International Political Sociology (2022) **16**, 1–26

What Can a Critical Cybersecurity Do?

Andrew C Dwyer
Durham University, UK
Clare Stevens
University of Portsmouth, UK
Lilly Pijnenburg Muller
King's College London, UK
Norwegian Institute of International Affairs (NUPI), Norway
Myriam Dunn Cavelty
Center for Security Studies, ETH Zürich, Switzerland
Lizzie Coles-Kemp
Royal Holloway, University of London, UK
and
Pip Thornton
University of Edinburgh, UK

Cybersecurity has attracted significant political, social, and technological attention as contemporary societies have become increasingly reliant on computation. Today, at least within the Global North, there is an ever-pressing and omnipresent threat of the next "cyber-attack" or the emergence of a new vulnerability in highly interconnected supply chains. However, such discursive positioning of threat and its resolution has typically reinforced, and perpetuated, dominant power structures and forms of violence as well as universalist protocols of protection. In this collective discussion, in contrast, six scholars from different disciplines discuss what it means to "do" "critical" research into what many of us uncomfortably refer to as "cybersecurity." In a series of provocations and reflections, we argue that, as much as cybersecurity may be a dominant discursive mode with associated funding and institutional "benefits," it is crucial to look outward, in conversation with other moves to consider our technological moment. That is, we question who and what cybersecurity is for, how to engage as academics, and what it could mean to undo cybersecurity in ways that can reassess and challenge power structures in the twenty-first century.

La cybersécurité a attiré une attention politique, sociale et technologique considérable tandis que les sociétés contemporaines devenaient de plus en plus dépendantes de l'informatique. Aujourd'hui, du moins dans les pays du Nord, la menace de la prochaine « cyberattaque » ou de l'émergence d'une nouvelle vulnérabilité dans les chaînes d'approvisionnement très interconnectées est toujours plus pressante et omniprésente. Cependant, ce positionnement discursif sur la menace et sa résolution a généralement renforcé et perpétué les structures de pouvoir et les formes de violence dominantes ainsi que les protocoles de protection universalistes. En revanche, dans cette discussion collective, six chercheurs spécialisés dans différentes disciplines abordent ce que signifie « effectuer » des recherches « critiques » concernant ce que beaucoup d'entre nous

Dwyer, Andrew C et al. (2022) What Can a Critical Cybersecurity Do?. *International Political Sociology*, https://doi.org/10.1093/ips/olac013
Corresponding author e-mail: andrew.dwyer@durham.ac.uk

qualifient, avec un certain malaise, de « cybersécurité ». Dans une série de réflexions et d'incitations à la réflexion, nous soutenons que tant que la cybersécurité pourra être un mode discursif dominant avec le financement et les « avantages » institutionnels qui lui sont associés, il sera essentiel de regarder vers l'extérieur dans un débat avec d'autres courants pour réfléchir à notre époque technologique. C'est-à-dire que nous nous demandons à qui et à quoi sert la cybersécurité, comment l'aborder en tant qu'intellectuels et ce que cela pourrait signifier de déconstruire la cybersécurité de manières à réévaluer et à remettre en question les structures de pouvoir au XXIe siècle.

La ciberseguridad ha atraído una importante atención política, social y tecnológica a medida que las sociedades contemporáneas han empezado a depender cada vez más de la informática. Hoy en día, por lo menos en el norte global, existe la amenaza apremiante y omnipresente del próximo «ciberataque» o de la aparición de una nueva vulnerabilidad en cadenas de suministro altamente interconectadas. Sin embargo, este posicionamiento discursivo de la amenaza y su resolución ha, tradicionalmente, reforzado e, incluso, perpetuado, estructuras de poder dominantes y formas de violencia, así como protocolos de protección universalistas. En contraste, en este debate colectivo, seis académicos de diferentes disciplinas debaten lo que significa «llevar a cabo» una investigación «crítica» sobre aquello a lo que muchos de nosotros denominamos incómodamente «ciberseguridad». En una serie de provocaciones y reflexiones, sostenemos que, por mucho que la ciberseguridad sea un modo discursivo dominante que conlleva financiación y «beneficios» institucionales asociados, es fundamental mirar hacia fuera, en un dialogo con otros movimientos, para analizar nuestro momento tecnológico. En otras palabras, nos preguntamos a quién se destina y para qué sirve la ciberseguridad, cómo nos podemos involucrar como académicos y qué podría significar descomponer la ciberseguridad en formas que permitan reevaluar y desafiar las estructuras de poder del siglo XXI.

Introduction

With the changing dynamics of everyday life through, by, and with computation, cybersecurity has become a transdisciplinary and seemingly global concern. Even as we write, there are attacks against "critical national infrastructures," a recent 2021 summit was held in Geneva between US President Biden and Russian President Putin centered on cybersecurity, and what appear to be incessant, and growing, "ransomware" attacks across supply chains, as well as concerning cyber operations in Ukraine prior to what is now, in early 2022, armed conflict. This makes cybersecurity simultaneously both extremely topical and excruciatingly transient as concerns and attention move to the next "big" attack. Thus, much attention within cybersecurity has tended to focus on the most recent news cycle, responding to events, the production of timely policy reports, aiding governments to better improve "national" strategies, and developing "secure" technologies to be deployed at speed.

Due to the widespread adoption of computation across our contemporary lives, cybersecurity has long been approached through the prism of "technical" expertise and strategic political assessment. Conventional "orthodox" approaches from international relations (IR) and strategic studies (e.g., Rid 2013; Kello 2017) to computer science (e.g., Saltzer and Schroeder 1975) have often centered on state-centric or particular technological concerns for abstract "users." This frequently manifests itself either through "black-boxing" the state as an isolated container of international engagement or through depicting a "user" as de-contextualized, often predicated on a rational, privileged, and able-bodied man. Such approaches, although

beneficial in some respects, contribute to a lack of focus on cybersecurity from the perspective of people and communities. Alternative dynamics and perspectives are thus sorely required to understand the fundamental changes that cybersecurity is casting upon societies, which challenge easily consumable "orthodox" material by states and their respective communities.

In recent years, alternative perspectives have started to emerge away from the mainstream of IR (Dunn Cavelty and Wenger 2020) as well as elsewhere, albeit at different points and with alternative trajectories—across critical security studies, participatory computer science, geography, and creative and artistic practice. These disciplinary perspectives have each worked to pluralize and contest what cybersecurity is, and who it speaks to. However, what a critical approach to "cyber" can contribute to beyond this pluralization—and beyond securitization frameworks—is not agreed upon. Therefore, we believe that this is a "timely" moment to reflect, draw threads, and assess the whirling winds of the discourses and materials of this thing called "cybersecurity." In so doing, we do not intend to isolate or bring forth a "critical cybersecurity" in a singular form and condition akin to other turns elsewhere but rather to reflect, discuss, and stretch the complexities of cybersecurity as a concept that is not settled upon, wholly known, and is hotly contested. In this collective discussion, both early career and senior scholars question what a "critical" cybersecurity could "do" that simultaneously questions, deconstructs, and even "hacks back" on the term and the insecurities that become manifest in its application. Rather than getting more niche, more "cyber" specific, such a project can and should have the capacity to make our sites and sources relatable to broader concerns with what technologies "do" to security, and vice versa.

Cybersecurity, at the very least in its contemporary forms, not only affects a typical white, male, unitary individual in the Global North but also works across communities, in intersection with the dynamics of gender, socioeconomic deprivation, financial markets, and nonhuman agencies. Cybersecurity has been understood and even perpetuated—at least by some—to be a "global" endeavor.[1] This collective discussion instead articulates how cybersecurity crisscrosses and challenges universalist perspectives, by instead focusing on its everyday uneven practices. Due to its breadth and impact across different places and disciplines, we are a (somewhat) diverse group who work across, through, and in tension with cybersecurity, but all for whom may be understood as taking a "critical" approach that does not adhere to the "orthodox" outlined above. In so doing, we attempt to critique *where* cybersecurity happens, and trouble *who* does cybersecurity as much as exposing angles where a critical approach could offer new perspectives, voices, and crucially power, to those who are not served well by its contemporary configurations.

To do so, we detail a conversation between six authors from IR, political sociology, politics, security studies, geography, creative practice, computer science, and beyond, from a range of methodological and conceptual backgrounds, many of us "meeting" for the first time. We follow a distinctly nonlinear process of writing, with interjections and thoughts punctuating the piece, on a first-name basis. This proceeds across two parts. First, we begin with each author offering an opening "provocation." These offer a starting point on various interpretations on critical approaches to cybersecurity, from "pluriverses" to "provincializing," on sociotechnical and material approaches, the hacking of "techno-dreams," its economics, and what it means to be "critical" in technological design. After each provocation, space is given to another author to respond to it. In the second substantive part of the discussion, we each write a set of "reflections" on the entire piece, speaking to one another inclusive of our opening provocations and subsequent responses.

[1] *MYRIAM*: Or: wants to be—it never truly was. This is a point to think about more, but there are localities where nobody has ever heard of it or localities where nobody wants to deal with it. It is the "West" who seeks to export cybersecurity to the globe (because money, mainly) and then they can help with capacity building, etc., and be benevolent colonizers again. *CLARE*: Agreed. This was something I was struggling with as I was writing my first piece....

This process took place exclusively online during the COVID-19 pandemic, with video calls and shared word processing files. This permitted the retention of some of the most pertinent discussions that occurred in the "comments" and that we provide as footnotes. We present these to illuminate how the conversation progressed, any divergences, and commonalities to stimulate a critical yet reflexive response where our "workings out" are laid bare. In the vastness of different potentials, and sometimes unwieldy and diverse perspectives that *doing* a critical cyber security must always involve, we finally provide some "paths forward." This offers how we may variously hack, be humble, challenge digital capitalism, reposition the human, as much as engage with, and through, decolonial and postcolonial thinking. In so doing, we agree on one thing: that perhaps a critical cybersecurity project may be more of an *un-doing*. This is by no means the same as *not doing*, but instead begins to sketch out how such a project could rewire the circuits of power and knowledge of cybersecurity today.

Provocations

Andrew C Dwyer: A Cybersecurity of Pluriverses?

Computation is infused across contemporary planetary life and is riddled with in/securities embedded within Eurocentric systems of thought, governance, and practice. A counter to a cybersecurity that is permeated by unequal power dynamics, technical "rationality," and an excessive focus on great power competition, all amid the exclusion of people of the global majority, is sorely required.

As with any "critical" response, I believe it must start with a recollection of where *we* stand as academics based in Europe, writing in English.[2] In so doing, this is not an attempt to articulate a grand narrative but rather to confront what I find most difficult in my own work—how to critique from a position of relative power. From the earliest days of securing computation and information, there has been a tendency to privilege (and actively promote) people like me: white men (see, e.g., Hicks 2018). Such people are dominant in all areas of what we might call cybersecurity—from technical development to those who craft policy in powerful corporations and states. The issue, as I understand it, is not only about representation but also *who* has the power to effect change and the capacity to act and shape ideas of what *cybersecurity/ies is/are* and what worlds they seek to create.

