Critical Studies on Security

ISSN: 2162-4887 (Print) 2162-4909 (Online) Journal homepage: www.tandfonline.com/journals/rcss20

Queering cybersecurity: An alternative research agenda

Sulagna Basu & Caitlin Biddolph

To cite this article: Sulagna Basu & Caitlin Biddolph (09 May 2025): Queering cybersecurity: An alternative research agenda, Critical Studies on Security, DOI: 10.1080/21624887.2025.2502716

To link to this article: https://doi.org/10.1080/21624887.2025.2502716

Published online: 09 May 2025.

CRITICAL STUDIES ON SECURITY
https://doi.org/10.1080/21624887.2025.2502716

Queering cybersecurity: An alternative research agenda

Sulagna Basu[a] and Caitlin Biddolph[b]

[a]Government and International Relations, University of Sydney, Sydney, Australia; [b]School of International Studies and Education, University of Technology, Sydney, Australia

ABSTRACT

Current scholarship on cybersecurity in International Relations tends to emphasise state-centric, militarised, and overly securitised perspectives. However, an emerging body of critical and feminist scholarship seeks to challenge this dominant perspective. This article draws from and extends these critical perspectives to propose a creative intervention of queering cybersecurity. By bringing queer scholarship, methodologies, and possibilities into conversation with critical cyber scholarship, the article sketches the contours of an alternative research agenda. This is developed firstly, by drawing necessary attention to the experiences of queer people in cyberspace, including both generative and violent encounters that enable spaces for queer flourishing. Secondly, by developing and maintaining a queer, subversive ethos committed to disrupting the cyber status quo through queering, hacking, and glitching the system. Thirdly, by exposing the violent hierarchies of cybersecurity, which sit at the intersections of cisheterosexism, coloniality, racism, and other structures of violence. Through empirical examples presented, the article demonstrates a proposed research agenda, which offers opportunities to expand cyber to include queer intimacies and subjectivities, disrupt binary logics of cyber securitisations, and challenge the boundaries of knowledge production in and on cybersecurity. Ultimately, the article's intervention for queering cyber scholarship invites further exploration and contemplation for reimagining cybersecurity otherwise.

KEYWORDS
Queer; cybersecurity; cyberspace; glitch; technology

Introduction

Scholarship on cybersecurity has long been dominated by technical perspectives focused narrowly on threats and vulnerabilities, while largely overlooking the human context and social dynamics within which cybersecurity operates. However, more recently, an emerging body of critical and feminist scholarship within and beyond International Relations (IR) has developed to challenge dominant militarised and technified perspectives of cybersecurity (Brown and Pytlak 2020; Dwyer Andrew et al. 2022; Mhajne and Henshaw 2024b; Mhajne, Luna, and Whetstone 2021; Millar and Shires 2024; Millar, Shires, and Tropina 2021; Slupska 2019). Drawing from and extending these critical approaches, we propose a creative intervention of *queering* cybersecurity, to unsettle narrow perspectives that

CONTACT Sulagna Basu sulagna.basu@sydney.edu.au

dominate prevalent disciplinary accounts. Our goal is to 'queer' cybersecurity – to expose and transgress the gendered, racialised, and cisheteronormative frames implicated in practices of cybersecurity, and engage in a broader exploration of the intricacies and complexities embedded within the frameworks of knowledge related to cyber technologies.[1]Just as queering IR is 'not about making IR queer as if it weren't already' (Wilcox 2014, 612), our exercise in queering cybersecurity is similarly about making explicit the queerness already installed in cybersecurity – that it is always already constituted by gender, sexuality, race, and other normativities, and that it is always already fluid and patently transgressive. We contemplate the plural visions and work that queer does by articulating it as a noun (i.e. attentive to the embodied experiences and identities of queer lives), a verb (i.e. to expose the taken-for-granted normativities and gendered, sexual power arrangements), and a logic (i.e. queerness constitutes everything) (Biddolph 2020, 408). For us, informed by queer scholarship within and beyond IR, queer is irreducible to LGBT politics or to matters exclusively concerning gender, sex, and sexuality (Giffney 2004). Attending to and centring queer people's experiences of cybersecurity is an important part of our queer approach, but it is not the only aspect. In this vein, it is imperative to emphasise that our queer approach does not abstract and strip queer from the lived realities of queer people, nor do we deploy queer as mere metaphor that disembodies it from specific social and material contexts (Stoffel and Roland Birkvad 2023, 861–863). Instead, recognising the concrete social relations that shape queer experiences of the digital, we centre these *alongside* queer analyses and critiques of cyber-normativities. The queer perspective we adopt shares a poststructural commitment to deconstruction but moves beyond poststructuralism through an equally important commitment to the (gendered and sexual) fluidities and pluralities that encompass the social world (Namaste 1994).

Our queer approach to cybersecurity, accordingly, reflects and extends feminist and postcolonial approaches (Mhajne and Henshaw 2024b). It does so by retaining a suspicion and criticality of the exclusionary assumptions and practices that dominate cybersecurity discourse and policies, such as its erasure of gender-based harms and its colonial hierarchies. We adopt a queer approach that sees gender and sexuality as interconnected with race, coloniality, class, and other vectors of power and experience that can and ought to be queered (Alexander 1994; Cohen 1997). Our queer perspective also embodies an antinormative, transgressive position, one that goes beyond feminist and postcolonial cybersecurity scholarship in IR to ask what it might mean to abandon the disciplining and securitising logics of cybersecurity,[2] and their attendant violent effects. As we elaborate throughout this article, these violent effects manifest in multiple ways, both online and offline. These include the intensification of surveillance systems that specifically target racialised and gendered bodies, the predatory digitisation of carceral systems that disproportionally impact marginalised communities, and the deployment of national security frameworks that render insecure the very populations they claim to protect. To be clear, our queering of cybersecurity is therefore a critique and rejection of cybersecurity as violent discourse and practice, rather than a project seeking queer inclusion within cybersecurity policies. Moreover, our queer approach decentres the white, global North, capitalist, straight, cismale cyber subject, and recentres the queer, subaltern outlaw as both cyber subject and cyber transgressor.

In this article, we follow Mhajne and Henshaw's definition of cybersecurity, 'referring to the security of digital systems, infrastructure, information, and data as well as the human security of those who interact through and within the digital space' (2024, 15). While Mhajne and Henshaw work with this definition at the scholarly and policy level, our own approach departs from a policy-focused analysis. As such, adopting a broad working definition allows us to push the boundaries of what could and might be classified as a question of cybersecurity, including the potentially violent, securitising moves this broadening would enable. Thus, the empirical examples we identify throughout this article do not reflect conventional cybersecurity concerns (e.g. cyber war, attacks on national cyber capabilities). Rather, we include examples of the patriarchal, homo- and transphobic, racist, and capitalist violences of cybersecurity as it manifests through artificial intelligence (AI), surveillance, and other forms of digital politics (see also Mhajne and Henshaw 2024b). We do not seek to securitise these areas of digital politics, noting that securitisation is a violent process that necessarily demarcates subjects and objects as variously (un)worthy of security and others as targets of securitised intervention. Rather, we do so in order to move beyond current critical cybersecurity scholarship, to provide a conceptual queering that broadens who and what constitutes cyber politics. So, while we define cybersecurity here, we offer this definition as a starting point and a springboard for considering how queer perspectives might challenge existing assumptions about what cybersecurity is, and the various subjects and objects that are brought into being by cybersecurity discourses and practices.

This article makes two significant contributions to the field of critical security studies. The first is conceptual in nature, as the article introduces insights from queer theory and queer scholarship in IR to critical perspectives on cybersecurity. This allows for a necessary engagement with the rich body of scholarship in queer studies along with the concomitant diversity of perspectives towards an area in security studies that has only recently begun to incorporate more critical perspectives. The second contribution of this article is the proposal of a queer cybersecurity research agenda aimed at addressing systemic silences insufficiently addressed in critical cybersecurity scholarship on matters of gender and sexuality. This adds to the broad landscape of critical perspectives in security studies and specifically paves the way for future research on cybersecurity driven by a 'queer intellectual curiosity' (Weber 2016), with the potential to extend, broaden, and reframe current ways of understanding and thinking about cybersecurity.

Our article is structured as follows. In the next section, we provide a brief literature review of critical cybersecurity scholarship and queer IR, situating our contribution as one that speaks to these two literatures, but also places them in conversation to ask what queer perspectives might offer to and for cybersecurity studies. The remaining sections of the article present our queer cybersecurity research agenda, which entails three main orientations. First, we explore the experiences of queer people in cyberspace, including both generative and violent encounters that enable spaces for queer flourishing, but also insecurity.[3]Second, we trace the power of antinormative cybersecurity, an approach which disrupts the cyber status quo and finds ways of queering, hacking, and glitching the system. Third, we scrutinise the cisheterosexist, colonial, racist, anthropocentric, and neoliberal capitalist foundations of cybersecurity. Finally, by way of conclusion, we reiterate the value of queering cybersecurity and propose this alternative research agenda for broadening, disrupting, and reimagining cybersecurity otherwise. Engaging in thinking otherwise is a necessary counter to the violent status quo of cybersecurity scholarship and practice. It offers alternative imaginaries for experiencing and/or rejecting cybersecurity, grounded in the lived realities of queer, racialised, and subaltern communities.

(Critical) cybersecurity and queer international relations

In recent years, critical cybersecurity scholarship has emphasised the necessity of shifting towards more social and human-centred understandings of cybersecurity that extend beyond state prerogatives to encompass a broader range of vulnerabilities experienced by communities across social worlds. Significantly, the critical turn has included important feminist contributions to cybersecurity that have established the relevance of gender to identifying the differential harms and inequalities in relation to cybersecurity practices and discourses (Brown and Pytlak 2020; Mhajne and Henshaw 2024a; Mhajne and Whetstone 2021; Millar, Shires, and Tropina 2021; Slupska et al. 2021). These perspectives bring feminist insights to cybersecurity both by arguing for the expansion of cybersecurity into spaces of prevailing policy practices related to gender-based violence (Whetstone and Luna 2024) as well as by highlighting the importance of recentring intimate, personal, and everyday spaces as legitimate sites for consideration in studies and practices of cybersecurity (Meuller 2023; Mhajne, Luna, and Whetstone 2021; Slupska 2019). While this remains a rich burgeoning area of scholarship, we argue that incorporating queer approaches can further illuminate the existing harms faced by queer people and marginalised groups, which remain largely unacknowledged even within critical cybersecurity studies.

