Participatory Threat Modelling

Exploring Paths to Reconfigure Cybersecurity

Julia Slupska
Oxford Internet Institute, University of Oxford
julia.slupska@cybersecurity.ox.ac.uk

Scarlet Dawson Duckworth
Darktrace
scarlet.dawson@darktrace.com

Linda Ma
Oxford Internet Institute, University of Oxford
linda.ma@oii.ox.ac.uk

Gina Neff
Oxford Internet Institute and Department of Sociology,
University of Oxford
gina.neff@oii.ox.ac.uk

ABSTRACT

We present "participatory threat modelling" as a feminist cybersecurity practice which allows technology research to centre traditionally marginalized and excluded experiences. We facilitated a series of community workshops in which we invited participants to define their own cybersecurity threats, implement changes to defend themselves, and reflect on the role cybersecurity plays in their lives. In doing so, we contest both hierarchical approaches to users in cybersecurity—which seek to 'solve' the problems of human behavior—and a tendency in HCI to equate action research with the development of novel technology solutions. Our findings draw highlight barriers to engaging with cybersecurity, the role of personal experiences (for instance of gender, race or sexuality) in shaping this engagement, and the benefits of communal approaches to cybersecurity.

CCS CONCEPTS

• **Human-centered computing** → Human computer interaction (HCI); Security and privacy; Human and societal aspects of security and privacy.

KEYWORDS

Cybersecurity, feminism, action research, community engagement, privacy, gender, race, sexuality

ACM Reference Format:
Julia Slupska, Scarlet Dawson Duckworth, Linda Ma, and Gina Neff. 2021. Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '21 Extended Abstracts), May 08–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3411763.3451731

1 INTRODUCTION

Cybersecurity research often starts by "threat modelling"—a security design method in which experts anticipate potential threats to a computer system [1]. Although often presented as abstract and impartial, this process usually relies on security experts' own experiences and assumptions about everyday users [23]. This results in research and policy which omits many forms of technological abuse: for example, most smart home threat models do not anticipate that a current or former partner could be a threat [22]. By positioning the researcher's imagination of possible threat scenarios as an abstract-threat model, such methods deploy the "god trick of seeing from nowhere" [26]. In contrast, feminist standpoint theoriesadvocatefor the use of socially situated experiences as an alternative lens for social science knowledge [24], [25].

Following Bardzell's call to use generative feminist approaches to help identify needs, requirements and solutions [2], we reconfigured threat-modelling practices to focus on citizen's experiences of online threats and how they relate to cybersecurity both as a concept and a practice. In a series of eight physical and virtual cybersecurity workshops, we invited participants to 1) model what they perceived to be security threats, vulnerabilities and priorities in their digital practices, 2) take tangible steps to improve their digital practices during "tech support sessions" and 3) share their thoughts and feelings on cybersecurity more broadly in an open and non-judgemental group discussion. Rather than dictating what threats citizensshouldbe worrying about, this project develops a method named "participatory threat modelling" for eliciting and listening to citizens' concerns to expand the scope of threats considered in cybersecurity.

This methodgenerateda variety ofnovel and unexpectedobservations.Experiences like creepy targeted advertisements, being profiled online, or harassed using Zoom-bombing fall outside of orthodox cybersecurity concerns but can make people feel unsafe online.Feelings of avoidance and jargony technical language prevent many from engaging with cybersecurity. Furthermore, people's digital practices are shaped by privilege and oppression. While advantages like wealth or education help people access knowledge about cybersecurity, experiences of abuse due to gender identity, race, or sexuality both expose people to greater harm and leave them more motivated to act. Lastly, our participants identified cybersecurity solutions beyond creating better tools. Cybersecurity cannot be limited to individuals changing passwords or downloading VPNs; structural change at the level of community action and legislation is crucial.

CHI '21 Extended Abstracts, May 08–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8095-9/21/05.
https://doi.org/10.1145/3411763.3451731

2 BACKGROUND & RELATED WORK

Action research (AR) is an umbrella term for a variety of approaches in which researchers and participants work together to address a problem and learn from this attempt in cycles of "action" and "reflection" [3]–[5]. This stems from the belief that all people affected by an issue should be involved in the processes of research inquiry [5]. In particular, intersectionalfeminist forms of action research seek to expose the power relations that lurk under thetrappings of expertise throughmethods which empower participants [6]. Digitally-mediated threats—from malware to trolling—affect people from all backgrounds (although trolling, and other forms of online harassment, disproportionately target people from minoritized backgrounds [7]). Yet many social groups are excluded or underrepresented in cybersecurityresearch and industry, while a fairly small and often homogenous group of experts get to determine what is considered a security threat.

