Othered, Silenced and Scapegoated: Understanding the Situated Security of Marginalised Populations in Lebanon

Jessica McClearn and Rikke Bjerg Jensen, *Royal Holloway, University of London;*
Reem Talhouk, *Northumbria University*

https://www.usenix.org/conference/usenixsecurity23/presentation/mcclearn

This paper is included in the Proceedings of the 32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Othered, Silenced and Scapegoated:
Understanding the Situated Security of Marginalised Populations in Lebanon

Jessica McClearn
Royal Holloway, University of London
jessica.mcclearn.2021@live.rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Reem Talhouk
Northumbria University
reem.talhouk@northumbria.ac.uk

Abstract

In this paper we explore the digital security experiences of marginalised populations in Lebanon such as LGBTQI+ identifying people, refugees and women. We situate our work in the post-conflict Lebanese context, which is shaped by sectarian divides, failing governance and economic collapse. We do so through an ethnographically informed study conducted in Beirut, Lebanon, in July 2022 and through interviews with 13 people with Lebanese digital and human rights expertise. Our research highlights how LGBTQI+ identifying people and refugees are *scapegoated* for the failings of the Lebanese government, while women who speak out against such failings are *silenced*. We show how government-supported incitements of violence aimed at transferring blame from the political leadership to these groups lead to amplified digital security risks for already at-risk populations. Positioning our work in broader sociological understandings of security, we discuss how the Lebanese context impacts identity and ontological security. We conclude by proposing to design for and with positive security in post-conflict settings.

1 Introduction

Experiences of political unrest, corruption and economic crisis shape the daily lives of people living in post-conflict Lebanon [1,2,13,95]. Post-conflict societies are characterised by being in a 'transition continuum', rather than in a fixed state of conflict or peace. Here, key transition milestones include ending violence, a peace agreement, disarmament, functioning governance, societal reconciliation and economic recovery [21]. The Lebanese Civil War (1975-1990) ended with the Al Taif Agreement, but the legacies of conflict have moved from (mostly) armed conflict to manifesting in Lebanese political and governance structures. A history of conflict rooted in fundamental disagreements between Christian and Muslim Lebanese on the historicity of the country and their visions for Lebanese identity has led to society-wide fragmentation [74]. Identity and security in Lebanon are linked to, and through, such sectarian divides, where distinctions between *them* and *us* dominate public discourse.[1]

The corrupt Lebanese regime whose politics functions along sectarian divides has flung the country into one of the world's worst economic crises in 150 years [10]. In 2021, the OHCHR reported that Lebanese political and financial leaders were "responsible for forcing most of the country's population into poverty" [70], while the World Bank labelled the economic collapse in the country a "ponzi scheme" [11] leading to a "deliberate depression" [9]. Stories of how Lebanese people have been locked out of their bank deposits have been covered in international media [8], with some reporting that "three-quarters of the Lebanese population are in poverty" [48] and that 80% of the Lebanese population have no access to basic rights such as education and healthcare [96]. Post-conflict legacies thus underpin our work on digital security in Lebanon, where sectarian tensions also manifest online.

Our work shows how marginalised groups in Lebanon, particularly LGBTQI+ identifying people and refugees, are *scapegoated* for Lebanese government failures, while women who speak out against such failings or challenge patriarchal norms experience amplified *silencing*. We refer to these practices as *othering*. We ground our findings in related digital security scholarship that has identified a diverse range of risks experienced by, e.g., refugees and migrants [50,78] and LGBTQI+ identifying people [38,45,56] in higher-risk contexts. Further, existing work has highlighted how the ability to secure digital access is of particular concern for displaced populations and is often intermittent [72,83]. Such work shines a light on how some populations become higher-risk due to their socio-economic status, political convictions or gender identity. Further, we position our work within wider conceptualisations of security and identity; particularly sociological concepts of ontological security, e.g. [41,62], and positive security, e.g. [62,71], to highlight the need for digital security research to consider the intersecting forms of marginalisation and societal structures of inequity and insecurity.

[1] In 'sectarianism', belonging to a religious sect is the main mechanism for legal recognition, political participation and, thus, social control [65].

Contributions. This work draws on ethnographically informed fieldwork over two weeks in Beirut, Lebanon, in July 2022. As well as observation *in situ*, the research involved 12 interviews with 13 people who had expertise in digital and human rights in Lebanon. The aim of the research was to explore how digital security is shaped by the Lebanese post-conflict context and the societal-wide failing infrastructures. We report on findings pertaining to notions of othering, scapegoating and silencing targeted at marginalised people. By positioning our work within digital security, we place the security of technology in the context of people and society.

Our work makes four distinct contributes to digital security scholarship. First, we show how already marginalised populations in Lebanon are targeted through practices of othering that are actively supported by the Lebanese sectarian leadership. This othering appears on a scale ranging from online silencing, to targeted abuse and hatred, to outright scapegoating. Our findings highlight how these practices amplify the digital security risks of those being targeted, particularly women, LGBTQI+ identifying people and refugees. We further show how the Lebanese government uses othering to shift blame for the political and economic crisis onto these marginalised populations. Our findings demonstrate how these forms of othering are rooted in perceptions that marginalised groups morally challenge the traditional politics that maintains the sectarian Lebanese regime, its state power and societal position. Second, we show how the failures of institutions within a post-conflict setting contribute to the fragmentation of Lebanese identities and allow for the normalisation of an ‘us’ and ‘them’ discourse, which further reinforces practices of othering and how they manifest online. Third, we draw on positive security for design interventions that enhance dialogue and reconciliation within post-conflict contexts. We show that to succeed in this endeavour, the security experiences of marginalised populations need to be identified through situated research that understands the enmeshed – social and technological – nature of digital security. Fourth, we conducted an ethnographically informed study that brings to the fore the situated security of the populations under study, as well as our interpretations of it. In doing so, we also contribute to a diversification of the methodological approaches employed to understand digital security.

2 Related Work

Our work speaks to broader conceptualisations of security, which we set out in this section. First, in Section 2.1, we bring ontological security into conversation with identity work, before engaging with the concept of scapegoating as it pertains to notions of blame and othering. We do so in Section 2.2. In Section 2.3 we engage with existing research on higher-risk populations. Collectively, these works lay the conceptual foundations for our presentation of findings in Section 4 and discussion in Section 5.

2.1 Ontological Security and Identity

We ground and deepen our discussion on the practices of othering that we observed in our findings by situating it within **ontological security**[2] as it relates to identity and positive security. Practices of othering create a distinction between ‘us’ and ‘them’ and is a process inherently linked to ontological security and the securing of the self. Concretely, we use sociologist Bill McSweeney’s [62] framing of security as encompassing both the freedom to live without fear and protection from harm. We thus understand ontological security as the creation of a sense of security through the leveraging of trusted relations and routines [24, 25]. Ontological security is the feeling that one’s understanding of and position within the world is stable and reliable, providing a sense of predictability [62, 71]. This definition also ties in with Steele’s [81] understanding of ontological security as “security as being” and Mitzen’s [66] “security of the self”, foregrounding the relationship between security and identity. We use ontological security as a framework for interrogating how security and identity are connected in the Lebanese context.

Identity is not fixed but is continuously shaping – and shaped by – how people relate to each other and to the world that surrounds them. Identity therefore is a dialogical practice through which people establish a sense of ontological security [26]. While the relationship between ontological security and identity work has many dimensions, essentially ontological security may lead to particular forms of identity work. For example, constructing and/or negotiating an identity that holds some form of power or ensures a sense of belonging may lead to greater ontological security. Recent HCI scholarship has also drawn on identity work as understood within ontological security. For example, the authors of [77] showed how refugees in Jordan, Lebanon and Uganda negotiated their digital identities within the UNHCR identity management system to maximise access to services and, in turn, their ontological security. In [28, 29], Dosono and Semaan referred to “identity work as deliberation” when exploring identity work among Asian American and Pacific Islander communities on Reddit during the 2016 US Presidential Election. The concept of ontological security has also been employed in research on isolated communities at the margins of society [51] and refugees (re)settling in and accessing a new country [22, 23]. These works raise the question of what kind of security is needed to better cater to marginalised populations whose threat horizons are amplified through digital technology [23].

Similar to ontological security, **positive security** builds on McSweeney’s [62] work where positive security is the ability to pursue one’s interests and fulfil one’s needs [42] through trusted relations. Indeed, McSweeney was one of the first to acknowledge the significance of positive security, arguing that the noun *security* refers to an object to be protected, but

[2] The concept of *ontological security* was developed by sociologist Anthony Giddens [41].

that the adjective *secure* refers to making something possible [62, p.14]. This is distinct from **negative security**, where security is gained through the protection from threats [42]. McSweeney [62] further articulated how people need day-to-day routines to establish a sense of self and be able to relate to others as central to positive security. Building on McSweeney's [62] work, Roe [71, p.778] notes that "[p]ositive security thus relates to the securities and insecurities that individuals, and the communities in which people live, routinely create for one another." A positive security lens thus enables us to identify the barriers and threats faced by individuals and groups when attempting to secure their aspirations and ambitions, i.e. making something possible. In Section 5.2 we consider how designing for positive security in post-conflict settings requires design interventions that focus on dialogue and building trust relations across fragmented societies.

2.2 Scapegoating: Blame and Othering

The use of scapegoating can be seen as a mechanism of restoring order and reinforcing group identity [52]. Scapegoating, or the threat of it, can thus be seen as a way to control someone's identity through processes of othering. International relations and statecraft literature has long considered the power of strategic scapegoating to control populations through the use of diversionary theory [34, 40] or through the link of violence and scapegoat ideology [90]. Despite this work providing insight into how populations have been painted as scapegoats little research exists into the relationship between security, marginalised populations and forms of othering.

