Defensive Technology Use by Political Activists During the Sudanese Revolution

Alaa Daffalla*§‡, Lucy Simko†§, Tadayoshi Kohno† and Alexandru G. Bardas*
* Department of Electrical Engineering & Computer Science and ITTC, University of Kansas
† Paul G. Allen School of Computer Science & Engineering, University of Washington

***Abstract*—Political activism is a worldwide force in geopolitical change and has, historically, helped lead to greater justice, equality, and stopping human rights abuses. A modern revolution—an extreme form of political activism—pits activists, who rely on technology for critical operational tasks, against a resource-rich government that controls the very telecommunications network they must use to operationalize, putting the technology they use under extreme stress. Our work presents insights about activists' technological defense strategies from interviews with 13 political activists who were active during the 2018-2019 Sudanese revolution. We find that politics and society are driving factors of security and privacy behavior and app adoption. Moreover, a social media blockade can trigger a series of anti-censorship approaches at scale, while a complete internet blackout can cripple activists' use of technology. Even though the activists' technological defenses against the threats of surveillance, arrest and physical device seizure were low tech, they were largely sufficient against their adversary. Through these results, we surface key design *principles*, but we observe that the generalization of design recommendations often runs into fundamental tensions between the security and usability needs of different user groups. Thus, we provide a set of structured questions in an attempt to turn these tensions into opportunities for technology designers and policy makers.**

I. Introduction

Though political activism has been a driving factor in geopolitical changes for centuries, the ubiquity of smartphones and social media has changed both the tools that activists use, and the extent of the legal and infrastructural power that nation-states have over activists [1]. Activists fighting oppressive regimes increasingly incorporate technology in their daily activities, using it to share knowledge and organize. At the same time, their adversary may aim to infiltrate their groups, arrest them, or otherwise forcibly deter them. Political revolution, a dramatic culmination of activism efforts, puts technology used by activists under extreme stress because it may not be designed for those directly colliding with a nation state adversary. Therefore, it is important to consider that while technology could support them, it could also make their tasks challenging or expose them to risk.

While significant progress has been made toward computer security and privacy for the general population, more work is necessary to address the needs of specific user groups. Indeed, there have been numerous efforts focused on specific populations (see Section III for an overview). However, political activists under an oppressive regime have not yet been extensively studied by the computer security community.

We suggest that it is fundamentally important for the computer security and privacy research community to (1) understand the computer security and privacy needs, practices, risks, and challenges facing activists under an oppressive regime and, specifically (in this work), during a national revolution. In doing so, it becomes possible to (2) empower future technology designers, policy makers, and researchers to consider if or how technology might best support the needs of activists under oppressive regimes or during a revolution. This understanding must provide technologists with a way to (3) reason about what issues might arise in the future, for whatever technology they are creating and for whatever world might later exist. Namely, technologists could benefit from guidance for reasoning about technology use during extreme political strife. In this paper we provide a foundation for addressing all three of these gaps.

One recent revolution is the 2018-2019 Sudanese revolution, which resulted in the ousting of Sudan's president of nearly 30 years, Omar Elbashir. Our work focuses on the needs, practices, risks, and challenges of activists during this revolution, with larger inferences to future movements and technologies. Our insights stem from in-depth interviews with 13 Sudanese activists. The study received IRB approval from our institutions, and we took extra precautions given the sensitivity of this topic, as detailed in Section IV.

Stepping back, before presenting our research questions and findings, we first observe that activists have multiple goals during a revolution, for some of which they rely on technology.

- Activists must organize, attend, and publicize protests and other activities in order to push forward political change. Simultaneously, they must also keep up with international and local news.
- Because activist groups are always changing, with members both leaving (due to arrest) and joining (some of whom may be adversarial), activists must build trust with each other.

While activists do the above in order to achieve their political goals, they must also contend with their adversaries in different contexts. The governmental bodies against which they are rebelling push back using various tactics (including flagrant human rights abuses in some parts of the world [2]):

- The adversary may control or have influence over infrastructure upon which the activists rely.
- The threats may be technological, e.g., fake Twitter accounts spreading misinformation, or a complete internet blackout.
- The threats may be physical, e.g., arrest, violence, tear gas.

Some political activists may not have planned to become activists until the government started to exert some control over them or their technologies. Many activists are not technology experts and hence information within the community

§Co-first authors listed in alphabetical order

‡Alaa Daffalla's name in native alphabet: الَاء دفع الله

of activists informs their technology use.

With this backdrop, we formulated the following research questions. Our interviews were semi-structured, thus, individual discussions with participants also explored other topics.

1) What was the threat landscape during the revolution?
2) What were the activists' security practices? In what ways did technology and design support them or hinder them? To what extent did they feel their security goals were met?
3) How did activists adopt new technologies, behaviors, or mental models? Who taught them?

Through these questions, we learn, for example, that:

- **Politics and society are driving factors of security and privacy behavior and app adoption**. For example, the Sudanese diaspora played a significant role in passing knowledge to activists on the ground, and formed a robust ad hoc content moderation team on Twitter. Additionally, international sanctions on Sudan influenced app availability and pushed users to use a foreign phone number as a second factor for social media accounts.
- **A social media blockade can trigger a series of anti-censorship approaches at scale, while a complete internet blackout can cripple activists' use of technology**. Sudanese activists were unfazed by the censorship of social media; they constantly adapted by using VPNs or different apps (e.g., Telegram's adoption). In contrast, the 5-week internet blackout drove activists to analog techniques, including the use of a coded language over (surveillable) SMS and telephone calls. Group adoption of mesh networking apps such as FireChat [3] proved highly unsuccessful.
- **Activists' defensive strategies—against threats of surveillance, arrest, and physical device seizure—were low tech, yet largely sufficient.** This was in part due to the variety of defenses, requiring more work for the adversary. For example, activists meticulously deleted messages and logged out of social media accounts before going to a protest, or hid apps in other ways such as through iOS's ScreenTime [4] or Android's TwinApps [5] feature. However, many of these defenses cost activists preparation time and data loss, revealing that mainstream apps do not support activists' needs, even though activists can find workarounds.
- **Key principles for contestational** [6] **and defensive design could be better supported by current technical and UI design, but also may be in tension with each other.** We surface key design elements that our results suggest would aid those facing an oppressive government, e.g., support for mesh networking in mainstream chat apps, alternate authentication methods, or data sanitization or deletion on trigger. However, we also find that it is difficult to generalize these recommendations because they may be in tension with other recommendations—e.g., some groups may prefer to use mainstream apps, while others may prefer apps with a smaller user base. At a high level, our findings suggest that it is difficult to generalize specific design recommendations that fit *all* user groups, and that users should have multiple options, e.g., design *principles* should be implemented in ways that are adoptable (or not) by the user.

II. Background on Sudan

Sudan is a country in North Eastern Africa with an estimated population of 45 million as of July 2020 [7]. Sudan has had a number of governments following independence from British rule in 1956. In 1989, Omar Elbashir led a military coup and seized control of the country. As Elbashir's government gained power, Sudan established itself as a regional ally for Islamic fundamentalist groups while building a reputation for human rights abuses [2] and censorship of print and electronic media [8]. In 1993, Sudan was designated a state sponsor of terrorism by the United States of America (US) [9].

In the past decade, telecommunications operators in Sudan have built well-equipped infrastructure and expanded cellular and LTE services by connecting more than 10 million users to the internet as of 2016 [7]. Android phones are the most popular smartphones in Sudan, followed by iOS devices [10], in part due to US sanctions impeding access to services such as downloading and updating apps from the Apple store and accessing iCloud which requires a VPN connection [11]. Access to the Google Play Store was initially curtailed, but in 2015, as the US eased its sanctions, some Google Play services became available to Sudanese users [12]. However, access to paid apps/features remains restricted [13].

In 2018, due to the dire economic situation in the country, a wave of protests erupted and led to the 2018 - 2019 revolution [14]. Figure 1 captures the main phases of the Sudanese revolution, starting in December of 2018 and leading up to the formation of the civilian transitional coalition. Throughout the different phases of the Sudanese revolution, protesters were targeted by a number of state actors, including the police, the National Intelligence and Security Services (NISS or "the security services"), the military, and a special division of armed forces, the Rapid Support Forces (RSF). A more detailed glossary of state and non-state entities is available in Appendix C. As shown in Figure 1, the major events leading up to and during the Sudanese revolution are:

Arab Spring protests: Sudan caught up on the early wave of the Arab Spring[1] when protests erupted in 2013 following unrest in neighboring countries. These protests were suppressed by the Sudanese government. In these uprisings, social media played an important role in promoting collective activism, with Facebook and Twitter among the most popular social media platforms for participating in protests and facilitating protest logistics [1, 15].

The beginning of the Sudanese revolution: Initial protests erupted in the city of Atbara on December 19, 2018. Within days, demonstrations were held in most cities across Sudan. An umbrella organization of professionals' groups and unions, the Sudanese Professionals Association, emerged as an organizer and a leader for the protesters and became a reliable

[1] A wave of democratizing protests/revolutions throughout Middle Eastern and North African countries, including Egypt, Tunisia, Libya, and Yemen.

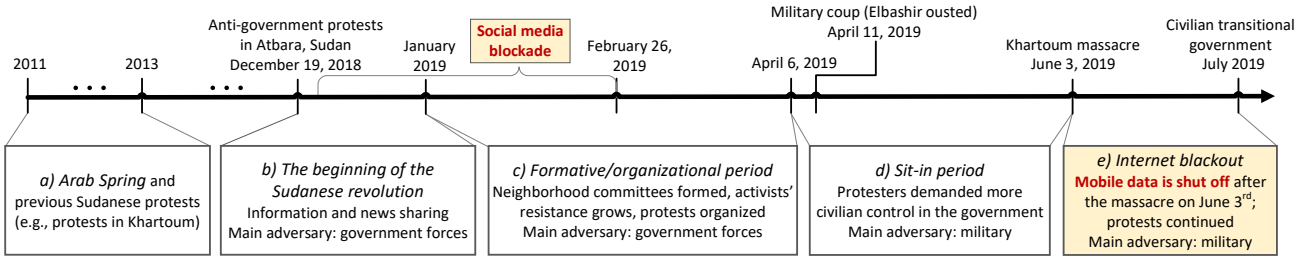

Figure 1. Timeline of the major events during and leading up to the Sudanese 2018 - 2019 revolution.

source of news [16]. As the protests gained momentum, on December 21 the government curtailed access to popular social media platforms including Facebook, Twitter, Instagram, and WhatsApp. According to NetBlocks [17], blocking measures were decentralized and carried out at the discretion of the telecommunication operators.

Formative/organizational period: Protests continued throughout this period. The movement evolved to become more organized and structured with neighborhood resistance committees being formed. Neighborhood committees were groups of activists who came together to lead the movement at a local level, acting as a robust information network covering the country while serving as independent and decentralized resistance hubs that worked under anonymous leadership [18]. Due to the growing support for the protests among the population and the pressure from the international community, the social media blockade ended towards the end of February 2019 [17]. On April 11, Sudan's president Elbashir was overthrown after tens of thousands of protesters encircled the military headquarters in the capital, Khartoum. Following that, a Transitional Military Council (which included the RSF) was formed to pave the way for a civilian rule.

Sit-in period: The protesters feared that if they left the massive protest scene in front of the military headquarters, their revolution would come to an end and their demands for a civilian rule would not be met [19]. So they stayed, creating a mini-city or sit-in area in a matter of days. The area had no cell towers; hence, mobile communications and internet access were limited. Most people relied on in-person communication. While the Transitional Military Council was still in power during this period, there were no violent attacks on the protesters and, according to our participants most people felt safe in the sit-in area.

