Security & Privacy Practices and Threat Models of Activists During a Political Revolution

Alaa Daffalla

B.S. Electrical & Electronic Engineering, University of Khartoum, 2017

Submitted to the graduate degree program in Electrical Engineering and Computer Science Department and the Graduate Faculty of the University of Kansas in partial fulfillment of the requirements for the degree of Masters of Science in Computer Science.

Chair: Alexandru G. Bardas

Fengjun Li

Bo Luo

Date defended: May 7th, 2021

The Thesis Committee for Alaa Daffalla certifies
that this is the approved version of the following thesis :

Security & Privacy Practices and Threat Models of Activists During a Political Revolution

Chair: Alexandru G. Bardas

Date approved: May 7th, 2021

Abstract

Activism is a universal concept that has often played a major role in putting an end to injustices and human rights abuses globally. Political activism in specific is a modern day term coined to refer to a form of activism in which a group of people come into collision with a more omnipotent adversary - national or international governments - who often has a purview and control over the very telecommunications infrastructure that is necessary for activists in order to organize and operate. As technology and social media use have become vital to the success of activism movements in the twenty first century, our study focuses on surfacing the technical challenges and the defensive strategies that activists employ during a political revolution. We find that security and privacy behavior and app adoption is influenced by the specific societal and political context in which activists operate. In addition, the impact of a social media blockade or an internet blackout can trigger a series of anti-censorship approaches at scale and cripple activist's technology use. To a large extent the combination of low tech defensive strategies employed by activists were sufficient against the threats of surveillance, arrests and device confiscation. Throughout our results we surface a number of design principles but also some design tensions that could occur between the security and usability needs of different populations. And thus, we present a set of observations that can help guide technology designers and policy makers.

Acknowledgements

I would like to start by thanking my family and friends for the support and time they have afforded me to work on this project. I would also like to thank my advisor Professor Alexandru Bardas at the University of Kansas for his continuous guidance and support throughout this academic journey. Finally, I would like to extend my acknowledgement to my collaborator in this work Lucy Simko, a PhD student at the University of Washington and her advisor Professor Tadayoshi Kohno.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The world is increasingly witnessing disruptive and sudden changes that forces people to embrace a temporary state of being. This could be as a result of environmental, political or economic factors. Many groups or populations surface amidst such world changes and need to make and constantly re-evaluate adaptations to a new form of living that would often involve some sort of collision with natural or human factors and artifacts. For example, recent immigrants facing persecution in their country of refuge. Or disruptive environmental phenomena that would lead to the displacement of groups of people. While technology is becoming more pervasive in the current day and age these populations will continue to use technology in their everyday lives and throughout their transition. There is little work in the computer security literature looking into the security and privacy practices and needs of populations or demographics that undergo severe disruptive changes and continue to use technology throughout their temporary state of existence to achieve individual or group goals. Some of the previous work looked into the study of vulnerable populations like refugees [2], survivors of human trafficking [3] and victims of intimate partner violence [4]. Despite the expanding body of work on security and privacy practices and needs of different populations, non WEIRD (Western, Educated, Industrialized, Rich, Democratic) technology users remain to be vastly underrepresented.

One user group, is the group of activists which forms as a result of political or social resistance and for political, economic or social gains. Furthermore, activism has become increasingly decentralized and democratized driven by ubiquity of social media and smartphones. However, with the increase in technology comes significant power *over* that technology and telecommunications infrastructure by the adversary. Political revolution pits people, who are often not security experts,

against powerful and resourceful nation states, yet, in some cases, the people are able to achieve their goals both *because of* their use of technology and *despite* it. For example, the 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. Indeed, there have been numerous efforts focused on computer security and privacy for specific populations (see Section 2.2 for an overview). However, political activists under an oppressive regime have not yet been extensively studied by the computer security community. This absence of prior studies is understandable, as there are only limited opportunities to study activists during revolutions. Further, any research on the needs and practices of activists during a revolution would benefit from deep knowledge about the cultural and contextual aspects of that country.

In this work, we interview 13 of the political activists who were active during the 2018-2019 revolution in Sudan because we think it is fundamentally important for the computer security and privacy research community to get a deeper understanding of the computer security and privacy practices, needs, risks and challenges that face activists when they collide with a more powerful and in most cases an oppressive regime. Furthermore, it is increasingly important that future technology is designed with the purview that the design could at best support populations of activists operating in spaces where an adversary has control over their communications and the very infrastructure that is required to establish these communications. This understanding is also key to reason about issues that are likely to happen in the future in terms of political revolutions or unrest that can cause or has caused users to use technology in ways for which the technology has not been designed for. Our work tries to address all of these gaps and provide a foundation upon which further studies can be conducted. As a lead into our research questions and an overview of some characteristics of the activists' population that we formulated when conducting our interviews and to understand more about their goals during a political revolution or in order to achieve political change we find that:

- The community of activists is most probably formed as a result of the assimilation of individuals who come from different backgrounds, professions, ages and gender. This means that there is a huge diversity among the activists' community in terms of literacy and in terms of their activism and organizational experience and all of these differences influence and dictate the use of technology among the community as we discuss later within the results section.

- News sharing within the activists community is of utmost importance to keep up with local, national and international news. In addition, the sharing of news is vital to the activists' organizational efforts in that it helps to shape movement, decisions and protests locations.

- For the activism movement to continue and gain traction and more followers among its ranks activists must continue to organize, attend and publicize protests throughout the duration of the movement in order to achieve any kind of political gains or influence political change.

- Activists' groups are always changing with a lot of members both leaving (due to arrests or the fear of arrests) and a lot of new members joining. A lot of new members onboard onto activism and tend to adopt the behavior, practices and technology use of the group. As a result, trust among the activists' community is of utmost importance and hence a number of different strategies are usually required to vet and recruit activists.

