Smartphone and ICT Use among Ukrainian Refugees: Technology Support during War, Flight, and Adaptation in Germany

ENNO STEINBRINK, LAURA GIANNA GUNTRUM, and CHRISTIAN REUTER,
Technical University of Darmstadt, Science and Technology for Peace and Security (PEASEC) Germany

In conflict-ridden environments, timely and accurate information is critical for those dealing with the dynamic of events. When individuals have to flee, it becomes evident that refugees frequently rely on information and communication technologies (ICT) for information acquisition, travel coordination, and maintaining connections with related parties. Based on 17 interviews, this research explores how Ukrainian refugees, who sought protection in Germany due to the 2022 Russian full-scale invasion, use ICT before, during, and after their flight. By providing empirical findings, the results show in depth how contextual factors, such as infrastructural instability, privacy concerns, and an advanced digitalization, interrelate with user behaviors. Analyzing the multifaceted civilian ICT use in the context of war and flight, this exploratory research contributes to the existing research on HCI in migration contexts and connects to several topics of CSCW. By contrasting case specifics, this work highlights what makes Ukraine a special case in this research area. Furthermore, this paper examines both existing and emerging affordances of ICT in the context of flight and identifies the crucial role of messenger groups for information gathering in all phases of the flight. Lastly, collaborative dimensions of the identified affordances are discussed.

CCS Concepts: • **Human-centered computing** → **Empirical studies in HCI**; **Empirical studies in collaborative and social computing**; • **Social and professional topics** → **Cultural characteristics**; • **Security and privacy** → *Social aspects of security and privacy*.

Additional Key Words and Phrases: Affordances, Crisis communication, Flight, Migration, Ukraine, Privacy

ACM Reference Format:
Enno Steinbrink, Laura Gianna Guntrum, and Christian Reuter. 2025. Smartphone and ICT Use among Ukrainian Refugees: Technology Support during War, Flight, and Adaptation in Germany. *Proc. ACM Hum.-Comput. Interact.* 9, 2, Article CSCW169 (April 2025), 32 pages. https://doi.org/10.1145/3711067

1 Introduction

In February 2022, the start of the Russian full-scale invasion of Ukraine triggered widespread humanitarian distress and prompted "the fastest and largest displacement of people in Europe since World War II" [95]. Over 5.8 million refugees from Ukraine were registered throughout Europe [94], of which over one million were registered in Germany in 2022 [88], making it the second most important destination in the EU after Poland [18]. Framed as a "special military operation" by Russian officials [32] and called a war by UN officials [72], the ongoing conflict also represents the largest land war in Europe since 1945 [34]. Nowadays, conflicts and wars are often influenced by

Authors' Contact Information: Enno Steinbrink, steinbrink@peasec.tu-darmstadt.de; Laura Gianna Guntrum, guntrum@peasec.tu-darmstadt.de; Christian Reuter, reuter@peasec.tu-darmstadt.de,
Technical University of Darmstadt, Science and Technology for Peace and Security (PEASEC), Darmstadt, Germany.

ACM 2573-0142/2025/4-ARTCSCW169
https://doi.org/10.1145/3711067

diverse technologies, marking a notable evolution in their dynamics. Amid the Ukraine invasion, hacktivism [63] and viral TikTok videos featuring soldiers [21] have become illustrative of this development. Since 2019, Ukraine's Ministry of Digital Transformation has spearheaded extensive efforts to digitalize public administration by 2024 [38, 69], a central aspect of crisis management during the ongoing attack. As of 2022, 76.6% of the population uses smartphones, reflecting the rapid pace of digitalization [87]. The refugee movement from Ukraine is similarly characterized by increasing digitalization and the reliance on smartphones for seeking assistance and accessing crucial information. Hence, gaining insight into how refugees use information and communication technologies (ICT) becomes crucial, as it allows us to identify challenges and advantages related to their use [81]. For the CSCW community, a detailed understanding is vital to tailoring research, design implications, and developments to local and specific needs, ensuring their work remains socially relevant, ethically sound, and positively impactful. Given the diversity of contexts, it is essential to examine each situation in depth rather than seeking "one-size-fits-all" solutions for the challenges related to migration and displacement. Moreover, the war in Ukraine raises questions of infrastructure resilience: While the rapid exchange of information could strengthen the self-help capacities of the civilian population, excessive dependence could have negative consequences if the systems are impaired, for example, by power outages, and affect the online cooperation of the population.