Through the practice of scapegoating 'the other' is identified as 'not me', which Mythen [67, p.101] articulates as "the not me – other" approach and highlighting it as a convenient way to dispatch blame towards targeted groups. Othering and scapegoating are thus often connected and surface in times of crisis, where they function as methods used to assign blame [30]. This is also reinforced by Joffe [52], who argues that the continuous degradation of 'others' across societies is a mechanism of assigning blame and "becomes magnified at times of crisis". Security scholar Neocleous [68] explores the role of othering in relation to identity construction and fear of threats, which are often grounded in feelings of uncertainty. Here, the production of 'others' is often amplified through government and media discourses, which can reproduce negative stereotypes about 'the other' and "apportionment of blame, masking the multicausal reproduction of risk" [67]. For the purpose of this study we understand scapegoating as "the act of blaming an out-group when the in-group experiences frustration or is blocked from obtaining a goal" [6].

2.3 Security for Higher-Risk Populations

Section 2.1 focused on ontological and positive security, while Section 2.2 foregrounded practices of othering. Here, we further contextualise our contributions by drawing on the growing body of security-driven work that has focused on higher-risk and marginalised populations, recognising that their security needs are not well served by the technologies they rely upon [3, 38]. The participants in our study can be considered *higher-risk* in multiple ways, where their situated security experiences of living through conflict also heighten their digital security needs. This intertwining of technological and societal-level security is exemplified in existing work with higher-risk populations. Research with migrants and refugees has identified how language and local customs or social structures, for example, become barriers to them fulfilling their security needs in different contexts and in addition to technological obstacles [23, 45, 50, 78]. These bodies of work highlight how unmet digital security needs lead to a series of informal and socially rooted practices that aim to mitigate experiences of ontological insecurity. Other groups of higher-risk users, such as political activists, have been shown to rely on the digital security practices performed by their social relations, such as other activists, as well as the security of the technology they use [3, 14, 27, 32]. This work highlights the significance of trusted relations for ontological security that translate to digital security practices. Recent work on LGBTQI+ identifying people has also shown how they look for support from trusted queer groups to navigate questions of identity, personal safety and security [38, 56]. Without doing so explicitly, these works speak to the enmeshed nature of ontological security and identity, as we note in Section 2.1; thus suggesting how the ontological security needs of marginalised populations manifests through digital security practices.

The intertwining of technological and societal security is further highlighted in research on higher-risk populations. For example, the authors of [76] show how South Asian women developed performative practices to protect their privacy. In [60], the authors demonstrate how survivors of intimate partner abuse develop distinct privacy practices that pertain to the different stages of their experiences of abuse. This work speaks to a broader body of scholarship that has focused on the security and privacy needs of those living with intimate partner violence, e.g. [35, 36, 93]. Further, research on the protection mechanisms developed by migrant domestic workers highlights how these are grounded in online and offline support networks [80]. Finally, tying together notions of financial insecurity and digital security, the authors of [79] explored how pressures related to homelessness and limited financial resources impacted people's security and privacy practices. The literature referred to here shows how marginalisation shapes digital security in different ways, while being rooted in wider societal contexts.

3 Methodology

Here, we outline the research design, including participant recruitment and the interview process as well as the ethical considerations that guided our research. We do so in Section 3.1. In Section 3.2, we discuss our data analysis and researcher positionalities.

3.1 Research Design

One author conducted ethnographically informed research in Beirut, the capital of Lebanon, over the course of two weeks in July 2022. This meant that she (see Researcher Positionalities in Section 3.2) spent time engaging with people in different settings, including in coffee shops and at public events such as at poetry readings and walking tours of the city. The research was designed to meet people in their everyday contexts; what Brewer [17] calls people's *naturally occurring settings*. We refer to our work as *ethnographically informed* to acknowledge the short-term nature of the fieldwork, and we use *situated security* as a methodological construct to identify and analyse the lived security experiences of Lebanese people. Situated security thus speaks to the ground-up nature of the research design where the ethnographically informed approach situates people's security in their everyday settings and activities.

Researcher observations and interactions with people in Beirut as well as reflections on such encounters were recorded as field notes and brought into the analysis as discussed in Section 3.2. These notes took the form of conscious and detailed recordings of the research sites and interactions, which are referred to as *thick description* in ethnography [39].

The researcher stayed in rental accommodation in an area of Beirut, Mar Mikhael, which still shows evidence of the 2020 Port Blast through the many destroyed buildings and dilapidated storefronts. Yet, the area is home to a vibrant community with many LGBTQI+ identifying people having made this area their home. With the researcher being situated in this community specifically and Beirut more broadly, everyday security challenges and technological barriers were felt and observed on a daily basis. The country-wide political and economic collapse had led to significant infrastructural breakdowns which, for example, meant that Internet access was limited as electricity was only guaranteed for two hours a day. The dilapidated sidewalks made it challenging to get to interview locations and it was thus necessary to rely on taxi services. Due to the economic crisis and extortionate currency exchange rates the researcher had to avail of local practices of exchanging currency. This, for example, involved contacting an unknown individual through WhatsApp and exchanging money from that individual's moped.

Participant Recruitment. The researcher recruited 13 participants who were knowledgeable about the digital security and socio-political landscape in Lebanon, and conducted 12 semi-structured interviews (nine in person and three online) (see Table 1). Recruitment was done by first identifying potential organisations and individuals who had a public voice on matters relating to digital privacy and security. No further criteria were applied. We emailed identified individuals to explain the research and ask whether they would be interested in participating and/or learning more. Three participants were recruited before arrival in Beirut, while the remaining 10 participants were recruited during the fieldwork either via telephone and/or by visiting their offices. It is perhaps not surprising that the velocity of participation increased significantly during the fieldwork in Beirut, given that the communities and networks of activists and digital rights organisations participating in the research were concentrated in Lebanon. This meant that introductions could be made quickly, with participants introducing new participants and acting as gatekeepers and, to some extent, trust facilitators. The sample size was thus not predetermined, but grew organically as a result of the ethnographically informed approach.

Table 1: Overview of interviewed participants in Beirut, the locations and lengths of the interviews.

ID	Organisation type	Location	Minutes
P0	Human rights foundation	office	74
P1	Human rights foundation	office	74
P2	Social change initiative	coffee shop	39
P3	Political party worker	office	53
P4	Digital rights researcher	online	34
P5	Internet governance	coffee shop	41
P6	Democracy & digital	office	71
P7	Digital rights	coffee shop	46
P8	Democracy & elections	office	93
P9	Independent media	online	31
P10	Diaspora & human rights	coffee shop	69
P11	Digital rights	online	24
P12	Digitalisation	office	47

Notes: We do not refer to participant IDs in the paper to avoid inferring identification. For a similar reason, we only provide high-level descriptions of the organisation types. P0 and P1 were from the same organisation and took part in the same interview.

Interview Process. The interviews were semi-structured and followed an interview guide,which was developed in consultation with Lebanese researchers and recent research outputs by civil society organisations in Lebanon to ensure its relevancy and sensitivity. Existing scholarship was reviewed to understand the gaps within the digital security literature and to inform the theoretical underpinnings. The interviews explored topics related to the wider security contexts in Lebanon including individual perceptions of and experiences with digital security and privacy in the country. The interviews were conducted in English, one of the three main languages spoken in Lebanon, and were audio-recorded with the explicit permission of each participant. Following each interview, the recording was transcribed and anonymised. Once the transcription was complete, the recordings were destroyed prior to leaving the field setting to avoid crossing international borders with potentially sensitive data.

Ethical Considerations. The research received full ethical approval from our institution's Research Ethics Committee and procedures for obtaining informed consent were followed. Additionally, given the political sensitivity of the context within which we carried out the research, one of the key harms that we aimed to mitigate was the potential for participants to become identifiable. Therefore, consent documents emphasised the voluntary nature of the research and the anonymisation procedures we undertook. Data minimisation was prioritised during data collection, transcription, analysis and presentation of the data. This also meant that we did not collect participant identifiers nor do we refer to individuals in the reporting of our findings. This is to further mitigate the potential risk of de-anonymisation at a later date. We also worked with our institutional health and safety office to put in place appropriate risk mitigation protocols. Engaging with the researcher posed minimal risks to participants as Beirut is a diverse city where talking to foreigners is common. The country has witnessed a growing community of Western humanitarian workers within Beirut since the beginning of the Syrian war in 2011 and the displacement of Syrian refugees to Lebanon. Lebanon also has a long history of being a space for collaborative research across the Global North and South.

3.2 Data Analysis

While we particularly draw on interview data in this paper, it was the researcher's presence in the Lebanese context that facilitated analysis and interpretation of the situated security of the populations we studied. Thus, our analysis was rooted in our ethnographically informed research design by drawing on ethnography as a methodology that not only shapes data collection but also data analysis by situating it within the context of the data. Transcriptions of the interviews and field notes were compiled into a single data corpus that was thematically analysed using Braun and Clarke's reflexive thematic approach [15]. The author who conducted the fieldwork carried out the first cycle of inductive coding of the full data corpus. This was done manually and involved annotating the data, grouping and sorting it into higher-level categories. Through this process, rich descriptions highlighting the researcher's interpretation of the data were recorded. In the second cycle of analysis, the higher-level categories as well as associated descriptions and annotations were presented to the wider research team during a series of collaborative data analysis sessions. During these sessions, the categories were reflexively interrogated, challenged, nuanced, refined and merged (and, indeed, unmerged) in line with individual and collective interpretations among research team members. Through this analytical process the categories were brought into conversation with and interpreted through wider literature on Lebanon and digital security, respectively. Through this process the conceptualisations of ontological security, identity work and positive security also emerged as analytical lenses, enabling a deeper understanding of the intertwining of technological and societal security in the Lebanese context.