Critical feminist accounts have fruitfully sought to attend to gender dynamics, whereas others have sought to pursue ethical "frameworks" that inadvertently evacuate much of the political. Both do not alone go far enough. I believe that most critical accounts have failed to grapple with the perpetuation of Eurocentric ideas of technology and security.[3] They broadly offer what may be considered a "fix" without really questioning what world views are sustained (although some work does seek to unsettle this; e.g., Coles-Kemp and Hansen 2017). This is because, ultimately, *we* work in similar places. Cybersecurity centers attention on solving problems for rational individuals, implementation without assessing technological affordances, improving awareness education, or securing computation for economic and strategic ends. This is not to say that all these are unimportant—and have helped particular communities—but critical approaches thus far have struggled to articulate and

[2] *MYRIAM*: Ah, but is there a "we" here at all? Academics based in Europe writing (often though not only) in English is already such a diverse crowd.... *LILLY*: Agreed, I would really like to see an expansion of this in your next section, an unpacking of the "we," as in what this would be/look like, versus who/what? *ANDREW*: You are both right - I italicised the "we" as it holds a lot of different weights!

[3] *LILLY*: Agreed. Would love to discuss this more, especially with the "cybersecurity in the global south" research (e.g., Schia 2018) putting western ways of understanding cybersecurity on to "developing" countries. Can/ should a global south approach be different? If so, why, and how?

sustain what cybersecurity beyond corporate, state, and Eurocentric approaches could be (including myself).

In so performing a critique, what would an alternative be to these dominant currents? I propose that *we* could think of cybersecurity through pluriverses (Escobar 2018) that intersect with debates on decolonialism, Blackness, and indigeneity (Stengers 2010; Povinelli 2016; Yusoff 2018) as well as with contemporary debates on new materialism, more-than-humanism, and computational agency (Dwyer 2021; Fouad 2021). This does not mean projecting potentially problematic cybersecurity "capacity" measures from the Global North elsewhere. However, as scholars, we must be able to speak to the worlds of (western) policy and the "international/national" dimensions of cybersecurity, if not only for the requirements of funding, as much as we may seek to decompose such institutional arrangements. This means questioning the foci of research, funding, and who leads such work. However, more fundamentally, it is about listening and centering people of the global majority to understand how and why they may be *insecure*, rather than "improving" cybersecurity as it stands through adapting technologies that emanate particular ways of living and securing.

Thus, my opening is to suggest a pluriversal cybersecurity that moves beyond an individualistic notion of privacy or security mechanism, offers alternatives to state and Silicon Valley–centric forms of technological security, and lets a more-than-human cybersecurity to take root.

Response by Lizzie Coles-Kemp: Moving to the Edge and Loosening the Academic Ties That Bind

The particular power that cybersecurity as an academic pursuit typically accrues comes from its links with industry and government and its usefulness to those entities. This power is layered on top of the already plentiful sources of power serving the Academy that Andrew so clearly acknowledges. A critical position on cybersecurity is, at its heart, an attempt to subvert this power dynamic. As cybersecurity scholars, the power and privilege imbued in each of us through our academic training, our social and professional networks, our socioeconomic resources, and our institutional promotion often bind us ever tighter into the academic–industrial complex particular to cybersecurity. Attempts to change this dynamic by working from within the cybersecurity paradigm have largely been unsuccessful. The rise of technological security has been accompanied by the mantra that humans are the weakest link (Yan et al. 2018) and a concomitant industry focused on "correcting" the way that people interact with data and technology. Counter messages (e.g., Pfleeger, Sasse, and Furnham 2014) have had little effect—even when coming from powerful voices within the cybersecurity community (e.g., National Cyber Security Centre 2017)—and the framing of people as inadequate and incapable of the task of safely engaging with technology has only stoked the inequalities of a digitally mediated world.

As Andrew neatly draws out, as cybersecurity scholars, we must confront our own roles in this power dynamic. For me, the following questions lurk in the shadows of this critical reflection: "*What future is my scholarship helping to create and who benefits from this future?*." For some of us whose careers have originated from within the cybersecurity industrial–academic complex, honestly answering such questions can change the way we see ourselves and at times leads to lifelong redemptive acts. In particular, such reflection often leads to a recognition that for critical cybersecurity scholarship to be effective, it must be dedicated to the redistribution of power for the benefit of those who lose most from a society where technology loads the dice in favor of the already powerful few. Such a shift in perspective dismantles the notion of "we" where a community of scholarship is our home. Instead, we find ourselves redefined in relation to the communities we work with. In my own case, redemption means serving communities to facilitate the building of safer worlds,

opening political spaces in which the intersections between cybersecurity and societal insecurities are acknowledged, and co-nurturing networks of solidarity and collaboration in which individual acts of security can reside.

Andrew's call for a pluriverse of perspectives also questions the notion of the universal user and the construction of the threat model upon which cybersecurity thinking is often grounded. Security as a felt and lived experience is composed of many securities and insecurities that intersect in different ways for each of us (Kazansky 2021). To embrace this pluriverse requires a simultaneous recognition of the universality and the particularities of security needs and wants (Hudson 2005), as well as a critical understanding of the relationships between securities at these different scales. There are moves in this direction from within the core subdisciplines of cybersecurity (Albrecht et al. 2021) but for such a move to be successful, the principles of honest critical reflection that Andrew draws our attention to must be at its core.[4]

Clare Stevens: Provincializing Politics and Disciplinary "Homes"

Cybersecurity is often presented as a symptom of "modernity," of risk and insecurity and rupture. The rest of the world is subsequently assumed to be external to this world-historical process (Bhambra 2007), which technologies diffuse or trickle "down" to poorer countries or "out" to the peripheries (Quet and Dahdah 2020). However, different spatial, temporal, geographic, or national contexts should not be viewed simply as a space for data extraction or a place to which European concepts about "cyber" and "security" diffuse. For those of us working in critical security studies and IR, a critical cybersecurity is not just adding (cybersecurity) politics and sites to studies of security, as a widening and deepening of "security," nor is it simply one in which voices from the periphery would be "allowed to enter into" debates with the center. I argue that a "critical cybersecurity" should instead be a site for theory *making* (Anderson 2017), for understanding more about "security." How should this be done?

First, a "critical cybersecurity" can be an "agonistic" form of "politics." In my own work, by subscribing to a critical project that wishes to challenge exceptionalist security narratives and to denaturalize technologically determinist statist discourses, the analytical concept of "cybersecurity politics" has offered me a crucial means of providing "nuanced analyses of the ways in which security is constructed and challenged in particular social, historical and political contexts" (Browning and McDonald 2013, 251; Hagmann, Hegemann, and Neal 2018; Dunn Cavelty and Wenger 2020). This has allowed me to address the criticisms of securitization or poststructuralist approaches, which view the politics of "security" as possessing a universal logic (Balzacq 2015).

However, there are many reasons why it may be problematic to mobilize "politics" in a critical project without first consciously reflecting on this term. If this project aspires to be an agonistic politics, without such a reflection, there is a risk that we unconsciously reproduce judgments about specific forms of liberal/democratic politics being the thing communities everywhere should aspire to (Aradau 2004; Hobson 2007; Bertrand 2018; Howell and Richter-Montpetit 2020). To act as an agonistic politics then, we must take these critiques seriously, so I propose that a "critical cybersecurity" can act as the assembly point for a "provincialized" critical cybersecurity.

[4] *MYRIAM*: This, to me, reads like a response to all our pieces. The struggle to define our own role in the system we are working for/in/against – and then changing what we identify as problematic. Ultimately, perhaps, this means we should all leave academia?
LIZZIE: Thank you :) I do agree - "staying in" academia is hard at times ... I do wonder whether there might be a future life for critical scholars where we are neither in nor out?

Second then, and in response to these critiques of implicit notions of politics of security, by *provincialized*[5] (Holmwood 2009; Bhambra 2010), I mean to acknowledge that the concerns of "cyber" and "security" are not the same everywhere. Specifically, they are not some disruptive symptom of modernity or a grand narrative experienced the same way everywhere, and neither should analyses of these specific contexts signify a particularism transformed into a universal (Bhambra 2010). By touching upon so many levels of analysis, sites of experience, and fields of practice, concerns with or of "cybersecurity" as an agonistic politics have wider relevance beyond seemingly esoteric "cyber": in this way, such an interdisciplinary, multisited, context-specific scholarship can instead offer a way to (re)build those core concepts of security studies (Barkawi and Laffey 2006; Bhambra 2007).

This is why International Political Sociology (IPS) can be the place for "the assembling of a deliberately untidy cognitive platform on which to build" a different critical security project through a postcolonial lens (Anderson 2017, 229), and the "home" for a multifarious range of scholars, new and established, from different "methodological hinterlands" (Law 2004). It is tempting to think in terms of impact and policy relevance for what this project can "do," but as one of the distinguishing features of a critical approach is that we do not claim to speak "the" truth (C.A.S.E. Collective 2006), then who is going to be interested in hearing that story? With a "provincialized" approach to cybersecurity I do not argue for simplicity or only making explanations more context specific. Our task is to make our stories relevant: rather than getting more niche, more "cyber" specific, we need to make the debates we have, the original research insights we have relatable to broader concerns with what technologies "do" to security, and vice versa. This is what this provincialized and agonistic critical cybersecurity can *do*.

Response by Myriam Dunn Cavelty: The End of Cybersecurity as We Know It

In her intervention, Clare expresses an aspiration for an alternative academic project: one that is free of disciplinary constraints and, more importantly, breaks with thoughts and practices that claim universal reach but are often divorced from actual human concerns. Like Andrew, she calls for a multiplication of conceptual lenses through which to scrutinize cyber politics in action, whereby the meaning of "politics" is contingent and needs situational unpacking, and like Lilly (below), she calls attention to alternative localities in which cybersecurity's homogeneity is challenged.

Beyond this and maybe unwittingly, Clare also suggests the end of all cybersecurity scholarship, critical or not. Surprisingly perhaps, given that we are gathered here to debate "what a critical cybersecurity can do," I agree with that point. A critical cybersecurity must stop being about cybersecurity to do its best work yet.

For a variety of reasons that merit their own discussion elsewhere, cybersecurity scholarship of all colours has emerged in a bubble of its own making (see Pip's provocation below for a similar point). At political science conferences, we used to mainly talk to each other. We were a slow growing club of geeks that knew how technological practices interact with political consequences and vice versa. That identity suited us well—there is a certain power in being different and we leveraged the outsider status to our benefit, with critical cyber scholars being double outsiders in a field dominated by rationalist approaches and US strategic concerns.