Additionally, an important contribution to expanding state-centric conceptions of cybersecurity has been the recognition that cybersecurity cannot be reduced to a binary conceptualisation as either an exclusively technical or social phenomenon. Rather, it is increasingly understood as a 'work-in-progress' (C. Stevens 2020, 133) involving complex interactions between technological systems, social processes, and political dynamics and therefore challenging the purported neutrality and objectivity of technical cybersecurity knowledge and practices (Cristiano 2018). Considering the lack of agreement about what cybersecurity is and how it should be governed, critical scholarship emphasises the 'ontological politics' of cybersecurity, meaning the ways in which cybersecurity discourses and practices actively produce certain realities while foreclosing others (Liebetrau and Kjærgaard Christensen 2021). This opens up space for examining how cybersecurity discourses and practices may reinforce or challenge existing power relations, allowing for greater interdisciplinary engagement to help unpack the normative assumptions and political effects of cybersecurity in specific contexts.

A crucial area of engagement has emerged that also highlights the importance of plural perspectives beyond Eurocentric universalisms to deconstruct dominant rationalities, and challenge power structures. Scholars have, for instance, applied a decolonial lens to identify racial hierarchies in cybersecurity expertise that valorise Western knowledge while marginalising perspectives from the Global South (Mumford and Shires 2023). Similarly, questioning Eurocentric paradigms, scholars have also interrogated the ways in which cybersecurity capacity building frameworks tend to reproduce North-South inequalities (Hurel 2022). While usefully broadening the conversation, these critical perspectives still overlook the unique cybersecurity challenges faced by queer communities. Specifically, these include heightened vulnerability to online harassment, surveillance, and censorship that disproportionately impact queer expression, further emphasising the critical need for insights that queer theory could bring to reimagining cybersecurity.

As Dwyer Andrew et al. (2022) argue, rather than isolating or bringing forth a singular 'critical cybersecurity', scholarship should 'reflect, discuss, and stretch the complexities of cybersecurity' as a contested concept (3). A queer broadening is vital to this project. It can help de-essentialise and decentre the universal, abstract, hegemonic frameworks implicit in much cybersecurity research and reorient attention to embodied, situated experiences of (in)security at the intersection of gender, sexuality, race, geography, and other axes of identity and oppression.

Our article also speaks to a growing body of Queer IR scholarship, a diverse agenda that emerged out of, builds upon, and (sometimes) challenges existing critical, feminist, and postcolonial approaches to global politics. Broadly conceived, Queer IR analyses how normativities of all kinds, but particularly those related to gender, sex, sexuality, race, nation, class, religion, and caste, constitute the international (see for e.g. Díaz Calderón 2021; Manchanda 2015; Rao 2020; Richter-Montpetit 2017; Richter-Montpetit and Weber 2017; Sjoberg 2017; Weber 2016; Wilcox 2014; Wilkinson 2017). Queer IR 'has demonstrated how sex(uality) connects to international politics, identifying, for instance, the sexualised logics through which international security works and how security discourses often rest upon gendered – sexualised – racialised constructions about what/who needs protection and what/who is a threat' (Cooper-Cunningham 2022, 10). It is not within the scope of our article to provide a comprehensive literature review of this scholarship (see instead Richter-Montpetit and Weber 2017), but rather to consider how cybersecurity might be queered, and contribute to a new area of Queer IR scholarship. We have yet to encounter Queer IR analyses of cybersecurity,[4] at least according to a widely accepted understanding of cybersecurity, which fixates on digital systems and networks, and the state-centric securitising moves and threats that emanate from this 'lawless frontier'. But when our understanding of what constitutes cybersecurity is broadened to include technologies such as AI, data, and digital surveillance, we can identify contributions from Queer IR that ostensibly form the foundations for queering cybersecurity.

Queer IR scholars have, for instance, taken drone warfare as a subject of analysis (Clark 2018, 2019; Daggett 2015). While again, we might consider drones outside the remit of a typical definition of cybersecurity, a queer approach asks that we broaden this conceptualisation and consider how drones – as a complex enmeshment of non-human material, digital technology and human inputs – are examples of lethal cybersecurity practices waging direct violence on people. Queer analyses have exposed the 'gendered and racialized assumptions' that are encoded into drone warfare so that particular people and populations are rendered threats (Wilcox 2017, 21). Moreover, categories such as race, age, and gender, when programmed into drone algorithms, assume a 'supposed perfectibility' (24) that cannot compute gender, for example, as anything other than a binary reality. Queer IR scholars have also scrutinised the transphobic and Islamophobic practices of full body scanners in airports, a form of (in)security that relies on a similar entanglement of human input, technological hardware, algorithm, and coding that surveils bodies and marks them as variously safe or risky (Shepherd and Sjoberg 2012; R. Hall 2015; Wilcox 2015; see also Puar 2018). A queer analysis reveals how trans people 'are produced as deviant in the airport security assemblage not just because they do not conform to gendered expectations, but because they do not conform to the state's desire to regulate bodies as fixed and unchanging, a desire that is undermined by the trans- disruption of the state's assumption of bodies and genders as fixed and immutable' (Wilcox 2015, 106; see also Currah and Mulqueen 2011).

In this article, we therefore situate our contribution within Queer IR and critical cybersecurity scholarship, recognising that for the former, there are opportunities to focus on cybersecurity as an analytical site, and that for the latter, queer perspectives could be brought to bear and extend existing feminist, postcolonial, and posthuman contributions. However, staying within disciplinary IR is insufficient for developing queer analyses of cybersecurity. In what follows, we propose an alternative queer cybersecurity agenda that draws on feminist, crip, critical race, decolonial, abolitionist, Indigenous, and queer perspectives to digital politics, in addition to the treatment of cyberspace and technology from disciplinary IR. In drawing from a wide scope of such anti-racist and anti-colonial scholarship we emphasise our proposed research agenda's commitment to interrogating the power relations and structures that inform current scholarship and practice on what counts as cybersecurity. By engaging with these distinct but often interrelated bodies of work, each of which offer rich, profound, liberatory critiques, we envision the work of 'queering' as the building of a compendium of tools that invite further engagement and critique within critical cybersecurity scholarship.

Queering cybersecurity: an alternative research agenda

Queering cybersecurity allows for a multitude of research possibilities. In this article, we identify three core contributions of a queer cybersecurity research agenda. However, we note that these are not the only avenues for queer research in this space. As we reflect in the conclusion, further research to expand this agenda could include a focus on queering cyber infrastructures, or the queering of cybersecurity policies and strategies. In what follows, we present what we believe are three essential elements or orientations of the research agenda we develop in this article. First, we argue that queering cybersecurity must situate and centre queer people as embodied, agential subjects of cybersecurity. Second, we put forward a queer approach to cybersecurity that challenges the various cyber normativities we explore throughout the article, by glitching the system. Finally, we propose that such a research agenda must also challenge and disrupt the cisheterosexist, racist, colonial, anthropocentric, capitalist, and militarist assumptions that underpin cybersecurity practices and theorising.

Queer subjects and/in cybersecurity

Queer people are subjected to the cisheterosexist and transphobic violence of cybersecurity. But they are also cyber agents, and the digital realm can be a site of queer activism, desire, and intimacy, even while it is also a site of violence (Cockayne and Richardson 2019, 13). The queer approach to cybersecurity we develop in this article owes much to existing feminist contributions, which have identified the gendered harms and inequalities of cybersecurity and the cyber realm (Brown and Pytlak 2020; Mhajne, Luna, and Whetstone 2021; Millar, Shires, and Tropina 2021). Mhajne, Luna, and Whetstone (2021, 2), for example, argue that women and girls are frequently subjected to cyber abuse including 'gender-based slurs and harassment, nonconsensual photography, defamation, death threats and rape threats, mob attacks, hate speech, stalking, unsolicited pornography, online impersonation, spying, and sexual surveillance'. Scholars from feminist and queer surveillance studies have also cautioned against the misuse of technologies that specifically target racialised and gendered bodies through the intensification of security and surveillance practices that (re)create the conditions of possibility for further enabling 'systemic forms of discrimination' (Dubrofsky and Magnet 2015, 16; see also Okafor 2022, 10). This similarly affects members of the LGBTQIA+ community, who may face 'threats … such as being outed as a trans or queer person, image-based sexual abuse, and misogynistic trolling' (Slupska et al. 2021, 4). In Iran, for example, queer bloggers have faced homophobic trolling (Shakhsari 2012, 28), while in China, lala feminists have faced trolling from Chinese cyber nationalists (Dian 2024, 462).[5] As feminist and queer perspectives reveal, these online violences cannot be separated from their 'offline' forms (Brown and Pytlak 2020, 6).

Moreover, cyber threats that do not necessarily target marginalised groups, nevertheless subject them to different and compounded experiences. Internet shutdowns can jeopardise the safety, economic situation, and education of many in precarious positions (Brown and Pytlak 2020, 9), often including people of colour, queer, trans, disabled, and poor folk. Personal data breaches can also have particularly detrimental effects. For example, when medical records are leaked or breached, 'people with the ability to become pregnant may be particularly affected by the publication of their reproductive history, while LGBTQ+ people's lives, livelihoods and well-being may be endangered through publication, and involuntary "outing", of their identities' (Millar, Shires, and Tropina 2021, 46; see also Mhajne and Henshaw 2024a, 13; Brown and Pytlak 2020, 12–13; Okafor 2022, 73). These existent harms faced by queer and marginalised groups are rarely acknowledged in cybersecurity studies, even from critical scholarship, and are certainly rarely 'considered in existing cybersecurity threat models' (Slupska et al. 2021, 4). If the cyber subject is defined as state-centric and male-dominated, then it is hardly surprising that these gendered harms rarely feature in cybersecurity policy and practice.

