production here are tied up with broader questions of regional identity.

Any adverse consequences faced by European academics in producing cybersecurity knowledge pale in comparison to those faced by their colleagues elsewhere in the world, where journalistic and academic freedoms can be highly limited. While I was conducting my doctoral research on cybersecurity in the Middle East, an Italian PhD student, Giulio Regini, was tortured and murdered by the Egyptian security services, and a British PhD student, Matthew Hedges, was imprisoned for six months in the UAE after one of his interviewees reported him to the UAE security services (Michaelson and Tondo 2020; Parveen 2018). These are the potential consequences for foreign researchers, who work under comparatively strong diplomatic and cultural protection. Researchers working in or on their own countries are subject to many severe constraints on knowledge production, ranging from the blunt and brutal to the subtle and insidious.

How did I deal with these risks? The simple answer is by getting approval from university research committees, but this is a small part of the solution. Such approval depends on a self-assessment of the risks, as the researcher often knows far more about the topic than those approving the research. During my fieldwork, I and my interlocutors were both hyper-aware of the risks created by our interaction, whether from suspicion of me directly or the risk that third parties could seek to access my data. More generally, in working with researchers in and from the region, I have sought to navigate the line between providing 'cover' for assertions they do not feel comfortable putting their name to, and ensuring that they receive appropriate credit for their excellent work. Foreign associations (especially with the 'West') can range from being a source of significant credibility to being highly dangerous, especially when governments view international NGOs and universities as vehicles for foreign espionage.

I have experienced informal censorship in academic and policy papers written for regional audiences many times, where cautious editors remove or alter sections that they deem to be sensitive, with no discussion or notification. When speaking at panels and conferences, similar requests are often made, such as to only cover certain states or issues. This was especially the case during the most recent Gulf crisis, with Egypt, the UAE, Saudi Arabia, and Bahrain boycotting Qatar, as my cybersecurity research was conducted in all these countries during this time.

Colonial structures and hierarchies of knowledge production have both facilitated and limited my research. During my research, interviewees frequently assumed that I was working for a commercial company or foreign government purely due to my appearance. As I have argued elsewhere, in the Gulf 'race operates as a marker of who in cybersecurity is a legitimate knower and who is not, and therefore whose understandings, experiences, and practices of cybersecurity are privileged' (Mumford and Shires forthcoming, 36).

I conclude with two less obvious aspects of instrumentalisation in cybersecurity research. First, the ambiguities of cybersecurity – its scope, disciplinary home(s), history

and appropriate policy audiences – have been a key subject of my research, especially in terms of the 'moral manoeuvres' that states and other actors perform to obtain strategic advantage from redefining cybersecurity in different ways (Shires 2021). However, I have also *deployed* the ambiguities around cybersecurity strategically: whether to reduce the risks of sensitive research in constrained settings, or provide a common thread when pivoting between different topics (or, as Fouad demonstrates in this issue, to teach cybersecurity topics). In this, my own performance of cybersecurity knowledge mirrors that of cybersecurity practitioners more than I'd like to admit.

Second, I have developed a useful but frustrating skill of writing about something while also *not* writing about it. The language used in this piece is deliberately vague – 'a Gulf government', 'a think tank', 'an NGO', 'an interlocutor', and so on. The obvious reason is to avoid naming entities who may not thank me for their inclusion, and more widely, for authors to circumvent commercial or governmental classification, NDAs and other restrictions. But it is also a style of writing and thinking that permeates cybersecurity to the extent that many researchers produce knowledge consisting of half-truths, half-empirics and half-secrets, almost automatically. One can see this impulse to keep something back, to retain the upper hand, as integral to cybersecurity knowledge as currently practiced; I hope for and consciously work towards a form of cybersecurity knowledge that is more honest, more frank and more vulnerable.

Notes

1. See: https://www.un.org/disarmament/open-ended-working-group/. This website also contains the contributions of Inter-governmental Organizations (IGOs) and Non-Governmental Organizations (NGOs) to the process.
2. For example, the podcast series *Inside Cyber Diplomacy* which interviews – predominantly likeminded – cyber diplomats involved in the 2019–2021 rounds of the GGE and OEWG.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Fabio Cristiano is Assistant Professor in Conflict Studies at Utrecht University and Associate Fellow of The Hague Program on International Cybersecurity. He is the co-editor of *Artificial Intelligence and International Conflict in Cyberspace* (Routledge, 2023) and *Hybridity, Conflict, and the Global Politics of Cybersecurity* (Rowman and Littlefield, 2023).