Researcher Positionalities. Our individual positionalities shaped how we interpreted the data. The researcher who conducted the fieldwork identifies as a white female researcher. Despite not having had any prior links to Lebanon, being from Northern Ireland she identified with some of the frustrations expressed by participants when they reflected on their experiences of living in a post-conflict society with fragmented national identities and divides. The research team also included a design researcher who has intimate experience with the conflict, socio-political and economic conditions in Lebanon from the position of a Lebanese woman. She has participated in and researched Lebanese activist spaces from socio-technical and marginalisation perspectives. Finally, the research team also included one researcher who identifies as a woman and uses ethnography to research digital security practices as they relate to at-risk populations. As such the data was analysed from the individual and collective epistemological positions and identities held by the research team [16].

4 Findings

In this section, we first detail the digital security landscape in which our research was situated. We do so in Section 4.1. In Section 4.2, we foreground the digital landscape that mediated the relationship between the Lebanese people and the government. In Section 4.3, we show how those on the margins of Lebanese society – refugees, LGBTQI+ people and women – experienced forms of othering. Our findings, while not exclusive to the Lebanese context when viewed individually, collectively demonstrate how gendered and identity-specific notions of exclusion, insecurity and risk are reinforced in Lebanon. In Section 4.4 we conclude this section by highlighting how the lack of accountability in Lebanon is shaped by a technology sector that has limited situated understanding of the Lebanese context and a corrupt judicial system.

4.1 Situating Digital Security in Lebanon

The digital landscape in Lebanon is situated in the wider post-conflict context, which is shaped by the financial collapse and legacies of corruption and sectarianism. In 2019, the Lebanese economy crashed due to government mismanagement of public finances, a lack of fiscal accountability and sectarian corruption and clientalism [11]. This led to hyperinflation, with the majority of the Lebanese population being forced to live in poverty [96]. During the fieldwork the researcher observed the militarisation of banks and ATMs in

Beirut, and read reports of protests which turned violent as personal savings were held from depositors.

The cost of data had increased exponentially over the preceding year reducing the affordability of accessing the Internet for many people. While data had become more expensive it had simultaneously decreased in availability. Participants reported that the 2-3G coverage across the country, which enabled those who could afford mobile data bundles to access the Internet, had been reduced. This was estimated to eradicate network access for nearly 300,000 people as it limited remote rural connectivity and services for those with lower incomes, including large refugee communities. The variance in Internet provision was compounded by sectarian governance. For example, ministries (e.g., the Ministry of Public Works and Transport) were rotated among the different sectarian parties, granting the benefits of certain services to communities who supported their political agenda. Participants explained that some neighbourhoods also had better access to electricity than others due to the political party who controlled the area. This fluctuation in service provision further led to communities in different geographic areas becoming marginalised.

Households typically had access to WiFi, with some sharing WiFi-related costs with their neighbours or visiting neighbours or public spaces to connect to the Internet. The research revealed how the pooling of resources was a common practice to maintain Internet access. Other research in Lebanon has shown that during times of financial strain, WiFi connectivity would be forfeited as households prioritised paying essential costs [85]. During the fieldwork it was observed that WiFi was available in some public places such as restaurants and cafés. However, while research on marginalised groups in Western contexts has shown the importance of publicly accessible digital services and the use of public computers in, for example, public libraries or through case managers or language teachers (see e.g. [23,78]), public spaces and services did not exist in Lebanon. The research thus revealed how marginalised populations in Lebanon relied on each other for Internet access, rather than government-provided services. Further, public spaces such as public parks where people would traditionally gather in Beirut had been closed down during the 2019-2020 protests and had remained closed. While COVID-19 was said to be the official reason for the continued closure of public spaces, some participants highlighted how such closures were the government's attempt to suppress public upheaval by preventing people from gathering.

Internet access was also restricted by electricity shortages. Electricity bills had continued to increase with inflation rising and reaching 170% in 2022 [48], leaving people to prioritise their essential needs. The researcher also experienced this while in Lebanon, where she would ensure to charge all devices when and where electricity was available as only two hours of electricity per day were guaranteed by the government. The researcher spent many evenings in Beirut with flickering lights and no Internet access due to electricity blackouts and noted the normalcy of doing grocery shopping in darkness, using a phone flashlight when the electricity cut off.

Mobile phones were the primary device used for Internet access in Lebanon, with several prior works also speaking to the role of such devices in refugee communities, e.g, [43,73]. Yet the complexities of the Lebanese context and the state of digitalisation in the country mean that the level of use and adoption is unclear. Some reports [53] suggest that around 85% of the Lebanese population are Internet users, yet, what such usage entails and how it is secured remains uncertain. The fieldwork revealed the reliance on WhatsApp as a central form of communication in daily interactions. This was also experienced by the researcher. Despite using service-specific applications such as Bolt for transport and Toters for food delivery, the communication often defaulted to WhatsApp despite the inbuilt chat function on those applications.

The economic crisis has also hindered wider technological advancements in Lebanon, with the expense of new technology soaring. This is exemplified by multiple threads on Reddit [82] discussing the increased costs of technology in Lebanon such as laptops, due to the devaluation of the Lebanese Lira. In the fieldwork, this was also highlighted as one of the reasons why people had to rely on mobile phones as these could still be purchased at a price that was seen to be affordable to many. The second reason for the slow technological advancement in Lebanon is the emigration of those who have received technological training within Lebanese universities to the Gulf countries or further afield for better opportunities in the face of the economic decline. Articulating this, one participant explained how this was not a brain drain but instead a "haemorrhage" that impacted both wider technological skills and security knowledge in the country.

4.2 Technological State Control

The digital landscape as it relates to government services is complex and shaped by a government historicised by corruption. One participant explained that the government was purposefully slow to digitalise services because "the more paperwork the better the corruption." However, another participant highlighted that increased digitalisation would not necessarily mean greater transparency within the Lebanese government: "It is challenging because just like a digital system can ensure governance and efficiency and effectiveness it can be used to hide the cheating also." The challenges ingrained in corrupt Lebanese government institutions and services were exemplified by participants with reference to the identity management system in the country. Here, participants noted that while digitalisation efforts had been realised, such as an online appointment booking system for passport renewal and the deployment of biometric passports, the service was overbooked due to legacies of nepotism and lack of staff resources. Further, applying for or renewing a passport still relied on paper-based systems, and a records system that dated back to the initial formation of the Lebanese government. One participant recounted the complexity of registering for government digital systems due to the incoherent approach to registering identity with the State: “Some people have ID and some do not [. . .] some people do not even have a passport. Even your birth certificate is handwritten.” Participants collectively highlighted how the corruption and sectarianism that underpinned the post-conflict political system were ingrained in digital government systems and processes.

4.2.1 Practices of Surveillance

During and since the end of the Civil War (1975-1990), varying levels of control exist in Lebanon [74] with some regions under the informal jurisdiction of different sectarian political parties and experiencing heightened surveillance. Participants explained how they enjoyed certain freedoms in Beirut which were not experienced elsewhere in the country: “We have to be really honest that certain forms of freedom and certain forms of expression are only possible, for example, in the capital that are not really possible in different parts of the country.” It was further noted that individuals from regions with tighter socio-sectarian control knew that they were being monitored online and that those of certain sects were more closely monitored. Participants explained that in reality “people who come from these areas [participant clarified: South of Lebanon, North and Bekaa regions], they are aware that their online presence is being closely policed.” Digitally enabled practices of surveillance thus extended beyond geographic boundaries that would traditionally have been bounded by sectarian strongholds. However, it is important to note that the Lebanese government does not have technological control similar to that reported in Iran [44] and one participant highlighted this aspect: “[they] just do not have the technology for it [. . .] if there were cameras everywhere I would be freaking out right now.” Further, the government has not, as of yet, exerted control of access to messaging applications and/or online platforms (e.g., Facebook or WhatsApp) that have previously been used to organise movements [3, 33]. However, the sense of being monitored was evident throughout the data with one participant noting: “I mean people do not trust, there is an assumption that the State has access to all our WhatsApp messages etc. as there is the feeling that the State has access to everything.” One participant linked the fear of online surveillance to their sense of being insecure, stating that “everyone is watching everyone and it is not a safe environment” when referring to digital platforms.

4.3 Practices of ‘Othering’

Marginalisation based on gender has been shown to be intimately linked to the Lebanese sectarian governance systems where State and religious institutions variably regulate sexuality to produce and maintain sectarian political differences (i.e. sextarianism) [64, 65] and in doing so contribute to acts of othering. This was echoed by participants who emphasised that gender rights were subject to scrutiny by the State and by the multiple religious courts in the country. One participant said sarcastically: “it is not common to have LGBT rights in Lebanon or women’s rights as it is ‘against’ our religions.” They pointed to how post-conflict sectarianism – sextarianism – constrained any potential for meaningful advancement in gender rights and, in turn, contributed to the othering of LGBTQI+ identifying people and women.