An obvious example of this diversity problem is the industry's gender imbalance , with only 24% of the global cybersecurity workforce identifying as women [8]. Furthermore, representation does not necessarily lead to inclusion: a recent UK study found that while they were not underrepresented in the national cybersecurity industry, Black employees continue to experience significant discrimination in the workplace [9].

AR methods involve community partners with the aim of conducting socially relevant, collaborative, and engaged research. There is evidence that these kinds of projects help bring women and other underrepresented groups into computing [4]. Yet action research in cybersecurity is exceptionally rare [10]. Although they are more common in Human-Computer Interaction (HCI), HCI AR projects usually consist of the "deployment of novel technologies" [4]. This recreates a narrow understanding of what solutions to social problems may be, and precludes legal, economic, political or cultural change. Community engagement in problem framing illustrates this tendency, for example by uncovering how framing algorithmic harms around "bias" suggests that more accurate data is the solution, at the risk of missing deeper questions about whether surveillance technologies should be used at all [11]. Creating spaces for reflection on existing technology can also be more valuable than framing research around developing a new technical solution [12].

This project builds on AR traditions and on a separate tradition named "participatory security design" by inviting citizens to define their own threats online and take action to address them. We follow Hayes [4] in conceptualising cybersecurity "design" as a set of practices rather than a set of properties in a completed system. Participatory security design avoids the assumption that the security of the individual will follow from the security of a technical system and includes the perspective of actors who may ordinarily be marginalized [13]. Thus we incorporated 'situated' knowledge and practices [14] in order to ground information security studies. Researchers have used participatory security design methods in studies of privacy mechanisms for smart homes [15] and security and privacy threats with survivors of intimate partner abuse [16]. In such research, users define or reframe digital security threats, showing how "differential vulnerabilities" can be socially contingent based on factors such as gender, race or age [17]. For example, when asked to define "cyber security" children focus more often on predatory or bullying behaviour, while adults focus on financial crimes and technical protection [18].

Cybersecurity research can discuss the "human factor" in ways that are at odds with theoretical and methodological advances in human-centred computing. Security research often focuses on defending companies or company property, with users portrayed as part of the problem. A popular cybersecurity mantra claims that "humans are the weakest link" in cyber-defense strategies [19]. Research on "human factors" often focuses on "solving" what is perceived as risky internet behaviour such as choosing weak passwords or clicking on phishing links, often through workplace training and awareness courses [20]. Many researchers in human-computer interaction (HCI), privacy-by-design and human-centred computing operate on the assumption that computer security can be achieved *with* users rather than in spite of them. Such approaches advocate for moving from "human-as-a-problem" to "human-as-a-solution" [21]. This is reflected in moves towards "usable", "user-centred" and "human-centred" cybersecurity [22]–[25]. However, research which sees humans as a solution still implicitly casts information systems (or organisations which own them), rather than the humans using them, as the "referent object" or the focus of protection [26].

Other research traditions focus on how to make technology design processes more just and equitable. Value sensitive design (VSD) examines how both pre-existing and emergent biases manifest in computer systems and proposes methods for designers to consider the values of various stakeholders [27], [28]. Calls for "feminist HCI" often centre values such as agency, fulfilment, identity, equity, empowerment, and social justice [2]. Some feminist and anti-racist critiques move beyond an unconscious bias framing to show how intersecting structures, such as patriarchy, white-supremacy, ableism and heterosexism are "hard-coded" into technology, often reproducing existing forms of oppression under the guise of technical neutrality [29]–[31]. The design justice movement seeks to "retool" design methods by centering the voices of those who are directly impacted by the outcomes of the design process [6].

3 METHODS

Weorganised theworkshopsas self-containedinterventionswhich created a safe space for participants to reflect on their online experiences and improvetheir digital privacy practices. We invited "ordinary", or "inexperienced" individuals to actively shape understandings of cybersecurity, precisely because we consider no individual to be truly ordinary or inexperienced. Our recruitment materials—fliers on community noticeboards, social media, and newsletters—emphasised that participants did not need any expertise tocontribute beyond their experiences of online life. For some workshops, we partnered with community and activist groups including Extinction Rebellion Oxford, Victims of Image Crime, and People & Planet.

