

Defensive Technology Use During the 2018-2019 Sudanese Revolution

Alaa Daffalla*[‡], Lucy Simko^{†§}, Tadayoshi Kohno[†] and Alexandru G. Bardas*

* Department of Electrical Engineering & Computer Science and ITTC, University of Kansas

† Paul G. Allen School of Computer Science & Engineering, University of Washington

Abstract—Technology has changed both the tools that activists use and the power that nation-states have over activists. Our work focuses on the needs, practices, risks, and challenges of activists during the Sudanese 2018-2019 revolution, with larger inferences to future movements and technologies.

Keywords—Defensive technology, Activists, Sudanese Revolution

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

One recent revolution is the 2018-2019 Sudanese revolution, which resulted in the ousting of Sudan’s president of nearly 30 years, Omar Elbashir. Our work focuses on the needs, practices, risks, and challenges of activists during this revolution, with larger inferences to future movements and technologies.

Through this article, we detail our findings about how and why activists used technology the way they did, drawn from in-depths interviews with 14 Sudanese activists, identified in our work as P1-P14. Given the sensitivity of this topic, we took extra precautions as detailed in our conference paper [2].

Through our work, we emphasize the importance of understanding users’ *political and societal contexts*, and in this article, we explore the political and societal influences on activists’ technical personal defenses. (See our paper [2] for a more detailed discussion about technical influences on usage.)

We encourage future researchers and technologists to follow our approach of examining users’ or potential users’ political and societal contexts when trying to examine, anticipate, and understand the privacy and security behaviors and needs of users, particularly activists under political strife, by asking questions such as the ones in Figure 1.

POLITICAL INFLUENCES ON THE TECHNICAL DEFENSIVE LANDSCAPE

The domestic and international political landscapes fundamentally change how users experience technology by dictating what technology is available to them (e.g., through sanctions and censorship), and what privacy features match their threat model (e.g., how the legal right to privacy is defined, and what practices law enforcement follow). We identify several key political influences on activists’ technology use, and encourage technologists and policy-makers to consider users’ needs and practices through a similar lens.

Timeline of the 2018-2019 Revolution in Sudan. In 2018, due to the dire economic situation in the country, a wave of protests erupted and led to the 2018 - 2019 revolution [3]. Figure 2 captures the main phases of the Sudanese revolution, starting in December of 2018 and leading up to the formation of the civilian transitional coalition. Throughout the different phases of the Sudanese revolution, protesters were targeted by a number of state actors, including the police, the National Intelligence and Security Services (NISS or “the security services”), the military, and a special division of armed forces, the Rapid Support Forces (RSF).

International politics dictate available apps and features. US sanctions on Sudan meant that mobile users in Sudan did not have access to all apps and app features, including the entire Apple App store, and paid apps and features in the Google Play store (P11) [4].¹ These restrictions shaped Sudanese activists’ technology use, and we encourage readers to reflect on how international politics can make it challenging to create security and privacy recommendations that fit multiple vulnerable user groups, since different groups have fundamentally access to different applications and features.

P11 described how users in Sudan downloaded 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.

¹The US first imposed economic sanctions on Sudan in 1996 after designating Sudan a sponsor of state terrorism. Sanctions were partially lifted in 2015, giving Sudanese users access to *unpaid* apps and features in the Google Play store; however, paid apps and features in the Google Play store, as well as the entire Apple App store, were unavailable until December 2020, when the remaining US sanctions were lifted.

[§]Co-first authors listed in alphabetical order

[‡]Alaa Daffalla’s name in native alphabet: آلاء دفع الله

Guiding questions about political and legal context:

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

Guiding questions about 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?

Figure 1. Questions for understanding context

Additionally, people in Sudan couldn’t 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, were not easily accessible. Sanctions also meant that Sudanese domestic phone numbers were not accepted as a second factor of authentication (2FA) “because in Sudan Twitter does not have verification for Sudanese numbers” (P1).

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 even 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 any 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.