Xymena Kurowska, Associate Professor of International Relations, is a social theorist who teaches at Central European University and analyses contemporary global politics, including global cyber relations, from an interpretive perspective.

Tim Stevens is Reader in International Security at the Department of War Studies, King's College London and Director of the KCL Cyber Security Research Group. His recent books include *What is Cybersecurity For?* (Bristol University Press, 2023) and *Research Handbook on Cyberwarfare* (Edward Elgar, 2024).

Louise Marie Hurel is a Research Fellow in the Cyber team at RUSI. Her research interests include incident response, cyber capacity building, cyber diplomacy and non-governmental actors' engagement in cyber security.

Noran Shafik Fouad is a Lecturer in Digital Politics at Manchester Metropolitan University. Her research lies at the intersection of technology, security, and governance, and her interests include cybersecurity, critical security studies, securitisation, risk theories, philosophy of information, and software studies.

Myriam Dunn Cavelty is Senior Lecturer and Deputy Head of Research and Teaching at the Center for Security Studies (CSS), ETH Zurich, Switzerland. She is the author of 'Cyber-Security and Threat Politics: US Efforts to Secure the Information Age' (Routledge 2008) and many other articles and books on the politics of cyber-security.

Dennis Broeders is Full Professor of Global Security and Technology at the Institute of Security and Global Affairs (ISGA) of Leiden University, the Netherlands. He is the Senior Fellow of The Hague Program on International Cyber Security and project coordinator at the EU Cyber Direct Program.

Tobias Liebetrau is a researcher at the Centre for Military Studies, University of Copenhagen. His research covers cybersecurity, infrastructure, digital technology, and the role of Big Tech in international politics.

James Shires is Co-Director of the European Cyber Conflict Research Initiative (ECCRI) and the European Cyber Conflict Research Incubator (ECCRI CIC). He is the author of *The Politics of Cybersecurity in the Middle East* (Hurst/Oxford University Press, 2021), and co-editor of *Cyberspace and Instability* (Edinburgh University Press, 2023).

ORCID

Fabio Cristiano http://orcid.org/0000-0002-0951-9648
Xymena Kurowska http://orcid.org/0000-0002-0182-7638
Tim Stevens http://orcid.org/0000-0001-6869-8810
Dennis Broeders http://orcid.org/0000-0002-8827-2814
James Shires http://orcid.org/0000-0002-7481-4037

References

Adams, Tony E., Carolyn Ellis, and Stacy Holman Jones. 2017. "Autoethnography." The International Encyclopedia of Communication Research Methods: 1–11. https://doi.org/10.1002/9781118901731.iecrm0011.

Adler, Emanuel. 1997. "Imagined (Security) Communities: Cognitive Regions in International Relations." *Millennium* 26 (2): 249–277. https://doi.org/10.1177/03058298970260021101.

Adler-Nissen, Rebecca, and Alena Drieschova. 2019. "Track-change Diplomacy: Technology, Affordances, and the Practice of International Negotiations." *International Studies Quarterly* 63 (3): 531–545. https://doi.org/10.1093/isq/sqz030.

Amoureux, Jack L., and Brent J. Steele, eds. 2015. *Reflexivity and International Relations: Positionality, Critique, and Practice*. New York: Routledge.

Anderson, Leon. 2006. "Analytic Autoethnography." *Journal of Contemporary Ethnography* 35 (4): 373–395. https://doi.org/10.1177/0891241605280449.

Aradau, Claudia. 2017. "Assembling (non) Knowledge: Security, Law, and Surveillance in a Digital World." *International Political Sociology* 11 (4): 327–342. https://doi.org/10.1093/ips/olx019.

Aradau, Claudia, Jef Huysmans, Andrew Neal, and Nadine Voelkner. 2015. *Critical Security Methods. New Frameworks for Analysis*. London: Routledge.

Arday, Jason, Dina Zoe Belluigi, and Dave Thomas. 2021. "Attempting to Break the Chain: Reimaging Inclusive Pedagogy and Decolonising the Curriculum Within the Academy." *Educational Philosophy and Theory* 53 (3): 298–313. https://doi.org/10.1080/00131857.2020.1773257.

Arquilla, John, and David Ronfeldt. 1993. *Cyberwar is Coming!*. Santa Monica: RAND Corporation.