In order for activists to achieve their political gains they must contend with their adversaries who have the power and capability to control or have influence over the infrastructure upon which the activists rely. In addition, the threats that the activists face could be technological (electronic surveillance and social media blockades) or they might be physical (for example: physical surveillance, arrests, violence and tear gas). With this background information in mind we present our work that tries to answer some of the research questions below:

- **What was the threat landscape during the revolution?** In specific, in chapter 4 we discuss in details what were the threats and risks that the majority of our participants perceived. Furthermore, we also try to understand more about activists threat models and the perceived adversaries.

- **What were the activists security practices and defensive technology use like during the revolution?** We aimed to get a deeper technical understanding of the activists' technology practices (what apps they tend to use?, why these apps and not others?, how do they stay secure while using these apps?)

- **How did technology design support or hinder activists' efforts to achieve their goals?** We tried to understand more about the usability of tech and app design for activists when communicating, organizing and protesting. For example: were the security controls within some apps usable and helped activists stay secure? What tensions arise when activists use technology in ways for which it wasn't designed for? And what new technology use cases were introduced as a result of this?

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, which may have strengthened their security measures against the Sudanese government.

- **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 [5] proved highly unsuccessful. Adopting a more secure SMS app such as Signal encountered important limitations and risks (e.g., the existence of a fake Signal app) while group adoption of mesh networking apps such as Firechat 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 or Android's TwinApps [6] 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** [7] **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.

At a high level, our findings suggest that understanding the political and societal context of specific user groups and populations forms a backdrop upon which further understanding of security and privacy practices and mental models is based and built. So, we come up with a set of structured questions or recommendations that can help guide future technology designers, policy makers and researchers when working with vulnerable or non-WEIRD populations.

Chapter 2

Background and Related Work

2.1 Background on Sudan

Sudan is a country in North Eastern Africa with an estimated population of 45 million as of July 2020 [8]. 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 [9] and censorship of print and electronic media [10]. In 1993, Sudan was designated a state sponsor of terrorism by the United States of America (US) [11].

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 [8]. Android phones are the most popular smartphones in Sudan, followed by iOS devices [12], 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 [13]. 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 [14]. However, access to paid apps/features remains restricted [15].

In 2018, due to the dire economic situation in the country, a wave of protests erupted and led to the 2018 - 2019 revolution [16]. Figure 2.1 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

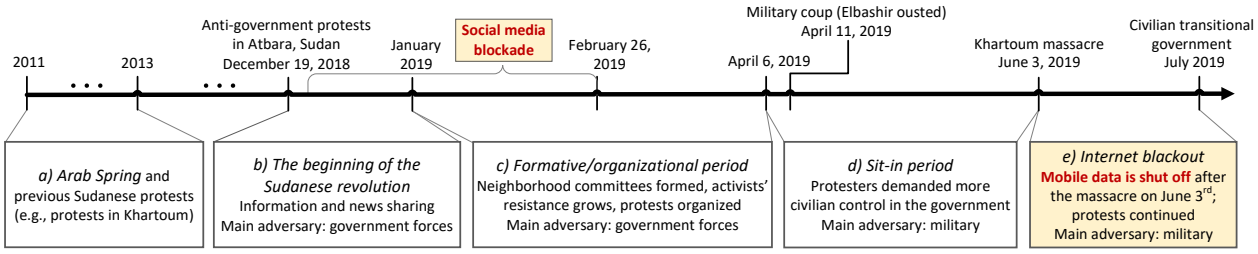

Figure 2.1: A timeline of the major events during the 2018-2019 revolution in Sudan

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). As shown in Figure 2.1, the major events leading 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 [17, 18].

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 source of news [19]. 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 [20], blocking measures were decentralized and carried out at the discretion of the telecommunication operators.

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

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 [21]. 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 [20]. 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 [22]. 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 [23]. 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 [8]. 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.

2.2 Related Work

Our work is informed by prior work on activism, security and privacy for specific user populations, and adoption of security behaviors. We first start our related works section with some background knowledge on surveillance and censorship. Within this section we find that most of the previous work discussed surveillance and censorship in countries other than Sudan or East and Sub-Saharan Africa. We also notice that surveillance and internet blackouts have been widespread in a lot of countries around the world especially during times of political turmoil (for example during protests and elections). Then we look into a section of the related works that studies activists and their use of technology. In specific, we tried to look into works that are at the intersection of Human Computer Interaction (HCI) and activism. We then look at the the study of the security and privacy practices of vulnerable populations or those in non-WEIRD contexts. Finally, we discuss adoption theories and the adoption of security and privacy practices to lay the foundation for an understanding of activists' technology adoption. We summarize these efforts below:

Surveillance and Censorship Censorship-oriented research has focused on China (e.g., [24, 25]) and other parts of the world such as Saudi Arabia, Iran, and Bahrain [26, 27], or Thailand [28]. Groups have also focused on the commercial tools used by nation states for surveillance and censorship, e.g., Blue Coat [29]. 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 [30]. For example, internet shutdowns happened in Egypt [31], Libya [32], and Syria [33] 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 [34–37].

Activists and Technology Use 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 [38–40] or feminist HCI [41, 42]. Along the lines of political activism, Tadic et al. [43] 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 [44]. Other groups have studied technology during political events, e.g., protesters during the Arab Spring [45–47], and by political refugees or other persecuted populations [2, 48–52]. 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 [7, 53, 54].

Security & privacy for vulnerable populations or in non-WEIRD contexts Prior works have found that security and privacy practices differ between cultures and countries [55–57]. 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 [58] or South Africans [59]. 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 [59]. 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 [2, 3, 48, 60]. 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 Chapter 4).

Chapter 3

Methodology

3.1 Semi-structured Qualitative Interviews

We conducted 13 interviews with 14 political activists, some of which were in Sudan while others have been based abroad. All interviews have been conducted remotely via a medium that the participants preferred and we gave them the choice of a video versus audio call. We also asked each participant about their consent before recording the interview which was stored in a secure location which only the lead researchers in this work would have access to. The consent form clearly indicated that the purpose of the work is to help develop better technical tools and communication mechanisms for activists. And that participants had the choice on whether they'd want to be recorded or not, and what language they want to conduct the interview in. We gave them the choice of either using the Arabic language or the English language during the interview and one of the lead researchers in this work and who is an Arabic native speaker translated interviews conducted in Arabic into English in preparation for the analysis phase later on. We also gave participants the choice of whether they would want the interview to be recorded or not. Most agreed on recording and we later transcribed all recorded interviews prior to the analysis.