Gendered harms intersect with homophobic, transphobic, racist, classist, and ableist violences (Tacheva and Ramasubramanian 2023, 3). Both mainstream and critical cybersecurity scholarship are overwhelmingly silent on these matters, a silence that prompts us to develop this queer research agenda. We therefore turn to feminist, queer, crip, and anti-racist technoscience and digital studies that have done much to problematise the intersectional violences of technology. AI and algorithmic biases are two areas which have received sustained scrutiny from these critical bodies of scholarship. Berg (2022, 2) notes that machine learning and algorithms increasingly support data collection and do this identification for us, which risks reinforcing the cis-heteronormative assumptions of those who designed these systems, in a sense automatizing gender, sex, and sexuality binaries in intersection with oppressions that relate to race, citizenship, and ability (see also Guyan 2022). Hall and Clapton similarly interrogate the '(cis)gendered, sexualised, and racialised' biases of AI in the context of European Union immigration and border governance (2021, 2–3). Such biases have meant that for queer migrants, the bureaucracies and surveilling practices of border control have 'material consequences on their legal status and deportability', requiring 'racialized, sexed, and gendered migrants' to navigate the labours and risks of digital engagement (Rachdi 2024, 188–190). Who creates and programs AI and algorithms matters. When AI is designed by and for the cishetero white man, it embeds white supremacist, cisheterosexist biases and assumptions into its code (Elwood 2021, 213; Slupska et al. 2021, 2). This has resulted in 'Facial recognition software [that] struggles to recognise people of color; voice recognition [that] struggles to respond to women's voices or non-North American accents; photos of anyone standing in a kitchen are labelled as women; people's bail is denied because a programme decided that a woman of colour was more likely to reoffend than a white woman' (Acheson 2020, 12). Unsurprisingly these technologies – integrated into social welfare, healthcare, and the criminal justice system – target 'the poor … LGBTQ+, [B]lack and [I]ndigenous people[s]' as threats or criminals for whom cybersecurity renders insecure, in order to make select groups secure (Varon and Peña 2021, 18; see also Benjamin 2019, 1).

A queer approach to cybersecurity unsettles the taken-for-granted violences that are embedded in and integral to cybersecurity practices, including who constitutes the cyber subject to be protected. Drawing on contributions from Queer IR, we develop and advocate for queering cybersecurity because queer as a theory, methodology, and orientation seeks to dismantle 'heterosexual, heteronormative, cis-gendered, homonormative, homophobic, and trans*phobic assumptions, orders, and institutions' (Weber 2014, 598). Queer approaches problematise how some subjects, objects, and practices are rendered 'normal' and others 'perverse', and this binary, reinscribed through gendered, sexual, racial, and other markers, similarly manifests in the designs, policies, and scholarship on cybersecurity. Dominant approaches to cybersecurity render people of colour, women, queer, trans, disabled, and poor folk insecure based on the prioritisation of national security that excludes the extensive scope of human experience (Deibert 2018). A queer approach asks who figures as human, as cyber, and as worthy of cyber protection, who is excluded from these conceptions, 'as well as a search for the possibilities of life for bodies who fail to inhabit normative conceptions' of the human in cyber scholarship and practice (Wilcox 2014, 615).

Queering cybersecurity also involves challenging violation-centric language, to consider how queer people are also cyber agents and activists. Queer theory disrupts depictions of cyber users 'predicated on a rational, privileged, and able-bodied man' (Dwyer Andrew et al. 2022, 2–3). Instead, it recentres queer, marginalised, and subaltern experiences, and that cybersecurity and digital politics are also occupied by queer, unruly, and uncontained bodies. To begin this broadening of who constitutes the cyber subject, we turn to feminist analyses of hacker spaces. These have troubled the notion that technical virtuosity and the ability to 'hack' supersede categories of gender, race, sexuality, class, and ability, as this disregards the shifting privileges distributed across a range of different individuals (Toupin 2014). The embodied, feminist, queer politics of feminist hackspaces strives to build 'communities of care, solidarity and critical empowerment in order to undercut tech's "old boys" club' with an intersectional and technologically oriented understanding of cyberfeminism' (Voigt 2023, 162). In her exploration of feminist hackspaces, Voigt highlights the 'collaborative "world-making" practice and political strategy' (Voigt 2023, 164) of feminist hackspaces that seek to 'counter the notion of commercially developed technologies built on certainty and predictability with collaborative, constantly changing, and diverse imaginaries of futures' (Voigt 2023, 172). Consequently, feminist hackspaces empower a wider, more inclusive, and intersectional collective that have greater access and right to the city. This echoes the sentiment of feminist intersectional approaches to cybersecurity that advocate for a greater understanding of the diverse experiences of cyberspace, making a 'one-size-fits-all policy' untenable, especially in conflict-affected contexts where lived experiences of individuals other than cis-male and white makes them uniquely vulnerable (Mhajne, Luna, and Whetstone 2021, 4). The example of lala activists in China discussed earlier is emblematic of the ways queer communities of 'friendship-based solidarity' offers a 'form [of] resistance in dark times marked by the strengthening of authoritarian hegemony and polarized cyber discourses' (Dian 2024, 463). For lala feminists who face the onslaught of misogynistic and queerphobic trolling from ultra-nationalist groups and individuals in China, queer activism (both on and offline) provides a means of care and resistance.

Queering these subjectivities extends existing feminist approaches that interrogate questions of epistemology and knowledge production and decentre the techno-militaristic securitising imaginations of white/cis/male security practitioners, engineers, and technical experts (Foley and Basu 2024). Indeed, our approach suggests moving beyond these technified and professionalised subjects to consider how queering cybersecurity might also extend to queer digital spaces, intimacies, and activisms (Cockayne, Leszczynski, and Zook 2017, 1120). Queer digital geographers have analysed platforms and apps such as Grindr, to explore how cyberspace can be a site where queer 'users can experience and negotiate shame, desire and intimacy' (Bonner-Thompson 2023, 6). When both offline and online worlds are sources of homophobic and transphobic violence, 'for many LGBTQ people digital systems are also necessary for everyday survival' (Cockayne and Richardson 2019, 13). For instance, 'computer-literate urban Iranian queers who have access to the internet… may find a community through connecting to others in cyberspace', such as through queer blogs and magazines (Shakhsari 2012, 20). In another example, queer Nigerian software developers have created an app called QTalk, 'Nigeria's first social and counselling mobile app for the lesbian, gay, bisexual, transgender, intersex, and queer [LGBTIQ+] community' (QTalk cited in Okafor 2022, 76). In other words, while cautious not to idealise or fetishise the digital realm (Nguyen 2003, 300), queer scholars note 'the possibilities for solidarities, self-determination, affirming and protecting Black, queer and trans life amidst material, structural and epistemological violence' (Elwood 2021, 212).

We are cautious not to romanticise queer experiences of digitality, however, noting that these glimpses of queer survival and joy occur in the context of broader physical and cyber violences. As Shakhsari (2012, 33) writes, referring to the example of Iranian queers, '[e]ven as [some might] find the Internet crucial to their livelihood and liberation, other queers in Iran may translate an online presence into being "outed" and exposed to new regulatory and disciplinary measures'. And crucially, as is evident across the world, but particularly pronounced during Israel's intensified genocide in Gaza since October 2023, we cannot 'overlook' in our identifying of queer digitality, 'the material effects of violence (such as military intervention) on bodies that are effected by online and offline practices' (Shakhsari 2012, 34). Israel's genocide in Gaza has been a sobering reminder of the power of social media to communicate the horrors of the genocide in the face of inaction and denial. For queer Palestinians in Gaza, the site 'Queering the Map' (queeringthemap.com) offers a platform to share queer connection, hope, and despair (see also Berg 2022, 2). In one submission, a queer Palestinian writes: 'Idk how long I will live so I just want this to be my memory here before I die … My biggest regret is not kissing this one guy. He died two days back. We had told how much we like each other and I was too shy to kiss last time. He died in the bombing. I think a big part of me died too. And soon I will be dead. To younus, i will kiss you in heaven' (O'Neal 2023; Queering The Map n.d.).

Queer perspectives recentre these stories and queer people as both violated and agential subjects of cybersecurity. These are the stories erased from cybersecurity policies and scholarship. We argue that such omissions occur because of the cisheterosexist, colonial and racist assumptions and hierarchies that underpin cybersecurity, which we elaborate on in the third section. Queering not only allows us to identify and challenge these violences but also offers subversive possibilities through glitch-thinking, a discussion to which we now turn.

Queering and glitching the system

In this section, inspired by queer, feminist, and Black media studies, we turn to the subversive potential of glitch-thinking. By embracing queer, feminist, anti-racist, and anti-colonial practices and renderings of cybersecurity, we highlight the importance of infiltrating, interrupting, and discomfiting the status quo. We understand glitch to mean a moment of entropic possibility that fractures into multifarious prospects of 'being and becoming' (Russell 2020, 11). We support our critique by suggesting a queer 'glitching' of the system and extend our propositions in this developing research agenda to reassess the myriad binaries, violences, subjectivities, and problematic securitisations coded in cybersecurity practices in the other two sections of our analysis. In other words, by queering cybersecurity, we propose to glitch the systemic ordering of knowledge production in cybersecurity studies through a queer epistemological and methodological orientation.

Glitches in cyber systems point to the moments of error, slippage, and dysfunction that redirect attention to the 'material base of digital events' (Nakamura 2013). A glitch, through its malfunction, makes visible the 'inner structure' of these systems, revealing the 'ghostly conventionality of the forms' that resonate with the normativities these cyber technologies inscribe (Goriunova and Shulgin 2008, 114). In this moment of revelation, the glitch opens the possibility of exploration and critique, 'as a methodological point of departure – a nexus of emerging perspectives' (Kayser 2021, 1157). A glitch posits a vision of alterity and ruptures the hegemony of systems that are 'singularly codified' (Menkman 2011, 26). Just as queerness defects from the rationalised schematics that perpetuate the oppressive totalities of dominant systems (Luchkiw 2016, 4), a glitch in its moment of abjection can 'infiltrate, make dirty, and ultimately put pressure on the norms and ideals' (Sundén 2016, 1; see also Rachdi 2024, 186) that reproduce the prevailing exclusions of cybersecurity. Importantly, our proposition is not to suggest a fixed approach, as a queer methodology revels in the possibilities of plurality (Warner 2004) but to offer a creative reshaping of our own approach to research in cybersecurity that enables us to recognise the transformative potential of queer thinking, both in the ways in which we view our subjects and ourselves as researchers (Ashford 2009, 310).

Drawing inspiration from Russell's celebratory exploration of glitch politics, where 'embracing the glitch' is considered a 'participatory action that challenges the status quo' (2020, 11), we also recognise its potential of generating 'ways of doing or being that dominant digital-social orders are aligned to render impossible, unspeakable and even unimaginable – but that have long existed anyway' (Elwood 2021, 213). Moreover, through our interventions of queering cybersecurity, we hope to introduce 'positive irregularities' into dominant knowledge systems that can guide us towards alternative frameworks and propitious futures (Russell 2020, 13–14). Thus, our queer reading can serve as a double move, as both 'critically revealing and (re)building' (Elwood 2021, 214).