The Khartoum massacre and the ensuing internet blackout: On June 3, armed forces brutally attacked those in the sit-in area in an attempt to disperse the protests, leading to the deaths of 120 people and injuries to more than 700 [20]. At the same time, the regime shut off the internet throughout the country. However, after a few days limited internet access was available through landline service providers since many vital institutions, such as banks, required internet service to operate. In contrast, internet (data) from mobile carriers was completely shut off, leaving most without data connection due to the low rate of home and public Wi-Fi networks [7]. The blackout continued for more than a month until an agreement between the military and a coalition of political parties was reached to form a civilian transitional government.

III. Related Work

Our work is informed by prior work on activism, security and privacy for specific user populations, and adoption of security behaviors. We summarize these efforts below:

Surveillance and censorship. Censorship-oriented research has focused on China (e.g., [21, 22]) and other parts of the world such as Saudi Arabia, Iran, and Bahrain [23, 24], or Thailand [25]. Groups have also focused on the commercial tools used by nation states for surveillance and censorship, e.g., Blue Coat [26]. While the studied techniques include keywords, IP addresses, and hostname filtering, Sudan additionally experienced a different type of censorship during the revolution: an internet blackout. Internet blackouts have occurred in the past decade during revolutionary movements or uprisings [27]. For example, internet shutdowns happened in Egypt [28], Libya [29], and Syria [30] during the protests that erupted in 2011 and 2012, and in 2019 and 2020, there have been blackouts after protests in Belarus, Ethiopia, India, Iran, Venezuela, and others [31, 32, 33, 34, 35].

Activists and technology. Activism involves advocating for social, political, or environmental change, tackling issues of injustice or uncovering corruption. Others in HCI have studied activism, e.g., health activism [36, 37, 38] or feminist HCI [39, 40]. Along the lines of political activism, Tadic et al. [41] studied Information and Communication Technology (ICT) use by activists in Bosnia and Herzegovina and likened it to the ICT use by non-profit organizations. They looked into the activists' ICT training and knowledge sources and concluded that enabling security, privacy and anonymity remain the biggest hurdle that activists face. Additionally, Gaw et al. examined how professional activists decide when to use encrypted email [42]. Other groups have studied technology during political events, e.g., protesters during the Arab Spring [43, 44, 45], and by political refugees or other persecuted populations [46, 47, 48, 49, 50, 51]. Finally, in a series of studies on how to design for activists and grassroots movements, Hirsch provided an analysis of contestational design processes, grounding their

findings on the importance of considering politics a significant factor in technology design decisions [52, 6, 53].

Security & privacy for vulnerable populations or in non-WEIRD contexts. Prior works have found that security and privacy practices differ between cultures and countries [54, 55, 56]. Others have focused on specific non-WEIRD (Western, Educated, Industrialized, Rich, Democratic) populations, such as work focused on the privacy and security concerns of Saudi Arabians [57] or South Africans [58]. For example, the latter found that privacy practices of users living in South Africa were heavily influenced by their sense of physical safety which is different from a Western country [58]. Additionally, studies on vulnerable populations also present some overlap with non-WEIRD groups. Among these populations are studies of journalists, refugees, survivors of human trafficking, and undocumented immigrants, which have broadly found that vulnerable populations have heterogeneous needs that may not be met by standard security assumptions made by developers [59, 46, 60, 47]. We expand on this work by revealing key factors that could guide future researchers and technologists when designing for specific populations. We encourage future researchers to systematically compare and contrast the technical recommendations, threat modeling, and user practices in vulnerable populations as a step towards understanding how to generalize findings about specific populations.

Adoption theories. A number of theories explain how behaviors spread within a given population. For example, in the Diffusion of Innovation theory, Rogers talks about the importance of communication channels in influencing the decision to adopt or reject a new idea or behavior [61]. Rice and Pearce expand on the Diffusion of Innovation theory to come up with the Digital Divide framework that examines the socioeconomic inequalities in developing societies through the lens of the adoption of mobile phones [62]. We build upon these works to provide an analysis of technology adoption, but as this is qualitative work with an exploratory objective, we do not contribute to the theory literature.

Adoption of security behaviors. Researchers have examined how specific factors influence the adoption of security and privacy behaviors. Das et al. concluded that social triggers were the most common triggers influencing security and privacy behavioral change [63, 64]. Wash and Rader identified the importance of narratives and their consequences on how computer users conceptualize security threats [65, 66]. Abu-Salma et al. found that social influences or recommendations for adoption that come from the participants' immediate social network were among the main criteria influencing participants to adopt a communication tool [67]. Our findings also reveal the importance of narratives in user adoption of behaviors and technologies (as detailed in Section VII).

IV. Methodology

We uncover key political, social, and technical factors that influenced activists' use and adoption of technology during the Sudanese revolution through semi-structured interviews. Our team was well positioned to conduct this research by combining security and HCI expertise. One of the lead researchers and interviewers is Sudanese and was in Sudan during the revolution, providing us with guidance on how to navigate the Sudanese cultural and political landscape, and serving as a layer of validation.

Recruitment process. To recruit participants, we reached out to known Sudanese activists; we omit specific strategies for finding the activists, for safety, but note that future researchers seeking to study activists may need to invest significant resources to find and build trust with activists.

In each initial message, we explained that we were academic security researchers studying the technology practices of activists during the Sudanese revolution. At the end of each interview, we asked the participant if they would be willing to either pass our contact information to any other activists, or share other activists' contact information directly with us after receiving their consent. However, we deferred to the participants' comfort level, being cautious to respect their boundaries with sharing information of other activists soon after a revolution in which the very information we were requesting was highly protected and could have previously resulted in physical harm to one or both parties. Ultimately, 4 participants were recruited through snowballing.

Semi-structured interviews and data analysis. We do not aim to quantify any one mental model or technical defensive strategy in the Sudanese activists community. Thus, we conducted semi-structured interviews, a qualitative tool commonly used for inquiry into vulnerable or understudied populations, e.g. [59, 46, 60]. We conducted 13 interviews with 14 activists of various experience levels, providing data with both depth and breadth, until reaching *thematic saturation*. We dropped one participant from our study after the interview because they did not identify as an activist, so we report on data from 13 participants (12 interviews). One interview had two participants (P7 and P8) because the participant we were planning to interview asked if their friend (who was also an activist) could join. In the interest of participant comfort, we accepted, but acknowledge that this interview had some of the drawbacks of focus groups, where a participant may choose not to share information that they do not want the other participants to know, or they may not share a story corroborating what the other participant has already shared.

We gave participants the choice of an interview in Arabic, but preferred English interviews because it meant two researchers could join instead of one. Ultimately, 5 interviews were conducted in Arabic by one researcher (who speaks Arabic natively) and the rest were conducted in English by two researchers (including the researcher who speaks Arabic). In the English interviews, participants were given the option to switch to Arabic at any point; some participants exercised this option for individual questions.

In our interviews, which lasted approximately one hour each, we asked participants first about news and information sharing during the revolution, a less sensitive topic. We then

dove into more sensitive questions about general technology use by activists (e.g., for inter- and intra-group communication), threat models throughout the revolution, and the role of technology in protecting protesters on the ground. We also specifically asked about technology use and adoption during the internet blackout if it did not come up organically. A summary of our interview protocol is in Appendix A.

For analysis, we first transcribed the recordings. The researcher who is a native speaker of Arabic translated the interviews from Arabic to English. We then developed a qualitative codebook through an iterative process in which we created memos, open codes, and then coalesced the open codes into hierarchical axial codes. Two researchers then applied the codebook to each interview, continuing to iterate through two full rounds of coding. Using Cohen's Kappa, intercoder agreement was 98.7%. To fully capture the landscape of technology use, we coded 'Yes' for behavior that the participant knew *of*, regardless of whether they used any given strategy personally.

Participant safety and ethics. Our study was approved by our institutions' Human Subjects Departments (IRB). Additionally, due to the sensitive nature of the topic, we took precautions to minimize the risk to participants. Most importantly, we let participants' own comfort level define their experience by giving them choices, including the technology we used to contact them and the amount of information they shared with us before and during the interview. All participants agreed to be recorded. Most participants preferred audio-only calls over video; in the interest of building trust, we kept our video on even if they did not. We also only collected enough information from participants to contact them on the day of the interview and did not pay participants, as our institutions required collection of name and address in order to dispense any payment, and international sanctions also prevented us from paying participants who were physically in Sudan.

Throughout the interview, we reminded participants that every question was optional, and that if they told us anecdotal stories, we did not want or need to know the names of the people involved. If participants seemed uncomfortable or reluctant, we changed topics or ended the interview, though we perceived this happened only once, which we attributed to the participant being tired because it was late in their timezone.

Looking beyond our specific procedures, a separate ethical question emerges about whether the publication of our results will ultimately help or harm the efforts of future activists. For example, will the findings in this report allow future governments to prepare for—and thus stifle—future activists? Our findings suggest that it is unreasonable to expect that all future activists will be technically sophisticated. However, it is reasonable to expect that nation states will have technical sophistication. Thus, we believe that while the findings in this paper can contribute to the creation of technologies to empower future activists, we do not believe that our findings go beyond what a sophisticated nation state could deduce. In short, we believe that publishing these results will be a net positive for activist communities.

Limitations. Although our sample size is sufficient to conduct a qualitative study due to reaching thematic saturation, our results should not be interpreted quantitatively. Additionally, we were unable to recruit participants from cities or towns in Sudan other than the capital, Khartoum, so activists from other parts of Sudan may have had different threat models or defensive strategies. However, because the activism and political movement is led from Khartoum, we argue that our participants represent an important population to be studied.

Also, it is possible that many of the participants did not fully trust us, so may have not revealed their most sensitive information, but given the candor with which most of them spoke (or said they wished to skip a certain topic), we do not think they would have provided inaccurate information.

Participant overview. For the safety of our participants, we did not collect demographic information, and we use they/them pronouns to mask participants' genders. Collectively, we report that of our 13 participants, 3 were female, meaning that men are overrepresented in our dataset, especially for a revolution in which women played a vital role [68], though prior work has observed gender differences in specific activist contexts too, e.g., hacktivism [69]. We believe the demographic imbalance is a consequence of our recruitment method, and while balance was a goal, our main goal was to simply recruit any activist who was willing to speak with us.

We also did not probe participants about their prior activism or their specific leadership or organizational role in the revolution. However, we do report information that participants spontaneously disclosed in the interviews: three participants said that they were part of neighborhood committees; two were part of the diaspora, and additionally, three were in Sudan for only some of the revolution. Two participants indicated they played a leadership role outside the neighborhood committees. We note that additional participants may fall into the preceding categories but may not have identified as such in the interview.

We present results from our qualitative interviews through the next three sections as technical, political and societal factors that drove the technical defensive strategies used by revolutionaries in Sudan. These factors emerged as natural classifications of topics from the interviews and form a lens through which to examine, anticipate, and explain the use of technology and defensive strategies in many contexts, including in other political movements, during internet blackouts, and against technically oppressive nation state actors.

V. Technical challenges: technical problems and app inadequacies drove adoption

In this section, we identify four fundamental technical challenges that drove activists to adopt a diverse set of low tech solutions. However, based on their stories, the *variety* of their defenses provided sufficient security by not giving their adversary one singular defense to focus on breaking. This section concludes with the actual security advice that participants received and which informed their technical practices.

A. *Misinformation challenges mitigated through manual heuristics, crowdsourcing, and some platform affordances*

Verification of information is a hard technical problem; politically motivated misinformation is rife throughout social media [70]. In Sudan, online misinformation was rampant during the revolution, though some participants considered it only a low-level threat (P8, P11). Misinformation originated from online accounts ("electronic chickens") paid by the Sudanese government [71, 72]. Misinformation ranged from fake news, to false reports about deaths at protests (P9), to false protest times and locations at which the police would be waiting to arrest activists (P5).

Some app features supported activists in building trust and disseminating verifiable information—such as livestreaming and the ability to report spam accounts—but activists largely relied on nontechnical methods to fact check. Additionally, some anti-misinformation policies on social media that are intended to reduce misinformation subvert activists' need to manage multiple online identities without pollution or context collapse, while heavily favoring an adversary that has control over the telecommunications infrastructure and companies.

