Keyboard Fighters: The Use of ICTs by Activists in Times of Military Coup in Myanmar

Laura Gianna Guntrum
guntrum@peasec.tu-darmstadt.de
Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt
Darmstadt, Germany

ABSTRACT

Amidst the ongoing anti-military protests in Myanmar since 2021, there is a noticeable research gap on ICT-supported activism. Generally, ICTs play an important role during political crises in conjunction with activists' practices on the ground. Inspired by Resource Mobilization Theory, I conducted qualitative interviews (N=16) and a qualitative online survey (N=34), which demonstrate the intersection between analog and digital domains, showcasing the ingenuity of the activists, and the rapid adoption of ICTs in a country that has experienced a digital revolution within the last few years. As not all people were able to protest on-the-ground, they acted as *keyboard fighters* to organize protests, to share information, and to support the civil disobedience movement in Myanmar. The study identifies, inter alia, the need for better offline applications with wider coverage in times of internet shutdowns, applications that cannot be easily identified during physical controls, and providing free and secure VPN access.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in HCI**; • **Security and privacy** → *Social aspects of security and privacy*; *Usability in security and privacy*.

KEYWORDS

ICT-enabled activism, protest participation, social media, social movement, Myanmar coup, internet shutdown, digital rights

ACM Reference Format:

Laura Gianna Guntrum. 2024. Keyboard Fighters: The Use of ICTs by Activists in Times of Military Coup in Myanmar. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3613904.3642279

1 INTRODUCTION

In recent years, the use of information and communication technologies (ICTs), particularly social media (SM) and instant messengers, during political crises have received increasing scholarly attention, including from the HCI community [6, 22, 53, 115]. In the early 2010s, the prevalence of ICTs became evident during widespread protests, including those that swept across much of the Arab world. Both activists and authoritarian actors skillfully harnessed technology's potential for multiple objectives, such as protest organization, gaining international attention, and surveillance [53, 108]. Since February 2021, many citizens from Myanmar have been using SM and instant messengers to protest against the military coup. The protest movement, locally also known as "Spring Revolution", emerged right after the military took over power and state counselor Aung San Suu Kyi was detained [95]. After the elections in 2020, the first legislative period of the democratically elected party, the National League for Democracy (NLD), was to begin on February 1st, 2021. On this day, the Sit-tat[1], the armed force under Min Aung Hlaing, staged a coup, claiming electoral fraud by Aung Sang Suu Kyi's NLD. In response, mass protests were organized across the country, primarily by young people [50]. Compared to previous protests in Myanmar (e.g., 1988, 2007, and 2015), information about the mass protests were now being spread (inter)nationally via SM, although hampered by blocked websites and internet shutdowns by the military [45]. Young people are "Myanmar's first generation of digital natives who participate and shape their identities in communication and dialogue with global digital media content" [50, p. 12]. With both the military using ICTs to consolidate control and civil society using it to gather information and as a "natural place for opposition" [45, p.14], the importance of ICTs, particularly SM, becomes highly evident since the coup.

To date, in contrast to numerous studies on e.g., the MENA[2] region, little research on Southeast Asia, including Myanmar, has examined the complex landscape of technologies used and the capabilities required to use them. Additionally, while existing studies in this region have primarily focused on Facebook (FB) and Twitter (known as X since July, 2023), relatively little research has been done on the use of instant messengers like WhatsApp and Signal during protests, as well as activists' technical requirements in conflict driven contexts. Building on this foundational perspective, the following research questions (RQs) will be addressed:

(1) How are ICTs used by protesters as a resource for mobilizing virtual and analog protests in the anti-military protest movement in Myanmar in 2021?
(2) What opportunities and challenges are encountered in the use of ICTs and how do protesters in Myanmar deal with them?

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
CHI '24, May 11–16, 2024, Honolulu, HI, USA
© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642279

[1]The military is often referred to as the Tatmadaw, a term that has drawn criticism by the population since Tatmadaw means "Royal Armed Forces". The term is considered problematic as it fails to reflect the non-royal nature of the military today. According to Desmond [25], "Now, we Burmese are not using the term *Tatmadaw* and are just referring to the armed forces as Sit-tat, or military, with no reference to glory".
[2]Middle East and North Africa.

(3) What technical requirements are identified by activists in times of protest?

Since the conditions during the protests in Myanmar are highly dynamic, the insights provide historical snapshots that reflect the state of affairs around mid-2021. Based on a qualitative online survey (N=34) and qualitative interviews (N=16) with activists in Myanmar conducted only shortly after the coup and in the midst of the protests, the study, using the lens of *Resource Mobilization Theory* (RMT) and qualitative content analysis [61], examines protesters' use of ICTs, especially regarding SM and messengers, how it has changed since the coup d'état, and how it has been used as an essential resource for mobilization. Furthermore, the study explores how activists adjust to varying circumstances, such as internet shutdowns and the implementation of a new Cybersecurity Law [100]. Lastly, context specific recommendations for improving technology to enhance the security and connectivity of activists during instances of military coups and suppression will be provided. The study captures relevant dynamics in Myanmar and thus provides a crucial and empirical contribution to existing literature on ICT-supported activism [117].

2 STATE OF THE ART: ICT AS A RESOURCE IN A POLITICALLY CONTENTIOUS CONTEXT

Since the emergence of ICTs, a substantial body of academic research has delved into the role of SM in fostering activism within conflict-affected contexts. In this section, RMT is presented as a theoretical framework for understanding the developments of both analog and virtual protests. Subsequently, studies dedicated to ICT-supported activism in fragile contexts are presented, aiming to draw relevant parallels.

2.1 Resource Mobilization Theory

In the study of social movements, RMT builds on a longstanding tradition of analyzing "contentious politics" [105] and the success or failure of collective action depending on the availability and use of resources which include material, human, social-organizational, moral, and cultural resources. Individual components are then categorized within these overarching groups (e.g., knowledge, money, solidarity) [27]. Generally, RMT understands protesters as rational actors (with grievances), who may be more likely to be successful when they have access to relevant resources (and know how to use them effectively) and follow organizational procedures that match their motives. By focusing on resources, the theory shifts attention away from simply examining grievances and instead emphasizes the strategic choices and capabilities of the movement [28].

ICTs can serve as valuable assets for social movements by reducing communication expenses and expanding their reach through increased user engagement (scale change) [32, 67]. It enables "resource-poor" actors, with fewer financial resources or facing contextual constraints, to communicate with a wide audience [23], and to build a widely interconnected movement more easily [67, 104, 105]. The availability of resources is profoundly embedded in existing social and economic relations, leading to substantial variation among social groups and zones. However, having access to ICTs does not guarantee success [29].

Besides rather positive aspects, such as enhancing mobilization and increasing international attention (which is particularly relevant for social movements facing domestic repression), ICTs as a resource can be inaccessible due to firewalls, and also contribute to surveillance, and persecution of protesters [67]. In the context of information systems research, Ortiz and Tripathi (2017) [75] pay special attention to socio-organizational resources, namely relevant actors for the successful mobilization on SM. They also refer to relational understandings of affordances of SM, which do not consider affordances for collective action to be established by mere properties of artifacts and human perceptions. Instead, they may be related to human agents' dispositions and social context [122].

2.2 Collective Use of ICTs by Activists during Political Crises

In recent years, numerous studies have examined activists' use of ICTs in politically contentious contexts, employing both quantitative and qualitative approaches [6, 54, 63]. In contrast to quantitative studies, qualitative studies offer a deeper understanding of the practical use of ICTs on the ground. As a result, they can also provide new insights for software design and implementation [77, 78], especially in contexts that have not been investigated by a large body of research work yet. Research, including studies conducted by [22, 31, 87, 96] show that, akin to the protests witnessed in Myanmar in 2021, numerous protesters incorporate ICTs into their activities, allowing a series of tasks such as networking groups, organizing on-the-ground demonstrations, and exchanging security measures. Zeitzoff (2017) [121] emphasizes that ICTs have different effects: ICTs increase the speed of information transmission, diminish costs of communication, alter which sources of information are accessible to actors, democratize participation, and offer alternatives to mainstream media through crowd-sourcing efforts. Starbird and Palen (2012) [102] further illustrate that individuals express solidarity with those on the ground by engaging in low risk, SM-based activities.

On the recipient's side, ICTs also affect information management, for example which information is considered credible and helpful in crisis situations and mass emergencies [12, 77]. The effective implementation of various of these aspects, such as enhancing the visibility and reach of content, is largely contingent on the role of language. In their study of SM behavior during the *thawra* (often referred to as Arab Spring), Al-Ani et al. (2012) [6] highlight different purposes of SM platforms depending on the predominant language used. They suggest that SM interactions in native languages might have a lesser impact on external, international communication, focusing more on reinforcing internal, domestic relationships. The nature of communication within these relationships is also of notable importance. Abdulla (2011) [1], drawing on insights from the Egyptian Revolution in 2011, demonstrates that communication, facilitated by SM, has evolved from a more vertical, top-down communication to a rather horizontal, bottom-up form of interaction. Via SM, not only can discrepancies between conflicting parties be reduced, but obstacles to participation can also be alleviated. In studies that delve into the possibilities of participation, intersectional approaches that consider different forms of discrimination (e.g., race, gender, ethnicity) often play a significant

role. Contributing to an intersectional perspective, Valenzuela et al. (2016) [111] conclude that SM reduces protest gaps associated with individuals' age, gender, psychological engagement with politics, and recruitment networks. In the context of Myanmar's diverse population, which includes numerous ethnic groups, the relevance of intersectional approaches becomes evident. It is also important to acknowledge the rural-urban divide in the country, particularly in terms of connectivity differences. Empirical findings in a similar vein were identified by Wulf et al. (2013) [120] in their ethnographic study of Palestinian activism.

Overall, in the realm of ICT-enabled activism, multiple empirical studies showcase meaningful interactions between analog and virtual spaces, emphasizing their interdependence. This is exemplified by Daffalla et al. (2021) [20], who highlight the building of trust through "non-technical approaches". Protesters, at times, use SM for background checks and to establish trust within the social networks of befriended SM users. Furthermore, they stress the significance of sociopolitical contexts in shaping privacy and security behavior, including international developments that may influence widespread app usage, for instance.

While numerous studies tend to emphasize the positive impacts of ICT-supported activism, there are also challenges linked to the use of technology during protest periods [69]. Social media blockades, misinformation, and internet shutdowns, as indicated by various sources [13, 20, 44, 108], can limit possibilities during political uprisings. In response to internet shutdowns, there is a growing reliance on mesh-messaging applications that empower users in close proximity to communicate independently of internet connectivity [9]. Moreover, numerous cases illustrate that governments have restricted internet access or specific websites to nationalize the internet [79]. Also, in Myanmar, internet shutdowns, whitelisted internet, and the implementation of the Cybersecurity Law have been noticeable since 2021 [16]. Specifically, the Cybersecurity Law imposes penalties for the use of VPNs, which allow access to prohibited applications like Facebook [30, 100]. Given these circumstances, activists exhibit a notable ability to adapt quickly to evolving situations. This is also evident in De Castro Leals's study [22], which examines how FARC guerrilla fighters quickly achieved a significant learning effect of new technologies (e.g., regarding localization), thereby avoiding life-threatening conditions.

Apart from instances of internet shutdowns, activists are contending with a rising pattern of digital surveillance, exemplified by technologies like the Pegasus spyware [3, 52, 112]. Therefore, numerous activists all over the world showcased ingenuity in creating strategies to bypass surveillance [110, 112]. Rohde et al. [87], for example, illustrate how the Free Syrian Army evade surveillance and how they deal with challenges arising from control by the Syrian regime. Moreover, they describe the criticality of mobile videos for documentation, mobilization, as well as propaganda. Generally, propaganda is seen often in situations of conflict, where various actors strategically try to manipulate perceptions to advance specific agendas [47, 82]. In the case of Myanmar, the military relies heavily on digital tools to spread online propaganda, seeking to achieve various goals, including strengthening soldiers' resolve and identifying dissent within their ranks [41, 73].

In sum, all studies consistently demonstrate that offline and online activities are mutually reliant, underscoring the necessity to view them as interconnected. To the best of my knowledge, there has not been any prior empirical study addressing ICT-supported activism in the immediate aftermath of the military coup in Myanmar in 2021. Generally, there is a notable lack of empirical studies focusing on Southeast Asia and of in-depth investigation into activists' technical demands and needs in times of protest and oppression (e.g., improved mesh networks). Moreover, it is crucial to understand the precise reasons that drive activists to use certain applications. This study builds on this research trajectory by exploring how activists in Myanmar leverage ICTs and navigate risks within an environment of internet shutdowns.