Asmolov, Gregory. 2021. "From Sofa to Frontline: The Digital Mediation and Domestication of Warfare." *Media, War & Conflict* 14 (3): 342–365.

Austin, Jonathan Luke, Rocco Bellanova, and Mareile Kaufmann. 2019. "Doing and Mediating Critique: An Invitation to Practice Companionship." *Security Dialogue* 50 (1): 3–19. https://doi.org/10.1177/0967010618810925.

Balzacq, Thierry, and Myriam Dunn Cavelty. 2016. "A Theory of Actor-Network for Cyber-Security." *European Journal of International Security* 1 (2): 176–198. https://doi.org/10.1017/eis.2016.8.

Basen, Nathaniel. 2021. "X-ray on the Abuse of Power.": Citizen Lab's Founder on Fighting for Human Rights. *TVO Today*, May 25, 2021. https://www.tvo.org/article/x-ray-on-the-abuse-of-power-citizen-labs-founder-on-fighting-for-human-rights.

Bellanova, Rocco, Katja Lindskov Jacobsen, and Linda Monsees. 2020. "Taking the Trouble: Science, Technology and Security Studies." *Critical Studies on Security* 8 (2): 87–100. https://doi.org/10.1080/21624887.2020.1839852.

Belli, Luca. 2021. *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Cham: Springer International Publishing.

Berling, Trine Villumsen, and Christian Bueger. 2015. *Security Expertise: Practice, Power, Responsibility*. London: Routledge.

Betz, David, and Tim Stevens. 2013. "Analogical Reasoning and Cyber Security." *Security Dialogue* 44 (2): 147–164. https://doi.org/10.1177/0967010613478323.

Bigo, Didier. 2002. "Security and Immigration: Toward a Critique of the Governmentality of Unease." *Alternatives* 27 (1): 63–92. https://doi.org/10.1177/03043754020270S105.

Bilgic, Ali, Mandeep Dhami, and Dilek Onkal. 2018. "Toward a Pedagogy for Critical Security Studies: Politics of Migration in the Classroom." *International Studies Perspectives* 19 (3): 250–266. https://doi.org/10.1093/isp/ekx016.

Broeders, Dennis. 2015. *The Public Core of the Internet: An International Agenda for Internet Governance*. Amsterdam: Amsterdam University Press.

Broeders, Dennis. 2016. "The Secret in the Information Society." *Philosophy & Technology* 29 (3): 293–305. https://doi.org/10.1007/s13347-016-0217-3.

Broeders, Dennis. 2021. "The (Im)Possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG: A Mid-Process Assessment." *Journal of Cyber Policy* 6 (3): 277–297. https://doi.org/10.1080/23738871.2021.1916976.

Broeders, Dennis, Els de Busser, Fabio Cristiano, and Tatiana Tropina. 2022. "Revisiting Past Cyber Operations in Light of New Cyber Norms and Interpretations of International Law: Inching Towards Lines in the Sand?" *Journal of Cyber Policy* 7 (1): 97–135. https://doi.org/10.1080/23738871.2022.2041061.

Buchanan, Ben. 2016. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. London: Hurst.

Bueger, Christian. 2015. "Making Things Known: Epistemic Practices, the United Nations, and the Translation of Piracy." *International Political Sociology* 9 (1): 1–18. https://doi.org/10.1111/ips.12073.

Burton, Joe, and Clare Lain. 2020. "Desecuritising Cybersecurity: Towards a Societal Approach." *Journal of Cyber Policy* 5 (3): 449–470. https://doi.org/10.1080/23738871.2020.1856903.

Buzan, Barry. 2000. "'Change and Insecurity' Reconsidered." In *Critical Reflections on Security and Change*, edited by Stuart Croft, and Terry Terriff, 1–17. Abingdon: Routledge.

Buzan, Barry, and Lene Hansen. 2009. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Calderaro, Andrea, and Anthony J. S. Craig. 2020. "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building." *Third World Quarterly* 41 (6): 917–938. https://doi.org/10.1080/01436597.2020.1729729.

Chadwick, Rachelle. 2021. "On the Politics of Discomfort." *Feminist Theory* 22 (4): 556–574. https://doi.org/10.1177/1464700120987379.

Chamon, Paulo. 2018. "Turning Temporal: A Discourse of Time in IR." *Millennium: Journal of International Studies* 46 (3): 396–420. https://doi.org/10.1177/0305829818774878.