Each workshop followed a similar format, starting with an introductionwelcoming participants and outliningourmotivations and goals. Next, we conducted a"threat modelling"session focusing on what participants wanted to protect in their online life, what made them feel threatened, and what parts of their digital security they wanted to improve.After that, we conducted a"tech support"session

in which we pointed participants to onlineresourcesandworked-with them to make practical changes. Lastly, we facilitated ageneral discussionon the nature of and future directions for cybersecurity.

We adopted a feminist approach in the design and facilitation of our workshops. Although there is no one unified "feminism", feminist theories and methods often pay close attention to care, emotionality and personal "standpoint" [14], [32], [33]. Accordingly, we aimed to create an environment of mutual care and support. Our questions focused on emotionality and personal experience—topics in which anyone's and everyone's answers would be valid. Thesemethods reflect the theoretical commitments of the project, which see research as a form of intervention rather than a neutral data-collection exercise. Theworkshops were designed to co-create knowledge with our participants: for example, sharing participant responses on a screen throughout the workshop allowed participants to comment and react to the contributions of others, creating a sense of communal sharing and debate.

In order to create safe spaces for discussion around sensitive topics, the "research" aspect of the project was entirely optional. If the participants chose to opt-in, they could anonymously share their thoughts and stories on their own devices using the Mentimeter-platform, in which case their contributions and would be projected on screen in realtime.Alternatively, participants could opt-in to recorded focus groups with the same questions. Four of our eight workshops were held physically in the UK, with the rest taking place digitally due to the Covid-19 pandemic. With 10-12 participantsper event, we had a total of approximately 90 participants. Ultimately, we recorded 419 individualMentimeterresponses and four focus groups across seven workshops. Follow-up interviews with seven participants explored their contributions in further depth.

Data was analysed qualitatively using thematic analysis [34].Following a first-pass inductive coding of the first workshop, we established a codebook with 18 topics and 29 themes, which we used to qualitatively code all Mentimeter responses and each fragment within the focus group and interview transcripts. Each document was coded separately by two researchers, who subsequently performed an intercoder reliability check to settle on final codes through consensus. Five topics and eight themes which were not noted in the initial analysis emerged in this process. We then cross-referenced the frequency with which each topic or theme appeared against the richness of the emergent qualitative data, to arrive at our findings.

As we did not collaborate withparticipantson the design of this methodology,our studywas notfully participatory.Future iterations of this projectwould be strengthened further by adopting a co-design approach to research design. Another limitation that emerged was the standalone quality of the workshops, as many participants did not have enough time to both identify threats and implement solutions in one workshop.Future workshops could be conducted iteratively, allowing for deeper participation and more robust results.

Lastly, participant recruitmentstrongly shaped the project. While the workshops were open to all, there was a high representation of women (65.6%) and non-binary people (9.8%).[1] Althoughour materials were inclusive to those who did not consider themselves "'tech-savvy"',due toour own environments, the nature of our partnerorganisationsand theurban locations of theworkshops, we found-participants tended to comefrom relatively privileged educational backgrounds who were alreadysomewhatcomfortable with technology. Going forward, we plan to focus recruitment on communities disproportionately targeted by online surveillance and harassment.

3.1 Our standpoint

As a form of "reflexivity", we shared our backgrounds and motivations for the project at the start of each workshop. By doing so we aimed to put participants, particularly those from marginalized or non-technical backgrounds, at ease. Reflexivity is a practice in which you reflect on how your own experiences, beliefs, and standpoint in the world shape your research [35]. For us, reflexivity involved aspects of our identities—being women from non-technical backgrounds—which were treated in various subtle ways as disadvantages in the context of cybersecurity. This and our desire to improve our own digital information security practices led to the idea of creating a collaborative, safe space where people could troubleshoot, discuss and educate themselves together.

It is worth noting that by sharing our positionality with our participants, we may have influenced their beliefs and attitudes going into the workshops. Furthermore, this form of (incomplete) reflexivity can obscure other types of privilege that also influence our work: we are cis-gendered, able-bodied and members (or graduates) of an academic institution that is inseparable from a colonial history. We found feminist theories and methods particularly useful both for making sense of our own experiences and as a normative framework for cybersecurity research and practice. A project which centered (for example) critical race, disability, or anarchist theory might have shared some of our assumptions but would likely have asked different questions, resulting in different findings.