3.2 Recruitment

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.

3.3 Qualitative Coding and Analysis

To analyze our interviews qualitatively, we used the grounded theory approach [68] to first create open codes through a memoing process but also by extracting major themes that we found within our data. We developed a qualitative codebook iteratively through a process by which a set of memos and open codes were created and then combined to form hierarchical axial codes. We then applied the codebook to each of the 13 interviews twice (once separately by each of the lead researchers in this work). The intercoder agreement between the two coders was 98.7%. The way we did the coding was that a "Yes" code was assigned for any behavior that the participant either adopted/used or have seen others adopting/using. And a "No" code was assigned for the contrary. We created a total of around 275 low level codes and a total of 5 themes or high level codes, namely: *Threats and Threat Models, Technology Behavior and Adoption, Security Needs and Practices, Internet Access During Blackouts and Blockades and Activists' Operational Needs and Goals*. A complete list of codes developed throughout our work is shown in the table in the Appendix. In the table below we take a look at the high level codes and the corresponding number of low level codes for each high level code. In addition, we also show the high level code count in our data (ie. the collective sum of participants coding a "Yes" for that high level code. This in a way shows where the majority of our data was concentrated and how the interview data has been coded. We also want to note that there exists an overlap between some of the low level codes and hence when coding we found that a

participant's quote could fit into multiple low level codes. An example of that is a low level code: "Choosing not to adopt a specific tech/behavior" Furthermore, a definition of both the high level codes and low level codes are provided in Appendix 2.

High Level Code (Themes)	**Number of low level codes**	**Count**
Threat Model and Threats	37	299
Technology Behavior and Adoption	6	67
Security Needs and Practices	65	335
Internet Access (Blackout and Blockade)	19	81
Operational Needs and Goals	11	131
Miscellaneous	14	79

Table 3.1: This table shows the high level themes or codes that emerged from our data. In addition, we also show the number of low level codes that emerged from each high level code and the number of times that we coded our data using this code

3.4 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. it's hard to say that our results are generalizable to the study of activists in the entirety of the Sudanese nation but we think it's a significant representation given that the activism and political movement has its leadership in the capital city Khartoum. However, given our knowledge about and connections to the Sudanese activism context, we think this study can be easily replicated to include participants from a number of different cities across Sudan. An additional limitation that is common in qualitative studies is that results could be influenced by the researchers' personal biases given that they were the ones conducting the interviews. 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.

3.5 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 [69], though prior work has observed gender differences in specific activist contexts too, e.g., hacktivism [70]. 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 note that while some participants were physically in Sudan during the revolution, a handful of the activists we interviewed were either based abroad or were travelling to and from Sudan during the 6-7 months period that the revolution lasted. Based on their movement activities or where they were located, participants' had different roles in terms of working at the neighborhood level, leadership level of the movement, media, news filtration and dissemination, etc. and what we report on Table 3.2 below is what they told us but it isn't necessarily the case that they have maintained the same role throughout the whole duration of the revolution.

Participants	**Location**	**Role During Revolution**
P1	travelling to and from Sudan	started a neighborhood group
P2	in Sudan	medic
P3	outside Sudan	member of the diaspora
P5	in Sudan	activist
P6	in Sudan	member of a neighborhood group
P7	in Sudan	activist
P8	in Sudan	activist
P9	travelling to and from Sudan	activist
P10	outside Sudan	member of the diaspora
P11	travelling to and from Sudan	member of the diaspora
P12	in Sudan	activist
P13	in Sudan	activist
P14	in Sudan	activist

Table 3.2: This table shows additional information about our participants in terms of where they were located (inside Sudan, outside Sudan or travelling to and from Sudan) during the revolution and what their role was: some identified just as "activists" while others

Chapter 4

Results

4.1 Threat Landscape and Technical Challenges

In this section, we identify four fundamental technical challenges that drove activists to adopt a diverse set of low tech solutions. In addition, we directly contrast the technical challenges to the political factors and the unique societal context that enabled these challenges. So, for each technical challenge we mention we also mention some of the political or societal constraints that helped shape the activists' defensive practices. We also notice that while these were considered challenges from our perspective as computer security and HCI researchers, based on what most of our participants have said they do not necessarily view them as challenges but rather they believe for example that the variety of defensive strategies they've adopted while low tech have provided them with sufficient security by not giving their adversary one singular defense to focus on breaking. To get a better understanding of the technical challenges that activists faced and that influenced their technology use and technical defensive strategies we first take a look at the threats and the adversaries within the activism community during the revolution in Sudan.

4.1.1 Threat Landscape

In Sudan, the state actors included the police, security services or what is known as the NISS, the military and special forces known as the rapid support forces or the RSF. Most participants reported that each of the actors mentioned above posed a different threat to activists and protestors during the different phases of the revolution. While many of those we talked to believed that the actors

were local, some attributed the threats to foreign powers or actors usually at the regional level, for example in countries like Saudi Arabia and the UAE. What we report in this section is not necessarily the exact capabilities of the adversary but rather the folk models of the threats as shared by the majority of the participants. They arrived at these models either through direct experience, like being arrested, through someone else's experience or through an insider's knowledge of the operations of the different actors in the state and their influence on third party entities like the telecommunication companies in the country. As Wash [65] argued in his study of folk models of home computer security, it is not important to know the extent to which these models were accurate but how it served the activists when making security related decisions.