Something is changing of late, however. In noncritical cybersecurity circles, the wish to become more relevant for broader discussions in IR and security is growing. This wish developed in parallel to an increasing amount of literature that depicts

[5] *CLARE:* I'd love to explore the links between a provincialized cybersecurity, and the ideas of collective security that Lizzie and Andrew talk to … I think there's something important there potentially about moving away from techno-rationalist conceptions of security and the importance of securing individual data for individualised liberal subjects, to different (provincialized/"decentred?") conceptions of what security might mean in this context?

cyber operations as far less effective than everybody used to think (Lindsay 2013; Borghard and Lonergan 2019), with cyber conflicts being cyber*ed* conflicts at the very most. In other words, the more normalized cyber whatsoever becomes in everyday life and politics, the less sense it makes to treat it as something different or exceptional.

Rather than giving up the "cyber" label to be more relevant for the mainstream, we should consider giving up the "cyber" label to step out of the discursive prison that is forming around us.[6] As scholars, we are complicit in giving cybersecurity more power than it arguably should have. We have used it as a label to create an identity for ourselves—but increasingly, cybersecurity stands for political strategies and modes of thinking that create insecurities across the planet in the name of security. We can challenge this by relabeling our approaches as "critical"; however, a critical cybersecurity is still caught in the same system of meaning, where our critical approaches are pitted "against" something.

One way out of this may be a provincialized approach that is radical in its refusal of dominant knowledge, dominant theory, and dominant concepts. Even dominant languages—in our case, English—become problematic if we want to give otherness a true voice. This creates an interesting opportunity for starting with the provincializing of the debate at the core, in localities that are close to us. If being relevant is a goal, challenging the dominant discourse from the inside out by engaging with problematic communities such as the military and intelligence agencies and not the outside in might be a strategy to consider. If we manage to rebuild at least parts of cybersecurity this way (and potentially lose, or at least severely destabilize, the term in the process), our research will more easily become "relatable to broader concerns with what technologies 'do' to security, and vice versa."

Lilly Pijnenburg Muller: A Sociotechnical Relational Approach to Cybersecurity

The making of cybersecurity is only possible through the relations between technologies and humans, and as such it is imperative that we study how objects and subjects interact and shape particular formulations of "threats" and the resulting practices in the name of "security." Being "critical," it is as such essential to question how cybersecurity is practiced across sociotechnical universes, as a way to complicate, and thereby challenge, commonplace narratives of technological determinism or essentialism. The critical project I advocate is a deconstructive project that speaks to bigger debates than just of "cyber." First, relating these practices back to the larger and generalized category-making efforts of "threat" and "cybersecurity" illuminates how generalized "cybersecurity" categories rest on problematic assumptions. Second, deconstructing categories of "threats" and "security" can illuminate how taken-for-granted categories (such as human/nonhuman, social/technical, threat/benign, security/insecurity) are produced in these practices.

[6] *CLARE*: So, could we say we're interested in studying "digital in/security," or "networked societies" or something like that, instead of the 'cyber' label, with all of its attendant problems and ambiguities? What can a critical cybersecurity do? It can stop calling itself that for starters…?!
LILLY: Agreed! this is echoing Mark Graham's (2013) early work, and Smeets and Shires' (2017) article on "cyber": that the label is actually empty, but we keep using it to get audience/funding....*PIP*: I see what you mean here, but I think it's important to acknowledge that it might be empty and a buzzword and fluffy etc., I don't think the actual label is "empty"... at least when we think about what the label - i.e., the name – does so much work – maybe as collateral in cultural narrative and in pure digital economics (i.e. how much capital is gained by the circulation of the word though platforms, portals. search, social media etc.?).
ANDREW: I think I may sit somewhere in the middle here - in that, yes, like all terms and descriptors, they are "empty" as such. But their emptiness comes "alive" in their relation to others – so yes, as Pip says, there is a real power to "cyber" as a label in how it comes to be performed by organisations, funding bodies, and so on. Thus, a question comes, do we wish to fill another "empty" term to do "our" work, or do we – in the terms of Donna Haraway (2016) – "stay with the trouble" of "cyber"?

So, how do we "do" a critical cybersecurity? Most broadly, I suggest this includes asking how knowledge circulates across transversal logics (Basaran et al. 2017; McCluskey 2019; Aradau in Salter et al. 2019, 24; Bellanova, Jacobsen, and Monsees 2020), and how they are relationally produced in-and-through each other or connected in a cognitive assemblage (Hayles 2016). A critical approach to cybersecurity in my current research means opening up the sociotechnical production in making indicators of threat and inversely how security measures are made against them in a continuum. To do so, I unpack the co-constitutive relation between the technological systems in which cybersecurity practices are embedded and the frames and capacities for decision-making (Hayles 2016). Following the shift of attention to the politics that takes place in the everyday construction and design of digital technology (Balzacq et al. 2010; Austin 2019), I decenter the human and place it within the material- semiotic web of relations in knowledge production that are geared toward efficient decision-making (Suchman 2012). In other words, the research must ask where the politics take place in the everyday construction of security.

Researching how indicators of threat are made, and inversely how security is made in response, means questioning what is included and excluded in the sociotechnical practices of threat indicator production, who produces this knowledge and how, and how this shapes the security measures, and policy developments made in response. To examine the sociotechnical making of indicators of threat, we must unpack their configuration. Studying the situated, the quotidian, and the ethnographies of day-to-day practices as such has a double intent. First, when focusing on new modes of knowledge production and what they mean, it is essential that the research attends carefully to the routinized mechanisms that produce distinctions between human/nonhuman/less-than-human/inhuman (Aradau in Salter et al. 2019, 23–24). Placing focus on these distinctions in turn opens up space to question "how agency is distributed . . . and in what ways actors contribute to systemic dynamics and consequently how responsibilities—technical, social, legal and ethical—should be apportioned" (Hayles 2016, 34). This is significant, as it can allow us to re-hink where the politics take place in the everyday construction of security (Schwarz 2021), while making visible how humans are intricately woven into the ecologies of technology.

Response by Pip Thornton: Which Came First—the Threat or the Security?

This is a sociotechnical approach to cybersecurity that I wholeheartedly agree with on some fronts but am less sure on others.

Immediately for me, I want to start thinking about this perceived threat/security axis—can I call it a co-dependence? Which came first in a chicken and egg scenario? Threat or security? Is there security without threat? Is there threat without security? As Lilly suggests, critical cybersecurity should rewind, deconstruct, and interrogate the constructs of threat and security. The bottom line is to work out who benefits from threat/security—and who benefits (politically, culturally, financially) from constructing, funding, and perpetuating this discourse? Lilly addresses this question in her proposal that we need to unpack what is included and excluded in these practices, who benefits and how, but I think a deeper dive into the semantics and economics of security and threat might be fruitful.

I do not want to turn this response into a philosophical conundrum, and I am sure there must be literature about the accepted/received dichotomy between threat and security, but I wonder if thinking about security without threat—and what that would mean—might be a productive critical lens (as Myriam does in her provocation below)? Likewise, has the literature accepted that threat and security are the protagonists in this play? What if they were not? Could a critical cybersecurity destabilize this and begin to reveal the protagonists in the construction of both threat and security? Lilly's call to de-center the human as a critical approach

to cybersecurity is key here, but from my own perspective it is often the economy that is the hidden actor in these systems, and unpacking the human/nonhuman in the economy is a whole new rabbit hole, especially if—as Louise Amoore suggests—economy can be understood "as extending to the oikos, to the attributes of population, cluster, and household" (Dwyer et al. 2021, 46).

A final comment is on Lilly's suggestion that looking at the politics of the construction of digital technologies allows "a critical approach [which] de-centers the human and places it within the material semiotic web of relations *geared towards efficient decision making*" [my emphasis]. On first reading, this seemed to place "efficient decision making" as the goal of digital technology, which I think would need an awful lot more unpacking beyond the scope of this piece, but I would be interested to understand more of what Lilly meant by this statement.

Myriam Dunn Cavelty: Hacking the Digital Techno-Dream

Critical cybersecurity scholars face at least two challenges: first, we need to prove the value of critical research in a field dominated by technical wizards who bend code, rewrite protocols, and patch holes to secure our dream of the techno-miracles to come (blockchain everywhere! artificial intelligence! quantum computing!); second, for decades, we have remained a small, and one could bemoan, marginalized group of scholars because our smart and brightest change their research topic[7] or even leave academia altogether since there are not enough positions.

The two challenges are interconnected: digital technologies have an eerie ability to center security discourses on their indisputable material deficiencies that need to be fixed—or else. Think of how vulnerable critical infrastructures such as the energy grid are! The consequences of a sustained outage would be devastating. And is it not true that politically motivated cyber incidents are on the rise? The urgent need to secure humanity's techno-dream against disruptions and the adverse Other is gaining rapid ground as a key policy concern, bringing forth new markets perpetually hungry for specialized knowledge.

If we understand security not as "a noun that names things" but "as a principle of formation that does things" (Dillon 1996, 16), then cybersecurity does a lot of things in increasingly powerful, expansive ways: the security of the digital is as much about technical practices and economic solutions to ensure the confidentiality, integrity, and availability of information as it is about refurbishing hardcore geopolitical security discourses with new life by colonizing the multiplicity of cybered spaces with a singular violent logic.

In a basic form, critical work means to "interrogate security as a form of productive power that makes reality intelligible and actionable in particular ways" (Aradau and van Munster 2017, 75). Cybersecurity is a form of productive power that needs urgent and sustained dismantling because of its invasiveness and because it works its magic through the merger of economic progress, social well-being, and security concerns. Even more importantly, we need to destabilize that power by disrupting its complacency. To accomplish that, critical cybersecurity can hack the digital techno-dream by inserting uncomfortable questions, alternative meanings, and new political options into its machinery.

Just like hackers exploiting vulnerabilities in the information infrastructure to gain access to a proprietary system, we need to employ a variety of steps and techniques to achieve our objectives. One of the most important ones in my experience is a close collaboration with security communities[8] of practice with the goal

[7] *LIZZIE*: This is interesting - do you mean they start out critical and then either leave or become more orthodox? Is there traffic back the other way? (I definitely started out more orthodox and became critical).
MYRIAM: I know many people who had to leave academia because they did not find academic jobs. They now work for banks and consultants, dropping their critical skin entirely

"to render interaction between publics, governing authorities, social scientists and techno-scientific experts productive in terms of transforming professional practices and creating responsiveness to societal values" (Evans, Leese, and Rychnovská 2021, 191). Objectively, the information infrastructure is insecure—with material, though varying, consequences for all of us. Picking up on the old debate whether there is such a thing as "positive" or "just" security (Floyd 2011; Roe 2012), critical cybersecurity is in an excellent position to show the world what a positive and just cybersecurity looks like.

Response by Andrew C Dwyer: Beyond a Hack of Cybersecurity?