So far, existing research, including within the HCI domains, has extensively explored refugees' use of ICT during their displacement [1, 8, 50, 89]. Generally, most studies conclude that refugees express diverse privacy concerns and exhibit varying technology preferences, shaped by factors like their specific context, threat perceptions, and individual dependencies. For example, scenarios in which one's own government or other entities, such as the military, might seek access to one's data can significantly influence these concerns and preferences. Unlike individuals fleeing from war-torn and internally unstable countries like Syria [65, 89], the situation in Ukraine involves people fleeing from a technologically more advanced country facing solely an external aggressor, namely Russia, thereby setting it apart from other countries [67]. The large-scale refugee movements within a highly digitalized country present a novel and pertinent topic for HCI research aiming to comprehend the context-specific technical needs. Abu-Salma et al. [2] find studies within the HCI community need to find holistic approaches to study digital security practices, and consider the past, the present, and the future. In a reflection on the role of HCI in responding to the refugee crisis, Talhouk et al. [91] identify main challenges faced by refugee to be "(1) access to services; (2) integration into host communities; and (3) journeying to safety." Our work studies these aspects for the case of Ukrainian refugees by examining the effects of war on ICT access and infrastructural stability and the availability of devices, examining the role of ICT during the journey, and the use of ICT during the arrival and resettlement phase in Germany. Recognizing the gap in academic studies that specifically focus on refugees fleeing from Ukraine, our research aims to address the following research question (RQ):

RQ: *How do refugees from Ukraine use ICT before, during, and after their flight?*

Employing qualitative methods, this paper endeavors to answer this RQ by delving into the individual experiences of 17 Ukrainian refugees who sought asylum in Germany throughout 2022. Our focus includes exploring the use of technology in war zones, the impact on necessary technical infrastructure, social media networking among civilians, online coordination of flight, challenges during the journey, and the use of ICT to facilitate arrival in Germany. Generally, gaining profound insights into local conditions and the needs of refugees can greatly improve the quality of subsequent technical design considerations [30, 82]. In response to the Ukraine invasion, the Director-General of the International Organization for Migration emphasized the

need to understand the intentions and needs of refugees [72]. According to Talhouk et al. [91] "there is great opportunity for HCI researchers to take on action-oriented research responding to the challenges faced by refugees." At the same time, Sabie et al. [81] conclude that HCI research on migration is still in its exploratory phase, to which we aim to further contribute with this paper.

2 Related Work

Recently published research on Ukrainian refugees in European countries [18, 31, 53, 55, 75] primarily concentrates on demographic characteristics, integration processes, policies, and individual experiences related to the war. Our study distinguishes itself by its emphasis on technology use, a dimension that has not been the central focus of prior research focusing on Ukrainians leaving their country since 2022, except the study by Khvorostianov [52].

Outside the scope of Ukraine, numerous studies extensively explore refugees' general ICT access and usage, social inclusion, and service access [81]. Sabie et al. [81] study the field of HCI research in the context of migration and refugees and provide an overview on topics, research sites and populations that have been studied. Alencar [8] and Moran [68] provide literature reviews examining the use of ICT by refugees in other contexts across different stages of displacement. This involves the use of technology in the preparatory phase, within the country of origin, during the actual flight, upon arrival in the destination country or within camps, and during subsequent stages of social inclusion in the host country. Given the variety of reasons for flight, our focus on smartphone use in the country of origin is limited to existing studies in the contexts of (civil) war, conflict areas, or with reference to Ukraine.

2.1 ICT and Smartphone Use in Times of War

The HCI and CSCW literature on civilian ICT and smartphone use during wartime is limited. Rohde et al. [79] investigated the use of ICT by opposition forces and activists during the Syrian civil war. They looked at the infrastructure and found civil war front lines were represented in the telecommunication infrastructures, highlighting heterogeneity and fragmentation of connectivity for civilians depending on their location, which could also apply to Ukraine. Wulf et al. [102] examined the use of ICT in the Syrian civil war by activists and opposition members. They also considered the role of social media, especially Facebook and Twitter, which were used despite surveillance. By monitoring social media, political opponents could have been identified. Talhouk et al. [91] reported that for conflict zones, telecommunication infrastructure may not be consistently accessible. Wulf et al. [102] discovered that Syrian rebel army officers countered this with satellite phones. They further point to the role of videos in documenting war crimes, spreading disinformation, and deploying propaganda, such as tactics aimed at demoralizing the enemy during the Syrian civil war [102].

Specifically for context of the war in Ukraine, there have already been some initial studies on ICT use. Horbyk [45], for example, looked at smartphone use by Ukrainian front line fighters in the Donbas conflict (2014-2022). They find a "hybridization of the military and the intimate", e.g., when the soldiers' personal mobile equipment closes gaps in military gear, or when a direct line of communication is established between the civilian population and the soldiers. Within the context of the Donbas conflict, Shklovski and Wulf [86] investigated the use of mobile phones among civilians, volunteers, and soldiers. They report of knowledge consisting of a mix of myths and deep technical knowledge helping to mitigate risks of government and enemy surveillance. The authors highlight problems arising from the "always-on always-connected" devices in a wartime context and discuss strategies such as handling SIM cards, changing positions before using phones, or turning off phones to evade surveillance or localization by Russian intelligence or military. Shklovski and Wulf [86] also mentioned social functions, e.g., being connected with beloved ones, dealing with boredom of war, and keeping up-to-date with information.