Coles-Kemp, Lizzie, Debi Ashenden, and Kieron O'Hara. 2018. "Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen." *Politics and Governance* 6 (2): 41–48. https://doi.org/10.17645/pag.v6i2.1333.

Collective, C. A. S. E. 2006. "Critical Approaches to Security in Europe: A Networked Manifesto." *Security Dialogue* 37 (4): 443–487. https://doi.org/10.1177/0967010606073085.
Collective, C. A. S. E. 2007. "Europe, Knowledge, Politics—Engaging with the Limits: The Case Collective Responds." *Security Dialogue* 38 (4): 559–576. https://doi.org/10.1177/0967010607085002.
Cristiano, Fabio. 2018a. "From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises." *Journal of War & Culture Studies* 11 (1): 22–37. https://doi.org/10.1080/17526272.2017.1416761.
Cristiano, Fabio. 2018b. "Bodies of Cyberwar: Violence and Knowledge Beyond Corporeality." In *Experiences in Researching Conflict and Violence*, edited by Althea-Maria Rivas and Brendan Ciarán Browne, 145–160. London: Policy Press. https://doi.org/10.1332/policypress/9781447337683.003.0011.
Cristiano, Fabio. 2022. *The Blurring Politics of Cyber Conflict: A Critical Study of the Digital in Palestine and Beyond*. Lund: MediaTryck.
Cristiano, Fabio and Bibi van den Berg. 2023. *Hybridity, Conflict, and the Global Politics of Cybersecurity*. Lanham: Rowman & Littlefield.
De Goede, Marieke. 2018. "The Chain of Security." *Review of International Studies* 44 (1): 24–42. https://doi.org/10.1017/S0260210517000353.
De Goede, Marieke. 2020. "Engagement all the Way Down." *Critical Studies on Security* 8 (2): 101–115. https://doi.org/10.1080/21624887.2020.1792158.
De Goede, Marieke, Esme Bosma, and Polly Pallister-Wilkins, eds. 2019. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*. London: Routledge.
De Orellana, Pablo. 2020. "Retrieving How Diplomacy Writes Subjects, Space and Time: A Methodological Contribution." *European Journal of International Relations* 26 (2): 469–494. https://doi.org/10.1177/1354066119868514.
Deibert, Ronald. 2018. "Toward a Human-Centric Approach to Cybersecurity." *Ethics & International Affairs* 32 (4): 411–424. https://doi.org/10.1017/S0892679418000618.
Delamont, Sara. 2009. "The Only Honest Thing: Autoethnography, Reflexivity and Small Crises in Fieldwork." *Ethnography and Education* 4 (1): 51–63. https://doi.org/10.1080/17457820802703507.
Delerue, François. 2020. *Cyber Operations and International Law*. Cambridge: Cambridge University Press.
Denshire, Sally. 2014. "On Auto-Ethnography." *Current Sociology* 62 (6): 831–850. https://doi.org/10.1177/0011392114533339.
DeSombre, Winnona, James Shires, J. D. Work, Robert Morgus, Patrick Howell O'Neill, Luca Allodi, and Trey Herr. 2021. *Countering Cyber Proliferation: Zeroing in on Access-as-a-Service*. Washington, DC: Atlantic Council Cyber Statecraft Initiative.
Dunn Cavelty, Myriam. 2008. *Cyber Security and Threat Politics: Us Efforts to Secure the Information Age*. London: Routledge.
Dunn Cavelty, Myriam. 2018. "Cybersecurity Research Meets Science and Technology Studies." *Politics and Governance* 6 (2): 22–30. https://doi.org/10.17645/pag.v6i2.1385.
Dunn Cavelty, Myriam, and Andreas Wenger. 2022. *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*. London: Taylor & Francis.
Dwyer, Andrew. 2021. "Cybersecurity's Grammars: A More-Than-Human Geopolitics of Computation." *Area* 55 (1): 10–17. https://doi.org/10.1111/area.12728.
Dwyer, Andrew, Clare Stevens, Lilly Pijnenburg Muller, Myriam Dunn Cavelty, Lizzie Coles-Kemp, and Pip Thornton. 2022. "What Can a Critical Cybersecurity Do?" *International Political Sociology* 16 (3): 13. https://doi.org/10.1093/ips/olac013.
Eggeling, Kristin Anabel, and Rebecca Adler-Nissen. 2021. "The Synthetic Situation in Diplomacy: Scopic Media and the Digital Mediation of Estrangement." *Global Studies Quarterly* 1 (2): 5. https://doi.org/10.1093/isagsq/ksab005.
Egloff, Florian J., and Myriam Dunn Cavelty. 2021. "Attribution and Knowledge Creation Assemblages in Cybersecurity Politics." *Journal of Cybersecurity* 7 (1): 2. https://doi.org/10.1093/cybsec/tyab002.