Arrest and physical device seizure: The threat of arrest was the most common threat experienced by those we talked to. The arrest was usually carried out by the police or the security services. The easiest way to get arrested was by participating in protests. In a protest, everyone might be the target of the police or security services (which are usually both present in a protest scene). Those spearheading the movement were at most risk of being personally targeted for harm or arrest. An arrest could also occur after an activist is physically or electronically surveilled due to their online or offline anti government activity. Once arrested, phones were confiscated and activists were forced to unlock their phones and sometimes forced to log in to their social media accounts. The police or security services would usually go over personal messages on the different apps and the social media feeds of those arrested. An arrest of one person was usually a trigger for a chain of arrests in that person's network. One participant reported that security services were able to inject spyware in a number of phones that belonged to a group of activists arrested during a specific period, *"There was a group that was arrested in the early days of the movement (after 31st December), people used to say that everyone who was arrested during that period had their phones confiscated and security services were able to plant a bug in these phones, something that would transfer all information in the device and allow security services to monitor the device even after you're released." (P12)*

Surveillance: Electronic surveillance was most known as a threat of the telecommunication companies which were known to be complicit with the security services in most of their adversarial activities. *"I read and I read many news articles and I have a friend who was a – I can't mention his name but he was a senior engineer at [ISP] – he conferred to me that the security forces can access the telephone conversation, and also the intelligence secure, the security forces actually have a unit inside these telephone companies, that is responsible for tracking and monitoring the conversations." (P9)* Most participants believed that regular phone calls and SMS messages were monitored. In addition, they went as far to talk about how telecommunication companies were able to figure out people's locations as they use the phone's mobile data to connect to the internet. For most people, the imminence of this threat was directly correlated to whether an activist considers themselves a target or one among the many using phone calls and sending SMS messages, which in the latter case was less likely to be monitored. *"Interviewee: So as an activist, you didn't think that using regular SMS text messages and phone calls were secure, right? P5: I started using them more freely after a month or a month and a half from the start of the revolution, because the numbers were big, no one can just target a specific someone."* Furthermore, there was the threat of security services infiltrating groups on WhatsApp or other social media apps usually by impersonating those arrested but also through other methods. This threat was often short lived and bound to the duration of arrest or word getting out of arrested individuals.

Misinformation and Propaganda: Online misinformation was rampant during the revolution, though some participants considered it only a lower-level threat (P11). Misinformation could be spread by anyone, but originated from online accounts, known in Sudan as "electronic chickens," that were paid by the Sudanese government to disseminate and propagate disinformation and propaganda [71, 72]. Misinformation ranged from fake news, false reports about deaths at protests (P9), to false protest times/locations that served as an ambush to arrest activists (P12). The Sudanese government wasn't necessarily the only source of misinformation. Any false information or reports that aimed to undermine the efforts of the movement was considered a threat to most activists.

4.1.2 Adversaries

There were a number of different adversaries during the revolution in Sudan. Our participants did talk about changing adversaries throughout the revolution (ie. the participants' perception of threat and who the adversary was at different times/periods during the revolution). For example, in the outset of the revolution, the main adversary was the Sudanese government. Some of the different players within the Sudanese government that were considered adversarial were: the electronic chickens that spread misinformation online, the security services that arrested and surveilled communications and the police forces that quelled activists' efforts to protest or organize physically on the ground. Following the crackdown on the sit-in and during the internet blackout participants' perceived other forces like the military forces and the Rapid Support Forces (RSF) to be more adversarial. We also note that throughout the revolution and to a large extent, telecommunication companies and some foreign governments were considered as adversarial. We believe that it's important to understand the adversarial background to get a thorough understanding of the threats and later on the security and privacy behavior and practices of activists. In the figures below we look at the different adversarial players during the formative period of the revolution and how this changes during the sit in and blackout period.

4.1.3 Activists' Security Goals

Below we talk briefly about some of the main security goals of activists that our participants mentioned.

- **Plausible deniability during protests and when arrested:** As mentioned in the previous section the threat of arrest and phone confiscation when detained was the number one threat that activists prepared for. They had a number of different strategies in place to provide plausible deniability upon arrest and these include things like: phone sanitization, denying the security services access to their accounts by logging out of social media accounts when going to protests, carrying a different decoy phone or not carrying a phone in the first place.

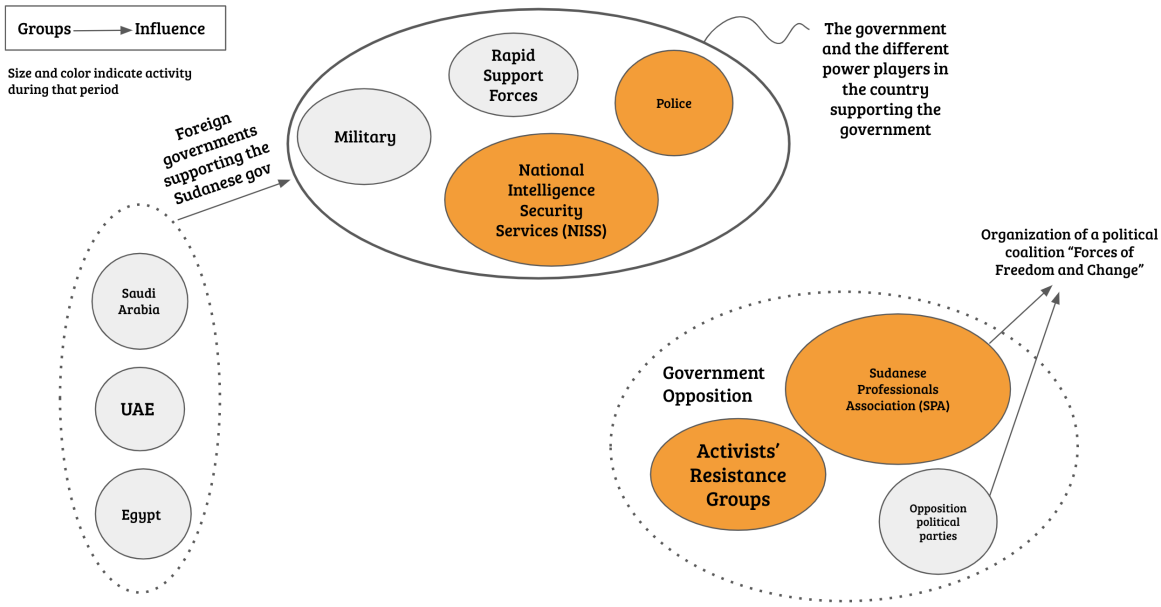

Figure 4.1: The different players and the interplay between them as identified by participants during the formative/organization period [1]. The orange color indicates the most active parties during that time. And the size indicates the parties that had the most influence on the scene.