Our data shows that practices of othering occurred on a scale from attributing moral blame, to experiencing abuse and hatred, to being scapegoated. Our findings further highlight how such practices manifested on online platforms such as social media. One participant also explained how these forms of othering were linked to the reduction of socio-economic stability: “The more the situation deteriorates, the more the marginalised groups get more marginalised [. . .] they [parliament] are not even taking into consideration LGBT rights.” This correlation between increased othering and economic instability in Lebanon was picked up by one participant who stated that “in times of crisis things become more protracted and more complicated”. They further highlighted that the majority of people “are so busy with surviving and securing their economic survival that, for example, a conversation on democracy, on civil rights and on women’s rights and domestic [migrant] workers it becomes less important.”

One participant suggested that the lack of space for dialogue over civil rights during the economic crisis and due to sectarianism further served the political elite: “In every society at the time of the crisis the masses need a scapegoat [. . .] there are always attempts by authorities alongside their friends in religious communities to actually stir trouble related to religious issues or moral issues.” Participants were concerned about the amplified risks that certain groups were experiencing online due to the atmosphere becoming increasingly violent, citing recent ‘movements’ on online platforms against distinct at-risk groups.

4.3.1 LGBTQI+ as an ‘Other’

Our findings show how the socio-political and economic situation in Lebanon placed those who identify as LGBTQI+ at a higher security risk. In particular, participants cited how identity was influenced by the patriarchal, sectarian and class-based structure that permeated Lebanese society, while articulating how this resulted in heightened security risks for gender diverse groups. Here, we specifically focus on examples of how such groups experienced online exclusion and threats. The othering of LGBTQI+ identifying people was exemplified by one participant: “We saw it a couple of weeks ago with the Ministry of the Interior saying ‘we don’t want any activity which is promoting LGBT society’, so they are trying always to find a scapegoat.” Participants further noted how demonstrations calling for LGBTQI+ rights in Beirut, in front of the Ministry of Interior, were met with threats on different platforms: “Dozens of groups were created online and most of them I would say are [government] intelligence, part of the system, threatening those who are willing to have a sit-in in front of the Ministry of Interior. Threatening them with attacks, beatings and even killing.”

Authority-driven incitements of violence became a recurring theme across interviews with participants in Beirut. For example, one participant explained: “the Ministry of Interior issued a statement accusing the LGBTQ community and not taking a single measure against those who are attacking or threatening [them]” (we explore this further in Section 4.4). The participant spoke for some time on how blaming LGBTQI+ identifying people and the subsequent threats made against them was a means of diverting attention away from the failures of the government: “These huge offline and online campaigns that were recently launched against LGBT+ community and individuals is very much a political decision, in the sense that it is not really about LGBT but in order to divert the public debate from key issues related to economic livelihood, political rights and political development.” Societal divisions normalised othering along sectarian lines and established an online environment in which hatred and oppression of LGBTQI+ identifying people was encouraged.

The incitement of violence against LGBTQI+ groups was present in everyday discourse during the fieldwork as well, underpinning the discourses that manifested online. For example during a poetry night one poet (spoken in English) emotionally spoke of their experiences, recounting how when leaving Beirut to visit their family in the South of Lebanon, by dressing differently and leaving their partner behind. They spoke about how these experiences were heightened “especially now”. While doing a walking tour of the city the researcher documented graffiti relating to LGBTQI+ rights such as one that stated: ‘the closet doesn’t fit us any more.’ Yet, when conversing with others regarding such forms of activism, it was observed that since the 2020 port blast – the explosion of ammonium nitrate in the Port of Beirut that destroyed around half the city – and with the ever deteriorating economic situation, the glimmer of support for LGBTQI+ people was decreasing. This was recognised in line with the upsurge in scapegoating narratives to divert blame from failing fiscal policies of the State. Insights shared through these observations were furthered by interview participants who reasoned that scapegoating occurred “because the LGBT community is threatening the system which is very patriarchal and very linked to religious leaders and institutions in Lebanon.” As emphasised here, participants articulated how LGBTQI+ identifying groups were being viewed as a direct challenge to traditional authority and established moral norms in Lebanon: “Whenever you threaten the religious and sectarian institutions, they [the institutions] say that the human rights rhetoric and LGBT rhetoric are imported by Westerners.” This was a common point of reflection for most interactions in Lebanon when talking about gender identity and marginalisation.

Participants also shared how othering was intimately tied to sectarian geographic strongholds in Lebanon and Beirut more specifically, with some neighbourhoods deemed safer than others for LGBTQI+ people. One participant stated: “You would see them [the political wings of Lebanese Christian groups] having big beards wearing a cross, and whenever they see a LGBT person even walking in the streets, they will attack him in the streets just because he is walking in their area.” These experiences of heightened LGBTQI+ targeted violence in certain neighbourhoods also manifested on social media. Platforms such as Facebook were described as further enforcing the “polarisation” of Lebanese society and was a space said to be rife with hatred targeted towards LGBTQI+ identifying individuals. One participant spoke about the challenges faced when liking social media posts related to LGBTQI+ groups and the backlash which often resulted in threats to personal safety: “They [LGBTQI+ groups] became silent as it has become violent, very very violent on social media, but also on the ground people wanted to protest and other religious groups saying they were preparing the guns.” One participant recounted the experiences of a well-known drag queen: “We have a drag scene in Lebanon and we have a famous drag queen [. . .] she will get lots of comments, hateful speech, she will be constantly reported and her account will be taken down and she experiences censorship by the platform, by people who are working to censor her.” Occurrences of LGBTQI+ related othering were particularly amplified online: “I could be sitting here and my information ecosystem could be telling me ‘oh you know there are more gays in Lebanon and you know they are getting money from NGOs to be gay and they are corrupting us’. So if the algorithm keeps promoting that, what happens?”. The speculative concern of this participant highlighted the potential danger of algorithms in promoting scapegoating and blaming through inciting fear of those who posed a challenge to traditional moral norms during a time of socio-economic decline.

4.3.2 Amplified Scapegoating of Refugees

The link between othering, specifically scapegoating, and amplified risks experienced by those on the margins of Lebanese society was further seen in the case of refugees. Lebanon is home to several refugee groups including Palestinian, Iraqi and Syrian refugees who have also been impacted by sectarianism [59]. For example, the naturalisation of Palestinian refugees that fled the Israeli-Palestinian conflict was and still is a contested topic in Lebanon with Maronite Christians fearing that granting citizenship would skew the demographics and, in turn, the power dynamics towards Muslims [54]. Tensions surrounding naturalisation resulted in Lebanon not signing the 1951 Convention related to refugees [54, 59], leaving the majority of refugees living in poverty due to the systematic social and legal exclusion and discrimination restricting their access to social and occupational institutions [47, 49]. Research has shown how such policies contribute to the othering of refugees within Lebanese society, limiting their access to health services [88] and food aid [86, 89].

While our research did not directly engage with refugees, participants voiced their concerns about the current politico-economic situation and how they witnessed refugees being placed as scapegoats for the many government failures: "I am being pessimistic about it, I feel like there might be some attacks, managed attacks, on the Syrians for example." Participants noted the correlation between the deteriorating political and economic situation and the amplified security risks for refugees: "The son in law of the President [and leader of a political party] [. . .] has been saying the Syrians are the problem, and the reason for the economic crisis because they took your money outside of the country." This form of politically driven scapegoating and assigning of blame to a particular refugee group was amplified through social media platforms where video snippets and quotes from this occurrence were widely shared. Participants emphasised how the digital security risks for these groups were amplified through their presence on online platforms. However, accessing digital content also enabled refugees to maintain social connections. This was underpinned by one participants who spoke about the wide use of mobile phones and social media among refugee groups: "Almost everyone, even someone who lives in a [refugee] camp, will have access to a smartphone and will have Facebook, Twitter etc. downloaded." Existing security-focused research with refugees has further shown how the mobile phone plays an important, yet doubled-edged, role for refugees, being both a security enabler and a security risk [23].

Participants further spoke of how politicians diverted blame for the economic crisis to refugees through powerful and fear-based discourses: "They need an outsider to scare people off and our politicians are very good at scaring people off." This was felt to such an extent that one participant explained how this was an online "campaign" against Syrian refugees, highlighting the organised nature of this rhetoric, especially around food insecurity. Further examples were found on social media where senior Lebanese politicians were observed to fuel the scapegoating of refugees. They did so through narratives of blaming refugees for the financial collapse by suggesting, for example, that their own salaries were less than what a Syrian refugee would receive from aid organisations. Participants also pointed to another online campaign which focused on subsidised wheat from the UN being given to refugee communities rather than Lebanese populations. This campaign was explained to be used to divert attention away from government corruption and the smuggling of wheat by the political elite in Lebanon. As noted by one participant: "What many civil society organisations have found is that actually algorithms tend to amplify content that is inflammatory because that is what gets reactions." Our findings also exemplify how social media posts, as part of politically driven scapegoating campaigns, went viral given the political power driving them. This amplified the digital security needs of marginalised groups.

While there was a general consensus that blame should not be placed on refugee groups, they explained how this form of scapegoating spoke to the pressures felt by many in Lebanon that were amplified by the scarcity of economic resources. One participant highlighted this when they asked: "If I am not able to sustain you [referring to the Lebanese people] how am I meant to sustain some stranger [refugees]?". Class was also seen to override non-citizenship status: "The very rich Syrians who sit with really rich Lebanese will say 'oh you know those poor refugees, they don't see themselves as this [refugees] because they have means, they have access, they have possibilities to leave etc.' [. . .] You have the differences I think more in the middle [class]." This highlights how economic tensions were a dividing factor, above ethnicity, furthering the scapegoating of 'poor' refugee communities. The division of 'rich' and 'poor', 'us' and 'them' re-emphasises how refugees were seen as 'the other'.