Bringing glitch thinking to cybersecurity studies invites necessary reflection on the politics of cybersecurity research that can open possibilities of heterodox thinking that 'trouble' (Bellanova, Lindskov Jacobsen, and Monsees 2020) prevailing patterns of meaning-making. An important step towards this involves exposing and dismantling the sedimented practices of knowledge production within cybersecurity studies. As much as queering cybersecurity calls for greater attention to the otherwise marginalised and trivialised effects of digital technologies on queer, trans, Black/Brown, disabled, and classed bodies, these interventions need to also acknowledge the marginalisation of their experiences not just as objects of study but also as speaking, embodied subjects. This means challenging the disembodied knowledge produced by cybersecurity experts that tend to idealise the white/cis/hetero masculine as the legitimate 'knower' of cybersecurity.[6] By acknowledging the epistemological premise of the situatedness of knowledge, we can proffer queer, feminist, and anti-racist epistemologies as a queer disruption that 'disorients and creates a new slant' (Ahmed 2006, 166) in the taken-for-granted, universalised narratives of cybersecurity. More practically, this involves interrogating the intersecting effects of gender, race, and sexuality in what is regarded as legitimate cybersecurity expertise. Our interventions on the current exclusionary dynamics of knowledge production complement and extend recent critiques of the 'racial-epistemic hierarchies' (Mumford and Shires 2023) in cybersecurity expert communities and encourage a queer attentiveness that invites us to embrace more expansive and nuanced ways of doing research and producing knowledge.

Another scarcely acknowledged aspect of the politics of knowledge production in cybersecurity studies is the alluring effect of cyber itself, that is, the construction of cyber as a brand that 'attracts funding, pay packets, and investment' (Dwyer Andrew et al. 2022, 14). Cybersecurity operates as a profitable industry that thrives on the commodification of security products and services, inevitably tying it to state and corporate interests that shape the dominance of specific insecurities in narratives of cybersecurity. The market-driven nature of cybersecurity (and its overlaps with the techno-military-industrial-academic complex coupled with the neoliberalisation of universities and funding agencies) has also compelled the need for 'marketable' research that can meet the priorities of funding agencies and corporations preoccupied with market impacts within prevailing paradigms of security thinking (Smart 2016, 464–465; see also Planqué-van Hardeveld 2023). Invariably, these prevailing arrangements rarely acknowledge the insecurities and intimacies of those bodies deviating from the normativities and orthodoxies embedded within established cybersecurity practices. Creative collaborations that bring together multiple curiosities across disciplines, practices, and assumptions can attend to the diverse cultural, social, and technological literacies required of a more expansive cybersecurity research agenda. Envisioning alternative ways of meaning-making can allow for collaborations between practitioners, artists, and academics (see L. Hall et al. 2022) to initiate more heterodox projects of deciphering cyber technologies. To be sure, then, a queer commitment transgresses prevailing dynamics of the 'authoritarian order of knowledge production, bringing it into crisis' (Luchkiw 2016, 10), while also progressing a more compelling, encompassing narrative of our social world.

Glitch thinking also offers valuable possibilities for queer critique. Specifically, it enables critiques of cybernormativities or the 'techno quo' (Benjamin 2019, 12) allowing questions on what cyber worlds and utopias might replace these violent arrangements. On the first task of critique, we reveal through the previous and following sections the exclusions and vulnerabilities of cybersecurity as it is currently practiced and understood, particularly for those gendered, sexual, and racialised bodies who do not fit or refuse to conform to conceptions of cybersecurity and its referent subjects. Queer approaches from IR and beyond have been critical in 'disrupting the modes of power that orient normative institutions and encounters . . . [including] the gendered and sexualised logics embedded in all social relations' (Biddolph 2020, 408–409; see also Richter-Montpetit and Weber 2017, 2). We ask, along with critical cybersecurity scholars, how we can conduct cybersecurity scholarship in ways that 'destabilize power structures and challenge inequalities . . . even if this means undoing the narratives of cybersecurity' (Dwyer Andrew et al. 2022, 23; emphasis in original). This approach is anti-normative (Browne and Nash 2010, 7) and urges scholars and practitioners who cultivate cybersecurity knowledge to always question the embodied, political, and violent effects of cyber practices. We therefore argue that a queer cybersecurity research agenda must 'transgress, disrupt . . . what is normal' (Cockayne and Richardson 2017, 1643) so that we may pave the way for alternative, more liberatory cyber presents and futures. It is this second task, then, of replacing cybersecurity practices with more queer, feminist, and anti-racist ones, that provides opportunities for reimagining cyber knowledges. The task of dreaming new cyber utopias involves 'produc[ing] a messy, speculative, and unpredictable method' (Chatterjee 2023, 2). As Benjamin writes: 'The task . . . is to challenge not only forms of discriminatory design in our inner and outer lives, but to work with others to imagine and create alternatives to the techno quo . . . as part of a larger struggle to materialize collective freedoms and flourishing' (2019, 12, emphases in original). We do not have all (or even any) of the answers to what this speculative, queerer future for cybersecurity looks like, but we suggest one way this might manifest is through queering/glitching the system.

Gender, sexuality, and the coloniality of cyberspace: queering digital territories, bodies, and securities

Following our queer analysis of cyber subjectivities and our proposal of queering/glitching the system, we explore the intersections of gender, sexuality, and coloniality in cyberspace, to interrogate the ways in which this shapes the conception of cybersecurity itself. Central to this inquiry is the recognition that cybersecurity, widely understood as the projection and implementation of security with respect to cyberspace (Shires and Smeets 2016), is shaped by the spatial connotations of cyber*space*.[7]Through spatial metaphors and spatialising discourses informed by 'culturally specific imaginaries and spatialized practices' (Dwyer Andrew et al. 2022, 14), cybersecurity is primarily conceived through the lens of static, territorial rigidities and apprehended as an exercise of national security. Indeed, this has facilitated more than a figurative spatiality where 'states have imposed territorial order on cyberspace by insisting that respect for national borders be built into internet protocols and ecommerce' (Herrera 2016, 88). This tendency to remain parochial to state borders naturalises and obscures the gendered, racialised, and sexualised nature of cyber spatio-temporalities. Furthermore, just as the specific disciplining capacities of spaces demarcated as territory 'rely on gendered relationships of power' (Wastl-Walter and Staeheli 2013, 151), cyber/digital/online spaces conceived within such frameworks remain constrained by the normative reproduction of such capacities (Cockayne and Richardson 2017). Bringing queer perspectives to bear on the spatial entanglements of cybersecurity allows for recognising how cyber technologies structure and regulate the production of space through 'the dichotomies that structure places as hetero and homosexual, public and private, and minority and universal' (Cockayne and Richardson 2017, 1643). Furthermore, we recognise in these spatial entanglements the deep implication of the social dynamics of both offline and online spaces as well as the recognition that not all organisations of space/spatiality are experienced evenly, equally or uniformly (Marshall 2001).

Our critique of the normative spatio-temporalities of cyber technologies draws on feminist, queer, and Black geographers who complicate these technologies as messy and contradictory, complicit in the production of cisheteronormative/racialised/colonial space (Elwood 2021; Elwood and Leszczynski 2018; McKittrick and Peake 2005). This approach necessitates a shift beyond the narrow focus on state/national/technological security, to encompass what Katz (2001, 711) terms the 'fleshy, messy, and indeterminate stuff of everyday life'. Recent feminist cybersecurity interventions have highlighted the importance of recentring intimate, personal, and everyday spaces as legitimate sites for consideration in mainstream studies on cybersecurity (Meuller 2023; Mhajne, Luna, and Whetstone 2021; Slupska 2019). Extending this trajectory, we advocate for a queer intervention that productively disrupts the geographical and spatial binaries embedded in current frames of thinking, which tend to privilege the national/global, state/infrastructural dimensions of cybersecurity. This resonates with the queer reimagining of space as envisioned in the 'Queering the Map' project referenced previously, which challenges cartographies of cyberspace that reinforce dominant power structures to instead reveal the potential for creating cyberspaces as digital commons unencumbered by traditional notions of borders, identity, or state authority (LaRochelle 2020). By embracing the rich tapestry of queer digital experiences and vulnerabilities we can recognise queer space as fundamentally relational and contingent, emerging through actions that negotiate and resist oppressive hierarchies. Thus, paying attention to 'whose digital knowledges are considered "authentic" or "truthful" or whose knowledges constituted through digital practices come to dominate' (Nash and Gorman-Murray 2019, 38) can have important implications for how we come to understand the possibilities and limitations of cyberspace.

Moreover, these perspectives enrich our understanding of the historical context within which the scholarship of cybersecurity emerges, particularly the colonial logics of libertarian spatial conceptualisations of cyberspace in the early years of the Internet. The persistent imaginary of the 'frontier', used to describe cyber technologies, continues rehearsing those familiar 'colonial violences captured within the capitalistic terrains' that have facilitated the material, infrastructural, and embodied entanglements of these technologies (Byrd 2014, 57). Projecting features of land and geography onto cyberspace risks reproducing colonial/imperial imperatives, a critique frequently levied by Indigenous and other critical scholars of technology (see Gaertner 2016). Instead, changing the narrative of land, property, and ownership to more relational approaches that recognise how these technologies are embedded and operate within social relations enables a view of digital technologies that 'stands in contrast to capitalist logic that dismisses all things digital as profitable, destroyable, servile resources' (Cordes 2020, 287). For Indigenous communities, this articulates a way of conceptualising digital spaces that allows them to 'operate sovereignty in ways distinct from settler colonial notions of space and time' (Cooper 2019, 502), thereby queering colonial frameworks of territoriality.

Similarly, we also draw on queer perspectives of temporality to conceptualise cyber-time. While cyber and digital technologies are often presented as 'creating new, more efficient, time and space' queer approaches to temporality challenge these notions (Bonner-Thompson 2023, 7) to recognise that 'time is "out of joint", "becoming" and multiply lived in ways that do not cohere with linear, universal time' (Biddolph 2020, 410). This involves troubling assumptions of teleological and transformative liberal progress often ascribed to cyber technologies. Instead, recalling cyber's entanglements with multiple histories and how these continue to structure the current function of cyber technologies allows for a critical destabilising of their future-oriented temporalities. Attention should also be paid to how digital technologies (re)produce past violences, facilitating and exacerbating their grievances in the present day. Black and other scholars have confronted the enduring practices of commodifying, spectacularising, and violating Black bodies and lives increasingly mediated through the representation, archiving, and circulation of anti-Black violence enabled by digital technologies and platforms (see for e.g. Noble 2018; Sobande 2021; Sutherland 2023; Whyte 2022). Queering temporal imaginings of cyber technologies 'complicates and contorts chrononormative imaginaries' (Cockayne and Richardson 2019, 18) and reveals the importance of examining 'how forgotten, repressed, and lost pasts come back, are folded into the present and persist' (16). Queering cyber spatio-temporalities marks an important shift in the epistemological space-time framings that inform current configurations of thinking.