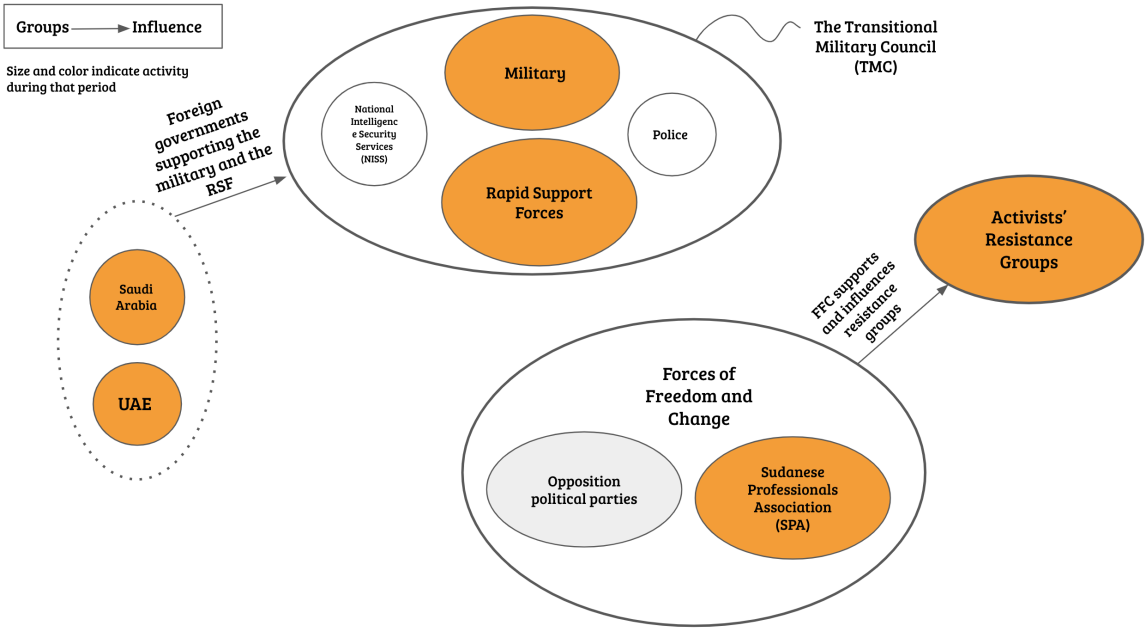

Figure 4.2: The different players and the interplay between them as identified by participants during the sit-in period [1]. The orange color indicates the most active parties during that time. And the size indicates the parties that had the most influence on the scene.

- **Security from remote and electronic surveillance:** Most of the participants reported that security from electronic surveillance and infiltration of chat groups was of utmost importance. They used a variety of strategies to evade electronic surveillance, most of which were low tech strategies or a combination of ad-hoc strategies that helped them achieve their goals. A number of participants used VPN's and remote desktop access through intermediary servers to obfuscate their location and browsing information, others had manual processes in place to perform a background check on WhatsApp group members and ensure that members comply with the group rules.

- **Physical Security:** As mentioned throughout this section, physical security was very important to activists because the security services had unfettered power to detain, arrest and violently abuse activists. In addition to arrest, most activists feared for the safety of their families and friends if any link or connection could be made to others upon arrest either by examining personal belongings or online activity.

- **Security of Communications during the internet blackout:** During the internet blackout there was an increasing fear of what the military and the RSF are capable of doing. So, activists needed to maintain an active communication channel but also needed to make sure that these communications aren't infiltrated or surveilled in any way.

4.1.4 Verifying Online Information

As we mentioned earlier, online misinformation was commonplace during the revolution in Sudan. 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. Eight 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).

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.*"

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.

Furthermore, 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.

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.

4.1.5 Communication 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.

Nine 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.

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.

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.

Political Influence: Sudanese Government's Control over Telecommunication 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.

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 the government's capability for censorship or blackout: during the revolution, social media access was initially curtailed for roughly 10 weeks, and the government imposed a complete mobile data blackout[1] after the June 3 Khartoum massacre.

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.*"

Political Influence: Foreign Governments' Control over Tech and Telecommunication Infrastructure 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

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

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 respond to any of the requests.[2]

4.1.6 Apps and App Adoption

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]).

In response to the government censorship of popular social media apps (including Facebook and WhatsApp) 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

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

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.*" 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].

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.

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.

Political Influence: International Sanctions 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.

Due to the US sanctions on Sudan, the entire iOS app store is inaccessible without a VPN (P11) [79, 80]. 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).

Societal Influence: Group's Digital and Security Literacy Drives App Adoption 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 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.

4.1.7 Device Security

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.*"

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.

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.

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: the extensive preparation time, in addition to a lack of confidence in their data hiding and deletion strategies, lead them to leave their personal phone at home and forgo any connection to her group while at a protest: "*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.*"

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.

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.*"

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).

Political Influence: State Power to Force 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 throughout the earlier sections 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.*"

4.2 Security Advice

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. [81, 82]), though it does have similarities with activist-specific advice given to protesters in the United States in 2020 [83].

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.

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*[3] that is distinct from *Signal Private Messenger*,[4] 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

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

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 was not always actionable). For example, the most common expert security practices in Busse et al [81] 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 [81], participants only mentioned using 2FA, with modified advice: use *foreign* 2FA. Outside the academic community, there has also been mixed advice and debate about whether WhatsApp should be considered safe by activists [84, 85].