3 METHOD

Throughout the study, extensive consideration was given to research ethics, the principles of do-no-harm, data security, and the legitimate presentation of findings. It needs to be stated that the publication of this paper was intentionally delayed until the situation in Myanmar had slightly calmed down to avoid unnecessary security risks.

3.1 Case Selection

Myanmar, the second-largest country in Southeast Asia, suffered under colonialism and decades of war and protests [59]. In Myanmar, the internet penetration rate increased from 0.23% in 2011 to 44% in 2023 [55], which is why the country is often perceived as an 'internet success story' [74, 86]. According to Sin Oo and Thant [99, p. 12] "Myanmar experienced a 'digital connectivity revolution' around 2014", amongst others, through the liberalization of its mobile telecommunications market. However, in 2007, Myanmar was one of the first countries to experience government-imposed internet shutdowns [114] and now ranks among the countries with the least favorable environment for internet freedom [38].

As previously noted, the specific focus lies on the use of ICTs in the protests since February 2021. To date, several academic studies examine the so-called "digital revolution", the media landscape more generally, and the role media plays in Myanmar's political transition (amongst others [15, 99, 100]). Studies such as that by Thein-Lemelson [107] illustrate that politically active individuals commonly use SM to build networks with other activists from all over the country. Since February 2021, this has been constrained through measures like internet censorship and deliberate shutdowns (mostly between 1am-9am) [16, 76]. Moreover, online propaganda, fake news, and hate speech persist from various entities, including the military, exerting a significant impact on socio-political life [58].

For identifying fake news, for example, media literacy programs for civil society are important. Therefore, a newly formed digital resistance movement in Myanmar recognizes its responsibility to educate people about the potential risks associated with digital activism and to provide guidance on safeguarding themselves in the digital sphere [34, 73]. The International Crisis Group [45, p.28] states that many people in Myanmar do not have in-depth knowledge about security-related issues:

> "Although digital security habits have improved significantly since 1 February, including through the uptake of VPNs and encrypted messaging applications such

> as Signal, it is largely younger and better-educated users who have tightened up their practices".

Hence, in contrast to previous research on contemporary protests and ICTs, which primarily relied on Twitter/X and Facebook data for their analysis [11, 90], this study aims to empirically investigate how activists employ ICTs and what technical needs they have in times of surveillance and internet shutdowns [3].

3.2 Data Collection

Since qualitative interviews with activists offer the possibility to get deeper insights into the interviewees' perspectives and individual strategies, an empirical qualitative research design was chosen. Obtaining in-depth understandings of local conditions and activity's needs can significantly enhance the quality of subsequent technical design implications [94]. Research findings can be used to advocate for context-sensitive capacity building and policy changes that address the needs of often underrepresented communities.

The explorative field access to the interviewees was provided through personal contacts living in Myanmar, recommendations (snowball sampling) [71], contacting local NGOs, and already established networks such as *Myanmar-Netzwerk*, Germany. The different actors were requested to disseminate the inquiry (encompassing project information alongside contact details) to diverse individuals and groups. Through these access points, people (aged 18 and above) interested in the interview contacted me on their own initiative. This underlines that all interviewees participated voluntarily out of their own interest in the topic. The voluntary participation corresponds with one of the main principles of ethical field research [106]. Following the principles of theoretical sampling, the primary focus was on ensuring the inclusion of individuals who possessed personal experiences and direct involvement in the protests. The sampling approach was deemed appropriate when data saturation was achieved, indicating that a sufficient amount of information had been gathered to gain a comprehensive understanding of the phenomenon under study [71]. Recognizing that I am not a member of Myanmar's politically active community and has only visited the country once, continuous dialogues with personal contacts in the country were sustained throughout the research process. These discussions encompassed various subjects, ensuring the implementation of culturally sensitive and ethical research practices. I am grateful for the support and guidance they have generously given me, providing valuable advice that has greatly enriched the research process.

Overall, 16 qualitative interviews ($x_{\max}$ = 101 min, $x_{\min}$ = 37 min, $\overline{x}$ = 73 min) with activists from Myanmar, who participated in the protest, were conducted virtually through "Signal" and "Jitsi.meet" between February and May (2021). The interviews took place during periods when internet connectivity was available and not constrained by internet shutdowns. Out of the 16 people interviewed, eight people identify as female and eight as male. 12 participants live in cities and four in rural areas. Since mostly persons from generation Z and Y are actively engaged in the protests using ICTs, mainly young people were interviewed from all over the country. Before the interviews, the interviewees were informed about the scope, the purpose, and the procedure of the study, including the option to withdraw from the study at any time. Participants gave their consent either by signing a consent form (with a chosen name) or by giving verbal consent at the beginning of the interview. None of the interviewees was compensated. In general, ethical considerations regarding the compensation of interview participants (living in safety-critical contexts) are a constant topic of discussion in academic circles. From my perspective, providing financial compensation is easier in the context of in-person interviews, as it alleviates the need to gather sensitive contact details such as full names and bank information. However, when interviews occur online, preserving complete anonymity becomes a more intricate challenge, given that interviewees cannot receive payment in person. I opted against providing financial compensation to the interviewees to avoid collecting additional personal data and the potential transfer of such information to university administration for billing purpose, where data is retained for an extended period. It would be generally outside of my control who could have access to this data. Although the risk is minimal, instances of data leaks involving several university administrations have been reported (e.g., [49]). This is why I have chosen to minimize data collection further, aiming to reduce potential risks for participants. Moreover, I aimed to ensure participants' voluntary involvement, to prevent the establishment of false incentives, and to deter dependencies that could arise from financial compensation. However, I also recognize that this decision is intricate, as it inherently gives rise to power imbalances and potential exploitative tendencies on the opposite end. I am in favor of a broader discussion on the development of secure mechanisms for the financial remuneration of respondents, while ensuring the protection of their identity. My considerations were carefully discussed in advance with other stakeholders conducting research in safety-critical contexts and were part of a risk analysis carried out.

To facilitate the structuring and comparison of the interviews, I used a semi-structured questionnaire (see Appendix A.1) that was abductively elaborated on the basis of RMT and current information on Myanmar from newspapers. The interview guideline included open questions on the following: personal background, digital literacy of the participants, questions about the digital culture and general practices, as well as the perceived security and safety and concerns about the current situation. In designing the questions and the research design itself, the principles of ethical field research and do-no-harm were followed [37, 43, 46, 56, 119]. It is worth noting that all interactions were exclusively in English due to my lack of proficiency in the languages of Myanmar, including Burmese, and the fact that live translation requested from translation agencies was unfortunately beyond the allocated budget. Moreover, the university's language center could not assist due to the unavailability of Burmese language services. The deficiency in my language skills introduced a potential bias in the study and limited the pool of eligible participants to those proficient in the English language. Consequently, this may result in overlooking essential perspectives and potentially neglecting cultural nuances within the community. After the interviews were conducted, any particularly sensitive information that made it into the recording was deleted. Then, the interviews were manually transcribed (offline), formally anonymized, and sensitive information was deleted. The anonymized data is securely encrypted (via VeraCrypt) and accessible solely to myself, ensuring strict confidentiality.

Additionally to the interviews, a GDPR-compliant online survey was conducted (using SoSci), available in both English and Burmese (translated by a Burmese translator living in Germany) to ascertain whether distinct outcomes would be observed in Burmese language. Remarkably, only ten participants completed the survey in Burmese. The reason for this remains uncertain. One possible explanation for participants opting to reply in English might be linked to my background, as outlined in the introduction of the survey. The survey questions closely mirrored the interview content, and participants provided informed consent before participating voluntarily.In total, 34 individuals commenced the survey, with 25 successfully completing it. Despite incomplete responses from some participants, the data remains valuable for extracting meaningful insights. Overall, 22 identified as female, 11 as male, and one selected "Other". The majority were relatively young, with 44% being between 18 and 24 years old, 32% between 25 and 30, 18% between 31 and 35, and 6% between 36 and 40. 91% indicated residing in a city.

3.3 Data Analysis

Due to the possibility of category formation, the data analysis of both the interview and online survey data was inspired by the qualitative content analysis proposed by Kuckartz (2014) [61]. Employing an abductive approach, the study sought to deduce theoretical trends from the data collected empirically while drawing insights from related studies and RMT. To enhance intersubjectivity in the coding process, I received support from another researcher during the coding phase, using the software MAXQDA (Analytics Pro 2020) and followed criteria proposed by Kuckartz (2014) [61]. Coding was first done independently, then the results were jointly discussed and an intercoder agreement was assessed. Subsequently, I completed the creation of the code book based on these discussions, inspired by RMT and existing studies. A total of 49 core categories (level 1), each with associated sub-categories (codes; level 2-4), were identified (see partly in Appendix B).

I acknowledge that my personal background (white, European, cis-gender, female) and political orientation make it difficult to achieve complete objectivity, a criteria that is often expected in academia. Additionally, I am aware that respondents may be reluctant to fully engage with me because of this background, which could potentially lead to a bias in the data collected. I concede that I might not fully understand the intricacies of local customs, traditions, or social norms, which can lead to misinterpretation of data. Although I try to be as critical and reflective as possible, I realize that preconceived notions may unintentionally influence the analysis and lead to a skewed understanding of the data. To provide as much transparency as possible for this process, the detailed coding scheme is provided as supplemental material. Lastly, I recognize that researchers, myself included, often wield the influence to shape narratives, potentially influencing the international community's perception of activists and their challenges.

4 EMPIRICAL FINDINGS

This section begins by addressing how activists use ICTs, followed by a discussion of its opportunities and risks. Subsequently, the technical needs are discussed, some of which are derived from the identified risks. Solely non-sensitive observations and insights from interviews that do not reveal personally identifiable details or any information that could potentially jeopardize the safety or well-being of the interviewees will be disclosed.

4.1 ICT Usage during Anti-military Protest: Perspectives from Myanmar Activists

In recent years, the significance of SM and messenger apps has grown substantially among almost all interviewees and online survey respondents (OSP1, IP15:40)[3]. This shift can be attributed to significant reductions in smartphone and SIM card prices (approximately 200 USD in 2014 and 1.5 USD in 2020), granting widespread SM and messenger access (IP9:37). Moreover, Wi-Fi and mobile data have simplified access for a major part of the population, however media literacy still seems to be quite low in the country (IP16:113). Particularly FB, which is often referred to as the internet (IP15:78), was considered to be the most frequently used social network during the protest (IP2:81). According to SinOo, when people talk about "going online" they often refer to being "active on Facebook" [99]. This has different reasons, such as Meta's Free Basics initiative between 2013 and 2017[4] and the fact that FB is often preinstalled on mobile phones [60]. FB enjoys a significant advantage over many other platforms due to its availability in Burmese and its ease of use. Yet Facebook's history in Myanmar has been marred by incidents of hate speech, violence against the Rohingya ethnic group, propaganda (including military-related content), and criticism due to inadequate measures to block radical viewpoints [15]. Recently, other applications such as Twitter (IP10:49), Signal (IP14:34), Instagram (IP6:29), Viber (IP13:23), WhatsApp (IP15:20), TikTok (IP4:83), YouTube (IP15:22), and Slack (IP6:144) have gained importance — but a minor one compared to FB. Activists actively use these apps to post and share content, with the frequency varying significantly from once an hour (IP10:41) to every few weeks (IP6:55). Respondents mentioned that the coup and the subsequent protests were dominant topics trending on SM (OSP9, OSP36). Furthermore, China's support of the military, the release of Aung San Suu Kyi, and international politics (e.g., R2P) were discussed (OSP15). IP4 (109) argues that

> "since the military coup they all just get interested in political issues and they are really helping in keyboard fight, they are really helping in delivering up-to-date news to the people who are going outside and who are staying at home to communicate more effectively".

Since the Sit-tat took power, interviewees expressed the desire for permanent connectivity (IP3:52) and elucidated the dominance of smartphones for using services due to their compact size (IP4:51) and portability (IP10:35). The results indicate that the ICT behavior by Myanmar activists has changed remarkably: Applications, such as Signal, gained importance and more time has been spent using SM and messenger (IP7:53). SM and messaging apps function as convenient and rapid means to distribute information regarding protest events (IP10:85) and provide guidance on future actions (IP1:90). IP3 (85) stated that "SM plays an important role, not just

[3] OSP = Online survey participant; IP = Interview participant + transcript line

[4] Meta's Free Basics initiative offers free access to a select range of online services and websites (including Facebook) to individuals in the Global South with limited internet access, without data charges on their mobile plans.

to connect with one another [...] it also gives us awareness, what to do in this political crisis in Myanmar". The majority of respondents believe that SM plays a crucial role in protests. SM provide avenues for organizing large gatherings (IP8:116), facilitating many-to-many communication (IP4:115), establishing mechanisms for mutual coordination (IP11:123), disseminating security instructions (OSP9, OSP32), bolstering local factions (OSP39), and exerting pressure on military authorities (OSP21). Digital organization about time and place is frequently considered a "starting point" (IP8:116) for further actions. The importance of organizing protests digitally prior to demonstrations on-the-ground seems evident to all interviewees.