Pre-trusted sources. 8 participants said that the Sudanese Professionals Association (SPA) was one of the only trusted sources of news during the revolution, especially in its earlier days: "*All the people agreed on the SPA Facebook page as the official and only source of verified information*" (P2).

Other sources of news were verified or well known activists who built trust over time well before the revolution: "*On Twitter, most of the activists are well known.... It's a circle of well known people, circles intersect with each other. So there is a system in place to fact check the news*" (P12). During the internet blackout, activists reverted to trusted mass media: "*During that period, television was the primary source of information. So we were closely following two channels, Aljazeera and Sudan Bukra. We got confirmed reports from these channels*" (P2).

The search for first hand sources. Activists built networks of contacts to enable them to get news from a trusted first-hand source. This network was sometimes multiple layers deep so that it would be harder for an adversarial observer to trace through the network between the sources and the destination. P9 constructed such a network in order to get to first-hand sources and verify news about deaths. P9 described their process to verify one such (alleged) death that happened in another city, in which they contacted a local friend whose family was from the other city, and that friend contacted their cousin, who found a doctor who worked at the hospital on the reported death date. They said: "*There was a chain of people who every one of them knows only one person. Even if they arrested, say, the doctor...they will find his phone and they will find 200 contacts. Are they going to arrest every single one of them? No. So there was no way to reach me, because I didn't contact the doctor.... There was no way to link all of them together unless they were very very very smart — and, believe me, the NISS wasn't that smart.*"

Fact checking through manual heuristics. None of the participants mentioned platform affordances explicitly built to aid fact checking (e.g. Facebook's info button), instead searching through unknown online profiles to identify patterns of fake news or suspicious handles, echoing Geeng et al.'s findings about how users investigate misinformation [73]. P11 explained one of their heuristics: "*if someone's account is AhmadXYZ234567, then everyone knows that's a troll. But if someone's name is AhmadHussein08, and he's having normal conversations, but like misleading or misinforming, or spreading fake news, then that's more dangerous.*"

Additionally, P3 helped create and share infographics about how to fact check; however, no other participant mentioned seeing or using these infographics. Another fact checking strategy involved checking news across different platforms. P12 used Twitter to fact check Facebook given that Twitter does not allow tweets to be edited, unlike Facebook which does allow users to edit posts. P12 also believed that misinformation was both most common and easier to spread on Facebook and hence required additional efforts from the activists' side to fact check on Facebook.

Crowdsourced content moderation. The Sudanese diaspora formed a content moderation team on social media, taking shifts and reporting and questioning suspicious online accounts (P11). P11 said that the content moderation community "*somehow... just became an organic expanded community, and the trolls would get shut down and reported right away.*" This ad hoc, organically crowdsourced, and effective (by P11's reporting) content moderation team may suggest that crowdsourcing and self-moderation can be effective within activist communities.

Producing verifiable information. Activists were also dedicated to producing information that would be unalterable and therefore trusted. 5 participants mentioned livestreaming as a way to produce information that others consider trustworthy (P6, P7, P9, P11, P12), despite it being a physically dangerous activity: "*[Live broadcasting] is one of the most dangerous activities, especially when you are dealing with a regime like the former regime, who was shooting anyone who was using their phones to document a protest*" (P8).

P7 and P12 used verbal or written measures indicating the date and time of protests when livestreaming or taking photos in order to increase verifiability: "*Facebook became more reliable when people actually wrote a paper that has the date, place and time in addition to saying it verbal*" (P12). Activists' ad hoc measures to fingerprint their own reporting suggests that mainstream social media platforms should work towards enabling automated and human-verifiable fingerprinting.

B. *Confidentiality over an adversarial network*

Activists in Sudan were working under an adversarially controlled internet and telephone network. Except during the blackout, all used end to end encrypted (E2EE) chat apps such as WhatsApp or Telegram, which some perceived to be more

secure because "*they have the self-terminated messages. So the conversation erases itself over 5 minutes, 10 minutes or something*" (P11). Furthermore, several had additional strategies in place to maintain privacy over these popular apps and they believed these strategies helped them stay more secure: P7 used a VPN to access WhatsApp, P13 used WhatsApp on an Android emulator instead of on their smartphone and obscured their network activity through intermediary servers, and P9 used the web version of Telegram.

Foreign Numbers as 2FA. 9 participants mentioned adding a foreign phone number to their Twitter or WhatsApp account instead of their Sudanese phone number, with three strategies for doing so: first, some obtained foreign SIM cards, and used those SIM cards on roaming (P1). We observe that though this made participants feel safer, because they believed the Sudanese government could not intercept their texts with a foreign SIM, this may not have provided privacy guarantees against interception or after-the-fact-reading for an adversary with purview over the telecommunications companies.

Second, some created fake US numbers online through a "phone service in an app provider" (P14 gave this advice), thinking that this would provide privacy by not going through the Sudanese telephone network, but relying on the security of the app provider and depending on the internet availability.

Third, others "*ask[ed] their friends and family overseas to verify their Twitter accounts by using their numbers over there*" (P1). This strategy provided the security of having their 2FA not go through Sudan, but required waiting for a message from someone who might be many time zones away when using the second factor, e.g., after getting locked out due to VPN usage making the logins appear suspicious (P1).

Low tech defensive strategies. With an entirely adversary-controlled network—including the possibility of apps backdoored upon download and fake cell towers at protest sites [74, 75]—activists did not find a wholly technical solution to ensure the confidentiality of their communications, and instead turned to a variety of solutions to supplement their preferred communication mode, relying on solutions that could not scale due to manual effort or hardware availability. Defensive strategies included using coded communication (8 participants) and making calls only over VoIP (not possible during the blackout, 3 participants). Others still used burner phones (9 participants) or burner SIM cards (7 participants) to distance their activist communications from their personal phones. P2 said that fake SIM cards were not difficult to come by, and that they did not require registration: "*there were a lot of fake SIM cards that people could purchase.... People can buy them without registering any sort of personal information*" (P2). We note that having either a burner SIM or a burner phone—but not both—may not provide the anonymity that participants thought they had.

Safety in numbers. During the blackout, many started using SMS and telephone calls to communicate (11 participants), despite the fact that most participants believed the government had full access to SMS and telephone calls (12 participants). Some took no further action to obfuscate their communications because they felt the government could not effectively process all the SMS and call data it had access to. P5 said: "*the numbers were big – everyone in the whole country was talking about the same thing: protests, killings. So looking for specific keywords via voice recognition, it would not work. The whole country is talking about it. It's a revolution.*" 7 participants said that safety in numbers is contingent on whether an activist is a target of the government.

C. Availability of communication on an adversarially controlled network

Through this section, we explore how the government's ability to partially or wholly censor the internet drove adoption of different communication methods — for example, Telegram and VPNs, during the social media blockade, and SMS and telephone calls, during the mobile data blackout. However, we observe that such adversarial control of app usage could have been purposeful, leading people to a communication method that was compromised (e.g. how many suspected the government could access SMS records and track phone calls, or—our conjecture—an app with a backdoor or traffic routed through adversarially-controlled servers [75]).

Reliance on VPNs to circumvent the social media blockade. In response to the government censorship of popular social media apps during the social media blockade in December 2018, some activists adopted various VPNs (7 participants). VPN usage allowed them to continue using the apps they were previously using, and added the additional security and privacy properties of encrypted and tunneled communications. Though P2 "*only used VPN during the... government enforced ...blockade on social media apps*," others continued using VPNs for their privacy properties (P5, P11, P12). P12 explained that "*even after the social media blockade...people were advising that to maintain your privacy it's better to continue with VPN uses especially if you were very active on social media*" — echoing Namara et al.'s findings [76] that users are driven by fear of surveillance when adopting VPNs.

However, P2, P6, P11 and P13 mentioned that VPNs would sometimes stop working, leading them to either search to find a new VPN or to stop using a VPN altogether. P13, a technical expert, attributed this to the Sudanese government blocking requests by IP ranges after a VPN became popular. P14, another technically experienced activist, began developing a VPN app that would help "*those who found difficulties with these international VPN apps.*"

Furthermore, when asked about the use of other more advanced anonymous network technologies like Tor, P13, a technically experienced activist, was against advice that would publicize the use of Tor because of a few (perceived) usability concerns: "*even if we use a Tor browser or gave advice for people to use it there are simple tricks or advice if people ignore it, for example while using a Tor browser don't minimize the screen because the moment you minimize the screen if someone is tracking you, you could be identified.*"

The shift to unblocked apps during the social media

blockade. In addition to VPNs, some activists adopted use of Telegram because it was not blocked during the social media blockade (P2, P6, P11, P13, P14). Others said that despite the blockade, WhatsApp and Twitter remained more popular (through the use of VPNs) (P5, P7, P12). We observe that the Sudanese government's power to influence app usage by blocking and unblocking apps could have funneled activists to specific apps that were advantageous to their adversary. Additionally, VPNs and other apps may be compromised or employ flawed implementations [77].

Group adoption of mesh networking apps during blackout faced difficulties. The internet blackout was also a period of (attempted) adoption of new apps and communication methods because most of the apps that activists had been using relied on an internet connection, which was not available. However, many activists did not sufficiently fill their communication and confidentiality needs during this period. Some turned to SMS after attempting to adopt Firechat or Signal Offline Messaging, both mesh networking applications (6 participants). There were a number of reasons why participants failed to adopt mesh networking apps during the blackout, including the lack of group adoption and buggy applications or usability issues. Some struggled with operating the app itself and did not give specific reasons besides the fact that they couldn't make it work. P13 attempted to develop a mesh networking app after failing to operate Firechat: "*there was this app called Firechat but people couldn't make it work. We even tried it but it didn't work. It didn't even join those who were in close proximity to each other. So we tried developing an app.*" However, they failed to deploy the app before internet access was restored: "*We were in the testing phase when the blackout was lifted.*"

Moreover, mesh networking chat applications suffer from the problem of group adoption—they are not useful until reaching a critical mass of users, and until then, users decide not to adopt them, preventing a critical mass. P1 said: "*[FireChat] didn't really work out because you had to have a large number of people who had Bluetooth on all the time, constantly, and they had to be next to each other, like actual next door neighbors.*" Furthermore, according to P14: "*We tried Signal at that time and tried to build a network but it wasn't effective. It wasn't effective because we wanted a communication tool with a larger reach.*"

More generally, another problem of mesh networking chat apps is the issue of download and setup without internet connection: "*There was a problem of, okay, it's an application, how am I going to download it while I have no access to the internet*" (P12). Unless a user can anticipate that they will not have internet, they will wait until they do not have internet, at which point they cannot download the app. Furthermore, although some mesh network apps use encryption, recent research has revealed vulnerabilities in Bridgify, a mesh networking app popular outside Sudan [78].

Thus, we find that mainstream apps are developed with too-rigid threat models with respect to *availability* over an adversarially-controlled network, and apps specifically developed for use under an adversarially controlled network—i.e. mesh networking apps—struggled with adoption during the internet blackout. These complexities point towards mesh networking and connection robustness as a design principle to be incorporated into mainstream applications.