Building on this spatio-temporal reconceptualisation, we turn our attention to cyber objects, proposing to redefine them as embodied, human-virtual (or 'socio-technical', Cristiano et al. 2024, 2–3) entanglements, and queer cyborgs. This approach, informed by feminist and crip technoscience, posthuman, and critical race theories illuminates the deeply human, 'embodied and "embodying"' (Wilcox 2017, 3, emphasis in original; see also Hamraie and Fritsch 2019) politics of cybersecurity. Notwithstanding a small body of critical cybersecurity scholarship (Cristiano 2018; Dunn Cavelty and Wenger 2020; Dwyer 2023), very little has been written in IR on the embodied nature of cybersecurity. While we focus on cybersecurity objects, which are conventionally understood as the various software and hardware that underpin virtual systems and networks, much can be gleaned from feminist and queer IR scholarship that traces the embodied nature of drone warfare, robotic technology, soldier enhancements, and algorithms (Clark 2019, 2022; Daggett 2015; Manjikian 2014; Masters 2005; Wilcox 2017). These technologies will always already be 'embodied in some combination of human and/or machine to be carried out… [as they] themselves cannot have meaning outside of the computer; the code must be embodied on a platform to acquire meaning' (Wilcox 2017, 16). A queer approach emphasises this entangled corporeality of cybersecurity objects even as it acknowledges that human ideas and bodily configurations are not fixed or universal. Rather, they can be altered, disrupted, and queered, so that we might transform how we think and do cybersecurity.

Posthuman cybersecurity scholarship offers insights for how we might queer the (more-than-) human and agential politics of cybersecurity (Dwyer 2023; Fouad 2022). We follow a queer curiosity that blurs binaries between virtual and human cyber objects, and that keeps open the question of where 'the human body end[s] and technology begin[s]' (Van Doorn 2011, 536). Marlin-Bennett points to digital technologies like social media as a reminder of how cyber-tools allow us to 'sense', to be 'hybrids' or 'cyber-humans' (Marlin-Bennett 2013, 621; see also Marlin-Bennett 2016). Greene Wade, working within and across radical Black feminist traditions, reimagines the virtual and physical activism of Black Lives Matter as a 'virtual-physical assemblage[]' where 'viral blackness' can flourish and enable 'what Sylvia Winter describes as "new genres of being human"' (Wade 2017, 34). These contributions expand the definition of cybersecurity objects as intimately entangled with and exceeding humanness.

The cyborg embodies the human-virtual entanglements we have discussed thus far (Cristiano 2018, 151). While predominantly theorised within feminist technoscience (Haraway 2016 [1985]; Jones 2018), the cyborg is queer and has much to offer in the way of rethinking cybersecurity objects. We do however, recognise the violent lineages of the cyborg within heterosexist, colonial, militarist, and capitalist systems (Haraway 2016 [1985]; Nakamura 2014), and of the ways its queer 'ambiguity' risks 'resubordinat[ing]' 'other kinds of cyborgs, highly gendered and racialized workers mechanized and merged as interchangeable parts' (Nguyen 2003, 300, 292). As Nguyen (2003, 302), argues, though, 'this does not mean we may not simultaneously take some pleasure in our cyborgs and yet interrogate the conditions of their existence.' We therefore also see the queer cyborg as a figure of cyber-utopia (Luchkiw 2016), potentially forging feminist or queer 'techno-futures[s]' (Jones 2018, 97–98; see also Jones 2023, 61; Nguyen 2003, 288). This queer reimagining of cybersecurity objects recognises the more-than-human agency of codes and software, of cybersecurity practices as human and embodied, opening up new possibilities for understanding and engaging with cyber technologies.

Finally, building on critical cybersecurity's interventions on the 'discursive positioning of threat and its resolution' (Dwyer Andrew et al. 2022, 1; see also Dunn Cavelty 2019), our queer feminist abolitionist analysis challenges the cisheteronormative assumptions deeply embedded in cybersecurity frameworks. This illuminates the intricate 'connections and overlaps between the experiences of queers and other groups that experience marginalization and insecurity' (Wilkinson 2021, 92), broadening our understanding of who is affected by and implicated in cybersecurity practices.

Feminist contributions to security studies have unmasked the gendered perceptions that typify what 'counts' as security, such as the ways in which mainstream security approaches tend to exclude violences that are deemed 'personal' (Enloe 1989). Queer critiques point to the precariousness of security as 'not only gendered, but straight' (Wilkinson 2017, 107). Paying keen attention to both alerts us to the violences of cyber securitisations and the way 'the virtual intersects with security in ways that also contribute to the hyperbolicisation of security' (Dillon 2003, 546), further perpetuating and compounding insecurities for those bodies in 'deviation from the racialised, ableist, embodied norms of gender' (Wilkinson 2021, 97). This has manifested in the ways in which the securitisation of anti-queer violence distends along homonationalist lines, with cyberspace a realm through which these normativities are upheld. This has resulted in, for example, 'glorifications of the liberatory potentials of the

Internet [which] construct cyberspace as a haven for Iranian queers awaiting rescue within the liberatory and civilizational discourses of the war on terror' (Shakhsari 2012, 16–17).

Moreover, we take heed of necessary critiques that draw attention to security practices 'founded on embedded cisprivilege' (Shepherd and Sjoberg 2012, 20), to instead recognise that 'a nuanced and sophisticated gendered theory of security needs to incorporate corporeality, including trans-corporeality' (19). We propose a capacious queer perspective that also confronts the colonial legacies of security reflected in the 'language of the Western-centric international order, feeding on a dichotomous representation of us versus them, reifying the colonial state as the lynchpin of the social order' (Vernon 2022, 5). This connects with abolitionist critiques that emphasise how security operates in the context of state violence, with abolitionism committed to the 'eradication of oppressive systems including, but not limited to, the abolition of prisons, immigration detention, policing, and other forms of state violence' (Okechukwu 2021, 157). Cybersecurity scholarship is largely silent on the ways in which digital technologies uniquely intersect with security practices to produce tangible harms, vulnerabilities, and precarity to people across diverse social worlds.

We envision a queer perspective that builds on these critical, abolitionist contributions to recognise the palimpsestic nature of security that lays bare the unique violences engendered by cyber technologies against a range of marginalised groups. For instance, Jefferson draws attention to the urgent need for a 'theory of carceral cyberspace' (2018, 982) in his exploration of the digitisation of the criminal justice system to expand surveillance, control, and disciplinary mechanisms which further intensify the reach of the 'carceral state'. By investigating New York City's Department of Corrections and Community Supervision's use of corrections and law enforcement software, Jefferson reveals how 'corrections personnel, police, and programmers envision computer code as medium for diffusing its field of action across urban space' (982), rendering incarceration ubiquitous through digital means. Under the guise of improving security, violent systems of criminalisation and incarceration are expedited by predictive algorithms and geo-surveillance software that monitor, evaluate, and capture individuals flagged as risky or suspicious based on coded criteria. Anti-racist, feminist, and abolitionist activists have long insisted on understanding 'the ways racist structures and assumptions facilitate the expansion of an extremely profitable prison system, in turn helping to reinforce racist social stratification' (Davis and Shaylor 2001, 5). Digital technologies thus become an alibi for this violence experienced disproportionately by marginalised communities, including people of colour, queer, trans, poor folk, and those multiply marginalised at the intersections of these, even as these technologies serve as a 'key translation mechanism in making carceral citizens legible to the public as criminals across physical geographic spaces' (Gurusami 2019, 439).

A queer approach interrogates these harms through an expansion of the current subjectivities of cyber securitisations to include all marginalised communities across a diverse range of sites, not limited to but often violently connected to centres of state power. Following from queer, feminist, and abolitionist perspectives to reconceptualise security, we urge attention to the ways in which security as an exercise of threat elimination reproduces harms.

Conclusion

In this article, we have proposed a queer cybersecurity research agenda to pay heed to systemic silences insufficiently addressed in critical cybersecurity scholarship on matters of gender and sexuality. This builds on emerging and important pockets of research bringing feminist and decolonial perspectives to bear on cybersecurity (Brown and Pytlak 2020; Mhajne and Henshaw 2024b; Mhajne, Luna, and Whetstone 2021; Millar and Shires 2024; Millar, Shires, and Tropina 2021; Mumford and Shires 2023; Slupska 2019). These and contributions from feminist and crip technoscience, queer theory, Indigenous studies, abolitionism, and critical race approaches beyond disciplinary IR, have all revealed the necessity of taking seriously cybersecurity as a source of violence for queer people, and the queer potential of cyberspace and digital politics. We have advanced a queer cybersecurity research agenda that advances three core elements. First, we argue that such an agenda must locate and recentre queer people as subjects of and in cybersecurity. Such a task entails calling out the ways in which queer and other marginalised groups are subject to cyber violences, in addition to recognising the digital realm as a space for queer agency. Queering cybersecurity recasts the subject of cybersecurity. Embracing the deconstructive ethos of queer theorising, the queer cyber subject is multiple, shifting, and embodied by gendered, sexual, racial, and other modes of power and experience. Suspicious of how the cyber subject is typically figured as a white, middle-class, cishetero man, we traced those subjects that are less visible but nevertheless make cybersecurity possible: women, queer people, Indigenous communities, people of colour, disabled, and poor folks. Moreover, queering who and what cybersecurity is for allows us to expose cyber's violences, especially for marginalised communities, and along gendered, sexual, racial, and class-based lines.Second, we put forward a case for queering and glitching the system. Such an exercise invites a 'queer intellectual curiosity' (Weber 2016) about the violences, normativities, and potentials of cybersecurity.Third, a queer cybersecurity research agenda must also attend to the cisheterosexist, colonial, racist, anthropocentric, and neoliberal capitalist foundations of cybersecurity. These foundations are so embedded in cybersecurity scholarship and policies that they are rarely discerned or questioned. Our mapping of these exclusionary assumptions suggests that cybersecurity discourse and practice will always be violent, even as and while queer and other marginalised groups are recognised as cyber subjects.