All interviewees participated in online protests to varying extents. Fourteen were actively involved in street protests, one abstained from physical participation, and another withdrew due to escalating violence (IP13:73). In the online study, 61% of respondents identified as "keyboard fighters", while 55% actively joined on-the-ground protests. Given the higher physical risk of street protests, SM provides an alternative for sharing information and anti-military content. IP9 (103) stated that many people join the Civil Disobedience Movement (CDM)[5] solely online and not on-the-ground. This had several reasons: people were hindered due to work obligations (IP15:126) or familial constraints (IP16:77). According to the interviewees, the majority of street protesters also exhibit active online involvement: "On the rest of the day, that I could not participate in the demonstrations, I shared information, and I shared knowledge, so I mostly do both" (IP2:120). During protests, some activists live-streamed incidents (IP14:74), ensuring quick and reliable transfer of information and giving advice (IP1:136). Livestreams are also helpful to attract international attention, to engage with global audiences, and to garner assistance (OSP35). Videos, in particular, showcased the firsthand experiences of protesters and the harsh actions of the military crackdown, providing a way for individuals to share their personal narratives. Some interviewees highlighted that live videos, especially those portraying violence, have a propensity to evoke intense emotional responses, such as feelings of sadness and grief, among individuals (IP10:109). This heightened emotional engagement, as noted in IP1 (131), was also seen to contribute partially to increased participation in the movement and the fostering of a collective consciousness.

IP10 (79) raised concerns about the capacity of SM-based protests to generate enduring political transformations. According to them, protests on-the-ground may be more effective since (inter)national media can capture events directly. They perceive physical protests as more effective than FB, a constraint of which being not able to reach an international audience: "If we want to break the news internationally, that has to be done by the press. So, I just use SM to motivate my own people, my friends, my colleagues to bring in to my protest only" (IP10:79).

4.2 Leveraging Technology for Activism: The Role of ICTs in Myanmar

Below, both the advantages and disadvantages of using ICTs in protests in Myanmar are illustrated to answer RQ2.

[5]The CDM refers to a widespread protest movement initiated by various sectors of society, including government workers, medical professionals, and teachers in response to the military coup [113].

4.2.1 Amplifying Voices: How ICTs Draw International Attention. IP3 (87) emphasized that posting on SM is "important for global awareness", so the international community "can take proper actions". Besides the international community, the Myanmar diaspora actively supports online protests, offering resources, amplifying messages, and coordinating international advocacy efforts. Solidarity groups such as "Myanmar people in Europe", mostly on FB, share news and personal stories to raise awareness. According to IP11 (177), support from people living and protesting outside of Myanmar is very helpful. Generally, Twitter is a suitable platform for generating international attention due to its international reach, fast-paced nature, and the simplicity of using hashtags, such as #RejectMilitaryCoup (IP13:71). Nevertheless, due to Twitter's relatively recent introduction to a significant number of Myanmar residents (IP1:90), its usage appears to be somewhat confined to individuals who are more inclined towards SM engagement[6]. In early February (2021), many people posted hashtags like #SaveMyanmar to draw attention to human rights violations. By May 2021, this was reinforced by concrete demands such as #WeNeedR2PinMyanmar. Another hashtag, as pointed out by IP5 (13), is #MilkTeaAlliance, symbolizing solidarity with the online democratic solidarity movement, initially originating from Hong Kong. Digital exchange with activists from other countries, such as Hong Kong and Thailand (IP1:33), is perceived as an important social-organizational resource for drawing on experiences from other "alliance groups" (IP16:135). OSP2 stated that activists in Myanmar are "inspired by Hong Kong and Thai protest movements to get international media attention and how to be safe in protest (especially clear tear gas, self-defense)". They received guidance on constructing defense equipment (IP15:132), responding to military crackdowns (IP1:134, OSP40), selecting appropriate attire and gear (IP3:149), and using technology in times of protest (IP8:186).

4.2.2 Empowering Causes: The Formation of Technology-Supported Solidarity Groups. Another significant facet of SM usage during the protests involved the coordination of groups (mostly on FB, Telegram, and Viber). Aiming to exchange firsthand information about blockades and gunshots (IP5:5), activists established networks to stay in contact with neighbors (n=5). IP16 (73) explained that

> "in the township we have a Telegram group and we do not share our Telegram group with all the people in the township. If we want to be in the group, we have to go to group leaders personally, and if they recognize us and if they know at which street I am living, they add us in the group. It is not a public group, they just add people who they know personally".

Hereby, analog and personal arrangements are crucial to ensure personal security, to build trust, and to verify that no spy (e.g., military member) may enter the group to gather information. After incidents became public, the "inner circle" of the group will meet e.g., in Zoom, where "people are allowed to join" (IP15:51). During internet shutdowns, conventional phone calls were employed (IP1:107). Many people benefited from creative (problem-solving) approaches from involved neighbors. Although security measures

[6]In 2021, Twitter was used by less than 10% of Myanmar's population [101].

are taken, opposing group members sometimes still seem to succeed in penetrating the groups and obtaining information (IP16:71). In addition to neighborhood watch groups, groups have been introduced for the purpose of organizing protests. Especially in response to escalated violence, guerrilla groups have emerged, organizing guerrilla tactics as a countermeasure to military strategies (IP16:71).

4.2.3 Communication Possibilities In Times of Internet Shutdowns. Faced with widespread censorship, surveillance, and human rights abuses, activists in Myanmar find themselves operating within a restrictive online environment. The internet was mostly shutdown right after the coup for almost two and a half months between 1am-9am (IP4:41), restricting people to communicate (IP1:107), to livestream (military) incidents and night-time crackdowns (IP13:103; OSP34), to stay informed about news (IP7:140), and to be entertained (IP6:130). Some areas of the country were more affected by the restrictions than others, as some parts were almost entirely truncated. A complete internet shutdown was not feasible, since businesses and banks rely on the internet, resulting in an entire system failure in case of a prolonged outage.

To stay connected during the night, Myanmar residents partially sent short text messages (SMS) and received condensed news updates by subscribing to portals that distributed current information via SMS (IP14:114). Six interviewees stated receiving a short text message in mid-February (2021) that Aung San Suu Kyi had been released. People had already begun celebrating in the streets, until many came to realize that the information was not accurate (IP11:139). In times of internet shutdowns, it seems almost impossible to verify such text messages. Most participants strongly agree or agree that internet shutdowns are a problem (OSP14, OS37). In response to inquiries about the entities responsible for the internet shutdown, a majority of interviewees and online respondents pointed to the military (IP12:128), followed by mentions of both the military and telecommunication providers (IP2:115). A smaller number attributed the responsibility solely to telecommunication providers (IP11:49). Even if they are seen as (partly) responsible, there is often a recognition of the presence of economic dependencies (IP11:149).

Besides internet shutdowns, Myanmar residents faced SM and messenger blockades (IP1:113). All interviewees and 72% of the survey respondents stated using a VPN, allowing them to continue accessing blocked websites and applications such as FB and WhatsApp, despite using a VPN being officially forbidden since the coup after the introduction of a new Cyber Security Law (IP7:2; IP1:138). VPN seems new for most of the people (IP1:113). As a result, younger generations play an important role in helping older individuals who are less familiar with new technical demands (IP14:88). According to the participants, paid VPN services generally offer enhanced security and privacy. However, it's important to acknowledge that disparities in financial means and technical proficiency exist, making it difficult for everyone to afford paid VPN services (IP5:3). Furthermore, for some, data security seems to be secondary when using VPN, as their primary focus is on acquiring information and facilitating communication (IP14:92). Regarding security measures only four individuals mentioned using Tor (free), which offers both censorship circumvention and anonymous internet browsing (OSP12, IP8).

Another, but rather limited way of dealing with the internet shutdown is using foreign SIM cards such as those from Thailand: "Most of the generation Z or the generation Y are using the Thailand SIM card. These SIM card users can access the internet every time" (IP9:124). An additional, albeit limited, method of communication involves using offline, Bluetooth-based mesh networks, allowing many-to-many communication over a distance of approximately 100 meters. Two interviewees mentioned using Briar (IP5:5) and Bridgefy (IP14:92), both of which are applications based on mesh networking technology. However, for mesh networking apps to function effectively, widespread usage is necessary — a condition that appeared to be lacking in Myanmar as of May 2021 (IP5:5). According to a news report in February (2021), offline messaging apps, such as Bridgefy, were downloaded over a million times [83]. The degree to which conventional communication tools like walkie-talkies are employed remains uncertain, with only one respondent indicating the use of a walkie-talkie (IP10:83).

4.2.4 Exploring Boycotting and Punitive Measures. Other examples illustrating the connection between analog and digital activities include the social punishment movement and the boycott campaign, which identify both individuals and products affiliated with the military:

> "I agree with boycotting the products. [...] Because, you know, if we cooperate, if we use their services, like for example Mytel Telecom companies, this is the military business. It's like we are paying them" (IP13:111)

To identify products and services linked to the Sit-tat, individuals have developed applications like Way Way Nay and Blacklist Myanmar that offer listings that reveal connections to the military (IP14:126). In total, 11 interviewees strongly supported the boycott campaign. Several respondents also stated to be active in the social punishment movement, publicly exposing military family members by disclosing photos and business information on SM (IP14:126).

Furthermore, some Myanmar residents boycott TikTok, Chinese mobile games, and other Chinese companies because of China's criticism for supporting the military in Myanmar (IP16:105; OSP6). On a rather individual level, it is evident that many activists agitate online against individuals related to the military. Sixteen survey respondents indicated that people who support the military are identified and publicly accused online. The objective is to put pressure on individuals and publicize who is supporting the coup (IP16:105). It seems that the campaigns are building a sense of cohesion and explicitly targeting individuals associated with the Sit-tat.

4.2.5 Impeded Use Of Resources Due To Misinformation and Censorship. Another significant aspect concerning the limitation of frequently accessed resources is the surge in misinformation, particularly evident since the coup (n=23). Eleven of the interviewees and all survey respondents mentioned that it is extremely important to check all news and posts because misinformation is so prevalent (IP15:96) and the verification of information is challenging (IP14:103). Misinformation ranged from false reports about internet shutdowns (IP14:103), injured and deaths at protests (IP14:103), violent crack downs and locations of the military (IP13:121), to

the apparent release of Aung San Suu Kyi (IP7:140). IP16 (113) acknowledged that even in their community, "[they] sometimes share information without knowing if it is right or wrong, although [they] have been using SM for so long. Sometimes [they] fail to check the information". Verification in conflict-affected contexts is even more challenging as many ambiguities exist. Responding to this, on the one hand, cross-checking with other sources is a common way to verify information (OSP4), on the other hand, friends living in the affected area may be contacted: "If I want to know if it is true I call my friends and ask them if it is true." (IP1:101). Some people in major cities, where a lot of protests took place, seemed to have better access to several sources than people in rural areas. There, it sometimes seemed difficult to assess what was really happening (IP13:91). Since misinformation and fake news may cause dangerous consequences, many people report them to FB and urge FB to be more proactive in deleting them (IP7:110). IP7 (112) even stated that while misinformation was reported, they were mostly not taken down. Notably, FB and Instagram do not seem to understand and tolerate the local context: Only in a few cases, FB blocked military pages to restrict misinformation and propaganda (IP3:111).

Besides checking on various news portals and talking to friends, Telegram channels were mentioned several times to verify news. Some interviewees mentioned that they follow certain journalists and activists to receive reliable news quickly and easily (IP14:105). Telegram channels might support activists in easily accessing the credibility of information since most media agencies have been banned recently by the military (IP16:43). In addition to the spread of misinformation, there's a regular occurrence of violent content being shared online. This includes videos showcasing instances of violence during protests (IP4:75) and intimidating videos originating from the military. Death threats by soldiers were captured e.g., on TikTok, but then commonly later deleted after numerous reports (IP7:166). According to 17 respondents, SM providers not only delete content by the military — they also erase and censor (inappropriate) content by individuals not complying with set rules. IP13 (95) explained: "My account has been reported. I think during these days very often. Like while I was broadcasting live". Others reported that China-related content has been restricted:

> "The most popular right now is that Facebook is taking down all the posts about China and we have to mention China in creative ways, so that Facebook does not recognize it" (IP16:115).

Thus, activists need to paraphrase certain words so that FB employees and FB's AI would not recognize them so easily. Due to the complexity of the Burmese language, there appear to be instances of misunderstanding on the part of service providers (IP6:108).