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 [86]. 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, or do not want to cost themselves access to social media, documentation, and their regular contact list (the same issues faced by Sudanese protesters), 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 [83]. 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, protesters in different countries require very different *concrete* advice.

4.2.1 Diffusion of 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.

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*[5] *did, so then we can adopt this.*"

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, 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 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.*"

Experience amongst activists is a continuum: some have been activists for years, and others became activists at the start of the revolution in December 2018. The more experienced activists in our participant pool agreed that in Sudan, experienced activists are a relatively 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. 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. 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*

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

2013[6] *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.*" 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).

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.*"

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*

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

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. Bootstrapping was also used for building 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.

4.2.2 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), and using their own phone numbers as 2FA for those in Sudan (P8, P10, P12).

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 for the advice-givers to understand the political and

societal constraints of each specific community.

4.3 Design Principles and Case Studies

Throughout the results section we have uncovered a number of design principles and tensions and to a large extent we have shown that these tensions and principles are influenced by the specific political and societal contexts in which the revolution took place. We introduce a number of case studies below to surface how the activists' use of technology in some cases comes into collision with universally acknowledged design principles embedded into the design of apps and technologies in the modern day and age. In some case studies we also talk about how activists were in some cases forced to use technology in ways for which it wasn't designed for to secure their communications, and organize and protest.

SMS Based Two Factor Authentication A number of participants faced issues configuring two factor authentication (2FA) with their local Sudanese phone numbers on platforms like Twitter (P1). So, the fact that participants couldn't use their Sudanese numbers for authentication purposes in addition to the distrust of the telecommunications companies, most participants opted for the use of foreign numbers for 2FA. And by foreign numbers, we mean numbers that aren't registered in and would go through the telecom infrastructure in the country. The cohesive social structure in place facilitated the use of these foreign numbers for authentication purposes by having friends and family living abroad connect their personal numbers to the activists' social media accounts. We understand that SMS based 2FA [87] is one of the most common and popular mechanisms for authentication on social media platforms. But, we also note that it's being designed in a way that doesn't accommodate for the fact that nation state adversaries usually have purview and control over the telecommunications infrastructure in some countries and hence have unfettered access to mobile users' SMS data. We also note that the lack of local laws and policies that would protect citizens against such violations weakens the use case of 2FA as a robust security measure for activists to protect themselves in some countries. Furthermore, the use of third party authentication apps or

services might have not been feasible given that device seizure was one of the most imminent threats that activists faced. In conclusion, the use of 2FA with foreign numbers have proved successful for activists and have allowed them to rely on the trust dynamic of the group rather than that of the individual to secure their online accounts but came with a cost of time and resources to set up and synchronize across multiple individuals and timezones.

Yield Access Credentials Upon Arrest Physical security and the threat of arrest was one of the major threats that activists faced throughout the revolution. Upon arrest, the arrestees phones were confiscated and they were compelled under violence and pressure to give up their passcodes or biometric authentication to allow the security services access to their personal information. In the US, domestic arrestees are protected by the 5th Amendment from being compelled to give a passcode [88]. Android and iOS support American users by providing a quick way to force passcode authentication over biometric authentication [89]. 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. So, this indicates that security and privacy policies and local laws vary significantly across countries and different populations and communities. Hence, technology designers should be aware of such differences throughout the tech design process.

Mesh Networking Apps Mesh networking apps rely on short range wireless technologies like Bluetooth to set up network connections and hence allow people to communicate offline. During the blackout period, activists found it hard to use technology for communications. The internet was cut off for almost a month and during that period most people relied on analog communication techniques like graffiti, face to face meetings and television news channels. In addition, many of the participants used things like mass SMS messages and telephone calls to consume and disseminate news. There were a number of challenges that activists faced with the use of mesh networking apps. First, many of our participants reported that it was hard to use a mesh networking app called Firechat.

In addition, an app that relies on Bluetooth connection requires that activists communicate in close proximity to each other and they wanted something to communicate over long distances and would not go through the regular phone line. Furthermore, some participants expressed their concern when using mesh networking apps that would require them to set up their contacts separately from other mainstream apps they've been using and with an existing user base. So, we find that mainstream apps are designed with too rigid threat models that doesn't accommodate for this kind of offline communication that is vital during unrest and political strife.

Maintaining Multiple Accounts Online without Context Collapse Activists had to switch between different facets of their identity. This led to the use of multiple online accounts that either serve to separate between their activism work/activities and their personal lives or as a distinction between multiple facets of their activism identity (like between working on a neighborhood committee and being a medic/paramedic). Also, many of the participants reported maintaining a different follower base and decoy content in each of their multiple accounts. We find that some social media platforms might not afford activists the use of multiple online identities without flagging their accounts or labelling them as bots. While some technology design did support activists' goals in creating that separation. For example, the use of private space, which is a feature on Huawei phones that allow users to set completely independent spaces which can be accessed using a fingerprint ID or password, the majority relied on analog techniques like maintaining two separate SIM cards or two separate mobile phones.

Introduction of Dual Use Cases for Apps or App Features Activists were able to introduce additional use cases for applications and technologies for which it was originally not designed for. For example, one participant (P1) mentioned that they used the message archive feature on WhatsApp to hide messages in anticipation for arrest or anyone searching through their phone. Another participant (P9) used WhatsApp read receipts to signal to the other party that they should delete the sent message without actually replying. The same participant used Twitter lists in order to synchronize between different neighborhood groups and disseminate news. Furthermore,

we realize that authentication through a trusted group dynamic was very popular. For example, using SMS based 2FA with foreign numbers belonging to trusted family and friends and in one instance one participant mentioned setting up biometric access to a personal phone through another trusted party to provide plausible deniability upon arrest (P9). Overall, we notice that some user groups/populations introduce dual use cases for apps or app features for which it wasn't originally designed and created. As a result, a number of design tensions might arise in the process and we believe that it's fundamental for future technology designers and policy makers to understand more about these design tensions and the underlying technology stresses that produced them. It's also a key to foster the design of secure tools that will protect vulnerable populations from oppression, abuse and other forms of injustices that are commonplace in this day and age.