4.3.3 Silencing of Women

The 'sextarian' divisions [64, 65] were said to be enabled because Lebanese society is "very patriarchical". This was exemplified by one participant who highlighted that as socio-economic conditions declined, certain groups would face greater online bullying and censorship: "LGBT people are going to face problems and Lebanese women will be scorned a lot." Another participant explained that women were the target of attacks, because "the level of sexism is extremely high along with sexual harassment both online and offline." One participant highlighted how women who were perceived to be of a certain socio-economic class would experience amplified online security risks: "As well as being a patriarchal society it is a very classist society." The participant relayed the case of a Lebanese singer who received a lot of online hatred due to the way she dressed and how she applied her makeup which was seen to signify belonging to a particular class, they concluded: "all of these things play out online." The threats faced by Lebanese women in public life were further articulated by one participant: "There is a journalist, a Shia woman who is very critical [of the government]. Everything she says is relentlessly criticised until it becomes a trend on Twitter saying she is a liar."

Another example was given of a woman doctor who was successfully providing sex education and female medical advice on TikTok. Following a campaign by religious institutions calling on people to report her, she was banned on social media platforms. One participant noted that "she kept getting banned over and over and over again" due to the organised silencing campaign. In some cases, online reporting and censorship of women led to them being taken in for government investigation. For example, a well-known female comedian protested online against COVID-19 restrictions that required providing internal security forces with details about when and why she wanted to leave the house, sharing online that she needed to buy period products. One participant explained how she was "joking to the soldiers about whether they're going to buy her pads or her tampons". This led to her being called for investigations at a military court under the charge of insulting the security forces.

Participants also commented how higher-risk groups in the Lebanese context, particularly women, often engaged in "a lot of self-censorship" as those who spoke out about human rights issues experienced "shadowbanning."[3] This was noted about women who publicly took a stand against the sectarian leaders (participants mentioned stand-up comedians, for example) and would experience that their content "is not being shown as much". One participant explained how they "will call out being shadowbanned. Or they will post a photo of themselves and then put important information in the text as a photo of a happy couple or whatever will trick the algorithm." Thus, participants pointed to distinct and sometimes subtle mitigation strategies to circumvent being shadowbanned.

Despite the digital security threats experienced by those marginalised in Lebanon, participants explained how taking online risks was a necessary form of education. One participant shared the pride they felt when they saw younger people sharing something "super feminist about women being under attack in the region" and feeling "grateful to social media" as many young people in Lebanon were unable to access progressive politics within their families. Online platforms were also seen as a "tool for accountability" for some, with participants citing intersecting issues of class, race and gender being raised online. As one participant noted: "Maybe it will be around a beach resort who ban migrant workers from swimming, and we will come out [online] and say you [the resort] are being racist we are boycotting this place and then they will put a clarifying statement." This highlights the dual role that social media platforms played in the Lebanese context, e.g, as spaces for advocacy and for amplified marginalisation.

4.4 Situating Accountability

Our findings illustrate the digital landscape in Lebanon and how this is enmeshed in societal conditions shaped by the post-conflict Lebanese context. While the participants in our study articulated how the Lebanese authorities exerted technological control and monitoring (particularly in some sectarian strongholds), they also gave several examples of how digital systems were either broken or not designed for the post-conflict challenges and cultural norms of Lebanese society. Further, and most prominently, our findings brought to the fore the interwoven practices of othering experienced by marginalised populations in Lebanon; forms of scapegoating and silencing that, whilst situated in the politico-economic crisis of post-conflict Lebanon, often manifested online. In Section 5 we discuss possible digital security responses, while foregrounding how designing with positive security may give rise to hopeful technologies that aim to foster dialogue and reconciliation. We conclude our findings by exemplifying how the lack of accountability in both the private and public sector allows for extensive forms of othering to continue within the Lebanese context, and how this is underpinned by sectarianism and a lack of situated security understanding.

Participants highlighted how current efforts by the private technology sector to mitigate online forms of violence were tokenistic and a "public relations face". They articulated how such efforts lacked cultural sensitivity, making them ineffective. One participant explained how social media platforms, in this case Facebook, did not have a system which could sensitively address digital risks experienced by Lebanese populations: "They'll hire someone who looks like you, a brown woman with curly hair and she will be Palestinian and my colleagues or whoever will say this [online harm] is outrageous and she will reply in a Palestinian accent and say we are looking into it [...] then she goes back inside the company and she isn't able to do anything." The lack of situated cultural understanding was also noted in how the positioning of employees to represent a region within global technology offices would not provide sufficient security to local communities. This was particularly the case in Lebanon where participants explained that Lebanese dialects were different to dialects in the region and the Standard Arabic Dialect. When compounded by ongoing sectarian divisions, distinguishing between what was inflammatory and/or harmful content without local cultural knowledge was explained to be impossible. With respect to shadowbanning (Section 4.3.3), participants also highlighted that "there is no transparency, which is the main problem when it comes to corporate accountability because when we go to them and say 'you are shadowbanning stand-up comedians in Lebanon' [...] they will ask, how, why, how do you know?".

Further highlighting the significance of situating technology design in the contexts they are being implemented and used, participants gave examples of how simply adopting standard Western-based digitalisation processes often led to tensions between cultural aspects and customs, and the implementation of digital systems. For example, digital systems developed to cater to Western norms were explained to be incompatible with the multiple paper-based identity systems in Lebanon. One participant highlighted with reference to Arabic names: "Your name, how it is written, how it could be written in so many variations [when translated from Arabic to other languages]; so in one [government] system it could be different to another [...] because of the lack of [consistent] identity [documents] you might find different variations of my name." Such inconsistencies required identity verification

[3] *Shadowbanning* refers to being blocked from social media without knowing that one has been blocked or that one's comments are not visible.

processes with which Western-based systems struggled, as the verification often needed to extend beyond the individual to include data such as parents' names and place of birth or even uncles', grandfathers' and great grandfathers' identity details. These insights speak to the findings of [78], where the authors highlight how authentication mechanisms, such as password recovery, are rooted in Western cultural norms.

Participants highlighted that within failing governance structures and tokenistic private sector systems, there was no expectation that those who engaged in online abuse would be held to account by the Lebanese authorities: "The authorities never protect victims [of] violence, they are always here to protect the perpetrators of violations and to perpetuate a culture of no accountability whatever happens." This lack of accountability extended to digital security where the jurisdiction and processes of government agencies such as the Cyber Crime Bureau (CCB) were explained to be opaque at best, with one participant noting how the CCB could "summon you for what you have posted online". One participant further explained the role of the CCB: "This is an attempt at or an attempt to curtail freedom of speech but if you have enough clout and you have the money to hire a lawyer or belong to a certain segment of society it doesn't affect you in the end." More broadly, our findings suggest that the corrupt Lebanese judicial and political system also meant that there was a lack of digital security and privacy policies in place to protect human and digital rights. Thus, the the lack of prioritisation and accountability of/for digital security was directly tied to the general lack of accountability in the country. This is supported by Salloukh [75], who shows how governance in Lebanon can be characterised as a fragmented system of clientalism and corruption with no accountability.

5 Discussion

Here, we outline our study's key takeaways. In Section 5.1 we focus on digital security of and for marginalised groups in the Lebanese post-conflict context, showing parallels with broader digital security research focusing on higher-risk populations. In Section 5.2 we draw on notions of positive security to support our argument for the need to design security technologies that enhance dialogue across fragmented and post-conflict societies. We conclude our discussion in Section 5.3, where we set out implications for digital security research.

5.1 Importance of Digital Security in Lebanon

Marginalised groups being othered during times of political and economic instability is not a new phenomenon as we highlight in Section 2.2. Yet, our findings show that marginalised groups in Lebanon are positioned as the drivers of societal-level failings as they are seen to challenge the traditional morals that protect the ontological security of the regime. This transfers blame from the political leadership to groups who are already marginalised, heightening their at-risk position in society. By framing such groups as an 'other', the Lebanese political leadership also constructs and reinforces its own identity as the (legitimate) ruler of Lebanon. Our findings show how such practices manifest in online contexts in Lebanon, leading to heightened and amplified digital security risks for already at-risk populations. While this is not in itself a matter that can – or indeed should – be solved through technological interventions, we argue for a digital security that is situated in the context of people and their daily lives. As our findings have shown, practices of othering as experienced by refugees, LGBTQI+ identifying people and women in Lebanon (Section 4.3) speak to the ontological insecurity of these groups as well as the need to protect technology, its availability and security.

Our findings show the need for digital security literature to consider intersecting forms of marginalisation and political, economic, social and cultural structures that create the conditions for high levels of insecurity. Not doing so ignores the drivers of key vulnerabilities and threats and, thus, contributes to the further marginalisation of populations who are especially impacted; those othered in the Lebanese context. We thus echo similar calls made by security researchers working with marginalised groups, e.g. [38, 78, 80], who have shown how the conditions of marginalisation directly impact the digital security threats experienced by these populations and that such digital security threats are neglected in the literature [80].