4.2.6 Data and Device Security In Times Of (Digital) Surveillance. Aspects like surveillance and the scrutiny of mobile devices highlight that SM does not yield solely positive effects. Since the coup, people are increasingly afraid of military controls and hacking attacks. This stems from the understanding that military personnel scrutinize FB profiles both in the digital realm and through physical means, occasionally inspecting smartphones in public spaces (IP15:110). Since FB is the predominant platform, individuals' FB accounts are primarily examined to ascertain whether they post anti-military and pro-protest related content. IP11 (107) mentioned that the "police checks on your phone randomly. They are checking your SM and if there is something they found against the dictatorship you would be arrested". In response, some people no longer have their own FB account (IP15:116), use a fake account (IP13:32) or do not talk about politics at all on SM (IP15:118). 13 interviewees asserted that they consistently remove sensitive information. IP1 (113) shared that in order to secure their employment status, "I log in my fake account" to share "some K-PoD news or some military news or even save some photos that supports military on my phone". Similarly, IP15 (24) mentioned that although they did not want to, they created a second account to protect themselves and their friends, posting random photos of animals and celebrities. Generally, FB has been criticized for not guaranteeing data security and for not deleting violent content in the past (IP7:99). Even though violent posts and hate speech have been a regular problem, not everyone switched to alternative providers. Nevertheless, there has been a change in behavior as an increasing number of individuals switched from FB Messenger to other, more secure (partly end-to-end encrypted) providers such as WhatsApp (IP3:27), Telegram (IP13:31), Signal (IP2:97), or uninstalled FB for a while (IP10:91).

Nine interviewees reported that since February 1st, Telegram has gained popularity and has been perceived as more secure (IP15:116). This could be attributed to the concern that some individuals have regarding FB (IP9:138, IP13:31). Overall, it's notable that many people consider Signal, WhatsApp, and Telegram to be on par in terms of data security, even though Signal assures more data security (IP16:33). Further, IP1 (115) highlighted that they "thought that WhatsApp is very safe to talk compared to messenger. Now I found out that WhatsApp is also not a good place to talk. It is not a safe place". IP7 (69) stated that they only FB messenger because of their friends and family and are "happy now that the government banned Facebook and everyone is coming to Telegram and Signal". This statement illustrates that some people do not switch to alternatives for own concerns and security reasons, rather for causes such as the military's ban on Facebook.

An additional security precaution taken after the coup involves the modification of personal settings (n=10). IP14 (92) mentioned that particularly active activists offered training on digital security, which is why "people are taking it seriously now. In the past, people didn't really care about security". IP14 (60) mentioned that most people involved in the "activist community" are aware of "digital issues", making their profile less public and changing privacy settings. IP14 (60) conveyed that some activists asked to keep profiles public, as locking all profiles could signify heightened apprehension about the military's actions. Moreover, "the more people [lock their profile], the easier it is for the military to arrest people, who didn't do that" (IP14:60). However, the availability of the "profile locking" feature on Facebook proves to be a valuable asset in situations of tension (IP14:60). The possibility of locking the account was introduced shortly after the coup, hindering, amongst others, people from seeing posts or photos on one's timeline (IP15:56). Nonetheless, the delay in Facebook's account locking process could potentially pose challenges, especially in cases of detention (IP16:172).

Additional security measures, although not widely adopted until May 2021, encompass the following: 1) having multiple SIM cards (IP3:135), 2) avoiding to use the military-owned company Mytel

(IP14:78), 3) using the Tor browser (OSP11), and 4) using (paid) VPN (IP13:107). Among the interviewees, no one reported using the Tor browser, while three acknowledged knowing about it. IP7 (152) explained that they refrain from using the Tor browser due to the already poor internet connection, which would be further compromised by Tor's usage. With regard to 4) it needs to be stated that although VPN usage was widespread, only IP13 (107) highlighted the importance of using a VPN for security reasons. Regarding live-streaming, some risks must be emphasized, notably,

> "[...] that these [...] have [given] access to the military, the crackdowns, the police to know the ins and outs of a protest movement. They were able to pinpoint more of where a protest is happening and thus arriving there more quickly compared to if people would not have uploaded them" (IP15:128).

The potential of revealing tactics and capturing activists on camera, leading to potential identification by the military, is a concern associated with live-streaming (IP10:109). IP16 (137) explained that due to increasing detentions, activists are live-streaming and posting less off protest activities than in February and March (2021). According to IP15 (116), in the digital age, every information can be spread and misused very easily by opponents such as the military. 15 survey participants strongly agree or agree on being concerned about the military having access to personal content. IP13 (109) said that in times of this crisis,

> "everybody needs to be concerned about their personal data, because your house can be searched anytime. And, even though you support military or not you might be arrested, because they arrest every people they see on the street".

Despite these existing risks, a minority of respondents displayed minimal concern about their data (n=3).

4.3 Emerging (Technological) Needs in Protest Environment

One goal was to grasp the technical needs of activists during protests (RQ3). The findings reveal divergent perspectives: OSP33 mentioned that "SM platforms and messenger apps are not missing anything. People are the ones who needs to use them more efficiently". The results indicate that, in total, 25 people think that most of the SM applications and instant messengers are easy to understand. However, when asked if people would like to see more options for anonymization, 15 responded yes. There was a notable consensus among respondents regarding the potential usefulness of indications for possible misinformation and fake news (n=20). IP1 (121) emphasized the importance of curbing the spread of fake news, as they hold the potential to inflict harm on individuals. Moreover, it should be easier to block certain accounts (n=9) and to efficiently tackle and denounce hate speech (n=16).

Activists suggest strategies, including a fast FB account deactivation for arrested individuals through a single comment or report, countering potential delays in reporting. Rapid actions are crucial, ensuring that confidential information and contacts are not misused by the military: "We have people who get arrested, but the reporting is very slow, so sometimes the security forces can check their FB accounts. I think it would be really helpful if we had that" (IP16:93). To better protect anonymity, it was stated that it would be helpful not to register with one's private number and to use nicknames more often instead of providing one's real name. IP7 (116) stated that "sometimes FB is forcing us to use real names".

Additional recommendations were the following: Firstly, IP10 (99) requested that it would be helpful to "check in safe" during each demonstration, using the "Safety Check" feature on FB (IP10:99). Secondly, receiving push notifications from SM providers, such as FB, to stay informed about security measures and privacy settings would be advantageous (IP16:99). Furthermore, more information about the protest should be publicly available on FB — similar to practices during the COVID-19 pandemic, where a constant stream of information was disseminated (IP15:56). Thirdly, IP8 (112) urged to secure individual chats, e.g., in WhatsApp, through a pin code. Generally, it would be advantageous if selected chats would be inaccessible in the general list of people one is talking to without having to delete them. Particularly during mobile phone checking, it would be helpful to prevent direct visibility of specific chat histories.

5 DISCUSSION

After outlining and discussing the findings (Section 5.1), I present context-specific recommendations tailored to activists affected by the consequences of the military coup (Section 5.2). These thoughts and ideas, derived from the presented data and existing literature, center around the use of specific applications and features.

5.1 Contextualizing ICT-Enabled Activism in Myanmar

The empirical research complements existing HCI work on ICT-enabled protest [6, 20, 22, 64] by providing concrete empirical findings and addressing context-specific technical requirements for activists, an aspect that has been relatively scarcely researched so far. Drawing on extensive interview and survey material, the study illustrates that the participants, forming part of anti-military protests in Myanmar, rely on different social, material, and human resources for mobilization [32] and quickly adapt to an environment marked by internet shutdowns, misinformation, and physical checkpoints (IP1; IP15). Unlike most studies concentrating exclusively on ICTs as a standalone resource, this research represents a pioneering effort in exploring the importance of looking more closely at the synergy among various resources for the effective use of ICTs in conflict-affected contexts. Myanmar stands out from most previous studies due to its rapid digital transformation [99], a long history of high levels of digital violence [15], and protest.

Both interview and survey data revealed that more study participants participated in online protests than in street protests, since street protests were generally perceived as significantly more dangerous (IP13). Participation was considered important in both forms of protest and partially complementary to each other (IP8). Principally, supporters were mobilized through SM to increase the size of the movement, consistent with RMT principles [27, 102]. Different applications with varying attributes were used for distinct purposes with FB being the dominant application to communicate [1, 98]. In addition to individual communication, messenger services were

used for group chats (IP15) and organizing neighborhood-watch-groups (IP16), aiming to adopt non-hierarchical networking between activists [1]. Examples such as neighborhood-watch-groups demonstrate that collaborative applications help to facilitate exchange between digital and analog spaces [50]. One particular novel finding is that physically reviewing documents of individuals seeking membership in neighborhood-watch-groups underscores the convergence of digital and physical realms, showcasing low-tech solutions that mitigate prevailing risks (IP16). Here, it becomes evident that diverse resources, encompassing both technical and human aspects, are crucial in finding effective solutions. The interplay of digital and physical realms also became clear in the social-punishment movement and the boycott campaign (IP13; OSP6). The data shows how online organized groups and applications influence real-life activities such as the exclusion of pro-military supporters, representing an important social-organizational resource.

Additionally, the analysis confirmed that activists in Myanmar, similar to protest movements in other countries, experience both benefits and challenges when using ICTs [108]. Misinformation, violent content, and incidents of surveillance seem to have increased since the military coup, thus reviewing information adequately becomes more evident (IP13). Since verifying information proves to be challenging, a desire to simplify the process has arisen. Study participants agreed by majority that it is important to control and verify misinformation and hate speech more efficiently, and to reduce violence and rumors, particularly against ethnic minorities (OSP4, IP1). Considering this, intersectional approaches are essential [111]. Since a merging between digital and the analog spaces is omnipresent, the Sit-tat also uses both digital and analog means to accomplish certain activities, such as spreading propaganda [15, 73] and limiting internet access by, e.g., introducing the Cybersecurity Law [57, 100]. Digital surveillance and on-street phone inspections (constraining factors of existing resources) seem to complement each other. Although it is well known that Myanmar scores poorly overall in terms of internet freedom, there is little in-depth knowledge about digital surveillance in Myanmar [73]. While the Sit-tat seeks to limit activists' ICT usage, protesters employ inventive strategies to overcome these, often by subverting their actions (IP1; IP7). It seems like a constant chain of action-and-reaction between protesters and the Sit-tat. According to the interviewees, there seems to be uncertainty regarding the extent of technical expertise possessed by the military and from which sources (e.g., China) it receives what kind of support (OSP6; IP16). However, since the coup, the perception of security and privacy among many study participants has changed, leading many to report using more data-secure apps [20]. This is, nonetheless, not the case for all study participants (IP14). Although more than half of the study participants claimed to be concerned about their privacy, only a few urged for the possibility of better anonymization and privacy of the applications used (IP8). Despite the fact that few very specific suggestions for (technical) improvement were made by the respondents, different recommendations for activists, research, and design can be derived from the empirical results that aim to facilitate secure and inclusive communication within the context of Myanmar.

5.2 Context-Specific Recommendations

It's crucial to highlight that these recommendations should be understood as suggestions derived from the empirical findings and existing literature [94] and should not be considered universally applicable, as contexts vary greatly. I underscore the complexity of delivering security recommendations for activists and recognize that my external perspective may not fully capture the nuances of the cultural context in which activists operate. This reflects an awareness of the potential implications and responsibilities associated with providing advice to individuals in challenging situations, such as activism. Generally, threat models are critical and it is essential to closely monitor changing circumstances while carefully assessing potential risks [97]. Additionally, it is important to have in mind that certain technical recommendations might generate tensions and trade-offs and that the generalization of design implications cannot cover the usability and security needs of everyone, as users' attitudes are heterogeneous and contextual conditions differ widely [85]. While Palen [77, 78] underscores the significance of integrating HCI principles into technology design for crisis response, this study shifts its focus to a distinct crisis scenario, specifically centered on protests. As Sas et al. [94, p. 1971] state,

> "a central tenet of HCI is that technology should be user-centric, with designs being based around social science findings about users. Nevertheless a repeated but critical challenge in design is translating empirical findings into actionable ideas that inform design, or generating implications for design".

In the following, selected aspects will be addressed in more detail, considering the diverse array of challenges outlined.