The technical capabilities of political allies and enemies shape threat models. Activists’ perceptions of the 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

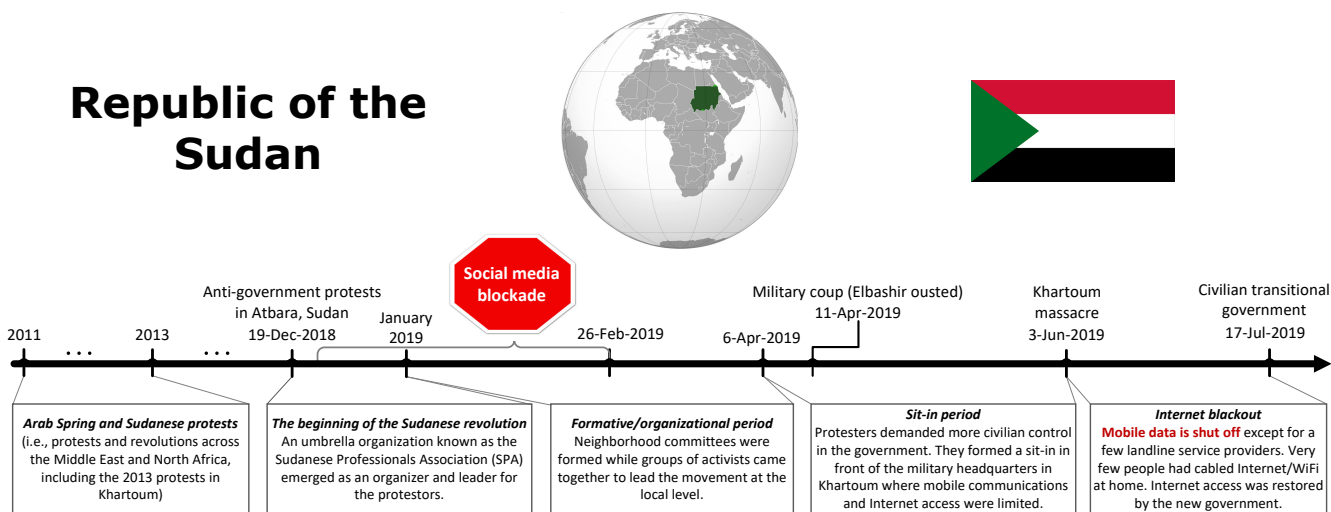


Figure 2. Summary timeline of the major events during and leading up to the Sudanese 2018 - 2019 revolution.

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.*”

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

The perception that privacy on social media was only as good as the money paid by a government, in combination with the lack of choices in apps, led some to feel a lack of control or sufficiency. Asked whether people continued to use Facebook despite the possibility that the Sudanese government could purchase information, P12 said: “*there wasn’t any other solution. We reached a phase where we were saying ‘what is the worst that could happen.’ People have died because of this.*” We cannot address the accuracy of P12’s perception about the availability of Facebook data to the Sudanese government, but we do note that according to Facebook’s public log of government requests, during January-July 2019 there were 15 requests by the Sudanese government for information on 23 user accounts, and the following period, for the latter half of 2019, had 52 requests. According to Facebook, they did not produce information in response to any of the requests.²

The power of the state to compel authentication. Users’ technical practices are shaped by their right to privacy as defined by the local laws and practices. While users in the US may have legal protection against being compelled to give their passcode to law enforcement, aided by their smartphones’ ability to force biometric authentication on demand or after a certain number of passcode attempts, Sudanese activists had no such protection and, thus, the same technical features did not provide protection for Sudanese protesters. Sudanese authorities obtained arrestees’ phone passcodes or biometrics in order to search their phones for anti-government activities and proof of 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 ‘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.*” 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 and meticulous defenses.

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.*” So, some of the 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. Others formatted their phones entirely, relying on backups. P1 planned to uninstall WhatsApp and Twitter and rely on a cloud backup if they were arrested, since they had two SIM cards, with the second SIM providing 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. 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.