Chapter 5

Conclusion

In this work, we surface how technology has been used by activists to help them organize and mobilize both online and offline. 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 and to continue to work and reveal further ones. 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? 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 4.1: misinformation; physical device security; and confidentiality, integrity, and availability over an adversarially controlled network. Such structured questions uncover *fundamental tensions* (e.g., the tension between recommending use of mainstream apps or more obscure ones) 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.

References

[1] Jean-Baptiste Gallopin, "Bad company: How dark money threatens sudan's transition." https://ecfr.eu/publication/bad_company_how_dark_money_threatens_sudans_transition/. [Accessed Sep. 2020].

[2] L. Simko, A. Lerner, S. Ibtasam, F. Roesner, and T. Kohno, "Computer security and privacy for refugees in the United States," pp. 409–423.

[3] C. Chen, N. Dell, and F. Roesner, "Computer security and privacy in the interactions between victim service providers and human trafficking survivors," pp. 89–104.

[4] S. Havron, D. Freed, R. Chatterjee, D. McCoy, N. Dell, and T. Ristenpart, "Clinical computer security for victims of intimate partner violence," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pp. 105–122, 2019.

[5] Uptodown App Store, "Firechat." https://firechat.en.uptodown.com/android. [Accessed Sep. 2020].

[6] ASUS Inc., "[zenfone] what is twin apps and how does it work?." https://www.asus.com/support/FAQ/1032388/. [Accessed Sep. 2020].

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

[8] 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].

[9] Human Rights Watch Org., "Sudan." https://www.hrw.org/africa/sudan. [Accessed Sep. 2020].

[10] 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].

[11] U.S. Dep. of State, "State sponsors of terrorism." https://www.state.gov/state-sponsors-of-terrorism/. [Accessed Sep. 2020].

[12] 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/, 6 2020. [Accessed Sep. 2020].

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

[14] 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].

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

[16] 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].

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

[18] Z. Tufekci, "Social movements and governments in the digital age: Evaluating a complex landscape," *Journal of International Affairs*, vol. 68, p. 1, 2014. SIPA Columbia University.

[19] 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. [Accessed Sep. 2020].

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

[21] R. Abbas, "In Sudan, neighbourhoods mobilised against Al-Bashir." https://www.aljazeera.com/news/2019/5/7/in-sudan-neighbourhoods-mobilised-against-al-bashir. [Accessed Sep. 2020].

[22] 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].

[23] 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/. [Accessed Sep. 2020].

[24] R. Clayton, S. J. Murdoch, and R. N. Watson, "Ignoring the great firewall of China," in *International Workshop on Privacy Enhancing Technologies*, pp. 20–35, Springer, 2006.

[25] J. R. Crandall, E. Barr, D. Zinn, R. East, and M. Byrd, "Conceptdoppler: A weather tracker for internet censorship," pp. 352–365.

[26] J.-P. Verkamp and M. Gupta, "Inferring mechanics of web censorship around the world,"

[27] 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," *Transactions on the Web (TWEB)*, vol. 9, no. 1, pp. 1–29, 2015.

[28] G. Gebhart and T. Kohno, "Internet censorship in Thailand: User practices and potential threats," pp. 417–432.

[29] 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/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/, 1 2013. [Accessed Dec. 2020].

[30] 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," pp. 1–18.

[31] M. Richtel, "Egypt cuts off most internet and cell service." https://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html. [Accessed Sep. 2020].

[32] 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].

[33] 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].

[34] L. H. Newman, "Belarus has shut down the internet amid a controversial election." https://www.wired.com/story/belarus-internet-outage-election/, 10 2020. [Accessed Aug. 2020].

[35] 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, 1 2020. [Accessed Aug. 2020].

[36] L. H. Newman, "How the Iranian government shut off the internet." https://www.wired.com/story/iran-internet-shutoff/, 1 2019. [Accessed Aug. 2020].

[37] R. Mahomed and R. Bendimerad, "Venezuela shuts down internet amid protests." https://www.aljazeera.com/news/2019/01/venezuela-shuts-internet-protests-190124124829727.html, 1 2019. [Accessed Aug. 2020].

[38] 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," pp. 99–108.

[39] S. Consolvo, K. Everitt, I. Smith, and J. A. Landay, "Design requirements for technologies that encourage physical activity," pp. 457–466.

[40] A. Grimes and R. E. Grinter, "Designing persuasion: Health technology for low-income African American communities," in *Proc. International Conference on Persuasive Technology*, pp. 24–35, Springer, 2007.

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

[42] C. Fiesler, S. Morrison, and A. S. Bruckman, "An archive of their own: A case study of feminist HCI and values in design," pp. 2574–2585.

[43] B. Tadic, M. Rohde, V. Wulf, and D. Randall, "ICT use by prominent activists in Republika Srpska," pp. 3364–3377.

[44] S. Gaw, E. W. Felten, and P. Fernandez-Kelly, "Secrecy, flagging, and paranoia: adoption criteria in encrypted email," pp. 591–600.

[45] 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," *International journal of communication*, vol. 5, p. 31, 2011.

[46] 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?," *Available at SSRN 2595096*, 2011.

[47] E. Stepanova, "The role of information communication technologies in the 'arab spring'," *Ponars Eurasia*, vol. 15, no. 1, pp. 1–6, 2011.

[48] 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," pp. 1–15.

[49] A. Dhoest, "Digital (dis) connectivity in fraught contexts: The case of gay refugees in Belgium," *European Journal of Cultural Studies*, vol. 23, no. 5, pp. 784–800, 2020.

[50] O. Portillo, "To liberate and lament: The duality of digital culture and Chechnya's concentration camps for Russian LGBT citizens," *EXCLAMATION*, p. 59, 6 2018.

[51] M. Panzica, "A difficult line to walk: NGO and LGBTQ+ refugee experiences with information and communications technology (ICT) in canada," Master's thesis, Dalhousie University, 2020.