5.2.1 Enhancing Awareness and Digital Security of Activists. As potential device inspections may reveal close contacts (IP15) and thereby potentially jeopardize not just oneself, **activists could consider to collaboratively adopt digital security measures to safeguard their privacy** [14, 26]. Generally, users often tend to be overwhelmed with privacy and data security decisions [5]. Hence, they could consider to engage more actively in discussions about the nexus of digital and physical spaces. This may contribute to increased knowledge sharing regarding data security, potential threats, and strategies for mitigation [66]. A better overall technical understanding about potential risks and opportunities of technology seems vital in Myanmar's context, particularly given instances of violence (against Rohingya) fueled by SM [15]. Comprehensive digital security training and digital literacy initiatives seem crucial [92], as are visualizations to help individuals navigate e.g., the various stages of installing and using secure apps. Since it is unrealistic to expect everyone to take part in training in practice, simple ways of explaining technology — with its opportunities and risks — and making it more accessible need to be created, for example by using clear explanatory images and videos [33, 40, 109]. As advocated by IP16, enhancing user awareness and engagement in secure practices could be actively facilitated by incorporating push notifications within widely-used applications to highlight various security features. While nudging can effectively encourage secure behavior [5], challenges related to ethics, cultural sensitivity,

and potential user misunderstanding of security implications may hinder the desired outcomes.

Generally, digital security organizations recommend specific measures for implementation, such as the adoption of two-factor authentication and the use of disappearing messages [36]. Self-deleting messages enhance privacy by automatically removing sensitive information after a predetermined period, which could be advantageous for activists in Myanmar. This feature and the chat log function, introduced by WhatsApp in 2023, aim to reduce the risk of unauthorized access or exposure [8]. As requested by IP8, the chat log function exclusively grants access to viewing or sending messages once one's chats are unlocked through device authentication, such as one's phone passcode, fingerprint, or a personalized secret code. These specific chats will be securely stored in a designated folder (locked chats), distinct from other conversations [68]. Chats secured with a code will only appear when the secret code is entered into the search bar [42]. Given that WhatsApp is not the primary messaging app in Myanmar, it would be advantageous to extend such a feature to other messaging services. An additional feature that activists might find valuable during potential device controls is the ability to mask apps. The capability to alter the name and icon of an app could be beneficial in scenarios involving device inspection, for instance. Additionally, using secure applications, including Signal (IP16), is recommended by numerous organizations dedicated to digital security [26, 36]. However, as analyzed by Sanches et al. [93], some activists opted not to use secure communication apps, citing concerns that employing an especially fortified software such as Signal might draw attention to them if they were subject to searches. Within the context of Myanmar, activists could consider to consistently exchange information about the specific applications that the military may be targeting, especially during cellphone inspections.

Based on the empirical findings, activists in Myanmar could also consider using alternatives like the Tor browser [39], rather than solely depending on VPNs (OSP11; IP13). This may enhance their ability to protect against surveillance and circumvent censorship. With VPNs, security and privacy depend completely on the provider of the VPN service. As the VPN provider can be a single source of failure, misconfigurations or potential cooperation with nation-state actors like Myanmar's military pose tremendous risk for users — and as mentioned by study participants, the quality of a VPN service highly depends on the price users are willing to pay for it. Tor, on the other hand, is an open protocol and an open network that is continuously verified independently to be secure and private, is free of cost, and provides anonymity, something VPN providers cannot provide. Universal access to cost-free secure VPNs is essential to mitigate inequalities and ensure that secure VPN usage is not restricted only to those who are financially privileged. Furthermore, it is important to mention that the implementation of the Cyber Security Law (IP7) introduces ambiguity regarding which applications and technologies might face prohibition and criminalization in the future.

In general, while it is crucial to implement specific security measures, there is a risk of developing a false sense of security. Activists could take these findings into considerations and could refrain from placing exclusive reliance on selected security measures [7]. Achieving comprehensive privacy protection may prove challenging, especially in instances of sophisticated surveillance [34].

5.2.2 Developing Applications for Users in High-risk Scenarios. In HCI research, there remains a gap regarding designing secure, offline, and user-friendly applications that meet specific demands of activists in terms of data security, usability, and connectivity in conflict driven contexts. Further research endeavors should incorporate empirical studies and privacy by design principles [118] like data minimization right from the beginning of the development process. Solutions (easy to understand and accessible) that protect against e.g., physical checks by the military shall be increasingly **developed for users in high-risks scenarios** [103]. One step is Signal's feature of changing the app's name and icon. This feature makes it probably more difficult for unauthorized entities to target individuals based on their app usage and allows users to quickly protect their content that could potentially put them in danger. When conducting a threat assessment, it is important to consider that while app masking enhances privacy, it can also pose risks to activists if entities become aware of their attempts to conceal certain information. Generally, there's room for further improvement, such as incorporating features like data masking or masking the app's appearance within itself [10]. For instance, when a user changes an app's icon and name to *weather*, the app could be configured to show weather-related information when accessed e.g., with an incorrect passcode.

Moreover, as mentioned by IP16, a faster process for deactivating or blocking SM profiles (in cases of inspections) is crucial to prevent unauthorized access to contacts or sensitive content that may pose risks. In this context, activists could consider creating networks of emergency contacts, who are well-informed about the situation and possess the required access to handle SM accounts. Exploring additional features, like implementing a deletion password that could promptly block a profile, could also prove beneficial and warrant further consideration. Additionally, IP16 requested that more SM and instant messenger applications should offer registration without the mandatory use of a personal phone number, similar to the approach adopted by the messaging app "Threema" [80]. Using e.g., a non-personal registration key, detached from a personal phone number, has the potential to minimize the risk of privacy breaches.

In general, the existing trade-off between usability and security is a fundamental challenge in the design and development of applications — also for users in high-risk scenarios. Applications that prioritize usability often have simpler interfaces and streamlined processes to enhance the user experience. More secure applications often tend to be more complex and might discourage some users from adopting secure practices [116]. Therefore, achieving an optimal balance between usability and security requires an understanding of users' specific needs and preferences and making informed decisions based on potential risks and benefits.

5.2.3 Fostering Resilience against Internet Shutdowns. Another important issue that demands additional research is to investigate which **technical solutions can help efficiently in times of internet shutdowns** [91]. Until now, mesh networks, facilitating offline peer-to-peer communication, have rarely been used in Myanmar (IP5; IP14). As effective and offline communication is however vital during protests and internet shutdowns, it is imperative to address

existing vulnerabilities like limited range and the significant drain on battery and data resources [88]. Furthermore, already existing applications, such as Briar, providing mesh networks, should be easier to understand and less complex, enabling individuals with limited technical expertise to utilize these features effectively. It would be an important step to integrate Bluetooth-based communication in well-known and widely used applications like Signal and WhatsApp, since e.g., in Myanmar people are already using these applications. The probability of a large number of individuals downloading another application, such as Briar or Bridgefy, is relatively low, which limits the functionality enormously. Moreover, reporting incidents of internet shutdowns and documenting key details such as duration, scope, and the specific regions affected appears crucial, a practice already observed in numerous instances. This not only helps in comprehending the profound impact on individuals and communities but also allows analysts to conduct impact assessments [89].

5.2.4 Adapting to Local Circumstances and Improving Representation by Considering Native Languages. Some interviewees indicated a desire for more linguistic diversity (e.g., IP6). Thus, there is a **need for translating applications into local languages** [62], like Burmese, that have historically received limited representation. Translating applications into local, non-hegemonic languages is a step toward creating a more inclusive and equitable landscape, helping to support digital literacy efforts, and to combat the spread of fake news and hate speech. Especially in Myanmar, multilingual content is essential, reflecting the linguistic diversity of ethnic groups that is often overlooked by SM and messenger platforms. Moving past basic translation, the integration of human-centered design and principles of technology localization is pivotal. This involves a comprehensive **consideration of socio-cultural, economic, and political dynamics**, as well as unique linguistic traits. Ensuring cultural appropriateness is paramount, guarding against unintended offense or misrepresentation [35, 51, 84]. Moreover, technological factors, such as predictive text and the design of the user interface, demand careful attention, as e.g., certain languages may necessitate more or less space compared to to others. In addition to the written content, it's crucial to consider culturally suitable colors and symbols [62, 81].

5.2.5 Reducing Dependencies on Multinational Companies. Another identified aspect that requires critical **reconsideration is the dependency on multinational companies** such as Meta in the context of addressing issues related to digital colonialism and the potential misuse of data [17, 18, 72]. Services, including Free Basics, have created dependencies that require dismantling. If other applications (e.g., Signal) would be offered free of charge as part of the internet package, the number of users could certainly increase. In scenarios where individuals are somehow disinclined to adopt data-secure apps due to existing dependencies, it becomes essential to establish alternative incentives for encouraging the use of different apps, particularly in conflict-prone settings such as Myanmar. It is important to emphasize that the responsibility should not be solely placed on individuals — companies also bear a significant responsibility to act more conscientiously in a timely manner. Providing activists with secure functionalities, e.g., the option of registration without necessitating a phone number, but rather employing an ID, akin to the Threema ID [80], would be helpful.

In summary, the findings yield numerous recommendations (see Table 1), which could not all be comprehensively discussed within the scope of this study. To assess context-specific requirements in a timely manner, it is imperative that different stakeholders engage in discussions with people on the ground and promote participatory design processes to include a wide range of different perspectives [24, 85]. As Wade et al. (2021) [112, p. 5] state, "more research needs to be conducted to fully investigate and validate if the recommendations given to protesters are actually working (...)." Conducting follow-up studies would be valuable, since Myanmar is not receiving the attention it requires [34] and this research specifically addresses the immediate aftermath of the military coup. I acknowledge the necessity for future research to be led primarily by individuals from the community or in collaboration, provided that security considerations permit. In certain situations, (co-)authors may face potential risks arising from their involvement in research. Incorporating the perspective of individuals from the communities is crucial for introducing a more diverse range of viewpoints and mitigating issues such as knowledge extractivism, power imbalances [21], ethnocentrism [2], and countering the potential bias of Western epistemology driven by self-serving interests [70]. Moreover, it is important to reflect on how interviewees and communities benefit from research [19, 21]. In this particular instance, this study holds an important role within a broader research project dedicated to comprehending how activists deploy ICTs in conflict-affected contexts. Within the scope of the project, an ongoing dialogue is taking place with app developers and digital security organizations, including those in Myanmar. This conversation revolves around defining the characteristics of a secure app, exploring the advantages and disadvantages associated with different features. Additionally, over the next 1-2 years, a booklet summarizing the study's findings in the local language will be distributed among activists and NGOs.

6 CONCLUSION

This study contributes to existing HCI research on ICT-enabled activism by presenting a qualitative case study that holds significant empirical value [117], shedding light on a country that is often overlooked, as emphasized by the perspectives shared by the interviewees. As already clarified, the results solely represent a non-representative excerpt of reality and can therefore not be applied to all activists in Myanmar. Nevertheless, the study provides an in-depth insight into different individual realities during the first weeks after the coup. Given Myanmar's complex nature, this study underscores the significance of seeing ICTs in conflict-affected contexts as part of a complex nexus, bearing culture, language, and social structures in mind. Generally, the data highlight that it is imperative to develop user-centric ICTs solutions that aid activists during internet shutdowns and surveillance. Here, it is vital to grant more agency to people affected by (power) misuse and thus jointly develop ICTs that truly benefit those affected. It's crucial to discard the notion that technology designed for and employed in the Global North is universally applicable to people around the

Table 1: Outline of potential challenges and risks, along with context-specific recommendations tailored to the circumstances in Myanmar as of 2021. Given the dynamic nature of these issues, circumstances have the potential to shift rapidly. Source: Own representation.