There is much to think about in the intersecting, and complex, ways in which cybersecurity becomes manifest in Myriam's response. I think this is most lucid in thinking about a "techno-dream" of cybersecurity. Such a techno-dream can be traced to broader movements in how technology has been used as a way to "colonize" power and centralize it with certain power brokers, such as Apple and Google (e.g., Wark 2019; Zuboff 2019). I cannot but think about COVID-19 mobile contact tracing using Apple and Google's protocol. Here, privacy concerns against the state were used to justify a singular centralization of pandemic security. Who permitted the power of corporations to dictate—writ large—the bodily securities of people across the world?

So, if we are living in this techno-dream, I think this is a broader societal (re)arrangement of the possibility of technologies, currently spurred through a narrative that algorithms are able to automate and are unproblematically knowable due to their mathematic arrangements (see Dwyer et al. 2021 for a discussion of Louise Amoore's critique in Cloud Ethics [Amoore 2020]). However, it is also one that has a significant lineage from cybernetics that form, arguably, an interweaving between cybersecurity and other technological imaginaries today, even if their earlier paths diverged. Thus, cybersecurity is but part of a systemic move to open up data (and thus our lives) to algorithms to be able to permit assessments of risk or, inversely, the best way to sell us books on Amazon. I think we can see that this techno-dream of rationality that is pervading our political institutions is one that demands an alternative to rationality. Hence, I might consider whether there is a "singular violent logic" but rather rationalities multiple that cohere into a violent, yet unequally distributed, weight borne by *others*?

To tackle this may mean speaking with people who I have found particularly inspiring in media studies (Parikka 2007; Sampson 2012) to those who have written about the promise of computation and our relations to algorithms and calculation (Hayles 1999; Browne 2015; Amaro and Khan 2020). Here, we see common attention to those who "bend" code to offer seductive narratives of social progress while promulgating a universalist worldview, or indeed obscuring that insecurity is a dominant reality for many of the global majority (and indeed within the Global North). How this then intersects with those in policy becomes absolutely pressing. Thinking toward what a normative position of a "positive" cybersecurity may be, I leave open to those who read this paper. Yet, perhaps, some paths may lead to an engagement with security communities and aligning with debates on algorithms and social justice. This may mean a deconstruction of cybersecurity's rationalities rather than a "hack" to rebuild, together, something subjective and wholly *scientific* in its

[8] *LIZZIE*: This is a very interesting start point - it often occurs to me that security technologies are not necessarily about security but more about the performance of security to make money. Security practice communities on the other hand are often a lot more about achieving a security goal.
MYRIAM: Isn't the problem with "cybersecurity" that there are many different securities at work at the same time - and that the goals are also multiplying? *LIZZIE*: I think you are right - but that's because cybersecurity becomes a "catch-all" for security in a digitally mediated world... I think the notion of cybersecurity has almost outlived its usefulness - time to re-think how we look at security in a digitally mediated environment.

own form. Work on gender-based violence demonstrates such an avenue in how it is speaking beyond, through, and with cybersecurity in inspiring ways (Slupska and Tanczer 2021). I would be coy to hack our way back.

Lizzie Coles-Kemp: Why Put the Critical into Technological Security Design?

Technological security at the technical core of cybersecurity is a collage of computer network security, computer security, and the security of the data itself. The object to be protected is the technology or the data produced and stored by the technology but there has always been an implicit/unspoken assumption that if digital technology[9] and the data it produces are protected, then the people using that technology are also protected. It is this assumption that a critical approach to technological security disrupts and challenges. While the implications of computing for the safety and security of the individual have been part of security analysis since the early days of computer security (Saltzer and Schroeder 1975), little attention has been given to the ways in which technological security might enable digital transformations that potentially render people more insecure in their day-to-day lives. With the advent of "usable security" (Zurko and Simon 1996; Adams and Sasse 1999) in the 1990s, users of security technology have been explicitly folded into technological security thinking. However, in a world where the boundaries between people and technology are blurred, I would argue that it is not enough to focus on technological security being compatible with people; an understanding is also needed of the security of people and how that relates to technology. To achieve this, critical evaluation needs to be embedded into all stages of the design and deployment of technological security.

A critical study of technological security, therefore, might start with the fundamental question "Technological security for whom?" and with the challenge "Who or what is doing the securing?." Graham Smith (2005) set out four security questions that can be used to challenge a technological security proposition:

- "Who or what needs to be secured?"
- "What is doing the securing?"
- "Why is the subject being secured?"
- "Who or what is the subject being secured from?"

Smith developed these from an earlier set of questions (Baldwin 1997) that explicitly focuses on the trade-offs and potential costs of adopting a particular security strategy. Baldwin structures these questions to show that trade-offs are predicated on an understanding of "security for whom" and "whose values are being secured." When we use these questions to critically analyze technological security, we rarely derive a simple answer and usually reveal that there are several parties benefiting in different ways from the security technologies, often at the cost of others. A critical approach to the design of technological security draws out these interdependencies and conflicts between parties. Such interdependencies and conflicts often

[9] *LILLY*: This connects nicely to Myriam's point of the old idea of as long as the vulnerabilities are secured, the users are secure too. Maybe this is something to discuss/open up more?
CLARE: But also brings to mind a question about how we can or do make "vulnerabilities" meaningful…there's a technical component at the level of code and software and hardware interacting in unexpected ways for example, but there's also the non-fungible quality of these vulnerabilities as emergent properties, but there's also the socio-cultural thing of some vulns being more worrying or relatable for some national cultures or groups…I wonder if vulns mean the same for all people?!
LIZZIE: Clare's point also makes me think how vulnerabilities are part of the "felt" experience of security. I would perhaps go as far as to say that meaningful vulnerabilities are the ones you feel (prepared to be disabused of this notion, though) ... what vulnerabilities you worry about varies greatly if you're in finance, a state, or an individual.

challenge the claims that can be made about the power of a technological security approach and alter the understandings around risks related to digital programs. To be effective as an agent of positive change that benefits the security of people, a critical understanding of technological security must, however, join forces with a wider critical security movement to fundamentally change the security discourse for society as a whole because technological security is embedded within a much larger security complex.

Response by Lilly Pijnenburg Muller: A Critical Study of Technological Security

In my engagement with Lizzie, I pick up on the tension between universal design and particular design, and the call for a critical evaluation to be embedded into all stages of the design and deployment of technological security**.** Starting from the premise that we need to go beyond thinking that security is connected to the technology that holds cyberspace together, there are two main points I want to follow up on.

The first one is the social construction of security through the building and creation of technology. Starting from Lizzie's blurred boundaries between people and technology I agree that it is "not enough to focus on technological security being compatible with people." The security of people in relation to the technology needs to be evaluated too. Placing critical evaluation into all stages of the design and deployment of technological security while embracing the "social" roots and impact of design is of utmost importance. However, the technology must not be forgotten in this analysis; it is a sociotechnical relational matter. What I mean by this is that technological security can indeed be seen as social security enacted through 1s and 0s, but the 0s and 1s impact the social as much as the social impacts the 1s and 0s. It is the relationship between them that design develops. Rather than moving back and forth between a discussion if it is the social or technical that matters, can we study these in relation to each other? Or is the social in the end the main factor and area that needs scrutiny?

Following up on this question leads me to my second point relating to the tension between universal design and particular design. Paying attention to the interdependencies and conflicts between parties indeed challenges the claims that can be made about the power of a technological security approach and our understandings around risks related to digital programs. However, I wish to draw attention to the awareness of the parties in this conflict. In questioning who is driving cybersecurity ahead and with what intent, is there an aware actor that gets to decide, act, and have "power" to set those parameters? Indeed, the international political economy (IPE) of cybersecurity, and the impact the market has on driving the (in)security ahead, is in urgent need of attention. Returning to the everyday design and usage of the agents that build the technology that upholds "cyberspace" and the need for critical evaluation at all stages of the design and deployment of technological security, is there an active and self-conscious power in everyday design? Are everyday designers and constructors aware of the power (and potential biases) embedded in their design? Or is it rather a lack of awareness of power (in the dispersed sense) that we need to pay attention to? If power is in the design of everyday technology, but the designers are not (necessarily) aware of the impact and possible biases built into microtechnology, where is the power? The IPE around cyber(in)security is in need of urgent scrutiny, but similarly the (potential lack of) awareness of power embedded in the everyday sociotechnical configuration of technology needs to be unpacked and critically assessed. The power structures built into the design effect not only the technology but also society at large, and vice versa. Questioning who and what gets to decide, act, and have "power" to set the parameters in designing security is of quintessential importance in a critical study of (cyber)security opening up the assumptions and power structures embedded in security making.

Pip Thornton: Who Will Buy My Cybersecurity?

A critical cybersecurity must also interrogate the emergence of "cybersecurity" as a keyword, a geopolitical issue, and, perhaps most importantly, as a *brand*.

"Cyber" as a buzzword attracts funding, pay packets, and investment. Back in the day it was "information security," but that does not have the same ring to it. So what work is that word doing?

What if cybersecurity is a bubble of its own creation? What if cyber *insecurity* is more important than cybersecurity—it is certainly in the interests of security companies that systems remain insecure—or at least that the prevailing narrative is one of insecurity. Antivirus software plays on our fears and tales of hacking and ransoming. A critical cybersecurity would interrogate these narratives from a social and cultural perspective, challenging the construct of cybersecurity, before even thinking about its technical workings. A critical cybersecurity must insist on disciplinary diversity.

A critical cybersecurity must ask who controls the cybersecurity industry. Who gains from "insecurity," both in economic and in political capital? This is in terms of not only dedicated "security" companies, but also digital platforms that gain advertising revenue from bot-spread viral stories, or Google, which actually earns money from the very word "cybersecurity." There are interesting insights to be had into the geopolitical and economic value of cybersecurity in search engine results. A quick look at the data produced by Google Ads shows that the word "cybersecurity" is more expensive for advertisers to link to their pages in different local and global geographic areas. Edinburgh is a hotspot in the United Kingdom, as is San Francisco in the United States, and India globally, revealing the market-driven nature of cybersecurity and its relative "value" in certain places—tech hubs maybe or outsourced production hubs (Thornton 2018).