3.2 Ethics

Ethical concerns for this study included the risk that participants may not feel comfortable discussing certain workshop topics, particularly those participants who had experienced sexual abuse and other identity-based attacks online. We addressed this through practices of informed consent, such as reminding participants that each question is optional and giving them multiple contribution opportunities and fora to choose from, including the questionnaire, group discussion and one-on-one interviews. For workshops focused on sensitive topics, we also allocated special breaks for self-care and designated an organiser that participants could speak to if they were feeling distressed. Furthermore, there are risks inherent to public events (both on- and off-line), such as harassment or trolling. These did not arise at our workshops as far as we are aware. However, we prepared strategies for dealing with such situations in collaboration with our tech support team. Our study was reviewed and approved

[1] These statistics are indicative rather than exhaustive, as all responses to questions were optional, and only about two thirds of participants answered this question. We note that we did not collect demographic data on race and ethnicity until the final three workshops and did not collect data on disability, class or education level. We view this as a significant oversight, as racial, class and educational disparities are also ingrained in cybersecurity culture and equally important to address.

by the University of Oxford's Central University Research Ethics Committee (SSH_OII_CIA_20_004).

4 FINDINGS

4.1 Threat modelling from a standpoint

Participants perceived online threats in unique and unexpected ways. Although many mentioned conventional cybersecurity threats such as password compromise and online banking as areas of concern, participants often reported being more concerned with reputational and interpersonal harms. As (P1,I)[2] said "*I'm more worried about being socially shamed, publicly shamed, than someone stealing my money.*"

These reputational concerns often tied into professional identities. Many participants learned about cybersecurity primarily in a work setting, and therefore their knowledge of company policies preceded that of their personal cybersecurity. The need to maintain a professional reputation drove many participants' concerns for privacy, with "*employers accessing old data*" often mentioned as a threat. (P2,W7), who had been a sex worker noted that the security of her professional life was extremely important, but that she was often met with an attitude she characterized as "*well you can't expect privacy when you've done that sort of work.*"

Many participants shared experiences of being condescended to, patronised or subjected to 'mansplaining' due to their gender. Participants noted that people providing IT lessons or tech support are often male: (P3, W2) explained that "*being a female getting tech support from a male can be disconcerting. Fears over what private info they might see, find, engage with . . . make women feel vulnerable.*" This gendered vulnerability encompassed subjects from location-tracking, sending nudes to misogynistic trolling (particularly on Twitter).

Experiences of privilege (or lack thereof) linked to wealth, class and education also shaped engagement with cybersecurity. Participants framed cybersecurity knowledge as a privilege that comes with good education. Being able to pay for technical or legal support (as well as tools such as VPNs) if necessary was cited as a big factor in limiting and enabling engagement online. Several participants hypothesized that their own privileged backgrounds had made them feel more complacent about security and privacy online. In contrast, several participants linked experiences of being in minoritized groups—due to race/ethnicity, sexuality or gender identity, to a greater need for digital security. Participants who had been in organisations focusing on race, or just spoken out about race online, reported increased online aggression and worries about "*doxxing*", a form of online harassment that "breaches perceived privacy boundaries by releasing information through online mass media channels, resulting in physical and online consequences for a target" [36].

Experiences of being queer and/or polyamorous online made people more aware of granular privacy settings which were necessary for "*managing what I present to different audiences that have different levels of awareness of my sexuality*" (P4, W2). This resonates with and extends past research on virtual communities as safe spaces for LGBTQ youth to communicate and express themselves [37]. (P5,I) outlined the ways in which online banking put them at risk as a trans person: as they live in a country in which changing your name to match your gender identity is not legal, their online banking still used their legal name, putting them at continual risk of being outed with each financial transactions.

Survivors of image-based sexual abuse faced a particularly challenging set of threats. Not only had they experienced ex-partners sharing intimate images —including videos filmed without their consent— online, they also described ongoing harassment on social media as strangers continuously re-shared links to pornography sites which refused to take down these images and videos. Many of these threats—such as being outed as a trans or queer person, image-based sexual abuse, and misogynistic trolling—are not considered in existing cybersecurity threat models. These participants' unique standpoints, informed by their lived experiences and varied identities, contributed to a more robust understanding of both online threats and possible solutions.