For us, queering cybersecurity is not about making cyber queer, as if it isn't already (see Wilcox 2014, 612, on queering IR). As we have explored in this article, cybersecurity – its spaces, objects, subjects, violences, and potential – is queer in all senses of the term. It is embodied; it is constituted by gender, sexuality, race, and other vectors of power; it is simultaneously conceived as but irreducible to binaries; it is queer. Queering cybersecurity therefore enables us to explicitly embrace cyber's queerness. Moreover, we have rejected singular notions of what cyber is, recognising that there is no definitional clarity about cybersecurity. The empirical examples we have integrated throughout speak to the broad approach we take to cybersecurity. We do this explicitly, recognising that the state-centric and militarist focus of conventional cybersecurity studies and practice precludes attention to voices and perspectives on the margins – of queer people under siege, feminist hackers, gendered and racial violences of AI, and the possibilities of queer connection and techno utopias. We hope the questions, possibilities, and provocations we have sparked in this article contribute to an emergent queer cybersecurity research agenda. We do not wish to prescribe particular research programs, remaining committed to a queer ethos of openness and possibility. While we envision future research in this area might extend, adopt, or apply some of the queer approaches to specific examples of cybersecurity policy and practice, we encourage interventions that reject the cyber status quo: of what constitutes cybersecurity, who it is for, and how it is produced. Queering cybersecurity can expose the violences of cyber capabilities, but it can also embrace the queer hope, resistance, and potential that always already resides in the cyber realm. In doing so, such a research agenda offers ways of thinking cybersecurity otherwise.

Notes

1. By cisheteronormative, we refer to the institutionalised acceptance of those who are cisgender (i.e. accept their gender identity assigned at birth), and heterosexuality, as the common sense.
2. Our critique of the securitising practices and logics of cybersecurity relate particularly to the context of state centred, militaristic perspectives of cybersecurity rather than a normative indictment of securitisation at large.
3. In this article, we use the terminology of 'queer' to describe people and practices that do not conform to cis-heteronormative visions of gender, sex, and sexuality. This can include lesbian, gay, bisexual, transgender, queer/questioning, intersex, asexual/aromantic, and other identity categories (LGBTQIA+). We note however, that the use of 'queer' and 'LGBTQIA+' can be Western centric, and that other terms and ways of knowing, doing, and being exist outside these terms.
4. This is true of English language publications, at least.
5. Lala is a Chinese slang term referring to 'a more diverse, inclusive, and flexible lesbian subjectivity' that diverges from Western notions of lesbianism (Dian 2024, 481).
6. On the subject of the cybersecurity expert, see Jacobsen (2020).
7. Insofar as cyberspace may be described as a discursive space informed by specific spatial representations, a socio-political space constituted by the dynamic evolution of complex socio-political subjectivities, it is important to note that the distinctions between cyberspace and the physical world remain, as Stone argues, 'fragmented, complex, diffracted through the lenses of technology, culture, and new technocultural formations' (Stone 1995, 36). Our analysis therefore understands the 'space' of cyberspace not as an ontological reality but rather as the effect of specific socio-technical arrangements and power relations.

Acknowledgments

An earlier version of this work was presented at the International Studies Association Virtual Conference in 2023 and the Australian Political Studies Association 2023 Annual Conference in Sydney, Australia. We thank the panellists and audience for engaging with the ideas presented. We thank the reviewers for their constructive feedback and willingness to think with and beyond us in reading the article. We especially appreciate the generosity of the editorial team, specifically Tom Gregory, for their careful suggestions and guidance throughout the publication process. We would also like to thank Laura Shepherd for reading an early draft of this article. Finally, we are particularly indebted to the intellectual foundations built by generations of Black, Indigenous, and Queer scholars, this intervention would not be possible without their contributions.

Disclosure statement

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

Notes on contributors

Sulagna Basu is a PhD candidate in the Discipline of Government and International Relations, University of Sydney. Her research focuses on cybersecurity policy discourses to illuminate the complex intersecting dynamics of empire, settler colonialism, and Indigenous dispossession. More broadly, her research interests include a focus on the politics of technology specifically examining its entanglements with race and gender.

Caitlin Biddolph is a Lecturer in International Relations in the School of International Studies and Education at the University of Technology, Sydney (UTS). Her research focuses on queer perspectives to international law and transitional justice, and queer, feminist, and decolonial approaches to global politics more broadly. Caitlin has recently published her first monograph, *Queering Governance and International Law: The Case of the International Criminal Tribunal for the former Yugoslavia* (OUP, 2025).

ORCID

Sulagna Basu http://orcid.org/0009-0000-7811-7696

References

Acheson, R. 2020. "Autonomous Weapons and Patriarchy." Women's International League for Peace & Freedom. October 20, 2020. https://reachingcriticalwill.org/images/documents/Publications/aws-and-patriarchy.pdf.

Ahmed, S. 2006. *Queer Phenomenology: Orientations, Objects, Others*. Durham: Duke University Press.

Alexander, M. J. 1994. "Not Just (Any) Body Can Be a Citizen: The Politics of Law, Sexuality and Postcoloniality in Trinidad and Tobago and the Bahamas." *Feminist Review* 48 (1): 5–23. https://doi.org/10.1057/fr.1994.39.

Ashford, C. 2009. "Queer Theory, Cyber-Ethnographies and Researching Online Sex Environments." *Information & Communications Technology Law* 18 (3): 297–314. https://doi.org/10.1080/13600830903424734.

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

Benjamin, R. 2019. "Introduction: Discriminatory Design, Liberating Imagination." In *Captivating Technology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life*, edited by R. Benjamin, 1–22. Durham: Duke University Press.

Berg, E. 2022. "Queer Data: Using Gender, Sex and Sexuality Data for Action." *International Feminist Journal of Politics* 25 (4): 788–790. https://doi.org/10.1080/14616742.2022.2137053.

Biddolph, C. 2020. “Queering Temporalities of International Criminal Justice: Srebrenica Remembrance and the International Criminal Tribunal for the Former Yugoslavia (ICTY).” *Griffith Law Review* 29 (3): 401–424. https://doi.org/10.1080/10383441.2020.1857493.

Bonner-Thompson, C. 2023. “Queering Digital Temporalities? Visceral Geographies of Grindr.” *Geoforum* 144:103815. https://doi.org/10.1016/j.geoforum.2023.103815.

Brown, D., and A. Pytlak. 2020. “Why Gender Matters in International Cyber Security.” Women’s International League for Peace and Freedom and the Association for Progressive Communications. https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf.

Browne, K., and C. J. Nash. 2010. “Queer Methods and Methodologies: An Introduction.” In *Queer Methods and Methodologies: Intersecting Queer Theories and Social Science Research*, edited by K. Browne and C. J. Nash, 1–24. Farnham and Burlington: Ashgate.

Byrd, J. 2014. “Tribal 2.0: Digital Natives, Political Players, and the Power of Stories.” *Studies in American Indian Literatures* 26 (2): 55–64. https://doi.org/10.5250/studamerindilite.26.2.0055.

Chatterjee, S. 2023. “Crisis Epistemologies: A Case for Queer Feminist Digital Ethnography.” *Journal of Gender Studies* 32 (5): 486–497. https://doi.org/10.1080/09589236.2023.2179606.

Clark, L. 2018. “Grim Reapers: Ghostly Narratives of Masculinity and Killing in Drone Warfare.” *International Feminist Journal of Politics* 20 (4): 602–623. https://doi.org/10.1080/14616742.2018.1503553.

Clark, L. 2019. *Gender and Drone Warfare: A Hauntological Perspective*. London and New York: Routledge.

Clark, L. 2022. “Delivering Life, Delivering Death: Reaper Drones, Hysteria and Maternity.” *Security Dialogue* 53 (1): 75–92. https://doi.org/10.1177/0967010621997628.

Cockayne, D. G., and L. Richardson. 2017. “Queering Code/Space: The Co-Production of Socio-Sexual Codes and Digital Technologies.” *Gender, Place & Culture* 24 (11): 1642–1658. https://doi.org/10.1080/0966369X.2017.1339672.

Cockayne, D., A. Leszczynski, and M. Zook. 2017. “#hotforbots: Sex, the Non-Human and Digitally Mediated Spaces of Intimate Encounter.” *Environment and Planning D: Society and Space* 35 (6): 1115–1133. https://doi.org/10.1177/0263775817709018.

Cockayne, D., and L. Richardson. 2019. “The Queer Times of Internet Infrastructure and Digital Systems.” In *The Geographies of Digital Sexuality*, edited by C. J. Nash and A. Gorman-Murray Singapore: Palgrave Macmillan. https://doi.org/10.1007/978-981-13-6876-9_2.

Cohen, C. J. 1997. “Punks, Bulldaggers, and Welfare Queens: The Radical Potential of Queer Politics?” *GLQ: A Journal of Lesbian & Gay Studies* 3 (4): 437–465. https://doi.org/10.1215/10642684-3-4-437.

Cooper, L. R. 2019. “A Future Perfect: Queer Digital Sovereignty in Joshua Whitehead’s Jonny Appleseed and Full-Metal Indigiqueer.” *Contemporary Literature* 60 (4): 491–514. https://doi.org/10.3368/cl.60.4.491.

Cooper-Cunningham, D. 2022. “Security, Sexuality, and the Gay Clown Putin Meme: Queer Theory and International Responses to Russian Political Homophobia.” *Security Dialogue* 53 (4): 302–323. https://doi.org/10.1177/09670106211055308.

Cordes, A. 2020. “Meeting Place: Bringing Native Feminisms to Bear on Borders of Cyberspace.” *Feminist Media Studies* 20 (2): 285–289. https://doi.org/10.1080/14680777.2020.1720347.

Cristiano, F. 2018. “Bodies of Cyberwar: Violence and Knowledge Beyond Corporeality.” In *Experiences in Researching Conflict and Violence: Fieldwork Interrupted*, edited by A.-M. Rivas and B. C. Browne, 145–160. Bristol: Policy Press.

Cristiano, F., X. Kurowska, T. Stevens, L. Marie Hurel, N. Shafik Fouad, M. Dunn Cavelty, D. Broeders, T. Liebetrau, and J. Shires. 2024. “Cybersecurity and the Politics of Knowledge Production: Towards a Reflexive Practice.” *Journal of Cyber Policy* 8 (3): 331–364. https://doi.org/10.1080/23738871.2023.2287687.

Currah, P., and T. Mulqueen. 2011. “Securitizing Gender: Identity, Biometrics, and Transgender Bodies at the Airport.”*Social Research*.” *An International Quarterly* 7 (2): 557–582. https://doi.org/10.1353/sor.2011.0030.