What this illustrates is how cybersecurity is interwoven in a wider political economy—and as cybersecurity becomes more weaponized, it is easy to see where it fits in a wider military industrial complex too. Another way of looking at this is to ask how cybersecurity is different from just security? As shown by the Google Ad data, "cybersecurity" is not universally equally valued or indeed equally *valuable*. Some final provocations might be what are we securing against? Is this political? Is it purely economic? Is cybersecurity the symptom rather than the cause?[10]

Response by Clare Stevens: Commodity Fetishes and Chronopolitics

Pip's closing point is a provocative one and chimes with my own sense of cybersecurity as a set of culturally specific *imaginaries* and spatialized practices. As societies become more networked, more interwoven with computation and communication technologies, so too do new insecurities, vulnerabilities, unexpected hiccups, and system turbulences emerge. Cybersecurity as a set of practices geared toward repair, maintenance, and anticipation is thus dependent on that dynamic: it portrays itself as a direct response to those emergent technological and social interactions and their unforeseen breakdowns and break-ins. Cybersecurity may thus be a "cultural materialisation of the economic" (Cook and Crang 1996, 134). However, there is also a really important element that I think all of the contributors are implicitly or explicitly seeking to interrogate, namely to understand how much "cybersecurity" in turn as a practice and a concept with its own political economy is also *producing* or perhaps unwittingly propagating those insecurities, as in Lilly's piece. Lizzie's pieces

[10] *CLARE*: Yes! I think it is…I was trying to make a case about this, that like "vulnerabilities" being socially/culturally meaningful (Bijker et al. 2012), that "cybersecurity" in US security politics at least has acted like an allegory for wider social and technological change-processes… cybersecurity politics are efforts to make sense of/impose some order on networked computation and associated social/political changes, but *these politics are constitutive of these broader changes too.* Imaginaries of vulnerabilities produce "cybersecurity," but cybersecurity imaginaries produce vulnerabilities too….?

in turn have eloquently drawn out the potential—and need—for *constructive* cybersecurity practices that should be oriented toward community-based considerations, of a social cybersecurity. However, Pip's piece also makes an important intervention about the commodity fetishization of the term itself. Commodification really is everywhere—as Pip highlights, even the word "cybersecurity" has its own political economy and circulatory value.

Thinking of it as a buzzword with its own "clickable" value is a fruitful way of moving discussions on from the ambiguity and "mess" of the term "cybersecurity." In contrast to approaches that have sought to point to how contested or apparently meaningless the term is, including my own work that has been about tracing the narrative processes of people trying to make sense of, and draw the conceptual and political boundaries of this category "cybersecurity" as a relatively *passive* entity, Pip's reflection instead suggests how the term may be an *active* participant in these economies. I interpret Pip's call to investigate the work this term does to mean it could perhaps be treated like a "mutable mobile" (Law and Mol 2001) with its own political economy, and perhaps even agency. This approach could investigate the work the term does as it travels, moves, is clicked, circulated, and also how it gets anchored to particular tech-hubs, locations, centers of technological production and exchange such as San Francisco, Edinburgh, Delhi, and more. This could begin to trace, or map, the commercial, political, economic, and circulatory value of a term as an abstracted entity, akin to tracing a "data journey" (Bates, Lin, and Goodale 2016). This could do the work of disclosing the spatial lives of commodities, a form of "geographical detective work," even while acknowledging that is not innocent work to map such spatiotemporal configurations (Castree 2001). This may pose—rather than answer—a more troubling set of questions about where the sites and unseen socialities of these commodities may lie (Castree 2001).

This brings me to my second point in response to Pip's urge that a "critical cybersecurity would interrogate these narratives from a social and cultural perspective, challenging the construct of cybersecurity, before even thinking about its technical workings." Marxist ideas of fetish commodities imply production and the links between "value" and capitalist time, and Pip's piece also thereby alludes to the interwoven and co-constitutive links between temporality and spatiality (Klinke 2013). Such an investigation into the spaces-and-times or the "chronopolitics" (Stevens 2016) that cybersecurity practices apparently congregate and congeal around suggests an opening for critical scholars to consider and actively explore the heterotemporalities at work, what Andrew referred to as the pluriverses of cybersecurity practices, which may exist beyond state and corporate interests. Ours is not a critical project with an implied narrative of *progress*, as though what a critical project does or says "now" can have any predictable outcome toward some liberal progressive future (Hutchings 2007). Instead, it is a call to attend to the different temporalities interacting, emerging, and perhaps pushing back against, the kinds of temporal narratives implicit in accounts that reference some essentialized characteristic of modernity in terms of speed and immediacy and urgency. I think Pip's intervention is a valuable prompt for us to ask: whose times, whose cultures, whose spaces are implicated in constructing cybersecurity?

Reflections

Andrew C Dwyer: Getting Stuck in, Being Humble

Throughout this discussion, *we* have grappled with being scholars of cyber(security). I have tended to feel uncomfortable about being *wholly* identified as such while also acknowledging its associated "costs." That is, regardless of cybersecurity as a thing, it has "real" impacts on early career scholars (which Myriam also raises): it affects which conversations you are invited to as well as the funding that you may receive.

To *not* talk about cybersecurity in my own work would be to isolate myself from the powerful institutions and framings that I simultaneously wish to challenge—or maybe "hack"—the domination of state-centric positions that sit at the core of the critique provided by IPS. Yet, as Lizzie suggests, we must participate in "lifelong acts of redemption." I am unsure whether there is such a redemption possible, but being continually aware, seeking to promote others, means re-centering, re-prioritizing, and leading (and knowing when not to lead) debates.

One way I have attempted to do this is the formation of the Offensive Cyber Working Group in the United Kingdom. I remain frustrated at the US- and state-centric approach to conceptualizing cybersecurity as well as those who are not considered essential to these conversations. As a "critical" scholar, I think becoming part of the flow of contemporary debates permits a shift, new articulations, and possibilities that "stay with the trouble" (Haraway 2016) of cybersecurity that have been highlighted across the pieces, and in particular here by Pip. As Myriam argues, "[i]f being relevant is a goal, challenging the dominant discourse from inside out by engaging with problematic communities such as the military and intelligence agencies and not the outside in might be a strategy to consider." This is one method of "doing" critical cybersecurity. Of course, there are great risks with such an approach, but I believe it imperative to be in and out (of this metaphorical space) to *make* new worlds as much as we must collectively, and with humbleness (Saville 2021), imagine.

In my opening on the potential of pluriversal cybersecurities, I implicitly pointed toward a crushing universality in computing infrastructures, as Lizzie has effectively brought out. However, I also wish to push this further to say that *we* are already implicated in a multitude of universes by our transdisciplinarity, the forces of the Anthropocene that are being unequally wrought upon *us*, as well as universes I have yet to encounter, which have been oppressed, marginalized, or simply ignored. I think this resonates with Clare's called for a "provincialized" security. I find the argument not to become more niche and "cyber" specific key in making "our stories relevant." So, what stories do *we* make relevant and what is our power in doing so? How should *we* be crafting such stories (Coles-Kemp, Ashenden, and O'Hara 2018)? In crafting such stories, I would be keen to develop ones that overlap, muddy, and render complex the sometimes-simple technological narratives of cybersecurity.

Yet, to assume *we* can do this would be an error—and even more so as Lilly highlights through thinking of and with nonhumans. Computation is not simply a "tool" awaiting activation—and thus our efforts are multiplied and require even greater pluriversal thinking—that is worlds beyond our discourses and knowledge. Thus, we must situate us (as differentially positioned people) among radically alternative ecologies that cannot be "solved" by a rational "human in the loop" (Schwarz 2021) nor by addressing a "human layer." Still further, as Science and Technology Studies (STS) has informed the practice of IR (Hoijtink and Leese 2019), its discussions must engage with indigenous thinking on nonhuman agency (Rosiek, Snyder, and Pratt 2020) as well as further challenge the everyday and international to be forever becoming pluriversal.

Clare Stevens: Rethinking the Categories of "Cyber" and "Security"

In my first piece, I wanted the term "provincializing" to signify that such a project is not about judging the "sites" and "spaces" of cybersecurity as though they are indicative of relative deprivation or "progress" of peripheries in relation to some putatively "developed" center, or that "we" should somehow be "provincial" in some value-laden sense. Instead, a critical project should be about *rethinking the very categories* by which we try to understand what is happening in the world today. We still need to theorize the world through categories, because they are crucial for a social science to address issues of social justice (Barkawi and Laffey 2006; Chakrabarty 2008, 17; Bhambra 2010). The question then becomes of how we do so in a way

that is cognizant of the heritage that these categories in theory and social thought contain.

Myriam's generous characterization of my call to "pay attention to alternative localities and temporalities" was something I struggled with as I wrote my first piece. I do not think that "cybersecurity" is as global as some of its more commercially and politically vested interests might suggest. It strikes me that although I was wanting to make an argument for taking a less Eurocentric focus to our sites of study, I wonder if that, as Pip has suggested, cybersecurity as a discourse is a *symptom* as much as it might be a *cause* of wider social processes, in the sense that it is an emergent property of, or allegory for, particular forms of capital and neoliberal economic value chains. Even in its most positive, emancipatory, or "social security" guises that we discuss elsewhere in the context of this piece, there is still something troubling me about the kinds of places and forms of life that cybersecurity practices and discourses center on, so that it makes me wonder if it is possible for a critical cybersecurity to be truly "un-Eurocentric."

Despite this, I think that while there may be sites that practices and interests in cybersecurity tend to coagulate around (including our own roles and positions as academics seeking publications and job security), I think our theorizations of what "security" means can be provincialized. By this, I mean that I think Myriam's response has articulated the issue powerfully, even if I had not followed my own logic through to the conclusion that we need to give up the "cyber" label. In trying to describe my underlying fascination with "cybersecurity," I see it as an (admittedly limited) yardstick of how societies, states, communities, and people are making, and *making sense of*, networked digital and computation technologies, and how that in turn may be shaping ideas of societal vulnerability. And this should not be limited to specific sites or times (in the Global North). A critical cybersecurity thus has the potential to be about theorizing and understanding (emergent, contingent, co-produced) relations between technologies and communal living, not just "security," even while recognizing the need to "provincialize or decenter [the] imaginary figure" of Enlightenment thought and its attendant categories that remain "deeply embedded in *cliched and shorthand forms* in some everyday habits of thought that invariably subtend attempts in the social sciences to address questions of political modernity" (Chakrabarty 2008, 4). So, a critical cybersecurity could jettison the term "cyber" altogether, to unpack what categories such as "security" mean in specific contexts for specific people(s) at specific times, so that things studied in the name of "cyber" (or "digital security" or "networked societies"?) can and should have insights for wider debates about "security." To "rebuild" cybersecurity, as Myriam neatly closed, this is going to be a fraught and uncertain project going forward, but an exciting one that "we" (whoever that may be) should not be dispirited about.

Lilly Pijnenburg Muller: Bringing the Relational in the Sociotechnical to the Forefront

In her reply, Pip raises key questions regarding how we draw attention to the sociotechnical processes that go into the construction and making of cybersecurity. I will not be able to resolve the issues she raises here, but I will try to fill in on three main points that she raises. The first item I want to engage with is that my intention is not to argue that digital technologies produce "more efficient decision making" nor that this is the goal of digital technologies. Rather, my point that is of utmost importance is that the configurations of technological systems that "cyber" constitutes, such as machine learning, are unpacked to fully comprehend their impact on knowledge production. A "critical cybersecurity" can as such assess technological systems' impact on the frames and capacities for decision-making *through* its capacity to produce different constellations of knowledge than the human brain. Unpacking the configurations of technological systems, and their

constitutive role in cybersecurity knowledge production, the kinds of implicit and tacit knowledge that later decisions and action frames are consequently informed by can be illuminated.