Egloff, Florian J., and James Shires. 2023. "The Better Angels of our Digital Nature? Offensive Cyber Capabilities and State Violence." *European Journal of International Security* 8 (1): 130–149. https://doi.org/10.1017/eis.2021.20.

Eriksson, Johan. 2001. "Cyberplagues, IT, and Security: Threat Politics in the Information Age." *Journal of Contingencies and Crisis Management* 9 (4): 200–210. https://doi.org/10.1111/1468-5973.00171.

Evans, Sam Weiss, Matthias Leese, and Dagmar Rychnovská. 2021. "Science, Technology, Security: Towards Critical Collaboration." *Social Studies of Science* 51 (2): 189–213. https://doi.org/10.1177/0306312720953515.

Finnemore, Martha, and Duncan B. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110 (3): 425–479. https://doi.org/10.1017/S0002930000016894.

Fouad, Noran Shafik. 2022. "The Non-Anthropocentric Informational Agents: Codes, Software, and the Logic of Emergence in Cybersecurity." *Review of International Studies* 48 (4): 766–785. https://doi.org/10.1017/S0260210521000681.

Fuchs, Christian. 2018. "Capitalism, Patriarchy, Slavery, and Racism in the Age of Digital Capitalism and Digital Labour." *Critical Sociology* 44 (4–5): 677–702. https://doi.org/10.1177/0896920517691108.

Georgieva, Ilina. 2019. "The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace." *Contemporary Security Policy* 41 (1): 33–54. https://doi.org/10.1080/13523260.2019.1677389.

Goertzen, Matt, and Gabriella Coleman. 2022. "Wearing Many Hats: The Rise of the Professional Security Hacker." *Data and Society*. January 14. https://datasociety.net/library/wearing-many-hats-the-rise-of-the-professional-security-hacker/.

Goldfarb, Avi, and Jon R. Lindsay. 2022. "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War." *International Security* 46 (3): 7–50. https://doi.org/10.1162/isec_a_00425.

Gomez, Miguel Alberto. 2021. "Overcoming Uncertainty in Cyberspace: Strategic Culture and Cognitive Schemas." *Defence Studies* 21 (1): 25–46. https://doi.org/10.1080/14702436.2020.1851603.

Grenier, Félix. 2016. "How Can Reflexivity Inform Critical Pedagogies? Insights from the Theory Versus Practice Debate." *International Studies Perspectives* 17 (2): 154–172. https://doi.org/10.1093/isp/ekv006.

Grigsby, Alex. 2017. "The End of Cyber Norms." *Survival* 59 (6): 109–122. https://doi.org/10.1080/00396338.2017.1399730.

Hansen, Lene. 2012. "Reconstructing Desecuritisation: The Normative-Political in the Copenhagen School and Directions for How to Apply it." *Review of International Studies* 38 (3): 525–546. https://doi.org/10.1017/S0260210511000581.

Hansen, Lene, and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53 (4): 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x.

Haraway, Donna J. 1991. *Simians, Cyborgs, and Women: The Reinvention of Nature*. New York: Routledge.

Haraway, Donna J. 2016. *Staying with Trouble: Making Kin in the Chthulucene*. London: Duke University Press.

Hassan, Robert. 2009. *Empires of Speed: Time and the Acceleration of Politics and Society*. Boston: Brill.

Hayles, N. Katherine. 1999. *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*. Chicago: University of Chicago Press.

Hom, Andrew. 2010. "Hegemonic Metronome: The Ascendance of Western Standard Time." *Review of International Studies* 36 (4): 1145–1170. https://doi.org/10.1017/S0260210510001166.

Hom, Andrew. 2018. "Silent Order: The Temporal Turn in Critical International Relations." *Millennium: Journal of International Studies* 46 (3): 303–330. https://doi.org/10.1177/0305829818771349.

Hom, Andrew. 2020. *International Relations and the Problem of Time*. Oxford: Oxford University Press.