Identified Risks and Challenges	Context-specific Recommendations and Design Implications
Little security and privacy awareness among activists	• Enhancing (collective) awareness of potential risks [34] • Existence of more workshops on digital security • Using data secure applications and security procedures (e.g., two-factor authentication [33, 36, 65]) and being aware of possible associated risks • Implementing push-up notifications with context-sensitive recommendations on (digital) security in commonly used apps to raise awareness • Conducting risk assessments and threat analysis to assess potential risks • Building support networks to share best practices within activist communities • Privacy settings should be set to the highest level by default
Applications are often perceived as too complicated	• Applications should generally be easier to understand (e.g., through explanatory images and easy language) • Close exchange with affected individuals to understand their technical needs • Promoting participatory design
Internet shutdown, blocked websites, and censorship	• Improving Bluetooth-based mesh networks and integrating Bluetooth-based communication in well-known and widely used applications • Facilitating offline peer-to-peer communication • Offering free and secure VPNs [34] • Using proxy servers • Documenting internet shutdowns and censorship • Seeking international support (e.g., for documentation & awareness raising)
Physical device inspections	• Data and app masking • Fast and efficient profile locking • Creating hidden or encrypted partitions on device storage • Data minimization (generally enhancing privacy by design principles) • Creating fake accounts • Carrying minimal data • If possible: use of clean devices or having burner phones [34, 65]
(Digital) surveillance	• Taking measures to protect devices • Consulting digital security experts and organization (e.g., AccessNow)
Little to no representation of native/local languages/Burmese	• Translating applications into native/local languages/Burmese and having socio-cultural nuances, linguistic particularities, and technological factors in mind
Dependencies on Meta and Free Basics	• Free Basics should not be provided exclusively by Meta • Ensuring net neutrality
Existence of misinformation, fake news, and hate speech	• Improving content moderation and reporting mechanisms • Enhancing media literacy education • Improving mechanisms to identify and reduce the spread of false information • Encourage crowd-sourced verification
Lack of anonymity (e.g., phone number identifiable in group chats; number often associated with personal ID)	• Registration without using own number • Possibility to use pseudonyms • Using Tor/VPN (e.g., TunnelBear) [65] • Adjusting SM privacy settings • Avoiding public Wi-Fi
Introduction of Cybersecurity Law	• International community should denounce law as it jeopardizes the rights of individuals to access information, privacy, and security [4] • Importance of creating awareness about the law (advocacy efforts) [34]

world, each confronting unique challenges (e.g., surveillance, poor connectivity, and physical inspections) [48]. In Myanmar for example, most activists continue to use less data-secure applications, indicating a tension between security and convenience. However, relatively shortly after the coup, more data-secure data applications like Signal were used by some activists, and creative methods were found to bypass restrictions imposed by the military. The number of initiatives for digital rights in the country underlines the great attention that is being paid to preserving and promoting digital rights. Nevertheless, a coordinated endeavor is essential to address the needs of often marginalized communities, emphasizing languages like Burmese for efficient detection of misinformation and hate speech. As technology continues to shape Myanmar's social and political landscape, sustained attention to these aspects is paramount for ensuring the responsible and inclusive use of ICTs. Since the tensions have eased in the meantime, follow-up studies on how ICTs are used and whether, for example, the boycott campaigns have evolved, might be promising.

ACKNOWLEDGMENTS

First of all, I would like to thank all the interviewees. I sincerely hope that they can soon live without repression and without further human rights violations. I'm equally thankful to the individuals and organizations with whom I engaged during my research. Their context-specific advice and support played a vital role in shaping the outcome of my study. Lastly, I would like to thank the anonymous reviewers for their insightful suggestions, which greatly enhanced this work. This contribution was funded by the German Federal Ministry of Education and Research (BMBF) as part of TraCe, the 'Regional Research Center Transformations of Political Violence' (01UG2203E), as well as by the Hessian Ministry of Higher Education, Research, Science and the Arts within their joining support of the National Research Center of Applied Cybersecurity ATHENE.

REFERENCES

[1] Rasha A. Abdulla. 2011. The Revolution Will Be Tweeted. *The Cairo Review of Global Affairs* 69, 10 (2011), 24–28. https://www.thecairoreview.com/essays/the-revolution-will-be-tweeted/

[2] Rediet Abebe, Kehinde Aruleba, Abeba Birhane, Sara Kingsley, George Obaido, Sekou L. Remy, and Swathi Sadagopan. 2021. Narratives and Counternarratives on Data Sharing in Africa. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (Virtual Event, Canada) *(FAccT '21)*. Association for Computing Machinery, New York, NY, USA, 329–341. https://doi.org/10.1145/3442188.3445897

[3] AccessNow. 2022. Exposed: civil society condemns use of Pegasus in El Salvador to spy on journalists and activists. https://www.accessnow.org/pegasus-el-salvador-spyware-targets-journalists-statement/

[4] AccessNow. 2023. Resist Myanmar's digital coup: International community must dismantle military dictatorship — or reap repercussions. https://www.accessnow.org/press-release/myanmar-coup-two-years-statement/

[5] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 1–41.

[6] Ban Al-Ani, Gloria Mark, Justin Chung, and Jennifer Jones. 2012. The Egyptian Blogosphere: A Counter-Narrative of the Revolution. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (Seattle, Washington, USA) *(CSCW '12)*. Association for Computing Machinery, New York, NY, USA, 17–26. https://doi.org/10.1145/2145204.2145213

[7] Hisham Al-Assam, Harin Sellahewa, and Sabah Jassim. 2010. Multi-Factor Biometrics for Authentication: A False Sense of Security. In *Proceedings of the 12th ACM Workshop on Multimedia and Security* (Roma, Italy) *(MM&Sec '10)*. Association for Computing Machinery, New York, NY, USA, 81–88. https://doi.org/10.1145/1854229.1854246

[8] Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. 2021. Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 3363–3380. https://www.usenix.org/conference/usenixsecurity21/presentation/albrecht

[9] Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. 2021. Mesh Messaging in Large-Scale Protests: Breaking Bridgefy. In *Topics in Cryptology – CT-RSA 2021*, Kenneth G. Paterson (Ed.). Springer International Publishing, Cham, 375–398.

[10] Feras M Awaysheh, Mohammad N Aladwan, Mamoun Alazab, Sadi Alawadi, José C Cabaleiro, and Tomás F Pena. 2021. Security by design for big data frameworks over cloud computing. *IEEE Transactions on Engineering Management* 69, 6 (2021), 3676–3693.

[11] Stefan Bächtold. 2022. The smartphone and the coup. How Myanmar's conflicts are entangled with digital technologies, policies, and violence. *International Journal of Public Policy* 16, 5-6 (2022), 293–310. https://doi.org/10.1504/IJPP.2022.10046665

[12] Melissa Bica, Leysia Palen, Jennifer Henderson, Jennifer Spinney, Joy Weinberg, and Erik R. Nielsen. 2021. "Can't think of anything more to do": Public displays of power, privilege, and surrender in social media disaster monologues. *Human–Computer Interaction* (2021). https://doi.org/10.1080/07370024.2021.1982390

[13] Zachary S. Bischof, Kennedy Pitcher, Esteban Carisimo, Amanda Meng, Rafael Bezerra Nunes, Ramakrishna Padmanabhan, Margaret E. Roberts, Alex C. Snoeren, and Alberto Dainotti. 2023. Destination Unreachable: Characterizing Internet Outages and Shutdowns. In *Proceedings of the ACM SIGCOMM 2023 Conference* (New York, NY, USA) *(ACM SIGCOMM '23)*. Association for Computing Machinery, New York, NY, USA, 608–621. https://doi.org/10.1145/3603269.3604883

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

[15] Lisa Brooten. 2016. Burmese Media in Transition. *International Journal of Communication* 10, 0 (2016). https://ijoc.org/index.php/ijoc/article/view/3358

[16] Stefan Bächtold. 2023. Blackouts, whitelists, and 'terrorist others': The role of socio-technical imaginaries in Myanmar. *Journal of Intervention and Statebuilding* 0, 0 (2023), 1–21. https://doi.org/10.1080/17502977.2022.2152940

[17] Danielle Coleman. 2018. Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Mich. J. Race & L.* 24 (2018), 417.

[18] Nick Couldry and Ulises A Mejias. 2019. Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media* 20, 4 (2019), 336–349.

[19] Melany Cruz and Darcy Luke. 2020. Methodology and academic extractivism: the neo-colonialism of the British university. *Third World Thematics: A TWQ Journal* 5, 1-2 (2020), 154–170. https://doi.org/10.1080/23802014.2020.1798275

[20] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G. Bardas. 2021. Defensive Technology Use by Political Activists During the Sudanese Revolution. In *2021 IEEE Symposium on Security and Privacy (SP)*. 372–390. https://doi.org/10.1109/SP40001.2021.00055

[21] Ranjan Datta. 2018. Decolonizing both researcher and research and its effectiveness in Indigenous research. *Research Ethics* 14, 2 (2018), 1–24.

[22] Débora De Castro Leal, Max Krueger, Kaoru Misaki, David Randall, and Volker Wulf. 2019. Guerilla warfare and the use of new (and some old) technology: Lessons from FARC-EP's armed struggle in Colombia. *Conference on Human Factors in Computing Systems - Proceedings* (2019), 1–12. https://doi.org/10.1145/3290605.3300810

[23] Donatella della Porta and Lorenzo Mosca. 2005. Global-net for global movements? A network of networks for a movement of movements. *Journal of Public Policy* 25, 1 (2005), 165–190. https://doi.org/10.1017/S0143814X05000255

[24] Lina Dencik, Arne Hintz, Joanna Redden, and Emiliano Treré. 2019. Exploring data justice: Conceptions, applications and directions. , 873–881 pages.

[25] Desmond. 2022. Please Don't Call Myanmar Military Tatmadawr. (25 May 2022). https://www.irrawaddy.com/opinion/guest-column/please-dont-call-myanmar-military-tatmadaw.html

[26] Digital Security Myanmar. 2024. Digital Security Myanmar. https://www.digitalsecuritymyanmar.com/

[27] Bob Edwards and Patrick F. Gillham. 2013. Resource Mobilization Theory. *The Wiley-Blackwell Encyclopedia of Social and Political Movements* (2013). https://doi.org/10.1002/9780470674871.wbespm447

[28] Bob Edwards and Melinda D. Kane. 2007. *The Blackwell Encyclopedia of Sociology*. Wiley, Chapter Resource Mobilization Theory, 1–5. https://doi.org/10.1002/9781405165518

[29] Bob Edwards and John D. McCarthy. 2004. Resources and Social Movement Mobilization. *The Blackwell Companion To Social Movements*. (2004), 116–152. https://doi.org/10.1002/9780470999103

[30] Rainer Einzenberger. 2016. "If It's on the Internet It Must Be Right": An Interview With Myanmar ICT for Development Organisation on the Use of the Internet and Social Media in Myanmar . *Austrian Journal of South-East Asian Studies* 9, 2 (2016), 301–310. https://doi.org/10.14764/10.ASEAS-2016.2-9

[31] Mohammed El-Nawawy and Sahar Khamis. 2012. Political Activism 2.0: Comparing the Role of Social Media in Egypt's "Facebook Revolution" and Iran's "Twitter Uprising". *CyberOrient* 6, 1 (2012), 8–33. https://doi.org/10.1002/j.cyo2.20120601.0002

[32] Nahed Eltantawy and Julie B Wiest. 2011. Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory. *International Journal of Communication* 5, 0 (2011), 1207–1224.

[33] Engage Media. 2022. #DigitalSafetyFirstMM:DigitalSafety Checklist for Myanmar Citizens. https://cinemata.org/view?m=ysncFEtRF

[34] Engage Media. 2023. Engaging Myanmar Digital Rights Advocates. https://engagemedia.org/2023/pretty-good-podcast-26-myanmar-digital-rights-advocates/

[35] Debbie Folaron. 2019. Technology, technical translation and localization. In *The Routledge Handbook of Translation and Technology* (1st ed.). Routledge, London, 203–219.

[36] Front Line Defenders. 2021. Security in a box-Digital-Security Tools & Tactics. https://securityinabox.org/en/

[37] Lee Ann Fujii. 2012. Research ethics 101: Dilemmas and responsibilities. *PS: Political Science & Politics* 45, 4 (2012), 717–723.

[38] Allie Funk, Adrian Shahbaz, and Kian Vesteinsson. 2023. The Repressive Power of Artificial Intelligence. https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence

[39] Ulaş Başar Gezgin. 2023. From targeted to pervasive surveillance: the rise of anti-surveillance activism against twin big brothers. (2023).

[40] María Belén Giménez Ciciolli, Ahmet Kocaker, Shikha Thakur, Carolina Haro, Parmarth Rai, Sarah Rüller, Konstantin Aal, and Volker Wulf. 2022. Digital Security Story Cards for Women with a Refugee and Migrant Background. In *Proceedings of Mensch und Computer 2022*. 409–419.

[41] Sarah Gordon. 2021. Using Technology to Preserve Military Loyalty: The Tatmadaw in Myanmar. In *Issues on the Frontlines of Technology and Politics*, Steven Feldstein (Ed.). Carnegie Endowment for International Peace, Washington D.C., 21–22.

[42] Andrew Griffin. 2023. WhatsApp update adds 'secret codes' for chats. https://www.independent.co.uk/tech/whatsapp-update-chat-secret-code-messages-b2456203.html

[43] Jannis Grimm, Kevin Koehler, Ellen M Lust, Ilyas Saliba, and Isabell Schierenbeck. 2020. *Safer field research in the social sciences: A guide to human and digital security in hostile environments*. SAGE.