Daggett, C. 2015. “Drone Disorientations: How ‘Unmanned’ Weapons Queer the Experience of Killing in War.” *International Feminist Journal of Politics* 17 (3): 361–379. https://doi.org/10.1080/14616742.2015.1075317.

Davis, A. Y., and C. Shaylor. 2001. “Race, Gender, and the Prison Industrial Complex: California and Beyond.” *Meridians* 2 (1): 1–25. https://doi.org/10.1215/15366936-2.1.1.

Deibert, R. J. 2018. “Toward a Human-Centric Approach to Cybersecurity.” *Ethics & International Affairs* 32 (4): 411–424. https://doi.org/10.1017/S0892679418000618.

Dian, D. 2024. “Lala Activists in Dark Times: Queer Feminist Resistance to the Cyber-Nationalist Attacks in China.” *Journal of Lesbian Studies* 28 (3): 460–485. https://doi.org/10.1080/10894160.2023.2281060.

Díaz Calderón, J. 2021. “A Decolonial Narrative of Sexuality and World Politics When Race is Everywhere and Nowhere.” *Critical Studies on Security* 9 (1): 17–21. https://doi.org/10.1080/21624887.2021.1904190.

Dillon, M. 2003. “Virtual Security: A Life Science of (Dis)order.” *Millennium Journal of International Studies* 32 (3): 531–558. https://doi.org/10.1177/03058298030320030901.

Dubrofsky, R. E., and S. A. Magnet. 2015. “Introduction: Feminist FurveillanceStudies: Critical Interventions.” In *Feminist Surveillance Studies*, edited by R. E. Dubrofsky and S. A. Magnet, 1–17. Durham: Duke University Press.

Dunn Cavelty, M. 2019. “The Materiality of Cyberthreats: Securitization Logics in Popular Visual Culture.” *Critical Studies on Security* 7 (2): 138–151. https://doi.org/10.1080/21624887.2019.1666632.

Dunn Cavelty, M., and A. Wenger. 2020. “Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science.” *Contemporary Security Policy* 41 (1): 5–32. https://doi.org/10.1080/13523260.2019.1678855.

Dwyer, A. C. 2023. “Cybersecurity’s Grammars: A More-Than-Human Geopolitics of Computation.” *Area* 55 (1): 10–17. https://doi.org/10.1111/area.12728.

Dwyer Andrew, C., C. Stevens, L. Pijnenburg Muller, M. Dunn Cavelty, L. Coles-Kemp, and P. Thornton. 2022. “What Can a Critical Cybersecurity Do?” *International Political Sociology* 16 (3): 1–26. https://doi.org/10.1093/ips/olac013.

Elwood, S. 2021. “Digital Geographies, Feminist Relationality, Black and Queer Code Studies: Thriving Otherwise.” *Progress in Human Geography* 45 (2): 209–228. https://doi.org/10.1177/0309132519899733.

Elwood, S., and A. Leszczynski. 2018. “Feminist Digital Geographies.” *Gender, Place & Culture* 25 (5): 629–644. https://doi.org/10.1080/0966369X.2018.1465396.

Enloe, C. 1989. *Bananas, Beaches & Bases: Making Feminist Sense of International Politics*. Berkeley and Los Angeles: University of California Press.

Foley, M., and S. Basu. 2024. “Decoding the Gendered Imaginary of Cybersecurity Careers: A Social Shaping of Technology Perspective.” *Information, Communication and Society* 1–17. https://doi.org/10.1080/1369118X.2024.2391818.

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

Gaertner, D. 2016. “A Landless Territory? Augmented Reality, Land, and Indigenous Storytelling in Cyberspace.” In *Learn, Teach, Challenge: Approaching Indigenous Literatures*, edited by D. Reder and L. M. Morra, 493–498. Waterloo, Canada: Wilfred Laurier University Press.

Giffney, N. 2004. “Denormatizing Queer Theory: More Than (Simply) Lesbian and Gay Studies.” *Feminist Theory* 5 (1): 73–78. https://doi.org/10.1177/1464700104040814.

Goriunova, O., and A. Shulgin. 2008. “Glitch.” In *Software Studies: A Lexicon*, edited by M. Fuller, 110–118. Cambridge, MA, USA: The MIT Press.

Gurusami, S. 2019. “The Carceral Web We Weave: Carceral Citizens’ Experiences of Digital Punishment and Solidarity.” *Punishment & Society* 21 (4): 435–453. https://doi.org/10.1177/1462474518790237.

Guyan, K. 2022. “Fixing the Wrong Problems: Queer Communities and the False Promise of Unbiased and Equal Data Systems.” *European Data Protection Law Review* 8 (4): 455–461. https://doi.org/10.21552/edpl/2022/4/5.

Hall, L., and W. Clapton. 2021. “Programming the Machine: Gender, Race, Sexuality, AI, and the Construction of Credibility and Deceit at the Border.” *Internet Policy Review* 10 (4): 1–23. https://doi.org/10.14763/2021.4.1601.

Hall, L., S. Paracha, G. Hagan-Green, C. Ure, and P. Jackman. 2022. “Cyber Eyes Wide Open: Creative Collaboration Between Artists, Academics & Cyber Security Practitioners.” *35th International BCS Human-Computer Interaction Conference*, Keele, Staffordshire, UK. Vol. 35, 1–10.

Hall, R. 2015. “Terror and the Female Grotesque.” In *Feminist Surveillance Studies*, edited by R. E. Dubrofsky and S. A. Magnet, 127–149. Durham: Duke University Press.

Hamraie, A., and K. Fritsch. 2019. “Crip Technoscience Manifesto.” *Catalyst: Feminism, Theory, Technoscience* 5 (1): 1–33. https://doi.org/10.28968/cftt.v5i1.29607.

Haraway, D. J. 2016 (1985). “A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century.” In *Manifestly Haraway*, edited by D. J. Haraway, 3–90. Minneapolis: University of Minnesota Press.

Herrera, G. L. 2016. “Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space.” In *Power and Security in the Information Age*, edited by M. D. Cavelty and V. Mauer, 67–93. Abingdon: Routledge.

Hurel, L. M. 2022. “Interrogating the Cybersecurity Development Agenda: A Critical Reflection.” *The International Spectator* 57 (3): 66–84. https://doi.org/10.1080/03932729.2022.2095824.

Jacobsen, T. J. 2020. “From Neurotic Citizen to Hysteric Security Expert: A Lacanian Reading of the Perpetual Demand for US Cyber Defence.” *Critical Studies on Security* 8 (1): 46–58. https://doi.org/10.1080/21624887.2020.1735830.

Jefferson, B. J. 2018. “Computerizing Carceral Space: Coded Geographies of Criminalization and Capture in New York City.” *Environment and Planning A: Economy and Space* 50 (5): 969–988. https://doi.org/10.1177/0308518X18767427.

Jones, E. 2018. “A Posthuman-Xenofeminist Analysis of the Discourse on Autonomous Weapons Systems and Other Killing Machines.” *Australian Feminist Law Journal* 44 (1): 93–118. https://doi.org/10.1080/13200968.2018.1465333.

Jones, E. 2023. *Feminist Theory and International Law: Posthuman Perspectives*. 1st ed. Routledge. https://doi.org/10.4324/9781003363798.

Katz, C. 2001. “Vagabond Capitalism and the Necessity of Social Reproduction.” *Antipode: A Radical Journal of Geography* 33 (4): 709–728. https://doi.org/10.1111/1467-8330.00207.

Kayser, C. 2021. “Narratives of Glitch: Towards a New Understanding of the Imaginal.” *International and Interdisciplinary Conference on Image and Imagination*, 1156–1164. Cham, Springer International Publishing.

LaRochelle, L. 2020. “Queering the Map: On Designing Digital Queer Space.” In *Queer Sites in Global Contexts: Technologies, Spaces, and Otherness*, edited by R. Ramos and S. Mowlabocus, 133–147. London: Routledge.

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

Luchkiw, J. 2016. “Situating Glitches: Networks of Knowledge Production.” *Signal/Noise* 1 (1): 1–17.

Manchanda, N. 2015. “Queering the Pashtun: Afghan Sexuality in the Homo-Nationalist Imaginary.” *Third World Quarterly* 36 (1): 130–146. https://doi.org/10.1080/01436597.2014.974378.

Manjikian, M. 2014. “Becoming Unmanned: The Gendering of Lethal Autonomous Warfare Technology.” *International Feminist Journal of Politics* 16 (1): 48–65. https://doi.org/10.1080/14616742.2012.746429.

Marlin-Bennett, R. 2013. “Embodied Information, Knowing Bodies, and Power.” *Millennium Journal of International Studies* 41 (3): 601–622. https://doi.org/10.1177/0305829813486413.

Marlin-Bennett, R. 2016. "Everyday Rules and Embodied Information: Anti-Money Laundering/counter-Terrorist Financing Practices and Radio Frequency Identification Tags as Security Politics." *Critical Studies on Security* 4 (2): 169–186. https://doi.org/10.1080/21624887.2016.1160199.

Marshall, J. 2001. "Cyber-Space, or Cyber-Topos: The Creation of Online Space." *Social Analysis: The International Journal of Anthropology* 45 (1): 81–102.

Masters, C. 2005. "Bodies of Technology: Cyborg Soldiers and Militarized Masculinities." *International Feminist Journal of Politics* 7 (1): 112–132. https://doi.org/10.1080/1461674042000324718.

McKittrick, K., and L. Peake. 2005. "What Difference Does Difference Make to Geography?" In *Questioning Geography: Fundamental Debates*, edited by A. R. NoelCastree and D. Sherman, 39–54. Oxford: Blackwell Publishing.

Menkman, R. 2011. *The Glitch Moment(um)*. Vol. 4. Amsterdam: Institute of Network Cultures.

Meuller, E. B. 2023. "A Feminist Theorisation of Cybersecurity to Identify and Tackle Online Extremism." Global Network on Extremism & Technology. May 25, 2023. https://gnet-research.org/2023/05/25/a-feminist-theorisation-of-cybersecurity-to-identify-and-tackle-online-extremism/ .

Mhajne, A., and A. Henshaw. 2024a. "Introduction." In *Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions*, edited by A. Mhajne and A. Henshaw, 1–22. New York: Oxford University Press.

Mhajne, A., and A. Henshaw, eds. 2024b. *Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions*. New York: Oxford University Press.