Other methods, including use of foreign SIMs and satellites. Activists also found a number of alternative communication channels, though none were scalable. Some activists acquired foreign SIM cards which worked on roaming data and hence allowed them to resume normal use of mainstream chat apps, though we observe that the use of foreign SIM cards may not have given them the privacy they thought they had (P1, P9, P11, P12). P11 described: "*everyone was kind of scrambling trying to get SIM cards to be roaming from like USA, Qatar, Egypt, all of that.*"

Others relied on those in their communities who had home internet to relay messages. There were a few landline service providers operating at the time who provided internet access to government institutions and some home users: "*One of the providers had one of its services working which is like Sudani DSL*" (P11). P1, who had internet at home, explained: "*what I used to do is relay messages to people who are not in Sudan and keep them informed about what is going on every time I get a chance.*"

In addition, activists largely turned to SMS and phone calls to continue communicating with each other (11 participants). To recreate the group nature of WhatsApp and Telegram, some moved their WhatsApp contact lists to SMS (P1); others created phone trees, like P5: "*everyone who's somewhere and they witness something happening, they would write ... an SMS, send it out to all of their list, their trusted people. And you have to spread that at least to 10 people if you trust the source.*"

Four participants (whom we keep anonymous) also worked to smuggle in alternative infrastructure options, e.g., satellite internet equipment, in order to provide internet scalably and with less threat of government intervention, but expense was an issue, and "*getting it into the country was a whole thing, because it's not something that, you know, you could just ship and it looks like biscuits.*"

Finally, activists also used analog communication channels such as pamphlets and public graffiti (P2, P8, P11), which were relatively anonymous, but cannot replace phones.

D. Device security against a physically present adversary or upon threat of arrest

In anticipation of arrest and physical compromise of their phones, activists used a variety of low tech defensive methods to hide or remove data. P12 reasoned: "*it's better to burn what they have than to risk the data on their phones getting into the wrong hands and risking their security and that of others.*"

Manually hiding or deleting information. Participants manually deleted or hid information like contacts, WhatsApp or SMS messages, group chats, images, and social media accounts with anti-government or activist posts (8 participants). Some formatted their phones entirely, relying on backups (P14). P1 planned to uninstall WhatsApp and Twitter and rely

on cloud backup if they were arrested, since they had two SIM cards and the second SIM provided plausible deniability. They also archived messages regularly. P11 used iOS's ScreenTime—a feature intended to promote time management by hiding apps from the user—to hide social media apps at certain key times, for example, when at protests, or when crossing the border.

One of the major strengths of these low tech strategies is that they made it appear there was no information hidden or deleted, though a complete lack of, for example, WhatsApp messages might be considered suspicious (P1). However, participants who chose to delete information temporarily or permanently rather than conceal it on the device chose the cost of (temporary or permanent) data loss.

Decoy or alternative information. Some activists also employed low tech strategies to increase plausible deniability if arrested: 9 participants added decoy social media accounts, alternative names for contacts on social media, or decoy messages on their WhatsApp accounts. P5 added a picture of Elbashir as their phone background, so as to appear pro-government if arrested: "*we had a joke, between me and my friends—we had our president's picture as wallpaper.*" As mentioned, P9 was released and deemed a non-activist after being arrested despite providing authorities their phone passcode: their release was due to their meticulous use of both manual information hiding and decoy information.

Going without technology. Those who did not feel sufficiently protected by the available strategies chose to leave their phones at home and forgo any connection in favor of no liability (9 participants). According to P2: "*We spent a lot of time trying to delete information from our personal devices so I was one of those people who stopped carrying around their personal phones when going out in protests. Because we did a lot of different preparations. A lot of prearranged agreements were made regarding timing and location of meetings.... All of the agreements we made could lead to other people and put them in danger. So this is not only about me but about others who I might have communicated with during that day or the few days prior to the protest. So, as I didn't know about any technique that could hide information it was much safer to keep my mobile phone at home.*"

Reliance on group adoption of security measures. As P2 said, security of the group was also part of the activists' decision to adopt certain security mechanisms: if one person in the group had poor security practices and was arrested, the whole group could be caught. Therefore, group adoption of security practices was critical, but activists could do little to ensure that their peers were truly following the same security strategies. For example, P9 used WhatsApp read receipts to signal to their contacts that they should delete the messages they had sent, but also admitted that there was no way to enforce this rule: "*you can't force someone to do something they don't want to do.*" P14, a WhatsApp group moderator put forth a set of conditions for those joining the group: "*We would send them a PDF document with all the measures they should take*" and "*Anyone who wasn't complying to this was excluded from the groups*." The strong need for group adoption of security measures suggests that within group chats, apps could enforce self-terminating messages as a rule of joining a group, adhering to a broader design principle of enforced self-moderation also found in Section V-A

Additional (burner) hardware. Some relied on burner hardware (phone, SIM, or both) in order to ensure they did not have incriminating or identifying information if they were arrested (7 participants). We note that unless the activists used both a burner phone and a burner SIM, the metadata transmitted by their phone / SIM combination would link their identity. P13, a technical expert, explained their cautious approach: "*No one carried with them their smartphone. From when the protests started erupting we all went to the market and bought burner phones. We even bought new SIM cards for the burner phones. Our goal was to be in the safe side in case anything happened, nothing would be leaked.*"

Technology-supported strategies. Less commonly, participants used apps or OS features specifically designed to conceal or delete information from their phones. P6 and P12 each used features from their Huawei phones to conceal information: Private Space, which allows users to conceal certain information behind a secret pin, and Twin Apps, which allows users to make a secret second copy of an app. For P6, these features provided sufficient protection, as they chose to not employ any other defensive strategies. In addition, P5 talked about an app that "*clears all of your data, and it sends out a message to pre-specified numbers that you got arrested*. Others relied on Telegram's self-deleting messages (P5, P11, P12, P13).

E. Security advice among the activist community

Now we turn to the content of the security advice that participants received. We find, broadly, that the common advice shared within the Sudanese activist community did not echo general-purpose advice given by the technical or academic security community (e.g. [79, 80]), though it does have similarities with activist-specific advice given to protesters in the United States in 2020 [81].

Advice: sanitize phone before a protest. Most commonly, participants received advice about sanitizing their phones or social media accounts, particularly before going to a protest (P2, P3, P8, P12). P2 said: "*Once people became a little bit organized around April, people were shown how to deal with their mobile phones and how to delete things,*" including manually deleting messages, removing information from social media accounts, logging out of social media accounts, or planting decoy pro-government or neutral information (strategies discussed further in Section V-D).

Advice: use secure chat applications. 11 participants used or tried to use Telegram, with several mentioning its privacy properties ("*more private than WhatsApp and Facebook*" (P8)). 4 participants mentioned Telegram's encrypted messages and capacity for self-deleting messages (P5, P11, P12, P13).

During the course of the interviews, 4 participants were familiar with the app "Signal," but one of them (and potentially two more) referred to it as a (buggy) app that had offline messaging capabilities (P6, P12, P14). We learned towards the end of the interviews that there is an offline messaging application called *Signal Offline Messenger*[2] that is distinct from *Signal Private Messenger*,[3] the secure messaging app that is relatively common in the US and Europe. Thus, the external advice to use "Signal" may have been misconstrued.

Advice: add foreign phone number as 2FA. P5, who attended a formal workshop run by activists, received advice to both add a foreign 2FA number to Twitter and to use VoIP and internet chat apps over regular telephone calls and SMS. P13, a technical expert, advised people to add a foreign number as 2FA. 7 other participants used a foreign number for 2FA.

Less common advice: passwords, misinformation. Advice that might seem more general and familiar to the security community was less common. P12, a technical expert, said, "*A group of IT professionals had an account where they posted such advice... change your passwords regularly, make sure it contains letters, names, numbers, unique characters, etc...*" However, only one participant mentioned changing passwords.

Similarly, P3, a fact checking expert, was part of an effort creating and sharing infographics "*to educate the wide public about how to verify news..., how to read the news, how to verify the claims, how to verify any anybody's photos using Google image application.*" However, no participant mentioned receiving specific advice on dealing with misinformation.

Comparison to general-purpose advice. Stepping back, we observe that the advice given to (and among) Sudanese activist does not directly echo common general-purpose security advice given by the US- and Europe-based technical communities, other than the general advice to use secure chat apps (which, as discussed in Sections V-C and VII-A, was not always actionable). For example, the most common expert security practices in Busse et al [79] are to update regularly, use password managers, 2FA, ad blockers, while the most common non-expert security practices are using antivirus software, creating strong passwords, and not sharing private info. Of the expert behaviors in [79], participants only mentioned using 2FA, with modified advice: use *foreign* 2FA (discussed in Section VI-A). Outside the academic community, there has also been mixed advice and debate about whether WhatsApp should be considered safe by activists [82, 83].

Comparison to worldwide activist advice. Through an anecdotal (news and social media as of September 2020) view of US Black Lives Matter (BLM) protesters and Hong Kong protesters, we observe that despite the different adversaries and political goals, there are important overlaps in advice and also significant differences. For example, protesters in Hong Kong are concerned about facial recognition, so they wear both facial masks and a black T-shirt [84]. Though our participants talked about physical security, and one suggested that anyone who was taking on the risky role of livestreaming should not wear bright colors so as to not stand out (P7), they did not adopt defenses against facial recognition or video surveillance, likely because they did not believe the Sudanese government was capable of it (P1, P5).

In a recent article, BLM protestors were advised to carry burner phones, but, if they cannot, the article advised protesters on a variety of preparatory tasks in anticipation of an adversarially-controlled network (e.g. IMSI catchers / Stingrays) and physical seizure of device (but still subject to US laws, which protect most from being forced to give up their passcode, unlike in Sudan)—for example: download Signal, change location permissions on their phones, back up and encrypt their phones, use a passcode instead of biometric authentication, write contacts on your body [81]. While the same high level concerns applied to Sudanese protesters, they were advised to use significantly different tactics, revealing that while advice can follow a certain high level framework to enumerate adversarial concerns (Section VI), protesters in different countries require very different *concrete* advice.

VI. Political influences on the technical defensive landscape and activist threat model

Here we examine the key political factors in pre-revolution Sudan that shaped activists' defensive strategies.

A. *International politics dictate available apps and features*

US sanctions on Sudan mean that mobile users in Sudan do not have access to all apps or app features. Through this subsection, we explore these restrictions, and find that the influence of international politics makes it challenging to create security and privacy recommendations that fit multiple vulnerable user groups, since different groups have access to different applications and features.

Restrictions on download and on 2FA. Due to the US sanctions on Sudan, the entire iOS app store is inaccessible without a VPN (P11) [85, 86]. P11 described how users in Sudan download iOS apps: "*You either get a VPN on your laptop and download things, and then get a VPN on the phone... but sometimes it doesn't work and it's a whole process. Or when you buy a new phone, you just have the store download everything for you. A lot of people do that. My dad does that all the time, and we end up with the store's Apple ID.*" Sharing Apple IDs may impede users' privacy, and an indirect download, or a download from a non-official app store, raises questions of app authenticity. Additionally, people in Sudan cannot directly pay for apps or app features due to the economic sanctions, so apps with paid security or privacy features, or security and privacy-focused apps that are not free, are not easily accessible. Sanctions also mean that Sudanese domestic phone numbers are not accepted as a second factor of authentication (2FA) "*because in Sudan Twitter does not have verification for Sudanese numbers*" (P1).

[2]play.google.com/store/apps/details?id=com.raxis.signalapp

[3]play.google.com/store/apps/details?id=org.thoughtcrime.securesms

B. *Technical capabilities of nations supporting Sudan*

Activists' perception of foreign capabilities and their ties to technology companies drives their threat models and tech use. The perceived technical capabilities of foreign governments that supported Elbashir's regime—e.g., Saudi Arabia and the United Arab Emirates—were a driving factor in some participants' threat models. P12 reasoned that the Sudanese government could have the same access to information from social media companies as wealthier countries: "*there were cases in Saudi Arabia where...the Saudi Arabian government would purchase information.... So there was this possibility that the government of Sudan was able to purchase such information from Facebook.*"

In addition, our participants' mistrust in Sudan's supporters extended to the foreign SIM cards they were comfortable using. P5 believed the Saudi government could acquire specific user data on behalf of Elbashir's regime through monetary influence and that they would pay Twitter to extract information about Sudanese users who had Saudi SIM cards: "*the Saudi government has shares on Twitter, so we are not very trustful... [there is] sharing between Twitter and the [Saudi] government, so your number should not be a Saudi number. It has to be something in Europe, for example*" (P5).