[44] Margarita Grinko, Sarvin Qalandar, Dave Randall, and Volker Wulf. 2022. Nationalizing the Internet to Break a Protest Movement: Internet Shutdown and Counter-Appropriation in Iran of Late 2019. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 314 (nov 2022), 21 pages. https://doi.org/10.1145/3555205

[45] International Crisis Group. 2021. *Myanmar's Military Struggles to Control the Virtual Battlefield*. Technical Report May. International Crisis Group, Brussels. 1–43 pages. http://www.jstor.org/stable/resrep31782

[46] Laura Gianna Guntrum, Benjamin Güldenring, Franz Kuntke, and Christian Reuter. 2022. Using digitally mediated methods in sensitive contexts: a threat analysis and critical reflection on data security, privacy, and ethical concerns in the case of Afghanistan. *Zeitschrift für Friedens-und Konfliktforschung* 11, 2 (2022), 95–128.

[47] Zain Halloush, Ahmed Aleroud, and Craig Albert. 2023. Socio-Emotional Computational Analysis of Propaganda Campaigns on Social Media Users in the Middle East. In *Companion Proceedings of the ACM Web Conference 2023* (Austin, TX, USA) *(WWW '23 Companion)*. Association for Computing Machinery, New York, NY, USA, 1413–1421. https://doi.org/10.1145/3543873.3587677

[48] Harry Halpin, Ksenia Ermoshina, and Francesca Musiani. 2018. Co-ordinating developers and high-risk users of privacy-enhanced secure messaging protocols. In *Security Standardisation Research: 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings 4*. Springer, 56–75.

[49] Ionat Ilascu. 2023. University of Michigan employee, student data stolen in cyberattack. https://www.bleepingcomputer.com/news/security/university-of-michigan-employee-student-data-stolen-in-cyberattack/

[50] Ingrid Jordt, Tharaphi Than, Sue Ye Lin, Ingrid Jordt, Tharaphi Than, and Sue Ye Lin. 2021. *How Generation Z Galvanized a Revolutionary Movement against Myanmar's 2021 Military Coup*. Singapore, 1–33.

[51] Naveena Karusala. 2019. How Technology Converses with Local Languages. *XRDS* 26, 2 (nov 2019), 36–39. https://doi.org/10.1145/3368068

[52] Sean D Kaster and Prescott C Ensign. 2023. Privatized espionage: NSO Group Technologies and its Pegasus spyware. *Thunderbird International Business Review* 65, 3 (2023), 355–364.

[53] Andrea Kavanaugh, Steven D. Sheetz, Hamida Skandrani, and John Tedesco. 2016. The Use and Impact of Social Media during the 2011 Tunisian Revolution. *ACM International Conference Proceeding Series* (2016), 20–30. https://doi.org/10.1145/2912160.2912175

[54] Andrea Kavanaugh, Steven D. Sheetz, Hamida Skandrani, John C. Tedesco, Yue Sun, and Edward A. Fox. 2016. The Use and Impact of Social Media during the 2011 Tunisian Revolution. In *Proceedings of the 17th International Digital Government Research Conference on Digital Government Research* (Shanghai, China) *(dg.o '16)*. Association for Computing Machinery, New York, NY, USA, 20–30. https://doi.org/10.1145/2912160.2912175

[55] Simon Kemp. 2023. *Digital Myanmar*. Technical Report. https://datareportal.com/digital-in-myanmar

[56] Erin Kenneally and David Dittrich. 2012. The menlo report: Ethical principles guiding information and communication technology research. *Available at SSRN 2445102* (2012).

[57] Nwet Kay Khine. 2022. Factors of Resilience and Constraint in the Myanmar Resistance Movement. *Political Science| Volume 132* (2022), 239.

[58] Jan Kleiner and Ondřej Šupka. 2020. The Myanmar conflict: A role of cyberspace in counterinsurgency. *International Journal of Cyber Criminology* 14, 1 (2020), 254–266. https://doi.org/10.5281/zenodo.3752991

[59] Tom Kramer. 2020. 'Neither war nor peace': failed ceasefires and dispossession in Myanmar's ethnic borderlands. *Journal of Peasant Studies* 48, 3 (2020), 476–496. https://doi.org/10.1080/03066150.2020.1834386

[60] KrASIA. 2021. Myanmar protestors use apps to boycott military-linked products and businesses. https://kr-asia.com/myanmar-protestors-use-apps-to-boycott-military-linked-products-and-businesses

[61] Udo Kuckartz. 2014. *Qualitative text analysis: A guide to methods, practice and using software*. SAGE Publications Ltd, London.

[62] Derek Lackaff and William J Moner. 2016. Local languages, global networks: Mobile design for minority language users. In *Proceedings of the 34th ACM International Conference on the Design of Communication*. 1–9.

[63] Jennifer M. Larson, Jonathan Nagler, Jonathan Ronen, and Joshua A. Tucker. 2019. Social Networks and Protest Participation: Evidence from 130 Million Twitter Users. *American Journal of Political Science* 63, 3 (2019), 690–705. https://doi.org/10.1111/ajps.12436 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/ajps.12436

[64] Yao-Tai Li and Katherine Whitworth. 2023. Redefining consumer nationalism: The ambiguities of shopping yellow during the 2019 Hong Kong Anti-ELAB movement. *Journal of Consumer Culture* 23, 3 (2023), 517–535. https://doi.org/10.1177/14695405221127346 arXiv:https://doi.org/10.1177/14695405221127346

[65] LocalizationLab. 2023. Myanmar Resources: 'Tactics' for Open Access and Safety. https://www.localizationlab.org/myanmar-resources

[66] Tetyana Lokot. 2018. Be safe or be seen? How Russian activists negotiate visibility and security in online resistance practices. *Surveillance & Society* 16, 3 (2018), 332–346.

[67] Marc Lynch. 2011. After egypt: The limits and promise of online challenges to the authoritarian Arab state. *Perspectives on Politics* 9, 2 (2011), 301–310. https://doi.org/10.1017/S1537592711000910

[68] Meta. 2023. How to turn on chat lock. https://faq.whatsapp.com/764072925284841/

[69] Marcus Michaelsen. 2017. Far away, so close: Transnational activism, digital surveillance and authoritarian control in Iran. *Surveillance & Society* 15, 3/4 (2017), 465–470.

[70] Walter D. Mignolo. 2009. Epistemic Disobedience, Independent Thought and Decolonial Freedom. *Theory, Culture & Society* 26, 8 (2009), 159–181. https://doi.org/10.1177/0263276409349275

[71] Albine Moser and Irene Korstjens. 2018. Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice* 24, 1 (2018), 9–18. https://doi.org/10.1080/13814788.2017.1375091 arXiv:https://doi.org/10.1080/13814788.2017.1375091 PMID: 29199486.

[72] Subhayan Mukerjee. 2016. Net neutrality, Facebook, and India's battle to# SaveTheInternet. *Communication and the Public* 1, 3 (2016), 356–361.

[73] Myanmar Internet Project. 2023. Digital Resistance. https://www.myanmarinternet.info/digital-resistance

[74] Yan Naung Oak and Lisa Brooten. 2019. The Tea Shop Meets the 8 O'clock News: Facebook, Convergence and Online Public Spaces. In *Myanmar Media in Transition. Legacies, Challenges and Change*, Lisa Brooten, Jane Madlyn McElhone, and Gayathry Venkiteswaran (Eds.). ISEAS-Yusof Ishak Insitute, 327–365.

[75] Jose Ortiz and Arvind Tripathi. 2017. Resource mobilization in social media: The role of influential actors. *Proceedings of the 25th European Conference on Information Systems, ECIS 2017* 2017 (2017), 3049–3059.

[76] Ramakrishna Padmanabhan, Arturo Filastò, Maria Xynou, Ram Sundara Raman, Kennedy Middleton, Mingwei Zhang, Doug Madory, Molly Roberts, and Alberto Dainotti. 2021. A Multi-Perspective View of Internet Censorship in Myanmar. In *Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet* (Virtual Event, USA) *(FOCI '21)*. Association for Computing Machinery, New York, NY, USA, 27–36. https://doi.org/10.1145/3473604.3474562

[77] Leysia Palen, Sarah Vieweg, and Kenneth Marc Anderson. 2011. Supporting "Everyday Analysts" in Safety- and Time-Critical Situations. *The Information Society* 27 (2011). Issue 1. https://doi.org/10.1080/01972243.2011.534370

[78] Leysia Palen, Sarah Vieweg, Jeannette Sutton, Sophia B Liu, and Amanda Hughes. 2007. Crisis informatics: Studying crisis in a networked world. In *Proceedings of the Third International Conference on E-Social Science*. 7–9.

[79] Carolina Vendil Pallin. 2017. Internet control through ownership: the case of Russia. *Post-Soviet Affairs* 33, 1 (2017), 16–33. https://doi.org/10.1080/1060586X.2015.1121712 arXiv:https://doi.org/10.1080/1060586X.2015.1121712

[80] Kenneth G Paterson, Matteo Scarlata, and Kien Tuong Truong. 2023. Three lessons from threema: Analysis of a secure messenger. In *32nd USENIX Security Symposium (USENIX Security 23)*. 1289–1306.

[81] Manuel A. Pérez-Quiñones, Olga I. Padilla-Falto, and Kathleen McDevitt. 2005. Automatic Language Translation for User Interfaces. In *Proceedings of the 2005 Conference on Diversity in Computing* (Albuquerque, New Mexico, USA) *(TAPIA '05)*. Association for Computing Machinery, New York, NY, USA, 60–63. https://doi.org/10.1145/1095242.1095268

[82] Francesco Pierri, Luca Luceri, Nikhil Jindal, and Emilio Ferrara. 2023. Propaganda and Misinformation on Facebook and Twitter during the Russian Invasion of Ukraine. In *Proceedings of the 15th ACM Web Science Conference 2023* (Austin, TX, USA) *(WebSci '23)*. Association for Computing Machinery, New York, NY, USA, 65–74. https://doi.org/10.1145/3578503.3583597

[83] Fanny Potkin and Jessie Pang. 2021. Offline message app downloaded over million times after Myanmar coup. https://www.reuters.com/article/us-myanmar-politics-bridgefy-idUSKBN2A22H0

[84] Mohammadhussein Rafieisakhaei and Babak Barazandeh. 2016. A Simulation-Based Model of Technology Localization in Developing Countries. In *Proceedings of the 2016 Winter Simulation Conference* (Arlington, Virginia) *(WSC '16)*. IEEE Press, 3682–3683.

[85] Thomas Reisinger, Isabel Wagner, and Eerke Albert Boiten. 2023. Unified Communication: What do Digital Activists need?. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 141–149.

[86] Victoire Rio. 2021. Myanmar: The role of social media in fomenting violence. *Social Media Impacts on Conflict and Democracy: The Techtonic Shift* 20 (2021), 143–160. https://doi.org/10.4324/9781003087649-10

[87] Markus Rohde, Konstantin Aal, Kaoru Misaki, Dave Randall, Anne Weibert, and Volker Wulf. 2016. Out of Syria: Mobile Media in Use at the Time of Civil War. *International Journal of Human–Computer Interaction* 32, 7 (2016), 515–531. https://doi.org/10.1080/10447318.2016.1177300 arXiv:https://doi.org/10.1080/10447318.2016.1177300

[88] Raúl Rondón, Aamir Mahmood, Simone Grimaldi, and Mikael Gidlund. 2019. Understanding the performance of bluetooth mesh: Reliability, delay, and scalability analysis. *IEEE Internet of things journal* 7, 3 (2019), 2089–2101.

[89] Zach Rosson, Felicia Anthonio, and Carolyn Tackett. 2023. Weapons of Control, Shields of Impunity: Internet shutdowns in 2022. (2023).

[90] Megan Ryan and Mai Van Tran. 2022. Democratic backsliding disrupted: The role of digitalized resistance in Myanmar. (2022). https://doi.org/10.1177/20578911221125511

[91] Julia Ryng, Guillemette Guicherd, Judy Al Saman, Priyanka Choudhury, and Angharad Kellett. 2022. Internet Shutdowns: A Human Rights Issue. *The RUSI Journal* 167, 4-5 (2022), 50–63.

[92] Nikita Samarin, Aparna Krishnan, Moses Namara, Joanne Ma, and Elissa M Redmiles. 2022. Examining the Landscape of Digital Safety and Privacy Assistance for Black Communities. *ArXiv* (2022).

[93] Pedro Sanches, Vasiliki Tsaknaki, Asreen Rostami, and Barry Brown. 2020. Under Surveillance: Technology Practices of Those Monitored by the State. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376889

[94] Corina Sas, Steve Whittaker, Steven Dow, Jodi Forlizzi, and John Zimmerman. 2014. Generating Implications for Design through Design Research. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 1971–1980. https://doi.org/10.1145/2556288.2557357

[95] Km Seethi. 2021. Military coup in Myanmar : 'Garrison State' back to dismantle democracy? *Global South Colloquy* February (2021), 1. https://doi.org/10.6084/m9.figshare.13697578.v1

[96] Irina Shklovski and Volker Wulf. 2018. The use of private mobile phones at war: Accounts from the Donbas conflict. *Conference on Human Factors in Computing Systems - Proceedings* 2018-April (2018), 1–13. https://doi.org/10.1145/3173574.3173960

[97] Adam Shostack. 2014. *Threat modeling: Designing for security*. John Wiley & Sons.