4.2 Solutions beyond new tools

Many cybersecurity solutions, including the ones in the guides we used in the "tech support" part of the workshops, focus on downloading tools such as password managers and secure browsers such as Tor. Many participants described navigating information about cybersecurity as "*intimidating*" and "*overwhelming*", leading to practices of avoidance. Exclusionary technical language was also commonly mentioned as a barrier to engaging with cybersecurity. (P6, W7) said, "*often tech help websites seem like they are written by men who are tech experts and not easy to understand.*" Resources are often not only full of technical language, but also in English and therefore not accessible for speakers of other languages. The fact that we conducted our workshops in English, with participants primarily from the Global North, unfortunately recreated the Anglo-centrism in technology education which recent projects [38]—as well as Bardzell's call for pluralism [2] have critiqued.

When we asked our participants to describe what tools they needed or wanted, participants sought simpler, user-centred, intuitive tools such as an "*erase me button*" that might to delete their data from any given website or regularly prompts to update their privacy settings. This echoes past research on, for example, poorly designed user interfaces for Cloud deletion functions [25]. But many participants consciously resisted the notion that they needed new tools, instead raising the need for different norms around cybersecurity. (P7, W3) wrote "*tech worlds encourage tech solutions, but I don't want more complex tech/ [or to] buy more tools.*"

We found that many participants were pessimistic about the "*unknown unknowns*" and the seeming impossibility of keeping abreast of latest cybersecurity practices and protections. Moreover, participants felt individual users should not be held responsible for learning about cybersecurity developments. Many participants reflected positively on the communal nature of our workshops, and called for similar coordinated, community-based responses which go beyond technically oriented solutions that can contribute to cognitive overload and alienation. As (P8, I) described it, the "*atmosphere we had in the workshop*" helped create "*confidence in hearing various tech terms and not being scared by them as such.*"

[2]P indicates participant number, W indicates workshop number, I indicates interview so (P1,I) indicates participant #1 in an interview

The notion of 'group privacy', which was continually raised by participants, suggested security for the individual improved that of the collective, and vice versa. Akiwowo [42] develops similar notions of "digital self care" and "digital citizenship" to articulate the relationship between individual and societal responsibility for online safety.

Beyond that, participants suggested structural changes were needed at the level of culture and legislation to improve the safety of our digital 'streets'. As (P9,I) put it: "*all these potential tools hinge around the fact that what you really want is [...] trust. Like if someone could just invent [. . .] some way of definitely holding Facebook [or] Instagram accountable.*" When asked what they would have wanted to learn more about, several participants mentioned the socio-economic aspects of data collection, such as how it creates profits for businesses. Focusing our "tech sessions" primarily on individual practices and improvements may have obscured structural aspects of online tracking and privacy. Future workshops could build on this by focusing less on individual actions and tool-based solutions, and more on developing community and finding structural solutions, reflecting the shift from "digital self-defense to data politics" [41].

Participants argued for their governments' responsibility to realign the incentives of digital platforms through instituting accreditation systems, or restrictions such as the GDPR. Companies, in turn, should be responsible for ensuring their platforms were accountable to users, transparent and trustworthy by default—for instance, through filters and controls to limit harassment. Lastly, many participants confirmed past calls for more cybersecurity education in schools, including education about consent in relation to data-sharing [39]. Achieving these structural changes, our findings suggest, will require concerted community pressure.

5 DISCUSSION

Our findings show integrating participatory methods into threat modelling yields substantial benefits, through revealing the nature and dimensions of threats sometimes seen as side concerns. These findings lend support to the idea that people experience online threats differently according to their identities and experiences. Cybersecurity research that engaged meaningfully with underserved groups would in turn inform the development of cybersecurity systems designed to be more resilient to the range of threats that humans actually experience.

In AR researchers and participants to create knowledge in partnership with one another. Creating a social, supportive space removed some of the barriers that individuals can often experience in engaging with cybersecurity. The workshops also, however, provided researchers an opportunity to gain an immersive understanding of participants' cybersecurity-related practices, knowledge and beliefs. This approach helped build a breadth of an understanding that an abstract security analysis would not.