[52] R. Dekker, G. Engbersen, J. Klaver, and H. Vonk, "Smart refugees: How syrian asylum migrants use social media information in migration decision-making," *Social Media+ Society*, vol. 4, no. 1, p. 2056305118764439, 2018.

[53] T. Hirsch and J. Henry, "TXTmob: Text messaging for protest swarms," pp. 1455–1458. Abstract.

[54] T. Hirsch, "Feature learning from activists: Lessons for designers," *Interactions*, vol. 16, no. 3, pp. 31–33, 2009.

[55] Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai, and A. Yamada, "Self-confidence trumps knowledge: A cross-cultural study of security behavior," pp. 2202–2214.

[56] S. Bellman, E. J. Johnson, S. J. Kobrin, and G. L. Lohse, "International differences in information privacy concerns: A global survey of consumers," *The Information Society*, vol. 20, no. 5, pp. 313–324, 2004.

[57] H. Cho, M. Rivera-Sánchez, and S. S. Lim, "A multinational study on online privacy: Global concerns and local responses," *New Media & Society*, vol. 11, no. 3, pp. 395–416, 2009. SAGE.

[58] Y. Rashidi, K. Vaniea, and L. J. Camp, "Understanding saudis' privacy concerns when using whatsapp," pp. 1–8.

[59] 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,"

[60] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner, "Investigating the computer security practices and needs of journalists," pp. 399–414.

[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," *Mobile Media & Communication*, vol. 3, pp. 401 – 424, 2015. SAGE.

[63] S. Das, A. D. Kramer, L. A. Dabbish, and J. I. Hong, "The role of social influence in security feature adoption," pp. 1416–1426.

[64] S. Das, L. A. Dabbish, and J. I. Hong, "A typology of perceived triggers for end-user security and privacy behaviors," (Santa Clara, CA, USA).

[65] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, (New York, NY, USA), Association for Computing Machinery, 2010.

[66] E. Rader, R. Wash, and B. Brooks, "Stories as informal lessons about security," pp. 1–17.

[67] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the adoption of secure communication tools," pp. 137–153, 2017.

[68] A. Strauss and J. Corbin, "Grounded theory methodology: An overview.," 1994.

[69] 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, 8 2019. [Accessed Aug. 2020].

[70] L. M. Tanczer, "Hacktivism and the male-only stereotype," *New Media & Society*, vol. 18, no. 8, pp. 1599–1615, 2016.

[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. [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, 10 2015. [Accessed Sep. 2020].

[73] C. Geeng, S. Yee, and F. Roesner, "Fake news on Facebook and Twitter: Investigating how people (don't) investigate," pp. 1–14.

[74] A. E. Kramer, "Ukraine's opposition says government stirs violence." https://www.nytimes.com/2014/01/22/world/europe/ukraine-protests.html, 1 2014. [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/, 6 2020. [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," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 1, pp. 83–102, 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," pp. 349–364.

[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] 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, 7 2015. [Accessed Aug. 2020].

[80] U.S. Office of Foreign Assets Control, "Sudan sanctions program." https://www.treasury.gov/resource-center/sanctions/Programs/Documents/sudan.pdf. [Accessed Aug. 2020].

[81] 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,"

[82] I. Ion, R. Reeder, and S. Consolvo, ""... no one can hack my mind": Comparing expert and non-expert security practices,"

[83] 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, 6 2020. [Accessed Aug. 2020].

[84] 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].

[85] 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].

[86] 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].

[87] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in *2009 IEEE/ACS International Conference on Computer Systems and Applications*, pp. 641–644, IEEE, 2009.

[88] K. Howell, "The fifth amendment, decryption and biometric passcodes." https://www.lawfareblog.com/fifth-amendment-decryption-and-biometric-passcodes, 11 2017. [Accessed Aug. 2020].

[89] 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/, 3 2018. [Accessed Aug. 2020].

Appendix A

Interview Protocol

A.1 Interview Questions

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?

High-level Code	Subcode
Threat model and threats: Refers to the activists' threat models and their perception of the adversaries and their capabilities	Risk assessment Trigger for change in threat model Changing adversaries Trusted party Adversary Asset Sudanese government capabilities Foreign government capabilities Outsourced capabilities
Adoption of technology and behaviors: Refers to activists' behaviors towards adoption and the challenges they faced	Learning process Trigger for adoption Choice not to adopt Challenges / barriers Discontinuing use Teaching
Security needs & practices: Refers to the security needs and practices of activists with regards to information verification	Building trust Sources of trust Making information verifiable Verification of information
Security needs & practices: Refers to the security needs and practices of activists that provide plausible deniability upon arrest	Built-in security mechanism Adhoc strategy Deny self access to info / regular device Deny others access to info Go analog Things you expect other people to do for your own security
Security needs & practices: Refers to the security needs and practices of activists with regards to electronic surveillance	Built-in security mechanism Ad hoc strategy Deny self access to info / regular device Deny others access to info Go analog Things you expect other people to do for your own security
Security needs and practices (physical security): Refers to the security needs and practices of activists with regards to physical security	no subcodes
Security needs and practices (offensive tactics/goals): Refers to the offensive security practices by activists	no subcodes
Security needs and practices: Refers to the security needs and practices of activists during the social media blockade and internet blackout	Blackout Social media blockade Other
Operational needs / goals: Refers to the operational needs and goals of activists with regards to news consumption	Platform News source Type of news
Operational needs / goals: Refers to the operational needs and goals of activists with regards to communications and news dissemination	subcodes were specific platforms
Comparisons: Refers to comparisons being made by participants with regards to previous protests/revolutions or the different technologies being used	Mention or compare to previous protests / revolution Preferred platform X to platform Y
Participant's overall experience: Refers to the participant's overall experience during the revolution	Was in Sudan during the revolution Was NOT in Sudan during the revolution (diaspora) Role during revolution Role of diaspora

Table A.1: 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 - Sudanese government capabilities'; we used it to report on how many participants mentioned electronic surveillance as a capability of the Sudanese government).