The perception that privacy on social media was only as good as the money paid by a government, in combination with the lack of choices in apps, led some to feel a lack of control or sufficiency. Asked whether people continued to use Facebook despite the possibility that the Sudanese government could purchase information, P12 said: "*there wasn't any other solution. We reached a phase where we were saying 'what is the worst that could happen.' People have died because of this.*" We cannot address the accuracy of P12's perception about the availability of Facebook data to the Sudanese government, but we do note that according to Facebook's public log of government requests, during January-July 2019 there were 15 requests by the Sudanese government for information on 23 user accounts, and the following period, for the latter half of 2019, had 52 requests. According to Facebook, they did not produce information in response to any of the requests.[4]

C. *The power of the state to compel authentication*

Sudanese authorities obtained arrestees' phone passcodes or biometrics in order to search their phones for anti-government activities and proof of activism or identity, a major threat for all participants. P11 explained the threat of legal (or legally unquestioned) violence at the start of the revolution: "*are they going to be killing people, or just torturing them, or just beating them? We had no idea the extent of the brutality.*"

P12 detailed the threat of physical device seizure: "*the security services would look into WhatsApp first, then Facebook. They would look into your latest posts and then they would say that this person has a history of anti-government posts.*" In recounting their arrest, P9 described that they were so confident in their defenses that they wrote down their passcode for the police: "*The first thing they told me, they told me to 'open your phone.' And I just told them, 'give me a pen and paper, I will write it down for you. So whenever you want to open my phone, you just open it.*" We explored P9's defensive strategies earlier throughout Section V, but P9's confidence was not unwarranted: per their telling, they were detained for 7 days, all through which the police had access to their phone, and the police were never able to prove P9's identity as an activist because of P9's low tech but meticulous defenses.

P5 knew someone who used biometric authentication to ensure plausible deniability upon arrest by using someone else's fingerprint to lock their phone, taking advantage of their knowledge of the adversary's legal power: "*One of them was a high ranking activist on the security people's sheets, and they were threatening [them] by telling [them], 'if you don't open your phone' because [they] used fingerprint, but [they] used someone else's fingerprint! So they couldn't open it.*"

D. *Government control over the telecom infrastructure*

The goverment's control over the telecommunication infrastructure shaped activists' threat model and drove adoption of technology. 12 participants believed that the Sudanese government could surveil their communications through a combination of control over the telecommunications infrastructure, influence over ISPs, and technical exploitation. P1 explained their perception of the government's surveillance capabilities, tying together the threat of arrest with the threat of surveillance: "*they can tap your phones for sure, like your phone calls and SMSes...but...they have to know who you are or which number is yours.... But if they got your phone, like if you got arrested and they got your phone, then they're definitely going to keep tabs on you if they release you after.*" P1's perspective points to the difference between surveillance and mass surveillance: some felt comfortable using mainstream applications—even SMS, during the blackout—if they did not already believe they were specifically targeted, as mentioned earlier in Section V.

P13, a technically experienced activist, explained how the threat of the government's influence over telecommunication companies led to incidents of people being locked out of their social media accounts: "*They can only do this using the old stupid way. For example on Facebook, I forgot my password and then they would enter the number and then they would get the code as they already have access to telecom companies. They would get the code and reset the password and then they would lock you out of your account.*"

In addition to surveillance, activists contended with censorship and blackout: during the revolution, the government initially curtailed social media access for roughly 10 weeks, and later imposed a complete mobile data blackout[5] after the June 3 Khartoum massacre. Both required people to find alternate communication solutions.

[4]Requests for Facebook data (Sudanese government): https://govtrequests.facebook.com/government-data-requests/country/SD/jul-dec-2019

[5]Most people do not have regular access to home internet; thus, a mobile data blackout is effectively an internet blackout for most people

Some anticipated the censorship and tried to prepare: "*we expected a digital shutdown ... it happened in 2013, a complete shutdown. And I also lived through the Egyptian revolution, so I also saw that happening there, albeit it was way shorter*" (P11). To prepare for a social media blockade that could expand to include the Google Play store, P13 developed a news dissemination app that was never uploaded to the store and could only be shared via Bluetooth, "*I was honestly expecting that they would block play stores, Google Play store and the others with VPNs. Because when they blocked VPNs I thought they will block the actual store because it's natural—you blocked this VPN, I will download another one.*"

VII. Societal context enables adoption

Now we turn to the social characteristics of the Sudanese activist community that both supported and hindered technological adoption.

A. *Operating at the lowest common denominator of the group's digital and security literacy*

Activists' practices are shaped by their own knowledge of technology, as well as others' digital and security literacy, because the security of the group depends on the security of every member. We find that differences in digital literacy between activists that needed to communicate with each other may have resulted in less secure behaviors by *all* parties. P11 explained that digital literacy is a barrier to secure practices: "*that's one of the key issues of Sudan, that people really don't have digital literacy, or digital security literacy.*"

P3 and P13, experienced activists, adjusted their technology use and advice to align with the technology use of the greater group. P3 was forced to use WhatsApp instead of Signal, which they perceived to be less secure because "*WhatsApp might be monitored by the security forces in Sudan*." P3 explained: "*For example if you need to reach out to an activist on the ground, some of them do not have the background how to use Signal... They might lack that technical ability to use these secure applications. So that's why we said, okay, we can use WhatsApp, but without going into details*." P13 chose not to ask their colleagues to adopt Telegram, a new app, because even if they did use the app, "*they will use it without making use of the main feature of self-destroying messages. And this way there isn't any reaped benefit.*"

P9, also an experienced activist, explained that others' digital literacy prevented their own adoption of new chat apps because they needed to be confident their colleagues could use the app correctly: "*having a new application, that means that you will need to let those people learn a new application and learn how to do it. But for me, everyone knows how to use Twitter, everyone knows how to use Telegram, everyone knows how to use WhatsApp. So I don't have to explain to the person talking to me how to delete a message on WhatsApp. So for me, working with someone through an application they're already using is better than working through another platform.*"

We observe that all of our participants were from the capital of Sudan, and that those outside the capital may have a lower level of of digital literacy, making this issue potentially more pronounced outside urban and developed areas. Because group adoption of technology and security practices is both necessary for group action and group security, the lower level of digital literacy may have had a part in participants' adoption of low tech defensive strategies. More broadly, this finding reveals that digital literacy is a barrier to group adoption and has implications on the design for specific user groups.

B. *Sharing institutional knowledge, including security and privacy advice*

We find that activists' social structure supports largely informal sharing of institutional knowledge, including security advice, in line with prior work about security behavior adoption [63, 65, 66], suggesting that a formal education or advertisement campaign for apps targeted at activists might be less successful than leveraging social narratives.

Knowledge sharing through narratives. The social structure within the Sudanese activist community supported the informal spread of technical and security advice as institutional knowledge. Although a few gave or received specific technical training, many relied on their friends and more experienced colleagues for security and technical advice through narratives and stories, echoing findings by prior work about security behavior adoption occurring socially [63, 65, 66]. P2 said, "*Most of the advice that I have received were from people around me, for example, from my brother*" or from "*my relative who was in the field [electrical engineering].*" P6, whose neighborhood committee had a resident security expert, taught their friends about both BetterNet, a VPN, and Private Space, a Huawei OS feature that they began using to hide information from the Security Services. P7 said that sharing advice "*with friends and family members... happened a lot*," and P8 even considered security advice "*a public discourse between young people on how to keep yourself safe.*" P9 also considered such advice "*shared knowledge... I would share the information with my friends and the people who work with me, and they will share it with others.*" P12 mentioned information being passed around about "*what people of Burri*[6] *did, so then we can adopt this.*"

Organized training. As the revolution continued, some formal training arose. P5 attended a "*security workshop, to carry out your activism without being noticed by the security people ... It was in someone's house, and there were handouts. So you get the training and then you're asked to spread the knowledge to the people you trust.*" They said they were invited to the workshop because "*[the more experienced activists] started seeing me as someone who was contributing to the revolution.*" Experienced activists also created infographics on social media with security or privacy advice, (literally) relying on social networks to share the advice (P2, P3, P5, P10, P14). In addition, P13 (a technically-savvy activist) taught journalists how to use encrypted emails: "*For example there were journalists*

[6]Burri is a neighborhood in Khartoum where many of the protests occurred and it was considered the fulcrum of the anti-government uprising

who wanted to send things but they're usually afraid of sending it via email because of being intercepted. So there was PGP that we taught people how to use. We taught this to close people whom we could meet face to face. We taught them how to encrypt a message to the entity they want to send it to, they enter its fingerprint. And this way they're sure that no one could intercept the content of this message."

A core group of experienced members. Experience amongst activists is a continuum: some have been activists for years, and others became activists at the start of the revolution. The more experienced activists in our participant pool agreed that in Sudan, experienced activists are a small, tight-knit group, enabling a free and informal flow of information between experienced activists that can then be spread further out of the core of the community. P3 explained: "*The activists who are active in Sudanese politics...they all know each other.... It's not like in the US or Europe. It's a very small community...there is a nickname, the 1000 person.*[7] *The 1000 person, it's kind of a joke, there is 1000 activists in Sudan who are mobilizing everything.*" The small community of experienced activists also supported the existence of institutional knowledge about how to protest more generally (P7, P8, P11). P7 said: "*there are some protest skills that have been developed throughout the years. From 2013*[8] *to 2018, we have developed a lot of skills about how to make a successful protest, how to make it safer, how to document it, and send it safely, and so on.*"

C. *Building trust in a constantly mutating group*

As activists' groups are constantly changing with members joining and leaving, there was a continuous need to build and maintain trust in a challenging environment rife with threats: "*We can't really trust everyone, and on the other hand we still have to trust other people so we can work together*" (P1).

Root of trust: in person. Activists did not rely on technology to build trust both in in-person neighborhood committees and chat groups, with the ultimate root of trust being an in-person meeting or a prior personal relationship (8 participants). Sometimes, activists used social media profiles as part of a "background check," but they did not have one single technology that they relied on for trust building, again, a theme of non-technical or low-tech approaches that are strengths *because* they decrease the technical attack surface (though it could be vulnerable to human intelligence infiltration).

P7 and P8 also spoke about the importance of physically meeting someone new before adding them to sensitive chat groups: "*That's what [P8] said, people have to sit down before, on the ground, and meet in meetings. And of course, if someone from my secure circles added me to a WhatsApp group...it depends also to what extent do you trust the other person who is adding you.*"

P1 described camouflaging trust building activities through street cleaning campaigns, which served as a way to meet in a natural environment and figure out who was trustworthy: "*So every other week, we go out and clean the streets, as to reflect that the protests are peaceful, and this is what we are actually trying to do, not just causing riots—we're actually trying to build the country and make it a better environment for everyone to live at. So at that time, when we did those, we sent public broadcasts to everyone who is willing to join, they can join, and then we follow up from there after we meet them and see if we can actually add them to our group.*"

Bootstrapping trust. Participants also relied on trusted contacts to add their own trusted contacts to the group or network, or to gain trust for themselves or their online presence (P1, P7, P8, P9, P10, P12). P1's neighborhood committee's Twitter page, seeking to be a source of news and grow in size, got a friend of a friend who was active and verified on Twitter to post that "*this is not a fake page or anything like that*," which resulted in their Twitter followers increasing from 50 to nearly 4,000. P9 stated that the practice of the SPA (a trusted entity) "verifying" neighborhood committee social media accounts was common. Boostrapping was also used for building in-person trust: P1 described that new neighborhood committee members were mainly "*mutuals who were already recruited trusted people,*" who were additionally vetted through the street cleaning campaigns described above.

D. *Support from abroad*

The Sudanese diaspora performed many roles throughout the revolution, including sending mass text messages to help organize and spread news about protests (P3, P5, P12), disseminating news from inside Sudan to both families and the international mass media (P5, P8, P10, P11), acting as backup communicators or coordinators in case those in Sudan were arrested (P9), factchecking on social media (P10, P11, P12) (Section V-A), and using their own phone numbers as 2FA for those in Sudan (P8, P10, P12) (Section VI-A).