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.

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.*” Other activists (mentioned by 4 participants) relied on Telegram’s self-deleting messages.

Government control over the telecommunication infrastructure. The extent of the government’s control over the telecommunication infrastructure strongly influenced activists’ threat model and drove adoption of technology. Twelve participants believed that the Sudanese government could surveil their communications through a combination of control over the telecommunications infrastructure, influence over internet

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

service providers, 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 internet 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 censorship and blackout: during the revolution, the government initially curtailed social media access for roughly 10 weeks, and later imposed a complete mobile data blackout³ after the Khartoum massacre on June 3rd, 2019. Both required people to find alternate communication solutions. In our conference paper [2] we describe adoption of Virtual Private Networks (VPNs); here we focus on the challenges with adoption of decentralized (“peer-to-peer”) networking apps such as mesh networking chat apps.

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. 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 were not able 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

³Most people do not have regular access to home internet; thus, a mobile data blackout is effectively an internet blackout.

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 [5].

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—e.g. 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.

SOCIETAL CONTEXT ENABLES ADOPTION

The social characteristics of a user population are critical factors in technology adoption. Activists in Sudan leveraged the strong existing social structure of the activism community and that of the general Sudanese society in order to spread security and privacy advice and adopt certain practices that helped them when contending with their adversary. Here we focus on the societal characteristics of the Sudanese activist community that supported their adoption of threat models and behaviors to mitigate misinformation (more details in [2]). We explore how institutional knowledge sharing, trust building, and external support manifested for the activist community.

Mechanisms of sharing institutional knowledge, including security and privacy advice. The activists’ social structure supported largely informal sharing of institutional knowledge, including security advice, suggesting that a formal education or advertisement campaign for apps targeted at activists might be less successful than leveraging social narratives. 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 [6], [7], [8]. 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].*”

P12 talked about how their “fake news filtration” strategy was collectively acquired through multiple instances of mitigating online misinformation on Twitter by the Sudanese Twitter community: “I think that in specific the Sudanese community of Twitter have gone through multiple experiences of fake news filtration. There is synthesis and a lot of self critique. There are always discussions on Twitter and it’s easy to reply to on the platform.” Furthermore, they add that knowledge sharing through Twitter was a constant process that involved “suggesting something online, analyzed and scrutinized by the online community and then implemented...signal, feedback, signal, feedback until people were improving and going to a higher level.”

P6, whose neighborhood committee had a resident security expert, taught their friends about both BetterNet, a VPN, and Private Space, a Huawei operating system feature that they began using to hide information from the adversarial security services, NISS: “Just the private space—I told my friends about it, especially those who had Android phones. Also the Betternet VPN, I downloaded it for people to help them access social media apps when we found out it was the only VPN that was working.” In addition, through their local neighborhood group, P6 learned a few strategies to get access to the internet during the blackout. This involved breaking into landline networks such as those powering automated teller machines (ATMs) or other government services/institutions. To attain internet connectivity, they used an app called WiFi WPS Connect to detect nearby networks and then followed that with a second app that “shows you the exact password of that WiFi so that you can break into it and get internet access” (P6). Though P6 did not mention the name of the second app or how it worked, there are a few ways such an app can infer WiFi passwords, from brute-forcing the WiFi Protected Setup (WPS) PIN to targeting known vulnerabilities in older WEP networks, or even by performing small dictionary attacks on current WPA/WPA2 networks. Dictionary attacks try to systematically enter every word from a dictionary to break into a password-protected personal (home or small-business) WiFi network. Dictionary lists can range from a handful to millions of entries. Though our interviews focused on defensive technology, rather than offensive operations, P6’s disclosure of the use of commercially available WiFi cracking apps underscores the importance of future work on the security properties of these apps and their use by different groups, including activists, and opens the door to further study of specialized offensive technical operations. It is worth noting that P6 acknowledged that activists were aware that cracking WiFi networks was “not right” but they often had no other options during the internet blackout to communicate with the outside world.