Hurel, Louise Marie. 2022a. "Interrogating the Cybersecurity Development Agenda: A Critical Reflection." *The International Spectator* 57 (3): 66–84. https://doi.org/10.1080/03932729.2022.2095824.

Hurel, Louise Marie. 2022b. "Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America." *Global Security Review* 2 (1): 21–31. https://doi.org/10.25148/GSR.2.009786.

Huysmans, Jef. 2002. "Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security." *Alternatives* 27 (1): 41–62. https://doi.org/10.1177/03043754020270S104.

Huysmans, Jef. 2011. "What's in an Act? On Security Speech Acts and Little Security Nothings." *Security Dialogue* 42 (4-5): 371–383. https://doi.org/10.1177/0967010611418713.

Ish-Shalom, Piki. 2015. "Away from the Heart of Darkness: Transparency and Regulating the Relationships Between Security Experts and Security Sectors." In *Security Expertise*, edited By Trine Villumsen Berling and Christian Bueger, 244–260. London: Routledge.

Jackson, Patrick T. 2011. *The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics*. Abingdon: Routledge.

Jackson, Richard. 2015. "On How to be a Collective Intellectual: Critical Terrorism Studies and the Countering of Hegemonic Discourse." In *Security Expertise*, edited By Trine Villumsen Berling and Christian Bueger, 202–219. London: Routledge.

Jeandesboz, Julien. 2018. "Putting Security in its Place: Eu Security Politics, the European Neighbourhood Policy and the Case for Practical Reflexivity." *Journal of International Relations and Development* 21 (1): 22–45. . https://link.springer.com/article/10.1057jird.2015.11.

Kaminska, Monica, James Shires, and Max Smeets. 2022. "Cyber Operations during the 2022 Russian Invasion of Ukraine: Lessons Learned (so Far)." London: European Cyber Conflict Research Initiative (ECCRI). https://doi.org/10.3929/ethz-b-000560503.

Kappel, Klemens, and Sebastian Jon Holmen. 2019. "Why Science Communication, and Does it Work? A Taxonomy of Science Communication Aims and a Survey of the Empirical Evidence." *Frontiers in Communication* 55: 1–12. https://doi.org/10.3389/fcomm.2019.00055.

Kello, Lucas. 2021. "Cyber Legalism: Why it Fails and What to do About it." *Journal of Cybersecurity* 7 (1): 14. https://doi.org/10.1093/cybsec/tyab014.

Kirby, Paul. 2013. "The Unapologetic Schoolmaster." *Critical Studies on Security* 1 (3): 349–351. https://doi.org/10.1080/21624887.2013.850222.

Knill, Christoph, and Jale Tosun. 2011. "Policy-making." In *Comparative Politics*, edited by Daniele Caramani, 373–388. Oxford: Oxford University Press.

Kostyuk, Nadiya, and Yuri M. Zhukov. 2019. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63 (2): 317–347. https://doi.org/10.1177/0022002717737138.

Kurowska, Xymena. 2019. "The Politics of Cyber Norms: Beyond Norm Construction Towards Strategic Narrative Contestation." *EU Cyber Direct: Research in Focus* 18. https://eucyberdirect.eu/research/the-politics-of-cyber-norms-beyond-norm-construction-towards-strategic-narrative-contestation.

Kurowska, Xymena. 2020. "Interpreting the Uninterpretable: The Ethics of Opaqueness as an Approach to Moments of Inscrutability in Fieldwork." *International Political Sociology* 14 (4): 431–446. https://doi.org/10.1093/ips/olaa011.

Kurowska, Xymena, and Benjamin Tallis. 2013. "Chiasmatic Crossings: A Reflexive Revisit of a Research Encounter in European Security." *Security Dialogue* 44 (1): 73–89. https://doi.org/10.1177/0967010612470295.

Kwet, Michael. 2019. "Digital Colonialism: Us Empire and the New Imperialism in the Global South." *Race & Class* 60 (4): 3–26. https://doi.org/10.1177/0306396818823172.

Latour, Bruno. 2007. *Reassembling the Social: An Introduction to Actor-Network-Theory*. New York: Oxford University Press.

Law, John. 2002. *Aircraft Stories: Decentering the Object in Technoscience*. Durham: Duke University Press.

Lawson, Sean. 2020. *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. Abingdon: Routledge.

Leander, Anna. 2016. "Ethnographic Contributions to Method Development: 'strong Objectivity' in Security Studies." *International Studies Perspectives* 17 (4): 462–475. https://doi.org/10.1093/isp/ekv021.