Second, my call to de-center the human is with the intent to move away from this split of the human and technology and the heavy focus on human discourse and practice. The majority of research in International Relations and Critical Security Studies on cybersecurity has been conducted through discourse or practice theory, with a focus on elites, strategies, and practices in and of state, international organizations, or expertise (Stevens 2016). This has left materialities understood as forming a passive background or simply an outcome of social forces (Aradau 2010). The technological dimension of security is not fully incorporated (Hoijtink and Leese 2019; Stevens 2020). Shifting attention and approaching the social and technology together allows for a rethinking of where the politics takes place in the everyday construction of security, and with what effect. Importantly, while calling for a de-centering of the human, the social is still understood to hold an important role in technological development. De-centering the human from the main protagonist, the human still holds a key role in relation to the development and ecologies of technology. By de-centering the human and not assuming any essential preceding categories of "social" or "technological," this approach allows us to draw out how cybersecurity is an emergent product of *relations*, thereby complicating and challenging any apparent dichotomy between technological and social analytical approaches.

This leads me to the third point and Pip's question regarding the threat/security axis as an accepted/received dichotomy. In answering the sets of questions posed by Pip, I return back to the word "inversely" in my original text. The aim is not to approach security as being made against a self-evident threat/risk, but rather to understand security and threats and risk as relational, co-producing each other. Indeed, neither threat nor security is understood as static; rather, they are continuously evolving, emergent, and iterative. Making an analytical and conceptual move away from understanding threat/risk as a dichotomous relation with "security" allows for the possibility to sidestep around the "chicken and egg" dichotomy Pip raises. Unpacking how security and threat-making are interrelated holds the potential to indeed allow for the called-for revelation (and destabilization) of the (human and technological and material and social) protagonists in the construction of both threat and security. By diving into the sites of their sociotechnical making and looking at the semantics or co-construction of threats and risks and security, the goal is indeed to provide a "deeper dive" into the semantics of security and threat.

Myriam Dunn Cavelty: Let Us All Become Activists

It is much easier to have grand ideas about how to do things "better" than to actually *do* the better things. I will not be able to solve this arguably pervasive problem of critical projects here, but I might attempt to fill two ideas sketched in my initial piece with a bit more than hot air after Andrew's thought-provoking response. The first item I want to reengage with is the idea of "positive" cybersecurity and the second is my previously superficial use of the term "hacking" that I would like to position more broadly as possible forms of resistance against the techno-dream.

From our discussion here, it becomes obvious to me that there cannot be just one form of "positive" cybersecurity. Desirable futures should be thought in multitudes to prevent alternative visions from becoming just as totalizing or patronizing as contemporary arrangements. Ultimately, we are looking to facilitate, in Lizzie's words, "a positive change that benefits the security of people." Yet, people are different, and their needs are different; to paraphrase Clare, we need to listen first before we start to engage. One aspect about security stripped bare of add-ons such as "cyber" or "international" that forces us to think in pluralities and pushes us toward action

beyond clever ideas is that security is transient,[11] a goal that we may continuously work toward through different practices in different localities and by engaging with different communities and materialities. If we think security in plurals, we enlarge the "attack surface"—the IT-security term for all possible points of entry to breach a system—for critical projects to be successful in bringing about change and we open the door for aligning critical cybersecurity "with debates on algorithms and social justice" as Andrew writes, and many more technologically infused security debates now and in the future.

In his response, Andrew suggests "a deconstruction of cybersecurity's rationalities rather than a 'hack'." My response is that a deconstruction, which I acknowledge as a necessity with high priority, equals a hack. I am shamelessly tapping into a romanticized idea of hacktivism here when I define "hacking" as a defiant act that breaks the rules of a system, technical or not, in often clever, sometimes creative ways, in order to expose the unwanted working of the system (on hacktivism as a form of political resistance, see Karagiannopoulos 2021; for an early debate about taking cultural and political resistance online, see Critical Art Ensemble 1994, 1996). Yet, desirable futures can be crafted through tools of resistance that I believe should become an integral part of a discussion about critical cybersecurity so that those who feel so inclined can move from intellectual ideas to activist practices that seek to bring about positive change in various ways.[12] One concrete way to do this is to follow in the footsteps of groups such as the Critical Art Ensemble or the Electronic Disturbance Theater, who use art and performance as nonviolent acts of defiance across and between digital and non-digital spaces.

Lizzie Coles-Kemp: How Might We Rewire the Circuits of Power?

Lilly's thoughtful reflections draw my attention to two key themes: the sociomateriality of technological security and the need for a critical awareness of power in relation to technological security. In exploring these themes, we begin to achieve clarity on what critical cybersecurity analysis might be.

Lilly points out that technological security is neither technological nor social but a point at which technological and social understandings of security come together. Cybersecurity technology is an "embodiment of societal knowledge" (Dunn Cavelty 2018) with the social understanding of security shaping the technical and vice versa. This is a mangle of practice as sociologist Andrew Pickering (1993) described this sociotechnical interaction. An example of this is the firewall with its logging and alerting of access events. The firewall is configured with a social understanding of what constitutes unauthorized access and the firewalls' responses to access events shape that social understanding. If we linger over the term "mangle of practice," we might ask ourselves whether in cybersecurity's case this technical–social interaction is not only a mangle of practice but also a mangle of security logic. While the social and technological conception of security might start with the same underpinning logic forged through a common understanding of who or what needs to be secured and from which threats, it is more often the case that this common understanding is arrived at through the to-ing and fro-ing of technical–social interaction. New forms

[11] *CLARE*: Pluralities, yes, this is an important way to think about it, and to reiterate the old point that "security" is a process not a final destination.

[12] *ANDREW*: I think this link to activism is fascinating and should be brought up in the conclusion more - makes me think of the C.A.S.E. Collective (2006) and also the Beirut School (Abboud et al. 2018).
CLARE: Yes! This point keeps recurring to me as I read our comments about what a critical cybersecurity looks like, and who could/should do it, and who could/should be listening (policymakers? practitioners? citizens?). This reminds me of something by David Hess (2009) on the role that NGOs and his study of civil society research, suggesting an alternative to traditional routes for research agenda setting in science, which are dominated by for- profit and government funding organizations. Could this be an interesting counter to our general dis-ease with the political economies of cybersecurity?

of security logic emerge from this interaction where not only is the technology and data to be protected but so too the social phenomena that they represent (Coles-Kemp 2020). In this case, the security logic has a social–technical relation as its primary referent object, and it is this relation that is so often the necessary focus of critical cybersecurity analysis.

In the examination of the social–technical relation, the argument in the second part of Lilly's response comes to the fore as these social–technical relations both shape and are shaped by networks of power. I agree that for software engineers, designers, and implementers to be aware of the societal and individual impacts of the technologies they make and implement would be an important step forward, but security technologies will only truly support the security of people when societal norms start to demand that this is so. To encourage a change in societal norms requires a different type of research engagement, one that facilitates rather than directs conversations about the roles of security technology in society and carries those conversations across the networks of power accessible to the researcher and their institution. Such facilitation requires a shift of power from researchers to participants and the communities they come from (Dunphy et al. 2014). Not only must the methods of data gathering be democratized and inclusive but so too the research design process. Research goals, questions, and design must also be in the hands of participants and their communities with the critical security researcher being only one of several voices shaping research direction. As critical security researchers, we are not only facilitators but also rewirers who have networks of power and influence that can be leveraged. By banding together and channeling the visions of cybersecurity emerging ground-up, critical security researchers can also rewire the circuits of power that are central to the academic–industrial complex that sustains cybersecurity.

Pip Thornton: The Cybersecurity–Industrial Complex

It strikes me in all this talk of deconstruction and thinking about what is being secured that it might be useful for a critical cybersecurity to unravel something I briefly mentioned before, namely the switch from *information* security to *cybersecurity*. An investigation of this semantic upgrade might reveal, for example, a different emphasis on information as the thing to be secured, to cyber—with its linguistic and cultural connotations pointing to an emphasis on the spatial and temporal—indeed chronopolitical—environment through which information moves/is moved. And I want to suggest that this shift in emphasis hinges on the ongoing commodification of information-as-data and its production, storage, and movement, and—as Clare suggests—the links between "value" and capitalist time and space.

As Powers and Jablonski (2015, 30) point out in their work on the information–industrial complex, the logistics of moving information around the globe—via email, social media, news outlets, etc.—is inexpensive and simple compared to the pre-internet era, indeed "[a] significant difference today is that transaction costs attendant with transnational flows of information approach zero." From here, we can perhaps look to Benedict Anderson (2006) to appreciate the vast geopolitical impact of technologically exponentially advancing flows of information. If the flows of information facilitated by print capitalism were key in the development of the "nation-state," so digital flows of information must be equally if not more (literally) ground-breaking/making in how they dissolve some boundaries yet are bound/bounded by the constructs and logics of the digital economy. Indeed, there is not just a near-zero cost to information flow today, but rather there is a significant profit to be made. The movement of information is now not only instantaneous but a lucrative form of income in systems of digital capitalism, and crucially this means that the quality of information suffers, while its quantity skyrockets. However, the vastness and speed of modern digital information flows make them inherently

difficult to secure, while also becoming a tool of power over citizens both in terms of fears over personal data security and in political debates about encryption, privacy, and policing. Likewise, the control over who sees (or believes) what information becomes an ever-growing problem to global security and stability.

Powers and Jablonski suggest that "digital information is commodified through its securitization" . . . "information that was primarily of use value, including phone call and internet-use metadata, was transformed into having exchange value through the lens of security" (Powers and Jablonski 2015, 73). In short, a critical cybersecurity must interrogate the agency of the narrative its nomenclature produces. It is the insecurity of information that makes it valuable economic and political capital, and that insecurity is fueled by the construct of cyber both as a brand and as a biopolitical tool, but also as an othered space through which we are now forced to communicate.

Calling it *cybersecurity* and not *information* security creates the narrative that constructs insecurity while simultaneously sustaining the security industry. It is this interdependent relationship of vested interests that—playing on the concept of the military–industrial complex—leads Powers and Jablonski to identify a "silicon triangle" between policy makers, industry, and the public (Powers and Jablonski 2015, 50). The title of their book identifies this new "information-industrial complex" as "The Real Cyber War," which is itself a telling insight into the marketability and popular impact of *cyber* as opposed to *information*. Going back to my first piece, the word cyber is worth far more in a Google advert than information.