Our study raises the question of what kind of digital security agenda is required to better cater to the needs of marginalised populations whose threat horizon is amplified through digital technology. In the Lebanese context, State technological control and online surveillance of particular groups that are seen to challenge societal norms amplifies the digital security risks of those populations (Section 4.2). Our work shows that marginalised populations in post-conflict Lebanon are not free from persecution by the State nor can they use technology freely. While presenting different challenges to digital security, broader literature on the computer security needs of higher-risk populations also points to more situated security technologies. This includes security-focused work with refugees and migrants [22, 23, 78, 87], LGBTQI+ identifying people [38, 45, 56] and migrant domestic workers [80], as we highlight in Section 2.3. What these studies show is how such populations mitigate their digital security risks by relying on trusted relations and routine activities to establish ontological security. In our study, this was for example evident in how those without Internet access or electricity would visit neighbours to use their WiFi and charge their mobile phones; or how refugees would remain active mobile phone and social media users to re-establish routine practices and connections that kept them connected to their homeland (Section 4.1).

Participants in our study noted how during the recent economic crisis, digital security risks were increasingly intertwined with offline risks. For example, the online scapegoating of LGBTQI+ people and the silencing of women were often accompanied by physical and State violence. Those responsible were said to not be held accountable by the Lebanese authorities or through accountability infrastructures such as the courts (Section 4.4). The intersections of online and offline security risks are foregrounded throughout our findings. This intertwining brings technical, social, political and cultural notions of security into conversation. We now turn to how digital security scholars might respond.

5.2 Positive Security for Post-Conflict Settings

In this section we discuss how designing within a positive security framework, which we outline in Section 2.1, presents an opportunity for security researchers to work with post-conflict communities to co-create hopeful security technology. Drawing on an understanding of positive security as "the freedom to live free from fear" [62], we call for a digital security that not only starts from the goal of countering existing threats, but which focuses on enhancing dialogue across fragmented societies. This speaks to the role that technology has been shown to have in post-conflict transitions (e.g. [57, 58]). In the context of Lebanon, designing for positive security draws on research that emphasises the need to design across the multi-life span of populations that have experienced conflict. This work highlights the importance of accounting for historically rooted, conflict-related fragmentation in a manner that enables transitioning towards peace [98]. This approach brings into conversation the fragmented identities inherited from the Lebanese Civil War to work towards a reconciliation of society [98]; disrupting the 'us' and 'them' rhetoric that we show underlies the mechanisms of othering in Lebanon. Here, digital security researchers can look to technologies designed for post-conflict reconciliation such as digital memorials [31], and research that calls for a re-orientation towards designing for the desire of those marginalised to achieve meaningful inclusion [91, 92, 97] and a participatory approach that actively designs across societal and sectarian divides [84]. This is important as our findings show how the lack of space for dialogue further served the political elite (Section 4.3).

Digital memorials. Digital memorials range from digital headstones to collective online spaces to share stories in commemoration. The authors of [37] note how curators of digital memorials in post-conflict settings act as stewards of stories of conflict, designing memorials underpinned by principles of accuracy, credibility, transparency, safety and security. We ask digital security researchers to collaborate with human rights groups and act as stewards of narratives of othering such as those presented in our work. Transparently curating narratives of othering that unfold online would enable credible accounts of violence to be presented back to current and future generations of Lebanese, in support of reconciling historically rooted violence. Digital security researchers are well placed to undertake this work given their expertise in formulating and navigating digital security safeguards [55], such as the shadowbanning mechanisms reported by participants in our work (Section 4.3.3). This work would make visible the narratives that would otherwise be hidden within Lebanon's post-conflict history. Van Ommering and el Soussi [94] show in their work on the digital memorial for the estimated 17,000 people who went missing during the Lebanese Civil War how such memorials "open up spaces that remain closed in the offline world, enabling survivors to share their stories, build collectives, demand recognition, and advocate for justice." Yet, key challenges for security remain. Digital memorials hold sensitive data about individuals, their stories, families and identities, while not designed with security in mind. Thus, the development and maintenance of secure digital platforms for such memorials while safeguarding accessibility and ownership are important matters for security in this context.

5.3 Implications and Future Research

Here, we concretise the implications of our findings for digital security researchers and practitioners, beyond positive security.

Situating digital security in post-conflict settings. Post-conflict contexts bring to the fore distinct digital security challenges, particularly for already at-risk groups as our findings on LGBTQI+ identifying people, refugees and women show. A wide range of existing security-driven work with higher-risk populations such as, for example, journalists [61], activists and protesters [3, 27] (see also Section 2.3) has aimed at protecting such populations against (State) surveillance and censorship while mitigating security risks. Speaking to this body of work, we argue that post-conflict societies should also be given particular attention within the security community. We do so because of the many, intertwining and continuous threats to security, safety, privacy and identity as well as economic and political risks that shape people's lives in the 'transition continuum' [21], sometimes for decades and across generations. At a technological level, we suggest working towards specific security choices and controls for people in post-conflict societies, building on existing protection mechanisms against politically motivated attacks and surveillance. Situating digital security in post-conflict settings moves beyond advocating for specific technological interventions, however. Here, computer and social scientists need to work together to uncover and understand the social foundations of the security technologies that are relied upon for protection.

Security misconceptions. Our findings indicate some security misconceptions among participants. Participants suggested that the Lebanese State had access to, e.g., WhatsApp messages, indicating a misconception about the promises of end-to-end encryption. The lack of visible surveillance technology present in Lebanon in comparison to neighbouring states also led some participants to question the ability of the Lebanese authorities to monitor interactions. Yet, our findings reveal less overt – and less reliant on technology – mechanisms of surveillance that took place between individuals and communities as an extension of the State (Section 4.2.1). Coupled with limited digital security expertise in Lebanon due to the emigration of those with technology and/or security education (Section 4.1), there is an immediate need for digital security information and education in the country. Our work further suggests how culturally-rooted misconceptions held within social media companies has meant that what might be considered harmful content in the Lebanese context is missed (Section 4.4). Others have also shown how common security practices such as password creation and related security questions rely on specific cultural (Western) knowledge [78]. To bridge not only technical and social knowledge, we advocate for collaborative security-driven research across the Global North and South, where researchers work together to formulate research problems and responses. As we note in Section 3.1, Lebanon has a long history of being a space for collaborative research across the Global North and South.

Shadowbanning. Participants commented how those who spoke out against the sectarian leadership experienced shadowbanning (Section 4.3.3), resulting in a lack of counter narratives to the upsurge in scapegoating and government-affiliated online groups (Section 4.3.1). Our research shows how the concealing of specific content amplified the silencing and scapegoating of marginalised groups in Lebanon. Hence, in the Lebanese context, the practice of shadowbanning across platforms is not a safeguard – quite the contrary. Our work thus contributes to an emerging body of scholarship pointing to the harmful effects of shadowbanning on marginalised groups [46, 63, 69]. Bloch [12] further highlights how States (through law enforcement) are increasingly influencing the governance of social media content. We caution against developing bespoke moderation policies and tools for the Lebanese context without further situated security research. Yet, we urge social media companies to work with security researchers, across the Global North and South, *and* populations in post-conflict contexts, to situate their technology development and content moderation approaches. Echoing Nicolas [69] we also call on social media companies (Facebook being the most prominent in our findings) to publicly and transparently report their moderation practices, enabling researchers to examine the impact of shadowbanning on at-risk populations.

Mesh messaging. Our findings demonstrate the unreliability of Internet access for those living in post-conflict Lebanon. This was underpinned by the rising costs of data, a reduction in 2-3G provision leaving rural and poorer communities without Internet access (Section 4.1) and growing State surveillance (Section 4.2.1); coupled with the pooling of resources (e.g., the sharing of WiFi) within communities and high levels of mobile phone use among marginalised populations (Section 4.1). These conditions represent key barriers for secure Internet-enabled communications and thus make the Lebanese post-conflict context a prime use-case for mesh network applications that provide communication capabilities over Bluetooth. Indeed, the market leader in this space, Bridgefy [20], is often promoted for use in situations of social unrest and Internet blackouts (e.g, [18]). However, recent work has shown devastating security vulnerabilities in the application [4, 5]. While the level of actual adoption of this technology is also limited [3], the spikes in downloads from within areas that witness conflict[4] suggest a need for offline messaging that is not provided by existing messaging applications. While other solutions exist (see [4]) none cater to at-risk people in post-conflict settings who require secure, offline, easily accessible and usable (mass adoption being a key criteria for a mesh network) and reliable solutions. This remains a pressing security question. Future mesh development work might involve grassroot groups to enable, as the authors of [7] note, "security engineers [. . .] to step into the language of collective action within a political project" to develop security tools that meet the needs of the populations they aim to serve.

Ethnography. We echo the authors of [80], who call for security researchers to expand the methods used to explore the security practices of populations at the margins. In [3] the authors call for security research grounded in ethnographic methods to uncover what higher-risk populations take for granted. While we adopted an ethnographically informed approach, our work did not allow for more extensive immersion in these communities due to the two-week fieldwork. Future work should thus consider longer-term ethnographic work in post-conflict settings to deepen the digital security insights that we have begun to uncover here. Our fieldwork was further informed by the involvement of digital and human rights organisations in Lebanon. This was important for our understanding of the political and legal landscape in the country. We suggest that digital security researchers seek out collaborations with interest groups, both as informants and interlocutors (or gatekeepers) to access often hard-to-reach settings and participants. Other security researchers have sought such collaborations. In [80] the authors partnered with Voice of Domestic Workers for their work with migrant domestic workers. In the context of security research with refugees, in [78] the authors engaged case managers, while in [22, 23] the authors worked with language teachers. In all cases, such interlocutors enabled the research to sensitively uncover distinct security needs and practices of such populations.

[4] Most recently from within Ukraine [19].