[98] Ellen Simpson. 2018. Integrated & Alone: The Use of Hashtags in Twitter Social Activism. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing*. Jersey City, NJ, USA, 237–240.

[99] Thant Sin Oo and Ye Min Thant. 2019. *Exploring Digital and Mobile Cultures in Myanmar 2019*. Technical Report. 41 pages.

[100] Robert Smith and Nucharee Smith. 2022. Use and Abuse of Social Media in Myanmar between 2010 and 2022. *Athens Journal of Law* 8, 3 (2022), 309–328. https://doi.org/10.30958/ajl.8-3-5

[101] Standard Insights. 2022. *Social Media Landscape: Myanmar*. Technical Report. https://standard-insights.com/blog/social-media-landscape-myanmar/

[102] Kate Starbird and Leysia Palen. 2012. (How) Will the Revolution Be Retweeted? Information Diffusion and the 2011 Egyptian Uprising. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (<conf-loc>, <city>Seattle</city>, <state>Washington</state>, <country>USA</country>, </conf-loc>) *(CSCW '12)*. Association for Computing Machinery, New York, NY, USA, 7–16. https://doi.org/10.1145/2145204.2145212

[103] Borislav Tadic, Markus Rohde, and Volker Wulf. 2018. CyberActivist: tool for raising awareness on privacy and security of social media use for activists. In *Social Computing and Social Media. User Experience and Behavior: 10th International Conference, SCSM 2018, Held as Part of HCI International 2018, Las Vegas, NV, USA, July 15-20, 2018, Proceedings, Part I 10*. Springer, 498–510.

[104] Sidney Tarrow. 2005. *The New Transnational Activism*. Cornell University, New York. TheNewTransnationalActivism

[105] Sidney Tarrow, Charles Tilly, and Douglas McAdam. 2001. *The Dynamics of Contention*. Cambridge University Press, New York. https://doi.org/10.1017/CBO9780511805431

[106] The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. 1979. *Belmont Report*. Technical Report.

[107] Seinenu M. Thein-Lemelson. 2021. 'Politicide' and the Myanmar coup. *Anthropology Today* 37, 2 (2021), 3–5. https://doi.org/10.1111/1467-8322.12639

[108] Stein Tønnesson, Min Zaw Oo, and Ne Lynn Aung. 2021. Pretending to be States: The Use of Facebook by Armed Groups in Myanmar. *Journal of Contemporary Asia* 00, 00 (2021), 1–26. https://doi.org/10.1080/00472336.2021.1905865

[109] Letícia Diniz Tsuchiya, Lucas Fiorini Braga, Otavio de Faria Oliveira, Raphael Winckler de Bettio, Juliana Galvani Greghi, and André Pimenta Freire. 2021. Design and evaluation of a mobile smart home interactive system with elderly users in Brazil. *Personal and Ubiquitous Computing* 25 (2021), 281–295.

[110] Zeynep Tufekci. 2017. *Twitter and The Tear Gas*. Yale University Press, New Haven. 359 pages.

[111] Sebastián Valenzuela, Nicolás M. Somma, Andrés Scherman, and Arturo Arriagada. 2016. Social media in Latin America: deepening or bridging gaps in protest participation? *Online Information Review* 40, 5 (Sept. 2016), 695–711. https://doi.org/10.1108/oir-11-2015-0347

[112] Kandrea Wade, Jed R. Brubaker, and Casey Fiesler. 2021. Protest Privacy Recommendations: An Analysis of Digital Surveillance Circumvention Advice During Black Lives Matter Protests. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. Association for Computing Machinery, New York, NY, USA, Article 246, 6 pages. https://doi.org/10.1145/3411763.3451749

[113] Tommy Walker. 2021. How Myanmar's Civil Disobedience Movement Is Pushing Back Against the Coup. https://www.voanews.com/a/east-asia-pacific_how-myanmars-civil-disobedience-movement-pushing-back-against-coup/6202637.html

[114] Stephanie Wang and Shishir Nagaraja. 2007. Pulling the plug: A technical review of the Internet shutdown in Burma. *OpenNet Initiative Bulletin* (2007).

[115] Nils B. Weidmann and Espen Geelmuyden Rød. 2019. Coding Protest Events in Autocracies. In *The Internet and Political Protest in Autocracies*. Oxford University Press. https://doi.org/10.1093/oso/9780190918309.003.0004

[116] Lydia Weinberger, Christian Eichenmüller, and Zinaida Benenson. 2023. Interplay of Security, Privacy and Usability in Videoconferencing. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI EA '23)*. Association for Computing Machinery, New York, NY, USA, Article 185, 10 pages. https://doi.org/10.1145/3544549.3585683

[117] Jacob O Wobbrock and Julie A Kientz. 2016. Research contributions in human-computer interaction. *interactions* 23, 3 (2016), 38–44.

[118] Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–17. https://doi.org/10.1145/3290605.3300492

[119] Elisabeth Jean Wood. 2006. The ethical challenges of field research in conflict zones. *Qualitative Sociology* 29, 3 (2006), 373–386. https://doi.org/10.1007/s11133-006-9027-8

[120] Volker Wulf, Konstantin Aal, Ibrahim Abu Kteish, Meryem Atam, Kai Schubert, Markus Rohde, George P. Yerousis, and David Randall. 2013. Fighting against the Wall: Social Media Use by Political Activists in a Palestinian Village. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 1979–1988. https://doi.org/10.1145/2470654.2466262

[121] Thomas Zeitzoff. 2017. How Social Media Is Changing Conflict. *Journal of Conflict Resolution* 61, 9 (2017), 1970–1991. https://doi.org/10.1177/0022002717721392

[122] Yingqin Zheng and Ai Yu. 2016. Affordances of social media in collective action: the case of Free Lunch for Children in China. *Information Systems Journal* 26, 3 (2016), 289–313. https://doi.org/10.1111/isj.12096

A APPENDIX

The appendix contains a version of the semi-structured interview guideline and the parts of the code book.

A.1 Semi-structured Interview Questionnaire

(1) Personal background
- What gender do you identify as?
- Do you currently live in a rural or urban area within Myanmar?
- Are you a part of Generation Z or Y, meaning you were born between the early 1980s and the early 2010s?

(2) Use of SM
- Which social media platforms do you use?
- When and how often do you use social media?
- Why do you use social media?
- Which people do you currently follow the most?
- Are you content / satisfied with the platforms?
- Do you rather post something new or share posts / retweet something? Do you post mostly text or images or both? On a normal day, how often do you post pictures, comments, etc. on your social media accounts?

(3) Actual protest in Myanmar
- What do you think of when you think of the current protest movement in Myanmar?
- What are currently main topics discussed in social media?
- Which role do social media play during the protest? Do you see an interconnection between online protest and the protests on the street?
- Which characteristics describe both the online protest and the protest on the streets?
- Would you consider that online activism puts pressure on political decisions?
- Do you motivate yourself because of posts you see on social media?
- Would you consider that there is a collective identity raising?
- Has your social media consumption changed because of the protest?
- Do you have concerns about using certain platforms at the moment?
- Are you personally concerned about your privacy settings?
- Are you concerned that e.g. the government / military could have access to personal things posted?
- Does the current protest differ from previous ones?
- Where you informed about the protests in Thailand last year? If so, would you say that the protests in Thailand had influence on ongoing protest in Myanmar?

(4) Technical requirements
- If you are considering the possibility of using SM or other technology related to your activism, what specific features would you like to have in order to enhance its effectiveness?
- What additional recommendations or suggestions do you have to improve the the technology that you use?

(5) Open questions
- Is there anything else you would like to mention?

B APPENDIX: CODING TABLE

In the following, the coding scheme, including the core categories (level 1) and sub categories (codes; level 2-4) will be presented. Each subsequent level provides a more detailed explanation of the code of the previous level. The full codebook is available in the supplementary material.

Core category	Level 2	Level 3	Level 4
Role of SM during protest (partly cultural resources)	informing international community	sharing news on Facebook, hashtags (Twitter & FB)	
	inform people about protests/ high reaching level	inform in real time about military actions, live stream	
	place for party politics, mobilization strategies, controlling each other, communication, question misinformation, emotional support, encourages (for peaceful protest), information gathering/information sharing, management, express feelings		
Role of messenger during protest (partly cultural resources)	Telegram channels, organizing protest, communication (friends/family/work etc.), inform people about military actions/protest, connect in groups		
Topics discussed on SM	topics currently discussed on SM & messenger	ASEAN, Hong Kong, ethnic conflict, COVID-19, detention, international statements, safety / own protection, violence, military coup/political conflict, protest activities, sexual harassment, IDP, pro military, CRPH	
	topics discussed on SM before Feb. 1st	gender-related topics, random, pleasure, ethnic/religious conflict, education/business/work related topics, election fraud, COVID-19	
Reason to use SM and messenger (human resources)	stay generally updated, express feelings, self-presentation, share knowledge/information, follow people, shopping, entertainment, news, education, work/business, communication (friends/family etc.)		
Characteristics protest on the ground (partly cult. resource)	Thanaka, sad/disappointing, aspects related to gender, all ages, small groups, different strategies, growing, fighting for democracy, unequal, showing who is responsible, peaceful, 3-finger salute (self-production RMT), empowering/encouraging, massive/powerful, dangerous/violent, scary, unifying		
Characteristics online protest	not authentic, weaker than on street, dangerous/scary, large coverage, generation Y, trust, country wide, emotions through live streaming, all ages, for people who cannot go out, Keyboard fighter, generation Z, easy to access		
Change of messenger consumption since coup (human resources)	reporting misinformation on SM/pro-military, deleting FB (messenger), questioning FB messenger/WhatsApp/FB, following people/news on Telegram channel, using WhatsApp, using Telegram, using Signal, using SM less, using SM more		
Change of SM consumption since coup/change of behaviour (Human resource)	deactivating FB (messenger) for a certain period, changing profile picture (3-finger-salute), more aggressive, interested in different topics, posting less about political issues, using Twitter, deleting apps such as Facebook/having a break from SM, using FB (again), using it less, using it more		
Misinformation/Fake News	zero data, about prisoners released, COVID-19, informing/warning others/protesting news, reporting misinformation on FB, prevention, differences in generation/education, problem/challenge, all the time, about military/police, quantity of misinformation, every information needs to be checked/ask friends, hard to check/complex, mostly by military, about release of Aung San Suu Kyi, decreasing, increasing		

Impacts of coup	military actions	other restrictions, intranet, kicking out international companies, propaganda, cooperation with China, release of combatants, Cybersecurity Law, violence, threatening people, spreading misinformation/Fake News, eliminating human rights, banning/blogging SM/internet shutdown, controls/surveillance, arrests, banning media agencies, whitelisting	
	internet shutdown	culprit (internet shutdown)	not specified, both military and telecommunication provider, solely telecommunication provider, solely military
		problems caused by internet shutdown	telecommunication provided by military, impossible to work/study, no entertainment, no information spreading / live streaming, no communication, no information gathering
		back since 27th of April, mobile internet cut off, from 1-9am	
	discussions with friends/family, no rule of law, less sleep/exhausted, curfew, no daily routines anymore, fear/danger/depressed, losing jobs		
Alternatives to internet shutdown (partly material resources)	free VPN	many people use it	
	paid VPN, some are having trouble, text messages/calls, people helping each other to install VPN, SIM cards from different country		
Desirable changes in SM or Messenger	no changes desired, hints of disturbing content, update information on FB, opportunity to post voice messages, improve security settings, providers should be more responsible, better control of misinformation, hint for misinformation, use of nicknames, mark "I am safe", better anonymization		
Consideration of SM and Messenger	concerns about personal data	not concerned/concerns are not common, no concerns, concerned (especially since Feb.1st)	
	disadvantages about SM/messenger	time-consuming, hate speech, hacking, fake accounts, sexual abuse, a lot of violence/depressing notes, misinformation, authorities (police/military) controlling SM, social pressure	
	important to read news		
Security/safety measures	very important/useful, silence apps, Tor browser, using safe messenger, backup on laptop instead of phone, self-Censoring, story function, information gathering/spreading online, paid VPN (material resources), deleting messages/blocking accounts, disappearing messages (Signal), turning phone off/leaving phone at home, not using Mytel, changing privacy/security settings, informing others, night watch/neighborhood watch groups, password rather than fingerprint/face recognition, more than one FB account, solely protesting near own house, gear (Helmets, goggles etc.), lock profile FB		