Building trust in a constantly mutating group is critical to finding trustworthy information. As any activist group may be constantly changing with members joining and leaving, there can be a continuous need to build and maintain trust in a challenging environment rife with threats. P1 explained the

situation during the revolution: “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. 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 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” (P7).

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’s neighborhood committee’s Twitter page, seeking to be a source of news and grow in size, got a friend of a friend who was active and verified on Twitter to post that “this is not a fake page or anything like that,” which resulted in their Twitter followers increasing from 50 to nearly 4,000. P9 stated that the practice of the Sudanese Professional Association (a trusted entity) “verifying” neighborhood committee social media accounts was common. Bootstrapping was also used for building in-person trust: P1 described that new neighborhood committee members were mainly “mutuals who were already recruited trusted people,” who were additionally vetted through the in-person campaigns to clean the streets after protests.

So, activists relied on trusted contacts and networks that are multiple layers deep 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.

Support from abroad. Activist groups, though each may be unique, are not isolated, and may be connected to a diaspora or other domestic or international activist groups. We found that external support—both from the Sudanese diaspora and from groups in other countries—provided a source of technical advice, information verification, and news dissemination during periods when journalists were not allowed in, and enabled critical communication. Thus, those who study and design

for activists must consider the wider network of support that exists, and how that network supports, advises, and influences the target activist group.

For example, 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.*” In an effort to automate the process of fighting misinformation online, P14, a developer activist in the diaspora, built a platform that allowed the general public to “*upload any piece of news that they wanted to check whether it was verified or not and based on peoples’ votes, (reddit style) people can vote up or down.*” They added that they relied on specific voting weights assigned to verified voters, like journalists to determine the overall credibility of a piece of news. To enable adoption of the platform they only collected “*basic information, the bare minimum just to create the account.*”

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...*”

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.

A CALL TO ACTION

In our work, we retrospectively studied one specific group of activists at a certain critical time, during a revolution. However, there many other political activist groups throughout the world in different political, societal, and technical contexts, which shape their use of technology. For example, political activists in Hong Kong recently contended with facial recognition by their adversary, and wore face masks until they were banned by the government [9]. Internet blackouts have also occurred in Iran, Venezuela, and other countries after political protests, and censorship of various apps, websites, and technology is common throughout the world, as well as international sanctions that restrict the availability of certain technologies [10]. These different political, societal, and technical contexts can create conflicting design needs between different populations, and we ask researchers and designers to consider how a design

that might provide affordances for one group, fitting their threat model and allowing them to protect themselves, and for another group that same design can create disaffordances and vulnerabilities.

We urge researchers and technologists to continue to study activists for multiple reasons:

- Activists are a **driving force of geopolitical change** and, in many cases, fight against oppressive, discriminatory, and harmful forces.
- Activists may contend with a nation-state adversary, which puts their **technology under stress** that it may not be designed to withstand.
- Activists may be **innovators**, using technology in new or unexpected ways, or creating new technologies to fill the gaps apparent to them.
- Activism is only one example of how technology is not apolitical and **design choices have physical and political consequences**.⁴

It is important for the technology community—and, in particular, the security and privacy community—to understand how technology both enables and restricts activists, as well as how it endangers them and keeps them safe. We encourage future researchers and designers to consider the political, societal, and technical contexts through the guiding questions proposed in this article. We also encourage researchers and designers to consider that just as technology has clear physical and political consequences, problems that we may initially see as technical do not always have technical solutions, or solutions at all.