Experienced activists in the diaspora were also important to the flow of security and technical advice, as they were exposed to a different set of tools and may have had connections to activists in their country of residence. P3, part of the diaspora, described the connections the diaspora may have, and recounted how their own use of Signal stemmed from a friend who introduced Signal to many colleagues: "*some activists... have connections with European and American activists. Some of them even come from the IT background...[which is] one of the main reasons that they are well introduced to Signal and other applications.... I had a friend of mine who majored in computer science and was a known activist in Sudan. He wrote so many times about similar applications.... The people I know, they're using it because of this.*"

The activist social structure even extended to activists of other nationalities who may pass knowledge amongst a global network of activists. P12 recounted that Signal was suggested by an Eastern European activist group that was "*in touch with our activists giving advice like it's better to use Signal.*" However, P12 went on to say that "*I don't think these calls [to use Signal] found a listening ear,*" revealing, again, the need

[7]P3 used the Arabic term ألف ناس By our interpretation of their words, P3 would not have considered all of our participants activists—they meant 1000 *core*, experienced, dedicated activists, who are connected to each other.

[8]Sudan's Arab Spring protests took place in 2013.

for the advice-givers to understand the political and societal constraints of each specific community.

VIII. Discussion and Conclusions

Activists' use of technology through political change shows that technology can be democratizing; however, technology can also be a tool of oppression. The burden to build tools that will protect communities from oppression lies on the shoulders of developers, technologists, and policy makers.

Throughout our results, we have surfaced a number of key design principles and tensions, and we have explored how these principles and tensions are influenced by our participants' political and societal context. We encourage future researchers and designers to consider these tensions, sampled here, and to continue to work to reveal further ones:

- In Section V-C, we explore the difficulties that activists faced to adopt new mesh networking apps during the blackout, instead adapting their technology use by falling back on other methods like SMS and telephone calls. The lack of mainstream app support for a robust connection might suggest that certain populations would benefit from mainstream apps including a mesh networking mode; however, this suggestion is in tension with the finding from Section VI-B that activists and others might prefer non-mainstream apps that they perceive to have no ties to governments.
- In the US, domestic arrestees are protected by the 5th Amendment from being compelled to give a passcode [87]. Android and iOS support American users by providing a quick way to force passcode authentication over biometric authentication [88]. However, in Sudan, and in any other country in which authorities can compel detainees to give up their passcode, this design offers no protection, driving Sudanese users to manually sanitize their phones. This costs them time, access to information or contacts, and puts them at risk if they are unable to sanitize their device properly.
- Many of the activists' defensive strategies were low tech, e.g., manually timestamping videos, or deleting texts. These strategies were sufficient, and we observe that the *variety* of the low tech strategies (which were usable because they were low tech) is a great strength of the movement as a whole. However, as technologists, we also observe that many of the strategies did not scale and left the activists open to technical exploitation, if the adversary had had the resources. Thus, we observe a fundamental tension between low tech strategies that are widely usable and provide security in practice, and cryptographically secure technologies or strategies that invite the adversary to focus their resources on technical exploitation and additionally may come with issues of usability and adoption.

Thus, to guide future researchers, technologists, and policy makers in expanding upon, solving, and continuing to discover key design tensions and principles, we build upon our results and present a set of example questions as a guide for understanding the security and privacy behaviors of populations around the world, particularly those facing political strife or those whose membership is mutating—for example, other activists (e.g., anti-racism groups in the US like Black Lives Matter, protesters in Hong Kong), internally displaced or persecuted groups, populations living in warzones, refugees, or non-governmental organizations. Due to the complex nature of politics and society, these are not all-encompassing; other researchers may discover further key issues to investigate.

In order to examine, anticipate, and understand the privacy and security behavior and needs of a population under political strife, it is important to first understand the political situation, both internationally and domestically:

- How does the legal structure define the right to technical and physical privacy? What power does it grant to the governing entity and law enforcement?
- To what extent does the government have control over or insight into the telecommunications infrastructure and industry? Are there any legal or technical restrictions? Is there a history of censorship or internet blackout?
- What foreign powers are allies or enemies with this nation and what are their technical capabilities? Are there any international sanctions and what do they restrict?

Additionally, examine societal characteristics:

- What is the baseline digital and security literacy?
- How does knowledge sharing take place within the group? How do members create trust?
- What is "common security knowledge" within the group?

Given the above, explore how technology responds to a number of hard technical challenges and how users adapt either the technology or their behaviors to fulfill their threat models, or whether their threat models are sufficed. Are their adoptions or adaptations sufficient from a security expert's point of view? Consider the hard technological problems presented in Section V: misinformation; physical device security; and confidentiality, integrity, and availability over an adversarially controlled network.

Such structured questions uncover *fundamental tensions* and *design principles* that may benefit further user groups (e.g., a robust connection through a mesh networking mode, device sanitization on demand or with an emergency-triggered authentication). We observe that the generalization of design recommendations often runs into fundamental tensions, and we encourage designers and researchers to consider how these fundamental tensions can drive innovative solutions, and, in contrast, how design principles might lead to fundamental tensions, in part by asking: what makes it difficult to generalize this solution for other user groups? What solutions would work for others that would not work for this group?

Finally, we encourage the study of diverse populations worldwide in order to reveal further key factors, tensions, and design principles. Particularly, more work is needed to study, understand, and anticipate how user groups, such as vulnerable ones, are influenced toward different uses of technology, and ultimately, how technology can better support those advocating for fairness and social good.

Acknowledgements

We thank Ayden Baily, Kaiming Cheng, Yousif Dafalla, Theo Gregersen, Maggie Jiang, David Kohlbrenner, Karl Koscher, Kentrell Owens, Franziska Roesner, Alison Simko, Anna Kornfeld Simpson, Miranda Wei, Karl Weintraub, Yasir Zaidan, and Eric Zeng for their valuable feedback on a draft of our paper. We are also very grateful to Tobias Fiebig for shepherding this paper, and to our anonymous reviewers for their thoughtful and constructive criticism, which made this paper much better.

This work was supported in part by the U.S. NSF under Awards 1565252 and 1915824 and the UW Tech Policy Lab, which receives support from: the William and Flora Hewlett Foundation, the John D. and Catherine T. MacArthur Foundation, Microsoft, the Pierre and Pamela Omidyar Fund at the Silicon Valley Community Foundation.

References

[1] Z. Tufekci. *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press, 2017.

[2] Human Rights Watch Org. *Sudan*. https://www.hrw.org/africa/sudan. [Accessed Sep. 2020].

[3] Uptodown App Store. *Firechat*. https://firechat.en.uptodown.com/android. [Accessed Sep. 2020].

[4] Apple Inc. *Use Screen Time on your iPhone, iPad, or iPod touch*. https://support.apple.com/en-us/HT208982. [Accessed Sep. 2020].

[5] ASUS Inc. *[ZenFone] What is Twin Apps and how does it work?* https://www.asus.com/support/FAQ/1032388/. [Accessed Sep. 2020].

[6] E. A. Hirsch. "Contestational design: Innovation for political activism". PhD thesis. MIT, 2008.

[7] U.S. Central Intelligence Agency. *The World Factbook, Africa: Sudan*. https://www.cia.gov/library/publications/resources/the-world-factbook/geos/su.html. [Accessed Sep. 2020].

[8] Human Rights Watch Org. *Sudan: End Censorship and Repression*. https://www.hrw.org/news/2009/02/18/sudan-end-censorship-and-repression. [Accessed Sep. 2020].

[9] U.S. Dep. of State. *State Sponsors of Terrorism*. https://www.state.gov/state-sponsors-of-terrorism/. [Accessed Sep. 2020].

[10] A. M. A. Musa and L. K. Majzoub. *The State of Sudan Digital 2019*. https://sudandigital.com/portfolio/sudan-report-2019-the-state-of-sudan-digital/. [Accessed Sep. 2020].

[11] S. Kemp. *Digital 2018: Sudan*. https://datareportal.com/reports/digital-2018-sudan?rq=sudan. [Accessed Aug. 2020].

[12] Radio Dabanga. *Google apps available in Sudan as US eases sanctions*. https://www.dabangasudan.org/en/all-news/article/google-apps-available-in-sudan-as-us-eases-sanctions. [Accessed Aug. 2020].

[13] Google LLC. *Supported locations for distribution to Google Play users*. https://support.google.com/googleplay/android-developer/table/3541286?hl=en. [Accessed Sep. 2020].

[14] Reuters News. *Residual U.S. sanctions keep Sudan's economy in chokehold*. https://www.reuters.com/article/sudan-economy/residual-u-s-sanctions-keep-sudans-economy-in-chokehold-idUSL5N1ZZ2NS. [Accessed Sep. 2020].

[15] Z. Tufekci. "Social Movements and Governments in the Digital Age: Evaluating a Complex Landscape". In: *Journal of International Affairs* 68 (2014). SIPA Columbia University.

[16] R. Abbas. *How an illegal Sudanese union became the biggest threat to Omar Al Bashir's 29-year reign*. https://www.thenational.ae/world/africa/how-an-illegal-sudanese-union-became-the-biggest-threat-to-omar-al-bashir-s-29-year-reign-1.819159. [Accessed Sep. 2020].

[17] NetBlocks Org. *Study shows extent of Sudan internet disruptions amid demonstrations*. https://netblocks.org/reports/study-shows-impact-of-sudan-internet-disruptions-amid-demonstrations-qr8Vj485. [Accessed Sep. 2020].

[18] R. Abbas. *In Sudan, neighbourhoods mobilised against Al-Bashir*. https://www.aljazeera.com/news/2019/05/sudan-neighbourhoods-mobilised-al-bashir-190506182950504.html. [Accessed Sep. 2020].

[19] J. Patinkin. *Inside the Massive Sit-In Fueling Sudan's Revolution*. https://www.vice.com/en_us/article/7xg89g/inside-the-massive-sit-in-fueling-sudans-revolution. [Accessed Sep. 2020].

[20] Amnesty International Org. *Sudan: All security agencies that attacked protesters must be held to account*. https://www.amnesty.org/en/latest/news/2020/03/sudan-all-security-agencies-that-attacked-protesters-must-be-held-to-account/. [Accessed Sep. 2020].

[21] R. Clayton, S. J. Murdoch, and R. N. Watson. "Ignoring the great firewall of China". In: *International Workshop on Privacy Enhancing Technologies*. Springer. 2006.

[22] J. R. Crandall, E. Barr, D. Zinn, R. East, and M. Byrd. "ConceptDoppler: A Weather Tracker for Internet Censorship". In: *Proc. 14th ACM SIGSAC CCS*. Nov. 2007.

[23] J.-P. Verkamp and M. Gupta. "Inferring Mechanics of Web Censorship Around the World". In: *Proc. 2nd USENIX FOCI Workshop*. Aug. 2012.

[24] P. Gill, M. Crete-Nishihata, J. Dalek, S. Goldberg, A. Senft, and G. Wiseman. "Characterizing web censorship worldwide: Another look at the opennet initiative data". In: *Transactions on the Web (TWEB)* 9.1 (2015). ACM.

[25] G. Gebhart and T. Kohno. "Internet censorship in Thailand: User practices and potential threats". In: *Proc. 2nd IEEE EuroS&P*. Apr. 2017.

[26] M. M. Boire, J. Dalek, S. McKune, M. Carrieri, M. Crete-Nishihata, R. Deibert, S. O. Khan, J. Scott-Railton, and G. Wiseman. *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*. https://citizenlab.ca/wp-content/uploads/2015/03/Planet-Blue-Coat-Mapping-Global-Censorship-and-Surveillance-ToolsPlanet-Blue-Coat-Mapping-Global-Censorship-and-Surveillance-Tools.pdf. [Accessed Dec. 2020].