6 Conclusion

Through an ethnographically informed approach our research highlights the interwoven historical, social and political factors in the post-conflict context of Lebanon and how this in turn amplifies digital security risks for marginalised populations during times of political instability. This is caused by the strongly rooted sectarian divisions. We show how populations on the margins – particularly LGBTQI+ identifying people, refugees and women – are targeted through practices of othering on a scale ranging from online silencing, to online targeted abuse and hatred, to outright scapegoating. We discuss how the threats facing already at-risk populations are heightened during times of crisis and amplified through digital technology. In doing so, we concluded our discussion by arguing for design interventions rooted in a positive security framework, where technologies are designed to enhance dialogue and reconciliation within post-conflict contexts.

Limitations First, the fieldwork took place over two weeks in Beirut and thus has the potential to be expanded both in time, scope and geography. Second, interviews were carried out with people who had a leading voice in political debates in Lebanon. The work can be expanded to work with different societal groups who are not ‘experts’ in the fields of digital and human rights. Third, not all participants had direct experience of being othered, yet all participants could discuss the practices of othering as being situated in the post-conflict context of Lebanon. Future work on othering should consider engaging those at the margins of Lebanese society. Fourth, the level of participation has limitations such as language barriers. While one of the authors speaks Arabic, the fieldworker does not, however English along with French is widely spoken in Lebanon. Finally, there is an inherent bias in research using interviews and focusing on security and/or politically charged topics, given that participants self-select. It could be that some participants decided against participation as a result. We tried to overcome this limitation by immersing ourselves in the setting through an ethnographically informed approach.

Acknowledgment

This work would not exist without the many contributions from people, both in and outside Lebanon, who so generously gave of their time to speak to us and who have remained engaged with the research throughout. We thank the anonymous reviewers for their constructive feedback. The research of McClearn was supported by the EPSRC as part of the Centre for Doctoral Training in Cyber Security for the Everyday at Royal Holloway, University of London (EP/S021817/1).

References

[1] Dana Abi Ghanem. Energy, the city and everyday life: Living with power outages in post-war lebanon. *Energy Research & Social Science*, 36:36–43, 2018.

[2] Ali Ahmad, Neil McCulloch, Muzna Al-Masri, and Marc Ayoub. From dysfunctional to functional corruption: The politics of decentralized electricity provision in lebanon. *Energy Research & Social Science*, 86, 2022.

[3] Martin R Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. Collective information security in large-scale urban protests: the case of Hong Kong. In *30th USENIX Security Symposium*, pages 3363–3380, 2021.

[4] Martin R Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. Mesh messaging in large-scale protests: Breaking bridgefy. In *Topics in Cryptology–CT-RSA 2021: Cryptographers’ Track at the RSA Conference 2021, Virtual Event, May 17–20, 2021, Proceedings*, pages 375–398. Springer, 2021.

[5] Martin R Albrecht, Raphael Eikenberg, and Kenneth G Paterson. Breaking bridgefy, again: Adopting libsignal is not enough. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 269–286, 2022.

[6] Gordon Willard Allport, Kenneth Clark, and Thomas Pettigrew. The Nature of Prejudice. 1954.

[7] Miriyam Aouragh, Seda Gürses, Jara Rocha, and Femke Snelting. Fcj-196 let’s first get things done! on division of labour and techno-political practices of delegation in times of crisis. *The Fibreculture Journal*, (26 2015: Entanglements–Activism and Technology), 2015.

[8] Timour Azhari, Issam Abdallah, and Laila Bassam. Depositors hold up two lebanese banks to grab their own money. https://www.reuters.com/world/middle-east/woman-holds-up-lebanese-bank-13000-her-own-money-advocacy-group-says-2022-09-14/, September 2022.

[9] World Bank. Lebanon economic monitor, fall 2020 : The deliberate depression. https://openknowledge.worldbank.org/handle/10986/34842, 2020.

[10] World Bank. Lebanon sinking into one of the most severe global crises episodes, amidst deliberate inaction. https://www.worldbank.org/en/news/press-release/2021/05/01/lebanon-sinking-into-one-of-the-most-severe-global-crises-episodes/, 2021.

[11] World Bank. Lebanon public finance review: Ponzi finance? https://openknowledge.worldbank.org/handle/10986/37824/, 2022.

[12] Hannah Bloch-Wehba. Content moderation as surveillance. *Berkeley Tech. LJ*, 36:1297, 2021.

[13] Elie Bouri and Joseph El Assad. The lebanese electricity woes: An estimation of the economical costs of power interruptions. *Energies*, 9(8):583, 2016.

[14] Maia J Boyd, Jamar L Sullivan Jr, Marshini Chetty, and Blase Ur. Understanding the security and privacy advice given to black lives matter protesters. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2021.

[15] Virginia Braun and Victoria Clarke. Reflecting on reflexive thematic analysis. *Qualitative research in sport, exercise and health*, 11(4):589–597, 2019.

[16] Virginia Braun, Victoria Clarke, and Nikki Hayfield. 'a starting point for your journey, not a map': Nikki hayfield in conversation with virginia braun and victoria clarke about thematic analysis. *Qualitative Research in Psychology*, 19(2):424–445, 2022.

[17] JD Brewer. Ethnography. Philadephia, 2000.

[18] Bridgefy. Myanmar flocks to bridgefy to challenge military coup. https://bridgefy.me/blog/myanmar-flocks-to-bridgefy-to-challenge-military-coup/, 2021.

[19] Bridgefy. Ukrainians download bridgefy as russian invasion starts. https://bridgefy.me/blog/ukrainians-download-bridgefy-as-russian-invasion-starts/, 2022.

[20] Bridgefy. Bridgefy messaging app. https://bridgefy.me/, 2023.

[21] Graham Brown, Arnim Langer, and Frances Stewart. A typology of post-conflict environments. *CRPD Working Paper*, 1:1–22, 2011.

[22] Lizzie Coles-Kemp and Rikke Bjerg Jensen. Accessing a new land: Designing for a social conceptualisation of access. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[23] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Reem Talhouk. In a new land: mobile phones, amplified pressures and reduced capabilities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2018.

[24] Stuart Croft. Constructing ontological insecurity: the insecuritization of britain's muslims. *Contemporary security policy*, 33(2):219–235, 2012.

[25] Stuart Croft and Nick Vaughan-Williams. Fit for purpose? fitting ontological security studies 'into'the discipline of international relations: Towards a vernacular turn. *Cooperation and conflict*, 52(1):12–30, 2017.

[26] Ann L Cunliffe. Managers as practical authors: Reconstructing our understanding of management practice. *Journal of Management Studies*, 38(3):351–371, 2001.

[27] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G. Bardas. Defensive technology use by political activists during the Sudanese revolution. In *2021 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, 2021.

[28] Bryan Dosono and Bryan Semaan. Identity work as deliberation: Aapi political discourse in the 2016 us presidential election. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2018.

[29] Bryan Dosono and Bryan Semaan. Moderation practices as emotional labor in sustaining online communities: The case of aapi identity work on reddit. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, pages 1–13, 2019.

[30] Tom Douglas. *Scapegoats: transferring blame*. Routledge, 2002.

[31] Abigail C Durrant, David S Kirk, and Stuart Reeves. Human values in curating a human rights media archive. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*, pages 2685–2694, 2014.

[32] Ksenia Ermoshina, Harry Halpin, and Francesca Musiani. Can Johnny build a protocol? co-ordinating developer and user intentions for privacy-enhanced secure messaging protocols. In *European Workshop on Usable Security*, 2017.

[33] Ksenia Ermoshina and Francesca Musiani. *Concealing for Freedom*. Mattering Press, 2022.

[34] Dennis M Foster and Jonathan W Keller. Rallies and the "first image" leadership psychology, scapegoating proclivity, and the diversionary use of force. *Conflict Management and Peace Science*, 27(5):417–441, 2010.

[35] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. " is my phone hacked?" analyzing clinical computer security interventions with survivors of intimate partner violence. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–24, 2019.

[36] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell.

Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on human-computer interaction*, 1(CSCW):1–22, 2017.

[37] Batya Friedman, Lisa P Nathan, and Daisy Yoo. Multi-lifespan information system design in support of transitional justice: Evolving situated design principles for the long (er) term. *Interacting with Computers*, 29(1):80–96, 2017.

[38] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. "like lesbians walking the perimeter": Experiences of us lgbtq+ folks with online security, safety, and privacy advice. In *31st USENIX Security Symposium*, 2022.

[39] Clifford Geertz. Thick description: Toward an interpretive theory of culture. In *The cultural geography reader*, pages 41–51. Routledge, 2008.

[40] Stephen E Gent. Scapegoating strategically: Reselection, strategic interaction, and the diversionary theory of war. *International Interactions*, 35(1):1–29, 2009.

[41] Anthony Giddens. *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Polity, Cambridge, 1991.

[42] Gunhild Hoogensen Gjørv. Security by any other name: negative security, positive security, and a multi-actor security approach. *Review of international Studies*, 38(4):835–859, 2012.

[43] Markus Balázs Göransson, Lotta Hultin, and Magnus Mähring. 'the phone means everything.'mobile phones, livelihoods and social capital among syrian refugees in informal tented settlements in lebanon. *Migration and Development*, 9(3):331–351, 2020.

[44] Margarita Grinko, Sarvin Qalandar, Dave Randall, and Volker Wulf. Nationalizing the internet to break a protest movement: Internet shutdown and counter-appropriation in iran of late 2019. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–21, 2022.

[45] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2018.

[46] Oliver L Haimson, Daniel Delmonaco, Peipei Nie, and Andrea Wegner. Disproportionate removals and differing content moderation experiences for conservative, transgender, and black social media users: Marginalization and moderation gray areas. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–35, 2021.