Lechner, Silviya, and Mervyn Frost. 2018. *Practice Theory and International Relations*. Cambridge: Cambridge University Press.

Leman-Langlois, Stéphane, ed. 2013. *Technocrime: Technology, Crime and Social Control*. Cambridge: Willan.

Levinson, Nanette S. 2021. "Idea Entrepreneurs: The United Nations Open-Ended Working Group & Cybersecurity." *Telecommunications Policy* 45 (6): 102142. https://doi.org/10.1016/j.telpol.2021.102142.

Liebetrau, Tobias. 2022. "Cyber Conflict Short of War: A European Strategic Vacuum." *European Security*, 31(4): 1–20. https://doi.org/10.1080/09662839.2022.2031991.

Liebetrau, Tobias, and Kristoffer Christensen. 2021. "The Ontological Politics of Cyber Security: Emerging Agencies, Actors, Sites, and Spaces." *European Journal of International Security* 6 (1): 25–43. https://doi.org/10.1017/eis.2020.10.

Lindsay, Jon R. 2020. "Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage." *Security Studies* 29 (2): 335–361. https://doi.org/10.1080/09636412.2020.1722853.

Lockman, Zachary. 2009. *Contending Visions of the Middle East: The History and Politics of Orientalism*. Cambridge, New York, UK: Cambridge University Press.

Malik, Shiera S. 2013. "Critical Pedagogy as Interrupting Thingification." *Critical Studies on Security* 1 (3): 361–364. https://doi.org/10.1080/21624887.2013.850230.

Mansell, Robin. 2017. "Imaginaries of the Digital: Ambiguity, Power and the Question of Agency." *Communiquer* 20: 40–48. https://doi.org/10.4000/communiquer.2261.

Maschmeyer, Lennart, Ronald J. Deibert, and Jon R. Lindsay. 2021. "A Tale of Two Cybers - How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society." *Journal of Information Technology & Politics* 18 (1): 1–20. https://doi.org/10.1080/19331681.2020.1776658.

McCarthy, Daniel, ed. 2017. *Technology and World Politics: An Introduction*. Abingdon: Routledge.

Michaelson, Ruth, and Lorenzo Tondo. 2020. "Italy Charges Egyptian Security Agency Officials over Murder of Giulio Regeni." *The Guardian*, December 10. http://www.theguardian.com/world/2020/dec/10/italy-charges-four-egyptians-over-of-giulio-regeni.

Millar, Katharine, James Shires, and Tatiana Tropina. 2021. *Gender Approaches to Cybersecurity: Design, Defence and Response*. Geneva: United Nations Institute for Disarmament Research. . https://doi.org.10.37559GEN/21/01.

Morgan, Patrick. 2000. "Liberalist and Realist Security Studies at 2000: Two Decades of Progress?" *Contemporary Security Policy* 20 (3): 39–71. https://doi.org/10.1080/13523269908404230.

Mumford, Densua, and James Shires. 2023. "Towards a Decolonial Cybersecurity: Interrogating the Racial-Epistemic Hierarchies That Constitute Cybersecurity Expertise." *Security Studies* 32 (4–5): 622–652.

Neumann, Iver. 2012. *At Home with the Diplomats: Inside a European Foreign Ministry*. Cornell: Cornell University Press.

Parveen, Nazia. 2018. "Matt Hedges: I Feel No Resentment to Friend Who Reported Me to UAE." *The Guardian*, December 29. https://perma.cc/DH4D-KHTQ.

Pawlak, Patryk, and Panagiota-Nayia Barmpaliou. 2017. "Politics of Cybersecurity Capacity Building: Conundrum and Opportunity." *Journal of Cyber Policy* 2 (1): 123–144. https://doi.org/10.1080/23738871.2017.1294610.

Rosa, Hartmut. 2015. *Social Acceleration: A New Theory of Modernity*. New York, NY: Columbia University Press.

Rosa, Hartmut, and William E. Scheuerman, eds. 2009. *High-Speed Society: Social Acceleration, Power and Modernity*. University Park, PA: The University of Pennsylvania Press.

Rubio, Fernando Domínguez, and Patrick Baert, eds. 2012. *The Politics of Knowledge*. London: Routledge.

Rychnovská, Dagmar. 2016. "Governing Dual-use Knowledge: From the Politics of Responsible Science to the Ethicalization of Security." *Security Dialogue* 47 (4): 310–328. https://doi.org/10.1177/0967010616658848.