[27] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescapé. "Analysis of country-wide internet outages caused by censorship". In: *Proc. 11th Internet Measurement Conference (IMC)*. Nov. 2011.

[28] M. Richtel. *Egypt Cuts Off Most Internet and Cell Service*. https://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html. [Accessed Sep. 2020].

[29] J. D. Sutter. *Libya faces internet blackouts amid protests*. http://www.cnn.com/2011/TECH/web/02/22/libya.internet/index.html. [Accessed Sep. 2020].

[30] E. Flock. *Syria Internet Services Shut Down as Protesters Fill Streets*. https://www.washingtonpost.com/blogs/blogpost/post/syria-internet-services-shut-down-as-protesters-fill-streets/2011/06/03/AGtLwxHH_blog.html. [Accessed Sep. 2020].

[31] L. H. Newman. *Belarus Has Shut Down the Internet Amid a Controversial Election*. https://www.wired.com/story/belarus-internet-outage-election/. [Accessed Aug. 2020].

[32] S. Getachew. *The internet is back on in Ethiopia but there's every chance it'll be off again soon*. https://qz.com/africa/

1884387/ethiopia-internet-is-back-on-but-oromo-tensions-remain/. [Accessed Aug. 2020].

[33] J. Hsu. *How India, the World's Largest Democracy, Shuts Down the Internet*. https://spectrum.ieee.org/tech-talk/telecom/internet/how-the-worlds-largest-democracy-shuts-down-the-internet. [Accessed Aug. 2020].

[34] L. H. Newman. *How the Iranian Government Shut Off the Internet*. https://www.wired.com/story/iran-internet-shutoff/. [Accessed Aug. 2020].

[35] R. Mahomed and R. Bendimerad. *Venezuela shuts down Internet amid protests*. https://www.aljazeera.com/news/2019/01/venezuela-shuts-internet-protests-190124124829727.html. [Accessed Aug. 2020].

[36] A. Parker, V. Kantroo, H. R. Lee, M. Osornio, M. Sharma, and R. Grinter. "Health promotion as activism: building community capacity to effect social change". In: *Proc. 2012 ACM SIGCHI CHI*. May 2012.

[37] S. Consolvo, K. Everitt, I. Smith, and J. A. Landay. "Design requirements for technologies that encourage physical activity". In: *Proc. 2006 ACM SIGCHI CHI*. Apr. 2006.

[38] A. Grimes and R. E. Grinter. "Designing persuasion: Health technology for low-income African American communities". In: *Proc. International Conference on Persuasive Technology*. Springer. 2007.

[39] J. P. Dimond. "Feminist HCI for real: Designing technology in support of a social movement". PhD thesis. Georgia Institute of Technology, 2012.

[40] C. Fiesler, S. Morrison, and A. S. Bruckman. "An archive of their own: A case study of feminist HCI and values in design". In: *Proc. 2016 ACM SIGCHI CHI*. May 2016.

[41] B. Tadic, M. Rohde, V. Wulf, and D. Randall. "ICT use by prominent activists in Republika Srpska". In: *Proc. 2016 ACM SIGCHI CHI*. May 2016.

[42] S. Gaw, E. W. Felten, and P. Fernandez-Kelly. "Secrecy, flagging, and paranoia: adoption criteria in encrypted email". In: *Proc. 2006 ACM SIGCHI CHI*. Apr. 2006.

[43] G. Lotan, E. Graeff, M. Ananny, D. Gaffney, I. Pearce, et al. "The Arab Spring—the revolutions were tweeted: Information flows during the 2011 Tunisian and Egyptian revolutions". In: *International journal of communication* 5 (2011).

[44] P. N. Howard, A. Duffy, D. Freelon, M. M. Hussain, W. Mari, and M. Maziad. "Opening closed regimes: what was the role of social media during the Arab Spring?" In: *Available at SSRN 2595096* (2011).

[45] E. Stepanova. "The role of information communication technologies in the 'Arab Spring'". In: *Ponars Eurasia* 15.1 (2011).

[46] L. Simko, A. Lerner, S. Ibtasam, F. Roesner, and T. Kohno. "Computer Security and Privacy for Refugees in the United States". In: *Proc. 39th IEEE S&P*. May 2018.

[47] T. Guberek, A. McDonald, S. Simioni, A. H. Mhaidli, K. Toyama, and F. Schaub. "Keeping a low profile? Technology, risk and privacy among undocumented immigrants". In: *Proc. 2018 ACM SIGCHI CHI*. Apr. 2018.

[48] A. Dhoest. "Digital (dis) connectivity in fraught contexts: The case of gay refugees in Belgium". In: *European Journal of Cultural Studies* 23.5 (2020).

[49] O. Portillo. "To Liberate and Lament: The Duality of Digital Culture and Chechnya's Concentration Camps for Russian LGBT Citizens". In: *EXCLAMATION* (June 2018).

[50] M. Panzica. "A Difficult Line to Walk: NGO and LGBTQ+ Refugee Experiences with Information and Communications Technology (ICT) in Canada". MA thesis. Dalhousie University, 2020.

[51] R. Dekker, G. Engbersen, J. Klaver, and H. Vonk. "Smart refugees: How Syrian asylum migrants use social media information in migration decision-making". In: *Social Media+ Society* 4.1 (2018).

[52] T. Hirsch and J. Henry. "TXTmob: Text messaging for protest swarms". In: *ACM SIGCHI CHI*. Abstract. Apr. 2005.

[53] T. Hirsch. "Feature Learning from activists: Lessons for designers". In: *Interactions* 16.3 (2009). ACM.

[54] Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai, and A. Yamada. "Self-confidence trumps knowledge: A cross-cultural study of security behavior". In: *Proc. 2017 ACM SIGCHI CHI*. May 2017.

[55] S. Bellman, E. J. Johnson, S. J. Kobrin, and G. L. Lohse. "International differences in information privacy concerns: A global survey of consumers". In: *The Information Society* 20.5 (2004). Taylor & Francis.

[56] H. Cho, M. Rivera-Sánchez, and S. S. Lim. "A multinational study on online privacy: Global concerns and local responses". In: *New Media & Society* 11.3 (2009). SAGE.

[57] Y. Rashidi, K. Vaniea, and L. J. Camp. "Understanding Saudis' privacy concerns when using WhatsApp". In: *Proc. 2016 USEC Workshop*. Feb. 2019.

[58] J. Reichel, F. Peck, M. Inaba, B. Moges, B. S. Chawla, and M. Chetty. "'I have too much respect for my elders': Understanding South African Mobile Users' Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp". In: *Proc. 29th USENIX Security*. Aug. 2020.

[59] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner. "Investigating the computer security practices and needs of journalists". In: *Proc. 24th USENIX Security*. Aug. 2015.

[60] C. Chen, N. Dell, and F. Roesner. "Computer security and privacy in the interactions between victim service providers and human trafficking survivors". In: *Proc. 28th USENIX Security*. Aug. 2019.

[61] E. M. Rogers. *Diffusion of innovations*. Simon & Schuster Publishing, 2010.

[62] R. Rice and K. E. Pearce. "Divide and diffuse: Comparing digital divide and diffusion of innovations perspectives on mobile phone adoption". In: *Mobile Media & Communication* 3 (2015). SAGE.

[63] S. Das, A. D. Kramer, L. A. Dabbish, and J. I. Hong. "The role of social influence in security feature adoption". In: *Proc. 18th ACM SIGCHI CSCW*. Mar. 2015.

[64] S. Das, L. A. Dabbish, and J. I. Hong. "A typology of perceived triggers for end-user security and privacy behaviors". In: *Proc. 15th SOUPS*. Aug. 2019.

[65] R. Wash. "Folk models of home computer security". In: *Proc. 6th SOUPS*. July 2010.

[66] E. Rader, R. Wash, and B. Brooks. "Stories as informal lessons about security". In: *Proc. 8th SOUPS*. July 2012.

[67] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. "Obstacles to the adoption of secure communication tools". In: *Proc. 38th IEEE S&P*. May 2017.

[68] J. Lynch. *Women fueled Sudan's revolution, but then they were pushed aside*. https://www.independent.co.uk/news/world/africa/sudan-revolution-women-uprising-democratic-transition-army-bashir-a9038786.html. [Accessed Aug. 2020].

[69] L. M. Tanczer. "Hacktivism and the male-only stereotype". In: *New Media & Society* 18.8 (2016). SAGE.

[70] L. G. Stewart, A. Arif, and K. Starbird. "Examining trolls and polarization with a retweet network". In: *Proc. 2018 ACM MIS2 Workshop*. Feb. 2018.

[71] M. Suliman. *As Sudan transitions to democracy, urgent reforms must tackle disinformation*. https://advox.globalvoices.org/2019/10/04/as-sudan-transitions-to-democracy-urgent-reforms-must-tackle-disinformation/. [Accessed Aug. 2020].

[72] K. Albaih. *How WhatsApp is fuelling a 'sharing revolution' in Sudan*. https://www.theguardian.com/world/2015/oct/15/sudan-whatsapp-sharing-revolution. [Accessed Sep. 2020].

[73] C. Geeng, S. Yee, and F. Roesner. "Fake News on Facebook and Twitter: Investigating How People (Don't) Investigate". In: *Proc. 2020 ACM SIGCHI CHI*. May 2020.
[74] A. E. Kramer. *Ukraine's opposition says government stirs violence*. https://www.nytimes.com/2014/01/22/world/europe/ukraine-protests.html. [Accessed Sep. 2020].
[75] D. Goodin. *Chinese bank requires foreign firm to install app with covert backdoor*. https://arstechnica.com/information-technology/2020/06/chinese-bank-requires-foreign-firm-to-install-app-with-covert-backdoor/. [Accessed Sep. 2020].
[76] M. Namara, D. Wilkinson, K. Caine, and B. P. Knijnenburg. "Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology". In: *Proceedings on Privacy Enhancing Technologies* 2020.1 (2020). Sciendo.
[77] M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson. "An analysis of the privacy and security risks of android VPN permission-enabled apps". In: *Proc. 16th Internet Measurement Conference (IMC)*. Nov. 2016.
[78] M. R. Albrecht, J. Blasco, R. B. Jensen, and L. Marekova. *Mesh Messaging in Large-scale Protests: Breaking Bridgefy*. https://martinralbrecht.files.wordpress.com/2020/08/bridgefy-abridged.pdf. [Accessed 9-2020].
[79] K. Busse, J. Schäfer, and M. Smith. "Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice". In: *Proc. 15th SOUPS*. Aug. 2019.
[80] I. Ion, R. Reeder, and S. Consolvo. ""... no one can hack my mind": Comparing Expert and Non-Expert Security Practices". In: *Proc. 11th SOUPS*. July 2015.
[81] M. Varner. *How Do I Prepare My Phone for a Protest?* https://themarkup.org/ask-the-markup/2020/06/04/how-do-i-prepare-my-phone-for-a-protest. [Accessed Aug. 2020].
[82] The Guardian Newspaper. *WhatsApp design feature means some encrypted messages could be read by third party*. https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages. [Accessed Aug. 2020].
[83] Z. Tufecki. *In Response to Guardian's Irresponsible Reporting on WhatsApp: A Plea for Responsible and Contextualized Reporting on User Security*. http://technosociology.org/?page_id=1687. [Accessed Aug. 2020].
[84] P. Mozur. *In Hong Kong Protests, Faces Become Weapons*. https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html. [Accessed Sep. 2020].
[85] Dabanga Radio. *Google apps available in Sudan as US eases sanctions*. https://www.dabangasudan.org/en/all-news/article/google-apps-available-in-sudan-as-us-eases-sanctions. [Accessed Aug. 2020].
[86] U.S. Office of Foreign Assets Control. *Sudan Sanctions Program*. https://www.treasury.gov/resource-center/sanctions/Programs/Documents/sudan.pdf. [Accessed Aug. 2020].
[87] K. Howell. *The Fifth Amendment, Decryption and Biometric Passcodes*. https://www.lawfareblog.com/fifth-amendment-decryption-and-biometric-passcodes. [Accessed Aug. 2020].
[88] J. Meyers. *Quickly Disable Fingerprints & Smart Lock in Android Pie for Extra Security*. https://android.gadgethacks.com/how-to/quickly-disable-fingerprints-smart-lock-android-pie-for-extra-security-0183475/. [Accessed Aug. 2020].
[89] Sudanese Professionals Association. *About Us*. https://www.sudaneseprofessionals.org/en/about-us/. [Accessed Sep. 2020].
[90] Amnesty International Org. *Agents of fear: the National Security Service in Sudan*. https://www.amnesty.org/download/Documents/36000/afr540102010en.pdf. [Accessed Sep. 2020].
[91] Al Jazeera. *Who are Sudan's RSF and their commander Hemeti?* https://www.aljazeera.com/news/2019/06/sudan-rsf-commander-hemeti-190605223433929.html. [Accessed Sep. 2020].
[92] A. Shahine and G. Carey. *U.A.E. Supports Saudi Arabia Against Qatar-Backed Brotherhood*. https://www.bloomberg.com/news/articles/2014-03-09/u-a-e-supports-saudi-arabia-against-qatar-backed-brotherhood. [Accessed Sep. 2020].
[93] BBC News. *Egypt's Muslim Brotherhood declared 'terrorist group'*. https://www.bbc.com/news/world-middle-east-25515932. [Accessed Sep. 2020].
[94] S. Zunes. *Sudan's Democratic Revolution: How They Did It*. https://www.nonviolenceinternational.net/zunes_on_sudan. [Accessed Sep. 2020].
[95] M. Hassan and A. Kodouda. "Sudan's Uprising: The Fall of a Dictator". In: *The Journal of Democracy* 30.4 (Oct. 2019). Johns Hopkins University Press.
[96] European Council on Foreign Relations. *Bad company: How dark money threatens Sudan's transition*. https://www.ecfr.eu/publications/summary/bad_company_how_dark_money_threatens_sudans_transition. [Accessed Sep. 2020].