One other important point in this critique is how a cybersecurity–industrial complex applies itself in the Global South. Just as the "preservation of colonial markets" was an important factor in the development of the military–industrial complex (Pursell 1972), so critical cybersecurity studies must also attend to the constructs of (in)securitization in developing countries. Quasi-philanthropic data grabs under the guise of free connectivity by companies such as Facebook and Google demonstrate the co-dependence of insecurity and security, revealing how and for whose profit such data are exploited, and in whose interests the insecure remain as such.

I started off writing this section with a view to picking up the previous thread about cybersecurity as symptom or cause, but it tied me in knots. However, through adopting the lens of a cybersecurity–industrial complex, it becomes clear why this thread is so inherently difficult to unpick; cybersecurity is a pharmakon—it is both the poison and the cure, and it is to this complex that a critical cybersecurity must urgently attend.

Paths Forward

> "Although critical theory takes many different forms, it always distinguishes itself from other forms of theorising in terms of its orientation towards change and the possibility of futures that do not reproduce the patterns of hegemonic power of the present." (Hutchings 2007, 72)

As Kimberly Hutchings reflects, there is an orientation in critical approaches toward articulating new futures with alternative forms of power. This is no different with regard to thinking about the dominant forms of power in cybersecurity, which range across those who create, control, sell, and leverage technology to often subjugate, control, and simply make life difficult against their interests. Within this discussion, we have provided a range of different ways of how to "do" critical cybersecurity, drawn from our various interpretations of what it means to be critical. These ranged from resituating our perspectives and frames of thought on economics and techno-dreams to opening up pluriverses, the role of nonhuman agencies to the potentials of provincializing cybersecurity. This was accompanied by an explicit methodological attention to hacking, to researching through STS,

to how to change technological design through facilitating, rather than directing, conversations. At its very broadest though, we have taken critical here to mean critical of positivist or technologically essentializing approaches.

As evident from our conversation, however, there is no one way to *do* cybersecurity. As much as cybersecurity is distributed, contested, and seeps into everyday life, there is no one way to engage in a critical project as much as there are alternative disciplinary perspectives and methodologies. We hope that we have reflected not only on such an impossibility but also on the many paths that we may take, which suggest a methodological and conceptual heterogeneity as much as practical reasons to engage in policy, technological design, and question the academic, political, (post-)colonial, and economic systems we find ourselves within. So, rather than offering "conclusions" as if to claim that there is *ever* a conclusion to a critical project, below we offer some collective thoughts and four potential pathways on what it may be to critically engage and do cybersecurity.

First, critical cybersecurity could act as a "home" for a range of perspectives and disciplines that do not have to converge on a particular theme.[13] However, what lingers is the plural "we" that pervades our collective discussion, and one that should remain central to any form of critical engagement, especially as we are all scholars from the global minority. Thus, what "we" do *we* wish to encourage? This may include stronger engagements—or facilitating—with disadvantaged communities.

Second, and relatedly, as with any critical project, this will involve constant self-reflexivity about the "we" that such a project envisions. As Myriam proposes, this encourages us to reflect on how we may all become "activists." This will require always asking who stands to benefit, as in Pip's contribution, or how we may be simply contributing to an ever-growing "cybersecurity–industrial complex." In asking who stands to benefit, we need to accept that we do not know how to do cybersecurity. It is only in conversation with others, centering their lives, practices, and knowledges—which Andrew terms pluriversal and Clare provincializing—that we may identify different futures. It means being an activist in sometimes subtle, sometimes more overt, ways depending on who we are working with, and in what contexts and places.

In setting up such a home with which we may become "activists," it requires, third, building coalitions and alliances. To "do" cybersecurity means we must also work with those who may not be our conventional "allies" as much as we may wish to build and assist those communities that are not given sufficient attention or are not heard enough (whether that be people of color, those from the global majority, women, persons with disabilities, and many others). This means articulating who we want to speak to, why, and what sites of future discussion should be. There may be times we simply promote discussions of others, developing new forms of setting the research agenda, or find ways of finding funding and time to build *with* these communities, rather than *for* these communities.

This brings us to a fourth path, which is about how we communicate and articulate the diversity of this thing we call cybersecurity. This may be through creative and artistic interventions, in hacking, and even developing new "stories" as Lizzie argues, within and outside of policy. These stories might inform new ways of engaging the figure of the "user" amid nonhuman agencies, as Lilly implores us to recognize, whereas hacking and interventions may create new spaces for politics, awareness, and change. It is on the latter two paths whereby our thinking and practice become *relevant*; we must translate, work with, and articulate why critical perspectives are important, whether that be through participatory methods, questioning academic work that perpetuates "cyber-hype," or challenging framings in policy reports.

[13] *MYRIAM*: What makes us "cyber" scholars though? There has to be some differentiation and some common ground, no? *PIP*: I would run a mile from being called a "cyber" scholar... I'm not sure how this works, but I want to be a scholar being critical of "cyber" without being a "cyber" scholar, which is possibly why it's so hard in disciplinary terms to get any purchase or impact.

Cybersecurity—although complex and riddled with discursive and material power differences—must have critical voices (that may not identify as cybersecurity at all). This may mean playing with different terms and accepting that sometimes one must use the tools provided for us to forge instruments that permit new formations to take place. It is then an effort to open up the field, one with disciplinary frictions that are productive for something anew, not a closing. This requires an expansion of possibilities, writing against boundaries, perhaps "hacking," getting stuck in, and being constitutive of what Lizzie terms as part of our redemption. Indeed, drawing on themes of resistance and the deconstruction of this subject we are meant to be studying, perhaps we should be thinking about what a critical cybersecurity might *undo* rather than what it can *do*—how can it destabilize power structures and challenge inequalities, for example, even if this means *undoing* the narratives of cybersecurity? As much as any "doing" does, it must also undo, to permit something new to emerge. Whatever it is, we all know that cybersecurity as it currently stands is ill-suited to the global majority, disadvantaged communities, and a project of critical cybersecurity is a broader project of resistance and revision in a world of computationally mediated interactions.

Acknowledgments

We would like to thank the generous comments from the three anonymous reviewers and to the current and past editors of IPS who have supported and encouraged this alternative form of writing in this collective discussion piece.

References

ABBOUD, SAMER, OMAR S. DAHI, WALEED HAZBUN, NICOLE SUNDAY GROVE, CORALIE PISON HINDAWI, JAMIL MOUAWAD, AND SAMI HERMEZ. 2018. "Towards a Beirut School of Critical Security Studies." *Critical Studies on Security* 6 (3): 273–95.

ADAMS, ANNE, AND MARTINA ANGELA SASSE. 1999. "Users Are Not the Enemy." *Communications of the ACM* 42 (12): 40–46.

ALBRECHT, MARTIN R., JORGE BLASCO, RIKKE BJERG JENSEN, AND LENKA MAREKOVÁ. 2021. "Collective Information Security in Large-Scale Urban Protests: The Case of Hong Kong." arXiv: https://arxiv.org/abs/2105.14869.

AMARO, ROMAN, AND MURAD KHAN. 2020. "Towards Black Individuation and a Calculus of Variations." *E-Flux* 109. Accessed June 2, 2020. https://www.e-flux.com/journal/109/330246/towards-black-individuation-and-a-calculus-of-variations/.

AMOORE, LOUISE. 2020. *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Durham, NC: Duke University Press.

ANDERSON, BENEDICT. 2006. *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. London: Verso books.

ANDERSON, WARWICK. 2017. "Postcolonial Specters of STS." *East Asian Science, Technology and Society: An International Journal* 11 (2): 229–33.

ARADAU, CLAUDIA. 2004. "Security and the Democratic Scene: Desecuritization and Emancipation." *Journal of International Relations and Development* 7 (4): 388–413.

———. 2010. "Security That Matters: Critical Infrastructure and Objects of Protection." *Security Dialogue* 41 (5): 491–514.

ARADAU, CLAUDIA, AND RENS VAN MUNSTER. 2017. "Poststructuralist Approaches to Security." In *Routledge Handbook of Security Studies*, edited by Myriam Dunn Cavelty and Thierry Balzacq, 75–84. Abingdon: Routledge.

AUSTIN, JONATHAN LUKE. 2019. "Security Compositions." *European Journal of International Security* 4 (3): 249–73.

BALDWIN, DAVID A. 1997. "The Concept of Security." *Review of International Studies* 23 (1): 5–26.

BALZACQ, THIERRY, ed. 2015. *Contesting Security: Strategies and Logics*. Abingdon: Routledge.

BALZACQ, THIERRY, TUGBA BASARAN, DIDIER BIGO, EMMANUEL-PIERRE GUITTET, AND CHRISTIAN OLSSON. 2010. "Security Practices." In *International Studies Encyclopedia Online*, edited by Robert A. Denemark and Renée Marlin-Bennett. Malden, MA: Blackwell Publishing.

Barkawi, Tarak, and Mark Laffey. 2006. "The Postcolonial Moment in Security Studies." *Review of International Studies* 32 (2): 329–52.

Basaran, Tugba, Didier Bigo, Emmanuel-Pierre Guittet, and R.B.J. Walker, eds. 2017. *International Political Sociology: Transversal Lines*. Abingdon: Routledge.

Bates, Jo, Yu-Wei Lin, and Paula Goodale. 2016. "Data Journeys: Capturing the Socio-Material Constitution of Data Objects and Flows." *Big Data & Society* 3 (2): 2053951716654502.

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.

Bertrand, Sarah. 2018. "Can the Subaltern Securitize? Postcolonial Perspectives on Securitization Theory and Its Critics." *European Journal of International Security* 3 (3): 281–99.

Bhambra, Gurminder K. 2007. "Sociology and Postcolonialism: Another 'Missing' Revolution?" *Sociology* 41 (5): 871–84.

———. 2010. "Sociology After Postcolonialism: Provincialized Cosmopolitanism and Connected Sociologies." In *Decolonizing European Sociology: Transdisciplinary Approaches*, edited by Encarnacion Gutierrez Rodriguez, Manuela Boatcă, and Sérgio Costa, 33–47. Aldershot: Ashgate.

Bijker, Wiebe E., Thomas P. Hughes, Trevor Pinch, and Deborah G. Douglas. 2012. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge: The MIT Press.

Borghard, Erica D., and Shawn W. Lonergan. 2019. "Cyber Operations as Imperfect Tools of Escalation." *Strategic Studies Quarterly* 13 (3): 122–45.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

Browning, Christopher S., and Matt McDonald. 2013. "The Future of Critical Security Studies: Ethics and the Politics of Security." *European Journal of International Relations* 19 (2): 235–55.

C.A.S.E. Collective. 2006. "Critical Approaches to Security in Europe: A Networked Manifesto." *Security Dialogue* 37 (4): 443–87.

Castree, Noel. 2001. "Commentary." *Environment and Planning A: Economy and Space* 33 (9): 1519–25.

Chakrabarty, Dipesh. 2008. *Provincializing Europe: Postcolonial Thought and Historical Difference*. Princeton, NJ: Princeton University Press.