Schatzki, Theodore R., Karin Knorr-Cetina, and Eike Von Savigny, eds. 2000. *The Practice Turn in Contemporary Theory*. London: Routledge.

Shires, James. 2018. "Enacting Expertise: Ritual and Risk in Cybersecurity." *Politics and Governance* 6 (2): 31–40. https://doi.org/10.17645/pag.v6i2.1329.

Shires, James. 2019. "Hack-and-Leak Operations: Intrusion and Influence in the Gulf." *Journal of Cyber Policy* 4 (2): 235–256. https://doi.org/10.1080/23738871.2019.1636108.

Shires, James. 2021. *The Politics of Cybersecurity in the Middle East*. Oxford: Oxford University Press.

Singh, J. P., Madeline Carr, and Renée Marlin-Bennett, eds. 2019. *Science, Technology, and Art in International Relations*. New York: Routledge.

Sjoberg, Laura. 2019. "Failure and Critique in Critical Security Studies." *Security Dialogue* 50 (1): 77–94. https://doi.org/10.1177/0967010618783393.

Slupska, Julia. 2019. "Safe at Home: Towards a Feminist Critique of Cybersecurity." *St Antony's International Review* 15 (1): 83–100. . https://www.ingentaconnect.com/content/stair/stair/2019/00000015/00000001/art00006.

Slupska, Julia, and Scarlet Dawson Duckworth. 2021. Reconfigure: Feminist Action Research in Cybersecurity." https://ora.ox.ac.uk/objects/uuid:d84dc398-5324-48c3-9af4-ca54fb92858f.

Smeets, Max. 2018a. "A Matter of Time: On the Transitory Nature of Cyberweapons." *Journal of Strategic Studies* 41 (1-2): 6–32. https://doi.org/10.1080/01402390.2017.1288107.

Smeets, Max. 2018b. "Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment." *Defence Studies* 18 (4): 395–410. https://doi.org/10.1080/14702436.2018.1508349.

Smeets, Max. 2022. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. London: Hurst & Co Publishers.

Solomon, Ty, and Brent J. Steele. 2017. "Micro-Moves in International Relations Theory." *European Journal of International Relations* 23 (2): 267–291. https://doi.org/10.1177/1354066116634442.

Stevens, Tim. 2016. *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press.

Stevens, Tim. 2018. "Global Cybersecurity: New Directions in Theory and Methods." *Politics and Governance* 6 (2): 1–4. https://doi.org/10.17645/pag.v6i2.1569.

Stevens, Clare. 2019. "Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet." *Contemporary Security Policy* 41 (1): 129–152. https://doi.org/10.1080/13523260.2019.1675258.

Stevens, Tim. 2023. *What is Cybersecurity For?* Bristol: Bristol University Press.

Swire, Peter. 2015. "The Declining Half-life of Secrets: And the Future of Signals Intelligence." *New America Cyber Security Fellows Paper Series* 1. Washington: New America Foundation.

Tanczer, Leonie Maria. 2020. "50 Shades of Hacking: How IT and Cybersecurity Industry Actors Perceive Good, Bad, and Former Hackers." *Contemporary Security Policy* 41 (1): 108–128. https://doi.org/10.1080/13523260.2019.1669336.

Tanczer, Leonie Maria, Ronald J. Deibert, Didier Bigo, M. I. Franklin, Lucas Melgaço, David Lyon, Becky Kazansky, and Stefania Milan. 2020. "Online Surveillance, Censorship, and Encryption in Academia." *International Studies Perspectives* 21 (1): 1–36. https://doi.org/10.1093/isp/ekz016.

Taylor, Charles. 2002. "Modern Social Imaginaries." *Public Culture* 14 (1): 94–124. . https://muse.jhu.edu/article/26276.

Van Milders, Lucas, and Harmonie Toros. 2020. "Violent International Relations." *European Journal of International Relations* 26 (1): 116–139. https://doi.org/10.1177/1354066120938832.

Visoka, Gëzim. 2019. "Critique and Alternativity in International Relations." *International Studies Review* 21 (4): 678–704. https://doi.org/10.1093/isr/viy065.

Whiting, Andrew. 2020. *Constructing Cybersecurity*. Manchester: Manchester University Press.

Yar, Majid, and Kevin F. Steinmetz. 2019. *Cybercrime and Society*. Thousand Oaks: SAGE.