[47] Sari Hanafi, Jad Chaaban, and Karin Seyfert. Social exclusion of palestinian refugees in lebanon: reflections on the mechanisms that cement their persistent poverty. *Refugee Survey Quarterly*, 31(1):34–53, 2012.

[48] Raya Jalabi. Lebanon devalues official exchange rate by 90%. https://www.ft.com/content/f37617e1-098b-459f-9502-50ffb50c6c0c, February 2023.

[49] Maja Janmyr. Precarity in exile: The legal status of syrian refugees in lebanon. *Refugee Survey Quarterly*, 35(4):58–78, 2016.

[50] Rikke Bjerg Jensen, Lizzie Coles-Kemp, and Reem Talhouk. When the civic turn turns digital: Designing safe and secure refugee resettlement. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

[51] Rikke Bjerg Jensen, Lizzie Coles-Kemp, Nicola Wendt, and Makayla Lewis. Digital liminalities: Understanding isolated communities on the edge. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

[52] Hélène Joffe and Hélène Joffé. *Risk and'the Other'*. Cambridge University Press, 1999.

[53] Simon Kemp. Digital 2023: Lebanon. https://datareportal.com/reports/digital-2023-lebanon/, 2023.

[54] Are Knudsen. Widening the protection gap: the 'politics of citizenship'for palestinian refugees in lebanon, 1948–2008. *Journal of Refugee Studies*, 22(1):51–73, 2009.

[55] Paddy Leerssen. An end to shadow banning? transparency rights in the digital services act between content moderation and curation. *Computer Law & Security Review*, 48:105790, 2023.

[56] Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. Privacy and activism in the transgender community. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[57] Ylber Limani, Larry Stapleton, and Peter P Groumpos. The challenges of digital transformation in post-conflict transition regions: digital technology adoption in kosovo. *IFAC-PapersOnLine*, 51(30):186–191, 2018.

[58] Charles P Martin-Shields and Nicholas Bodanac. Peacekeeping's digital economy: the role of communication technologies in post-conflict economic growth. *International Peacekeeping*, 25(3):420–445, 2018.

[59] Nur Masalha. Secretarianism and the rejection of tawteen: Lebanon and the palestinian refugees. *YB Islamic & Middle EL*, 9:110, 2002.

[60] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI conference on human factors in computing systems*, pages 2189–2201, 2017.

[61] Susan E McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the computer security practices and needs of journalists. In *24th USENIX Security Symposium*, pages 399–414, 2015.

[62] Bill McSweeney. *Security, identity and interests: a sociology of international relations*. Number 69. Cambridge University Press, 1999.

[63] Callie Middlebrook. The grey area: Instagram, shadowbanning, and the erasure of marginalized communities. *Shadowbanning, and the Erasure of Marginalized Communities (February 17, 2020)*, 2020.

[64] Maya Mikdashi. Sextarianism: Notes on studying the lebanese state. *The Oxford handbook of contemporary Middle Eastern and North African history. Oxford University Press, Oxford UK. https://doi.org/10.1093/oxfordhb/9780199672530.013*, 24, 2018.

[65] Maya Mikdashi. *Sextarianism: Sovereignty, Secularism, and the State in Lebanon*. Stanford University Press, 2022.

[66] Jennifer Mitzen. Ontological security in world politics: State identity and the security dilemma. *European journal of international relations*, 12(3):341–370, 2006.

[67] Gabe Mythen. *Ulrich Beck: a critical introduction to the risk society*. Pluto Press, 2004.

[68] Mark Neocleous. *Critique of security*. Edinburgh University Press, 2008.

[69] Gabriel Nicholas. Shedding light on shadowbanning. https://cdt.org/insights/shedding-light-on-shadowbanning/, 2022.

[70] OHCHR. Lebanon: Un expert warns of 'failing state' amid widespread poverty. https://www.ohchr.org/en/press-releases/2022/05/lebanon-un-expert-warns-failing-state-amid-widespread-poverty, 2022.

[71] Paul Roe. The 'value'of positive security. *Review of international studies*, 34(4):777–794, 2008.

[72] Dina Sabie and Syed Ishtiaque Ahmed. Moving into a technology land: exploring the challenges for the refugees in canada in accessing its computerized infrastructures. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies*, pages 218–233, 2019.

[73] Randa Salamoun, Charlotte M Karam, and Crystel Abdallah. A feminist-affordance lens: examining the power outcomes of the actualization of smartphone affordances. *Information Technology & People*, (ahead-of-print), 2022.

[74] Kamal Salibi. *A house of many mansions: The history of Lebanon reconsidered*. Univ of California Press, 1990.

[75] Bassel F Salloukh. Taif and the lebanese state: the political economy of a very sectarian public sector. *Nationalism and Ethnic Politics*, 25(1):43–60, 2019.

[76] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth F Churchill. " privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia. In *SOUPS*, pages 127–142, 2018.

[77] Emrys Schoemaker, Dina Baslan, Bryan Pon, and Nicola Dell. Identity at the margins: Data justice and refugee experiences with digital identity systems in lebanon, jordan, and uganda. *Information Technology for Development*, 27(1):13–36, 2021.

[78] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer security and privacy for refugees in the united states. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 409–423. IEEE, 2018.

[79] Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo. Tough times at transitional homeless shelters: Considering the impact of financial insecurity on digital security and privacy. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[80] Julia Słupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. "they look at vulnerability and use that to abuse you": Participatory threat modelling with migrant domestic workers. In *31st USENIX Security Symposium*. USENIX Association, 2022.

[81] Brent J Steele. Ontological security and the power of self-identity: British neutrality and the american civil war. *Review of international studies*, 31(3):519–540, 2005.

[82] SurgeryFx. Laptop prices are more expensive (on the dollar). https://www.reddit.com/r/lebanon/comments/j03njk/laptop_prices_are_more_expensive_on_the_dollar/, 2020.

[83] Franziska Tachtler, Reem Talhouk, Toni Michel, Petr Slovak, and Geraldine Fitzpatrick. Unaccompanied migrant youth and mental health technologies: A social-ecological approach to understanding and designing. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–19, 2021.

[84] Reem Talhouk and Sarah Armouch. Dialogues on decolonial participatory design praxis during a revolution. In *Proceedings of the Participatory Design Conference 2022-Volume 2*, pages 52–57, 2022.

[85] Reem Talhouk, Lizzie Coles-Kemp, Rikke Bjerg Jensen, Madeline Balaam, Andrew Garbett, Hala Ghattas, Vera Araujo-Soares, Balsam Ahmad, and Kyle Montague. Food aid technology: The experience of a syrian refugee community in coping with food insecurity. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):1–25, 2020.

[86] Reem Talhouk, Lizzie Coles-Kemp, Rikke Bjerg Jensen, Madeline Balaam, Andrew Garbett, Hala Ghattas, Vera Araujo-Soares, Balsam Ahmad, and Kyle Montague. Food aid technology: the experience of a syrian refugee community in coping with food insecurity. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):1–25, 2020.

[87] Reem Talhouk, Lizzie Coles-Kemp, Rikke Bjerg Jensen, Madeline Balaam, Andrew Garbett, Hala Ghattas, Vera Araujo-Soares, Balsam Ahmad, and Kyle Montague. Food aid technology: The experience of a syrian refugee community in coping with food insecurity. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):1–25, 2020.

[88] Reem Talhouk, Sandra Mesmar, Anja Thieme, Madeline Balaam, Patrick Olivier, Chaza Akik, and Hala Ghattas. Syrian refugees and digital health in lebanon: Opportunities for improving antenatal health. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 331–342, 2016.

[89] Reem Talhouk, Kyle Montague, Hala Ghattas, Vera Araujo-Soares, Balsam Ahmad, and Madeline Balaam. Refugee food insecurity & technology: Surfacing experiences of adaptation, navigation, negotiation and sharing. *Computer Supported Cooperative Work (CSCW)*, 31(2):341–372, 2022.

[90] Scott M Thomas. Rethinking religious violence: Towards a mimetic approach to violence in international relations. *Journal of international political theory*, 11(1):61–79, 2015.

[91] Kentaro Toyama. Design, needs, and aspirations in international development. In *International Conference on Social Implications of Computers in Developing Countries*, pages 24–32. Springer, 2017.

[92] Kentaro Toyama. Designing for aspirations. *Interactions*, 27(3):61–63, 2020.

[93] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. A digital safety dilemma: Analysis of computer-mediated computer security interventions for intimate partner violence during covid-19. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2021.

[94] Erik Van Ommering and Reem el Soussi. Space of hope for lebanon's missing: Promoting transitional justice through a digital memorial. *Conflict and Society*, 3(1):168–188, 2017.

[95] Éric Verdeil. Infrastructure crises in beirut and the struggle to (not) reform the lebanese state. *The Arab Studies Journal*, 26(1):84–113, 2018.

[96] Human Rights Watch. Lebanon: Events of 2020. https://www.hrw.org/world-report/2021/country-chapters/lebanon, 2020.

[97] Marisol Wong-Villacres, Aakash Gautam, Deborah Tatar, and Betsy DiSalvo. Reflections on assets-based design: A journey towards a collective of assets-based thinkers. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–32, 2021.

[98] Daisy Yoo, Katie Derthick, Shaghayegh Ghassemian, Jean Hakizimana, Brian Gill, and Batya Friedman. Multi-lifespan design thinking: two methods and a case study with the rwandan diaspora. In *Proceedings of the 2016 CHI conference on human factors in computing systems*, pages 4423–4434, 2016.