Mhajne, A., K. C. Luna, and C. Whetstone. 2021. "A Call for Feminist Analysis in Cybersecurity: Highlighting the Relevance of the Women, Peace and Security Agenda." LSE Centre for Women, Peace and Security Blog. September 21, 2021. https://blogs.lse.ac.uk/wps/2021/09/17/a-call-for-feminist-analysis-in-cybersecurity-highlighting-the-relevance-of-the-women-peace-and-security-agenda/ .

Millar, K., and J. Shires. 2024. "Masculinist Actionism: Gender and Strategic Change in US Cyber Strategy." *Security Studies* 33 (4): 670–703. https://doi.org/10.1080/09636412.2024.2351918.

Millar, K., J. Shires, and T. Tropina. 2021. *Gender Approaches to Cybersecurity: Design, Defence and Response*. Geneva, Switzerland: United Nations Institute for Disarmament Research.

Mumford, D., and J. Shires. 2023. "Toward a Decolonial Cybersecurity: Interrogating the Racial-Epistemic Hierarchies That Constitute Cybersecurity Expertise." *Security Studies* 32 (4–5): 622–652. https://doi.org/10.1080/09636412.2023.2230879.

Nakamura, L. 2013. "Glitch Racism: Networks as Actors within Vernacular Internet Theory." Culture Digitally. December 10, 2013. https://culturedigitally.org/2013/12/glitch-racism-networks-as-actors-within-vernacular-internet-theory/.

Nakamura, L. 2014. "Indigenous Circuits: Navajo Women and the Racialization of Early Electronic Manufacture." *American Quarterly* 66 (4): 919–941. https://doi.org/10.1353/aq.2014.0070.

Namaste, K. 1994. "The Politics of Inside/Out: Queer Theory, Poststructuralism, and a Sociological Approach to Sexuality." *Sociological Theory* 12 (2): 220–231. https://doi.org/10.2307/201866.

Nash, C. J., and A. Gorman-Murray. 2019. "Queer Mobilities and New Spatial Media." In *The Geographies of Digital Sexuality*, edited by C. J. Nash and A. Gorman-Murray, 29–48. Singapore: Palgrave Macmillan Singapore.

Nguyen, M. 2003. "Queer Cyborgs and New Mutants: Race, Sexuality, and Prosthetic Sociality in Digital Space." In *Asia America.Net: Ethnicity, Nationalism, and Cyberspace*, edited by R. C. Lee and S.-L.-C. Wong, 281–305. New York: Routledge.

Noble, S. U. 2018. "Critical Surveillance Literacy in Social Media: Interrogating Black Death and Dying Online." *Black Camera* 9 (2): 147–160. https://doi.org/10.2979/blackcamera.9.2.10.

Okafor, L. 2022. "Digital (In)security: Safety for Queer People of Colour in a Digitalised World." Masters thesis, University of Oslo.

Okechukwu, A. 2021. "Watching and Seeing: Recovering Abolitionist Possibilities in Black Community Practices of Safety and Security." *Du Bois Review Social Science Research on Race* 18 (1): 153–180. https://doi.org/10.1017/S1742058X21000035.

O'Neal, S. 2023. "Gaza's Queer Palestinians Fight to Be Remembered." *The Nation*. November 16, 2023. https://www.thenation.com/article/world/gaza-queering-the-map/.

Planqué-van Hardeveld, A. 2023. "Securing the Platform: How Google Appropriates Security." *Critical Studies on Security* 11 (3): 161–175. https://doi.org/10.1080/21624887.2023.2239002.

Puar, J. K. 2018. *Terrorist Assemblages: Homonationalism in Queer Times*. Durham: Duke University Press.

Queering The Map. n.d. "Queering the Map." https://www.queeringthemap.com/.

Rachdi, H. 2024. "Glitchy Transnationalism: When Queer Migrants Meet the State Online." *Communication, Culture & Critique* 17 (3): 185–192. https://doi.org/10.1093/ccc/tcae027.

Rao, R. 2020. *Out of Time: The Queer Politics of Postcoloniality*. New York: Oxford University Press.

Richter-Montpetit, M. 2017. "Everything You Always Wanted to Know About Sex (In IR) but Were Afraid to Ask: The 'Queer Turn' in International Relations." *Millennium Journal of International Studies* 46 (2): 220–240. https://doi.org/10.1177/0305829817733131.

Richter-Montpetit, M., and C. Weber. 2017. "Queer International Relations." In *Oxford Research Encyclopedia of Politics*, edited by W. R. Thompson, 1–39. Oxford: Oxford University Press.

Russell, L. 2020. *Glitch Feminism: A Manifesto*. London: Verso.

Shakhsari, S. 2012. "From Homoerotics of Exile to Homopolitics of Diaspora: Cyberspace, the War on Terror, and the Hypervisible Iranian Queer." *Journal of Middle East Women's Studies* 8 (3): 14–40. https://doi.org/10.2979/jmiddeastwomstud.8.3.14.

Shepherd, L. J., and L. Sjoberg. 2012. "Trans-Bodies In/Of War(s): Cisprivilege and Contemporary Security Strategy." *Feminist Review* 101 (1): 5–23. https://doi.org/10.1057/fr.2011.53.

Shires, J., and M. Smeets. 2016. "What Do We Talk About When We Talk About 'Cyber'?" SSRN. https://ssrn.com/abstract=2860839.

Sjoberg, L. 2017. "Queering IR Constructivism." In *The Art of World-Making: Nicholas Greenwood Onuf and His Critics*, edited by H. Gould, 68–79. London: Routledge.

Slupska, J. 2019. "Safe at Home: Towards a Feminist Critique of Cybersecurity." *St Antony's International Review* 15 (1): 83–100.

Slupska, J., S. Dawson Duckworth, L. Ma, and G. Neff. 2021. "Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity." *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama, Japan.

Smart, B. 2016. "Military-Industrial Complexities, University Research and Neoliberal Economy." *Journal of Sociology* 52 (3): 455–481. https://doi.org/10.1177/1440783316654258.

Sobande, F. 2021. "Spectacularized and Branded Digital (Re) Presentations of Black People and Blackness." *Television & New Media* 22 (2): 131–146. https://doi.org/10.1177/1527476420983745.

Stevens, C. 2020. "Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet." *Contemporary Security Policy* 41 (1): 129–152. https://doi.org/10.1080/13523260.2019.1675258.

Stoffel, A., and I. Roland Birkvad. 2023. "Abstractions in International Relations: On the Mystification of Trans, Queer, and Subaltern Life in Critical Knowledge Production." *European Journal of International Relations* 29 (4): 852–876. https://doi.org/10.1177/13540661231176907.

Stone, S. 1995. *The War of Desire and Technology at the Close of the Mechanical Age*. United Kingdom: MIT Press.

Sundén, J. 2016. "Glitch, Genus, TillfälligtAvbrott." *lambda nordica* 21 (1–2): 23–45.

Sutherland, T. 2023. *Resurrecting the Black Body: Race and the Digital Afterlife*. Oakland, California: University of California Press.

Tacheva, J., and S. Ramasubramanian. 2023. "AI Empire: Unraveling the Interlocking Systems of Oppression in Generative AI's Global Order." *Big Data & Society* 10 (2): 1–13. https://doi.org/10.1177/20539517231219241.

Toupin, S. 2014. "Feminist Hackerspaces: The Synthesis of Feminist and Hacker Cultures." *Journal of Peer Production* 5:1–11.

Van Doorn, N. 2011. “Digital Spaces, Material Traces: How Matter Comes to Matter in Online Performances of Gender, Sexuality and Embodiment.” *Media Culture & Society* 33 (4): 531–547. https://doi.org/10.1177/0163443711398692.

Varon, J., and P. Peña. 2021. “Artificial Intelligence and Consent: A Feminist Anti-Colonial Critique.” *Internet Policy Review* 10 (4): 1–25. https://doi.org/10.14763/2021.4.1602.

Vernon, P. 2022. “Sexuality, Gender, and the Colonial Violence of Humanitarian Intervention.” *International Studies Review* 24 (3): 1–22. https://doi.org/10.1093/isr/viac035.

Voigt, M.-L. 2023. “We Built This City on Rocks and (Feminist) Code: Hacking Corporate Computational Designs of Cities to Come.” *Digital Creativity* 34 (2): 1–16. https://doi.org/10.1080/14626268.2023.2205406.

Wade, A. G. 2017. “‘New Genres of Being Human’: World Making Through Viral Blackness.” *The Black Scholar* 47 (3): 33–44. https://doi.org/10.1080/00064246.2017.1330108.

Warner, D. W. 2004. “Towards a Queer Research Methodology.” *Qualitative Research in Psychology* 1 (4): 321–337. https://doi.org/10.1191/1478088704qp021oa.

Wastl-Walter, D., and L. A. Staeheli. 2013. “Territory, Territoriality, and Boundaries.” In *Mapping Women, Making Politics: Feminist Perspectives on Political Geography*, edited by L. A. Staeheli, E. Kofman, and L. Peake, 141–151. New York: Routledge.

Weber, C. 2014. “From Queer to Queer IR.” *International Studies Review* 16 (4): 596–601. https://doi.org/10.1111/misr.12160.

Weber, C. 2016. *Queer International Relations: Sovereignty, Sexuality, and the Will to Knowledge*. New York: Oxford University Press.

Whetstone, C., and K. C. Luna. 2024. “A Call for Feminist Insights in Cybersecurity: Implementing United Nations Security Council Resolution 1325 on Women, Peace, and Security in Cyberspace.” In *Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions*, edited by A. Mhajne and A. Henshaw, 25–51. New York: Oxford University Press.

Whyte, J. 2022. “Cybersecurity, Race, and the Politics of Truth.” *Security Dialogue* 53 (4): 342–362. https://doi.org/10.1177/09670106221101725.

Wilcox, L. 2014. “Queer Theory and the ‘Proper Objects’ of International Relations.” *International Studies Review* 16 (4): 612–615. https://doi.org/10.1111/misr.12187.

Wilcox, L. 2015. *Bodies of Violence: Theorizing Embodied Subjects in International Relations*. New York: Oxford University Press.

Wilcox, L. 2017. “Embodying Algorithmic War: Gender, Race, and the Posthuman in Drone Warfare.” *Security Dialogue* 48 (1): 11–28. https://doi.org/10.1177/0967010616657947.

Wilkinson, C. 2017. “Introduction: Queer/Ing In/Security.” *Critical Studies on Security* 5 (1): 106–108. https://doi.org/10.1080/21624887.2017.1294830.

Wilkinson, C. 2021. “Queer Our Vision of Security.” In *Feminist Solutions for Ending War*, edited by M. MacKenzie and N. Wegner, 89–104. London: Pluto Press.