Many threats described in the workshops, such as "*being stalked by strangers or friends of friends*" or targeted advertising would not be treated as "attacks" in conventional cybersecurity literature [40]. Yet these experiences of feeling threatened do provide an interesting hypothetical: what would cybersecurity look like if it defended users against threats like targeted advertising? By respecting these experiences as a valid source of knowledge about cybersecurity, we challenge a monolithic, orthodox understanding of what "counts" as a cybersecurity issue. This *reconfigured* cybersecurity is more sensitive to lived experiences of privilege and discrimination that inevitably shape life online.

6 CONCLUSION

We present "participatory threat modelling" as a feminist cybersecurity practice which allows technology research to centre traditionally marginalized and excluded experiences. Through a series of community workshops, we incorporate a wider variety of threats into security analysis and challenge a narrow focus on novel technical solutions within HCI. We hope this project seeds change on multiple levels. In the short term, we believe our workshops empowered participants to improve their own cybersecurity practices and engage critically with the concept of cybersecurity. More broadly, our research demonstrates an alternative approach to threat modelling both for research and security training. We hope to see a popularisation of these methods and those of like-minded researchers as a path to democratise cybersecurity.

ACKNOWLEDGMENTS

This project would not exist without the hard work of the remaining members of the Reconfigure Network (Nayana Prakash, Selina Cho, Laura Shipp, Hayyu Imanda, Hubert Au, Antonella Perinni and Romy Minko), as well as the contributions of community partners and workshop participants throughout the project. We are forever indebted to everyone's enthusiasm and generous collaboration. This work was supported by UK Research & Innovation, grant BB/T018593/1.

REFERENCES

[1] A. Shostack, *Threat Modeling: Designing for Security*. Wiley, 2014.
[2] S. Bardzell, "Feminist HCI: Taking Stock and Outlining an Agenda for Design," *CHI*, 2010, doi: 10.1145/1753326.1753521.
[3] S. Kindon, R. Pain, and M. Kesby, "Participatory Action Research: Origins, approaches and methods," in *Participatory Action Research Approaches and Methods: Connecting People, Participation and Place*, 2007.
[4] G. R. Hayes, "The relationship of action research to human-computer interaction," *ACM Trans. Comput. Interact.*, 2011, doi: 10.1145/1993060.1993065.
[5] S. Kemmis, R. McTaggart, and R. Nixon, *The action research planner: Doing critical participatory action research*. 2014.
[6] S. Costanza-Chock, "Design Justice: towards an intersectional feminist framework for design theory and practice," in *DRS2018: Catalyst*, 2018, doi: 10.21606/drs.2018.679.
[7] G. UK, "The Ripple Effect: Covid-19 and the Epidemic of Online Abuse," 2020.
[8] $(ISC)^2$, "$(ISC)^2$ Cybersecurity Workforce Study: Women in Cybersecurity," 2019.
[9] NCSC, "Decrypting diversity: Diversity and inclusion in cyber security," 2020.
[10] D. Fujs, A. Mihelič, and S. L. R. Vrhovec, "The power of interpretation: Qualitative methods in cybersecurity research," in *ACM International Conference Proceeding Series*, 2019, doi: 10.1145/3339252.3341479.
[11] M. Katell *et al.*, "Toward situated interventions for algorithmic equity: Lessons from the field," in *FAT* 2020 - Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 2020, doi: 10.1145/3351095.3372874.
[12] A. Strohmayer, J. Clamen, and M. Laing, "Technologies for Social Justice," 2019, doi: 10.1145/3290605.3300882.
[13] C. P. R. Heath, P. A. Hall, and L. Coles-Kemp, "Holding on to dissensus: Participatory interactions in security design," *Strateg. Des. Res. J.*, 2018, doi: 10.4013/sdrj.2018.112.03.
[14] D. Haraway, "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective," *Fem. Stud.*, 1988, doi: 10.2307/3178066.
[15] Y. Yao, J. R. Basdeo, S. Kaushik, and Y. Wang, "Defending my castle: A co-design study of privacy mechanisms for smart homes," in *Conference on Human Factors in Computing Systems - Proceedings*, 2019, doi: 10.1145/3290605.3300428.