APPENDIX

Appendix A – Interview Protocol

As the interviews were semi-structured, we worded questions in different ways in each interview. While we covered the topics listed here, we also asked other questions.

Consent process:

- Brief introductions of researchers, recap. research goals
- Verbal summary of the consent form:
  - Every question is voluntary
  - We'd like to record because it makes it easier on us
  - If recording, you can ask us to turn it off at any time
- Any questions before we begin?

Post consent process, pre audio recording:

- Remind participants: don't share anything you don't want to share *and* we will not publish any PII
- Ask them (again) whether they consent to recording

Interview questions: The following list is our short-form interview protocol, which we had in front of us during each interview. There were 7 main topics. Sub questions are *sample* questions; we did not ask all of these questions in a single interview. We typically started with 1) and ended with 7), but the order of the rest varied based on what felt comfortable during the interview.

1) **News and information sharing.**
   - How did you follow the news about the revolution?
   - What websites/apps were your main news sources?
   - Who did you get news from? Where did they get their news? Did you talk to them in person or online?
   - What kind of news did you seek?
   - Was there anything in specific where you had a hard time finding enough information about? How did you know whether to trust the information you received?
2) **Role of technology in protecting protesters.**
   - Any non-tech advice for evading arrests, tear gas, etc.?
   - Any tech advice? (may include: burner phone, burner SIM, VPN, proxy, Tor, alternate online accounts)

- Were you given any advice that you did not follow?
- Do you wish you'd been given any other advice? Did you feel the need to implement more measures than advised?
- Did you ever feel like technology put you in danger?

3) **Learning / adoption / onboarding.**
   - How did you learn the advice that we just talked about? In general, from a person or by yourself?
   - For the guidelines/advice: Did you follow that advice? Was it hard? Easy? If not, why not?
   - Who gave you that advice? How did you meet them? Why did you trust them? How technically knowledgeable are they? How did you communicate with them? How frequently? Did you have to take any precautions?
   - Was the instruction one-on-one or were others there? Was it a formal setting, like a class, or an informal setting?
   - Teaching: Did you taught anyone else do [*fill in*]?
4) **Sit in.**
   - April - June, in which ways did you use technology?
   - Who was your adversary?
   - Any things you stopped doing because you felt safe?
5) **Internet blackout.**
   - During the internet blackout in June 2019, did you continue to use technology for activism? For the things that stopped working, what did you do instead?
   - Because of the very limited internet access, did that force you as activists to share accounts, devices, etc.?
   - As a whole, how do you think the activism community changed their use of technology during the blackout?
6) **Threat model.**
   - What are/were the dangers you are/were facing as an activist? Who is an adversary to you?
   - If they mention the government as an adversary: what arm(s) of the government might be harmful? For each: what are their capabilities? What do you use to defend against them? Is that enough to protect you?
7) **Final / meta questions.**
   - Is there anything else you want to tell us?
   - Is there anything we should have asked but we didn't?
   - Do you have any questions for us?
   - Can you refer us to more activists?

Appendix B – Codebook

High-level Code	Subcodes	
Threat model and threats: *Refers to the activists' perceptions of who their adversaries are and what their capabilities are*	Risk assessment Changing adversaries Adversary Sudanese government capabilities Outsourced capabilities	Trigger for change in threat model Trusted party Asset Foreign government capabilities
Adoption of technology and behaviors: *Refers to activists' behaviors towards adoption and the challenges they faced*	Learning process Choice not to adopt Discontinuing use	Trigger for adoption Challenges / barriers Teaching
Mis-/disinformation security needs & practices: *Refers to activists' needs and practices toward information verification*	Building trust Making information verifiable	Sources of trust Verification of information
Security needs & practices towards plausible deniability: *Refers to activists' needs and practices that provide plausible deniability upon arrest*	Built-in security mechanism Deny self access to info / regular device Go analog	Ad hoc strategy Deny others access to info Expect others to do something
Security needs & practices against surveillance: *Refers to participants' needs and practices to defend against electronic surveillance*	Built-in security mechanism Deny self access to info / regular device Go analog	Ad hoc strategy Deny others access to info Expect others to do something
Physical security needs & practices: *Refers to security practices to maintain physical security*	*no subcodes*	
Offensive security practices: *Refers to offensive practices by activists (as opposed to defensive)*	*no subcodes*	
Censorship and blackout security needs & practices: *Refers to the security needs and practices of activists during the social media blockade and internet blackout*	Blackout Social media blockade Other	
News consumption operational needs & goals: *Refers to participants' practices with regards to news consumption*	Platform Type of news	News source
Communications operational needs & goals: *Refers to participants' practices with regards to communications and news dissemination*	*subcodes were specific platforms*	
Comparisons: *Refers to comparisons between previous protests/revolutions or the different technologies being used*	Compare to previous protests / revolution	Preferred platform X to platform Y
Participant's overall experience: *Refers to anything not covered above about the participant's role in the revolution*	Was in Sudan during the revolution Role during revolution	Not in Sudan during the revolution Role of diaspora

Table I

THIS TABLE CAPTURES OUR CODEBOOK. WE SHOW EACH HIGH LEVEL CODE AND ITS SUBCODES. SUBSUBCODES ARE NOT INCLUDED (AS IN [58]) BECAUSE THEY WERE USED ONLY FOR GIVING COUNTS OF SPECIFIC ACTIONS OR THREAT MODELS (E.G., THE SUBSUBCODE 'ELECTRONIC SURVEILLANCE', WHICH IS NOT SHOWN, APPEARED UNDER 'THREAT MODEL AND THREATS—SUDANESE GOVERNMENT CAPABILITIES'; WE USED IT TO REPORT ON HOW MANY PARTICIPANTS MENTIONED ELECTRONIC SURVEILLANCE AS A CAPABILITY OF THE SUDANESE GOVERNMENT).

Appendix C – Glossary of State and Non-state Actors

Sudanese Professional Association (SPA)	**Revolutionary force (ally)**: The SPA is an umbrella organization for a number of professional associations—e.g. Teachers' Committee, Central Committee of Sudanese Doctors, etc [89]—that helped publicly organize protests and push forward the revolution. The SPA was a trusted source of news throughout the revolution.
Neighborhood resistance committees	**Revolutionary force (ally)**: Neighborhood committees were decentralized local committees formed during or sometimes even before the revolution [18]. They communicated with the SPA and each other.
Transitional civilian government	**Revolutionary force (ally):** The SPA and a number of opposition political parties coalesced to form a body known as the Freedom of Forces and Change. This body was the political representation of the activism community and further helped negotiate an agreement with the Transitional Military Council to form a transitional civilian government that continues to lead the country in a democratic transition that began in July of 2019.
National Intelligence and Security Service (NISS)	**Government (adversary)**: The NISS is an intelligence unit that served as a "secret police" under Elbashir's regime. The NISS was granted extensive authority by the government and was responsible of a lot of human rights abuses throughout Elbashir's rule [90]. According to our participants, the NISS was heavily involved in repressing protesters.
Rapid Support Forces (RSF)	**Government (adversary)**: The RSF are armed forces originally operating under Elbashir's government with a history of violence and human rights violations both prior to and during the revolution [91]. The RSF coalesced with the state military to form the Transitional Military Council in April 2019.
Sudanese Military	**Government (adversary)** (during sit in): The official military of the Sudanese state. In the beginning, many did not consider them an adversary; however, they started to turn adversarial during the sit in, and following the crackdown on protesters on the 3rd of June Khartoum massacre [20].
Police	**Government (adversary):** Regional / city police that were arresting protesters. However, sometimes participants used the word "police" to describe units from the NISS who were arresting protesters as well.
Transitional Military Council (TMC)	**Government (adversary)** (during sit in): The TMC was formed following the fall of Elbashir's regime to lead the country and occupy the power vacuum. The council consisted of the state military and the Rapid Support Forces (RSF). During this period the NISS was stripped of its authority and remained idle.
Saudi Arabia	**Foreign power (adversary)**: The government of Saudi Arabia was historically a supporter of Elbashir's regime. In the early days of the revolution, and as protests gained momentum, Saudi Arabia reinstated its support for the Sudanese government and for stability in the region. After the fall of the regime in April, the government of Saudi Arabia became an ally to the Transitional Military Council (TMC), pledging millions of dollars in support of the council and pushing towards a military rule of the country.
United Arab Emirates (UAE)	**Foreign power (adversary)**: The UAE was among a number of foreign powers supporting the Sudanese government as the protests erupted by helping the Sudanese economy. They also supported the TMC along with Saudi Arabia by providing mostly financial support.
Qatar	**Foreign power (adversary)**: In January of 2019, the Emir of Qatar emphasized their support for Elbashir's rule.
Egypt	**Foreign power (adversary)**: Egypt was a strong regional ally of Elbashir's government throughout the revolution.
Muslim Brotherhood	**Domestic and foreign movement:** The Muslim Brotherhood is a multi-national political group backed by Turkey and Qatar, and considered as terrorists by others, including the UAE, Saudi Arabia, and Egypt [92, 93].

Table II

THIS GLOSSARY SUMMARIZES THE ROLES OF THE MAIN ACTORS (ENTITIES) MENTIONED IN THE MAIN CONTENT OF THE PAPER. BOLD TEXT INDICATES THE WAY THESE ACTORS WERE PERCEIVED BY OUR PARTICIPANTS. THIS IS INTENDED TO SUPPORT THE READER THROUGHOUT THE PAPER BUT IS IN NO WAY A COMPLETE REPRESENTATION OF THE ACTORS IN THE SUDANESE REVOLUTION. WE INVITE INTERESTED READERS TO BEGIN WITH [94, 95, 96] FOR MORE INFORMATION ABOUT THE FORCES THROUGHOUT THE REVOLUTION.