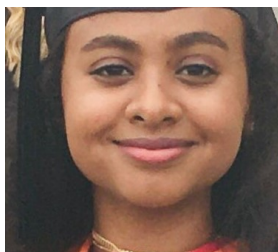
Where technical solutions do exist, we specifically call on mainstream apps to build features that may be vital for oppressed or vulnerable individuals. For example, one key challenge our participants faced was secure communication during the internet blackout. Though some were aware of—and tried to use—mesh networking chat apps such as FireChat, the lack of group adoption ensured its own downfall. Others had access to end-to-end-encryption apps like Telegram, but could not rely on others to safely use a new app. P9 explained: “*working with someone through an application they’re already using is better than working through another platform.*” So, mainstream inclusion of both mesh networking and a variety of privacy features such as disappearing messaging and end-to-end encryption would have helped the activists we spoke with. Technologists must consider such challenges and, where appropriate, carefully implement design principles that allow multiple access and threat models to coexist safely within an app’s community of users, while prioritizing the safety of vulnerable or oppressed users.

⁴For further work on how technology can impact users’ physical safety, see the related works section in our conference paper, as well as numerous other papers about vulnerable populations.

REFERENCES

- [1] Tufekci, Z., *Twitter and tear gas: The power and fragility of networked protest*, Yale University Press, 2017.
- [2] Daffalla*, A., Simko*, L., Kohno, T., Bardas, A.G., “Defensive Technology Use by Political Activists During the Sudanese Revolution,” *Proceedings of the 2021 IEEE Symposium on Security and Privacy (S&P)*, pp. 372-390, May 2021.
- [3] 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 Aug. 2021].
- [4] U.S. Office of Foreign Assets Control, “Sudan Sanctions Program,” <https://www.treasury.gov/resource-center/sanctions/Programs/Documents/sudan.pdf>, [Accessed Aug. 2021].
- [5] Albrecht, M.R., Blasco, J., Jensen, R.B., Marekova, L., “Mesh Messaging in Large-scale Protests: Breaking Bridgefy,” <https://martinralbrecht.files.wordpress.com/2020/08/bridgefy-abridged.pdf>, [Accessed Sep. 2021]
- [6] Das, S., Kramer, A.D.I., Dabbish, L.A., Hong, J.I., “The Role of Social Influence in Security Feature Adoption”, *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, pp. 1416–1426, February 2015.
- [7] Wash, R., “Folk Models of Home Computer Security,” *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS)*, July 2021.
- [8] Rader, E., Wash, R., Brooks, B., “Stories as Informal Lessons about Security,” *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS)*, July 2012.
- [9] Mozur P., “In Hong Kong Protests, Faces Become Weapons,” <https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html>, [Accessed Sep. 2021].
- [10] Newman, L.H., “How the Iranian Government Shut Off the Internet,” <https://www.wired.com/story/iran-internet-shutoff/>, [Accessed Aug. 2021].

SHORT BIOS



Alaa Daffalla received her M.S. degree in Computer Science from the University of Kansas in May of 2021 and her B.S. in Electrical Engineering from the University of Khartoum in Khartoum, Sudan. Alaa is primarily interested in usable security and privacy research and digital privacy in non-western contexts. Contact email:

alaashibeika@gmail.com



Lucy Simko is a PhD candidate at the University of Washington’s Paul G. Allen School of Computer Science and Engineering and was recently a remote intern at the Max Planck Institute for Security and Privacy. Her work focuses on the security and privacy-related needs and practices of populations experiencing crises or times of instability. Her research has been published at IEEE Security & Privacy, PETS, CHI, and IDC, and she is the recipient of a National Science Foundation Graduate Research Fellowship. Contact email: simkol@cs.washington.edu



Tadayoshi Kohno is a Professor in the Paul G. Allen School of Computer Science & Engineering at the University of Washington. His research focuses on helping protect the security, privacy, and safety of users of current and future generation technologies. Kohno has a BS from the University of Colorado and a PhD from the University of California San Diego. Contact email: yoshi@cs.washington.edu



Alexandru G. Bardas received his B.S. degrees from the Romanian-American University in 2008 and 2009, a master’s degree in Secure Software Systems from James Madison University, in May 2010, and a Ph.D. degree in Computer Science from Kansas State University in May 2016. He is currently an Assistant Professor in the Department of Electrical Engineering and Computer Science at the University of Kansas. His research interests include cybersecurity, mainly from a system’s perspective. Contact email: alexbardas@ku.edu