[16] R. Leitão, "Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse," *ACM Conf. Des. Interact. Syst.*, pp. 527–539, 2019.
[17] S. Fox, N. Merrill, R. Wong, and J. Pierce, "Differential vulnerabilities and a diversity of tactics: What toolkits teach us about cybersecurity," *Proc. ACM Human-Computer Interact.*, 2018, doi: 10.1145/3274408.
[18] S. L. Jones, K. Muir, E. I. M. Collins, A. Joinson, and A. Levordashka, "What is 'cyber security'?: Differential language of cyber security across the lifespan," in *Conference on Human Factors in Computing Systems - Proceedings*, 2019, doi: 10.1145/3290607.3312786.
[19] C. McMahon, "In Defence of the Human Factor," *Front. Psychol.*, vol. 11, no. 1390, 2020.
[20] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, 2017, doi: 10.1016/j.heliyon.2017.e00346.
[21] V. Zimmermann and K. Renaud, "Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset," *Int. J. Hum. Comput. Stud.*, 2019, doi: 10.1016/j.ijhcs.2019.05.005.
[22] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in *8th USENIX Security Symposium*, 1999.
[23] Z. Benenson, G. Lenzini, D. Oliveira, S. Parkin, and S. Uebelacker, "Maybe poor johnny really cannot encrypt - The case for a complexity theory for usable security," in *ACM International Conference Proceeding Series*, 2015, doi: 10.1145/2841113.2841120.
[24] S. McKenna, D. Staheli, and M. Meyer, "Unlocking user-centered design methods for building cyber security visualizations," in *2015 IEEE Symposium on Visualization for Cyber Security, VizSec 2015*, 2015, doi: 10.1109/VIZSEC.2015.7312771.
[25] K. M. Ramokapane, A. Rashid, and J. M. Such, "'I feel stupid I can't delete...': A study of users' cloud deletion practices and coping strategies," in *Proceedings of the 13th Symposium on Usable Privacy and Security, SOUPS 2017*, 2019.
[26] U. D. Ani, H. He, and A. Tiwari, "Human factor security: evaluating the cybersecurity capacity of the industrial workforce," *J. Syst. Inf. Technol.*, 2019, doi: 10.1108/JSIT-02-2018-0028.
[27] B. Friedman, P. H. Kahn, and A. Borning, "Value Sensitive Design and Information Systems," in *The Handbook of Information and Computer Ethics*, 2009.
[28] B. Friedman and P. Kahn, "Value sensitive design: Theory and methods," *Univ. Washingt. Tech.*, 2002.
[29] S. U. Noble, *Algorithms of oppression: How search engines reinforce racism*. 2018.
[30] R. Benjamin, "Race After Technology: Abolitionist Tools for the New Jim Code," *Soc. Forces*, 2019, doi: 10.1093/sf/soz162.
[31] J. Wajcman, "Feminist theories of technology," *Cambridge J. Econ.*, 2009, doi: 10.1093/cje/ben057.
[32] S. Harding, "Feminist Standpoint Epistemology," *Gend. Sci. Read.*, 2001.
[33] P. H. Collins, Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment. Routledge, 1990.
[34] V. Braun, V. Clarke, N. Hayfield, and G. Terry, "Thematic analysis," in *Handbook of Research Methods in Health Social Sciences*, 2019.
[35] N. Gould, "Reflexivity," in *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*, 2015.
[36] S. Eckert and J. Metzger-Riftkin, "Doxxing," in *The International Encyclopedia of Gender, Media, and Communication*, 2020.
[37] L. Lucero, "Safe spaces in online places: social media and LGBTQ youth," *Multicult. Educ. Rev.*, 2017, doi: 10.1080/2005615X.2017.1313482.
[38] M. Wong-Villacres *et al.*, "Decolonizing learning spaces for sociotechnical research and design," in *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*, 2020, doi: 10.1145/3406865.3418592.
[39] D. Pencheva, J. Hallett, and A. Rashid, "Bringing cyber to school: Integrating cybersecurity into secondary school education," *IEEE Secur. Priv.*, 2020, doi: 10.1109/MSEC.2020.2969409.
[40] J. Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity," *St. Anthony's St Antony's Int. Rev.*, no. Whose Security is Cybersecurity? Authority, Responsibility and Power in Cyberspace, 2019.
[41] Becky Kazansky, "'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance," *Big Data Soc.*, vol. 8, no. 1, 2021.
[42] S. Akiwowo, "Digital Self Care," *Fix the Glitch*, 2020. [Online]. Available: https://fixtheglitch.org/digitalselfcare/.