Coles-Kemp, Lizzie. 2020. "Inclusive Security: Digital Security Meets Web Science." *Foundations and Trends in Web Science* 7 (2): 88–241.

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): 41–88.

Coles-Kemp, Lizzie, and René Rydhof Hansen. 2017. "Walking the Line: The Everyday Security Ties That Bind." In *Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9–14, 2017, Proceedings*, edited by Theo Tryfonas, 464–80. Cham: Springer International Publishing.

Cook, Ian, and Philip Crang. 1996. "The World on a Plate: Culinary Culture, Displacement and Geographical Knowledges." *Journal of Material Culture* 1 (2): 131–53.

Critical Art Ensemble. 1994. *The Electronic Disturbance*. New York: Autonomedia.

———. 1996. *Electronic Civil Disobedience and Other Unpopular Ideas*. New York: Autonomedia.

Dillon, Michael. 1996. *Politics of Security: Towards a Political Philosophy of Continental Thought*. London: Routledge.

Dunn Cavelty, Myriam. 2018. "Cybersecurity Research Meets Science and Technology Studies." *Politics and Governance* 6 (2): 22–30.

Dunn Cavelty, Myriam, and Andreas Wenger. 2020. "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." *Contemporary Security Policy* 41 (1): 5–32.

Dunphy, Paul, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. 2014. "Understanding the Experience-Centeredness of Privacy and Security Technologies." In *Proceedings of the 2014 New Security Paradigms Workshop*, NSPW '14, 83–94. New York: Association for Computing Machinery.

Dwyer, Andrew C. 2021. "Cybersecurity's Grammars: A More-than-Human Geopolitics of Computation." *Area* 1–8. doi:10.1111/area.12728.

Dwyer, Andrew C., Nathaniel O'Grady, Pip Thornton, Till Straube, Emily Gilbert, and Louise Amoore. 2021. "Cloud Ethics: Algorithms and the Attributes of Ourselves and Others." *The AAG Review of Books* 9 (3): 36–49.

Escobar, Arturo. 2018. *Designs for the Pluriverse: Radical Interdependence, Autonomy, and the Making of Worlds*. Durham, NC: Duke University Press.

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

FLOYD, RITA. 2011. "Can Securitization Theory Be Used in Normative Analysis? Towards a Just Securitization Theory." *Security Dialogue* 42 (4–5): 427–39.

FOUAD, NORAN SHAFIK. 2021. "The Non-Anthropocentric Informational Agents: Codes, Software, and the Logic of Emergence in Cybersecurity." *Review of International Studies*. 1–20. doi:10.1017/S0260210521000681.

GRAHAM, MARK. 2013. "Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities?" *The Geographical Journal* 179 (2): 177–82.

HAGMANN, JONAS, HENDRIK HEGEMANN, AND ANDREW NEAL. 2018. "The Politicisation of Security: Controversy, Mobilisation, Arena Shifting: Introduction by the Guest Editors." *European Review of International Studies* 5 (3): 3–29.

HARAWAY, DONNA JEANNE. 2016. *Staying with the Trouble: Making Kin in the Chthulucene*. Experimental Futures. Durham, NC: Duke University Press.

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

———. 2016. "Cognitive Assemblages: Technical Agency and Human Interactions." *Critical Inquiry* 43 (1): 32–55.

HESS, DAVID J. 2009. "The Potentials and Limitations of Civil Society Research: Getting Undone Science Done." *Sociological Inquiry* 79 (3): 306–27.

HICKS, MAR. 2018. *Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computing. History of Computing*. Cambridge, MA: MIT Press.

HOBSON, JOHN M. 2007. "Is Critical Theory Always for the White West and for Western Imperialism? Beyond Westphilian towards a Post-Racist Critical IR." *Review of International Studies* 33 (S1): 91–116.

HOIJTINK, MARIJN, AND MATTHIAS LEESE, eds. 2019. *Technology and Agency in International Relations. Emerging Technologies, Ethics and International Affairs*. Abingdon: Routledge.

HOLMWOOD, JOHN. 2009. "The Challenge of Global Social Inquiry." *Sociological Research Online* 14 (4): 100–104.

HOWELL, ALISON, AND MELANIE RICHTER-MONTPETIT. 2020. "Is Securitization Theory Racist? Civilizationism, Methodological Whiteness, and Antiblack Thought in the Copenhagen School." *Security Dialogue* 51 (1): 3–22.

HUDSON, HEIDI. 2005. "'Doing' Security as Though Humans Matter: A Feminist Perspective on Gender and the Politics of Human Security." *Security Dialogue* 36 (2): 155–74.

HUTCHINGS, KIMBERLY. 2007. "Happy Anniversary! Time and Critique in International Relations Theory." *Review of International Studies* 33 (S1): 71–89.

KARAGIANNOPOULOS, VASILEIOS. 2021. "A Short History of Hacktivism: Its Past and Present and What Can We Learn from It." In *Rethinking Cybercrime: Critical Debates*, edited by Tim Owen and Jessica Marshall, 63–86. Cham: Palgrave Macmillan.

KAZANSKY, BECKY. 2021. "'It Depends on Your Threat Model': The Anticipatory Dimensions of Resistance to Data-Driven Surveillance." *Big Data & Society* 8 (1): 2053951720985557.

KELLO, LUCAS. 2017. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press.

KLINKE, IAN. 2013. "Chronopolitics: A Conceptual Matrix." *Progress in Human Geography* 37 (5): 673–90.

LAW, JOHN. 2004. *After Method: Mess in Social Science Research*. Abingdon: Routledge.

LAW, JOHN, AND ANNEMARIE MOL. 2001. "Situating Technoscience: An Inquiry into Spatialities." *Environment and Planning D: Society and Space* 19 (5): 609–21.

LINDSAY, JON R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (3): 365–404.

MCCLUSKEY, EMMA. 2019. *From Righteousness to Far Right: An Anthropological Rethinking of Critical Security Studies*. Montreal: McGill-Queen's University Press.

NATIONAL CYBER SECURITY CENTRE. 2017. "People: The Strongest Link." *Cyber UK, Liverpool*, March 28. Accessed July 13, 2021. https://www.ncsc.gov.uk/speech/people—the-strongest-link.

PARIKKA, JUSSI. 2007. *Digital Contagions: A Media Archaeology of Computer Viruses*. New York: Peter Lang.

PFLEEGER, SHARI LAWRENCE, M. ANGELA SASSE, AND ADRIAN FURNHAM. 2014. "From Weakest Link to Security Hero: Transforming Staff Security Behavior." *Journal of Homeland Security and Emergency Management* 11 (4): 489–510.

PICKERING, ANDREW. 1993. "The Mangle of Practice: Agency and Emergence in the Sociology of Science." *American Journal of Sociology* 99 (3): 559–89.

POVINELLI, ELIZABETH A. 2016. *Geontologies: A Requiem to Late Liberalism*. Durham, NC: Duke University Press.

POWERS, SHAWN M., AND MICHAEL JABLONSKI. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana, IL: University of Illinois Press.

PURSELL, CARROLL W., ed. 1972. *The Military–Industrial Complex*. New York: Harper & Row.

QUET, MATHIEU, AND MARINE AL DAHDAH. 2020. "Technologies without Borders? The Digitization of Society in a Postcolonial World." *Science, Technology and Society* 25 (3): 363–67.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. London: C. Hurst & Co.

Roe, Paul. 2012. "Is Securitization a 'Negative' Concept? Revisiting the Normative Debate over Normal versus Extraordinary Politics." *Security Dialogue* 43 (3): 249–66.

Rosiek, Jerry Lee, Jimmy Snyder, and Scott L. Pratt. 2020. "The New Materialisms and Indigenous Theories of Non-Human Agency: Making the Case for Respectful Anti-Colonial Engagement." *Qualitative Inquiry* 26 (3–4): 331–46.

Salter, Mark B., Carol Cohn, Andrew W. Neal, Annick T.R. Wibben, J. Peter Burgess, Stephan Elbe, and Jonathan Luke Austin et al. 2019. "Horizon Scan: Critical Security Studies for the Next 50 Years." *Security Dialogue* 50 (4_suppl): 9–37.

Saltzer, J.H., and M.D. Schroeder. 1975. "The Protection of Information in Computer Systems." *Proceedings of the IEEE* 63 (9): 1278–1308.

Sampson, Tony D. 2012. *Virality: Contagion Theory in the Age of Networks*. Minneapolis, MN: University of Minnesota Press.

Saville, Samantha M. 2021. "Towards Humble Geographies." *Area* 53 (1): 97–105.

Schia, Niels Nagelhus. 2018. "The Cyber Frontier and Digital Pitfalls in the Global South." *Third World Quarterly* 39 (5): 821–37.

Schwarz, Elke. 2021. "Autonomous Weapons Systems, Artificial Intelligence, and the Problem of Meaningful Human Control." *The Philosophical Journal of Conflict and Violence* V (1): 53–72.

Slupska, Julia, and Leonie Maria Tanczer. 2021. "Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things." In *The Emerald International Handbook of Technology Facilitated Violence and Abuse*, edited by Jane Bailey, Asher Flynn, and Nicola Henry, 663–88. Bingley: Emerald Publishing Limited.

Smeets, Max, and James Shires. 2017. "Contesting Cyber: Introduction and Part I." *New America*. December 4. Accessed July 15, 2021. http://web.archive.org/web/20210715102722/https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/contesting-cyber/.

Smith, Graham M. 2005. "Into Cerberus' Lair: Bringing the Idea of Security to Light." *The British Journal of Politics and International Relations* 7 (4): 485–507.

Stengers, Isabelle. 2010. *Cosmopolitics I*, translated by Robert Bononno. Minneapolis, MN: University of Minnesota Press.

Stevens, Clare. 2020. "Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet." *Contemporary Security Policy* 41 (1): 129–52.

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

Suchman, Lucy. 2012. "Configuration." In *Inventive Methods: The Happening of the Social*, edited by Lury, Celia and Wakeford, Nina, 48–60. Routledge: London.

Thornton, Pip. 2018. "A Critique of Linguistic Capitalism: Provocation/Intervention." *GeoHumanities* 4 (2): 417–37.

Wark, McKenzie. 2019. *Capital Is Dead: Is This Something Worse?* New York: Verso Books.

Yan, Zheng, Thomas Robertson, River Yan, Sung Yong Park, Samantha Bordoff, Quan Chen, and Ethan Sprissler. 2018. "Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment?" *Computers in Human Behavior* 84 (July): 375–82.

Yusoff, Kathryn. 2018. *A Billion Black Anthropocenes or None*. Minneapolis, MN: University of Minnesota Press.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

Zurko, Mary Ellen, and Richard T. Simon. 1996. "User-Centered Security." In *Proceedings of the 1996 Workshop on New Security Paradigms*, NSPW '96, 27–33. New York: Association for Computing Machinery.