In a study on Ukrainian adolescents fleeing from the invasion in 2022, Khvorostianov [52] identified three primary functions of ICT use: (1) emotional shelter, (2) social shelter, and (3) a "time capsule": This refers to the preservation and continuation of the disrupted life in Ukraine, the continuation of hobbies, and the preservation of memories. During the invasion on site, the adolescents used smartphones with headphones to block out negative stress stimuli, such as the sounds of explosions and shelling. Zarembo et al. [104] explored how ICT contributed to civil resilience in Ukraine after the invasion and highlighted the importance of the smartphone as a "resilience hub". They particularly pointed to the prominent role of Telegram among other social media platforms. Other researchers have looked at the 2022 invasion from a technical perspective: Jain et al. [48] looked at the stability of the internet connection by inspecting network package loss and found that the degradation of the connection correlated with the presence of Russian troops in the region.

2.2 ICT and Smartphones Use in Transit

As flight often occurs within the framework of mixed migration, with comparable routes and challenges [33, 85], we include studies that specifically address the use of ICT in a broader migration context. Some studies concentrate on individuals from the extended MENA region migrating to Europe [6, 9, 17, 26, 37, 58, 65, 66, 89], while others explore the ICT practices of migrants and asylum seekers in Latin America [74], or others aspiring to reach the US [71]. Many studies emphasize the importance of the smartphone as a means of agency [9, 89]. Merisalo and Jauhiainen [65] discovered that even individuals who had not used ICT before were likely to adopt them during the journey. One of the most crucial use cases is for route planning and to facilitate movement [9, 26, 89]. Alencar et al. [9] describe the smartphone as an organizational hub with various purposes: localization, liaising to deal with uncertainty or lack of information, and administration of personal and legal documents. It would serve as a lifeline, offering support in emergencies, providing a source of mental reassurance and enhancing feelings of safety [9]. The aspects of the smartphone as way for "diversification of available information" [26] and social media as a "key source of information" [6] is mentioned by most studies [6, 26, 37, 58, 65, 89]. Generally, social media can offer cheap and easily accessible information [26]. Commonly used apps and platforms are *WhatsApp* and *Facebook*, which is also found by research of digital practices of migrants and refugees coming to Europe [37, 66, 89], although this might be biased by a strong cultural influence depending on the user's origin. Other apps commonly mentioned are *YouTube, Skype, Viber, Instagram*, and *Twitter* [37, 66].

AbuJarour et al. [6] describe the uncertainty deriving from lacking or unreliable information and the importance of dealing with it for decision making. Wall et al. [98] coined the term "information precarity" to describe this. Borkert et al. [17] highlight the challenge of dis- or misinformation and the importance of strategies to validate rumors on social media. In these situations, Piste Beltran and Mendieta-Ramírez [74] emphasize the significance of relying on personally known contacts as sources (e.g., of information within Latin American migrant networks), as opposed to considering media reports, which are viewed as unreliable by some. Often, word-of-mouth tended to be the most important source of information. They also found a tendency to ignore information which might be important but could cause concern, distraction, or uncertainty.

Another negative aspect is the heightened vulnerability to digital surveillance and privacy violations, either by governments, border police or other entities [35, 37, 42, 58, 89]. Further risks arise by using the data for social sorting within asylum procedures or within refugee camps [16, 59]. These risks are often addressed by strategies like clearing Facebook and using pseudonyms [37, 89], using encrypted platforms to connect with smugglers [37], and protecting information about their intended routes [37]. Other strategies can be changing SIM cards, the disposal of smartphones or anonymity efforts like the use of a VPN client, the anonymous purchase of SIM cards, and

smartphones or use of code language [89]. Different authors emphasize that the connectivity of refugees is dependent on (potentially fragile) infrastructural aspects such as charging infrastructure for batteries, SIM cards, and WiFi hotspots [9, 37]. Gillespie et al. [37] highlight problems that can result from not being able to provide documents when buying a SIM card and are dependent on (sometimes illegal) help by others. Expanding beyond commonly discussed elements like route planning, information retrieval, and communication with close contacts [91], Khvorostianov [52] in the context of Ukraine, reveals that smartphone use serves to alleviate waiting times, e.g., at borders, through activities like watching videos. Additionally, the author notes the emotional and social support provided by smartphones in situations of limited privacy within refugee camps.

2.3 ICTs and Smartphones for Arrival and Social Inclusion

To fully grasp ICT use during displacement, it is essential to explore how ICT and smartphones help to arrive and foster social inclusion for refugees in their host countries [14, 103]. Fisher [30] highlights that the majority of HCI/CSCW studies exploring how refugees integrate into receiving communities have been conducted in European countries. Nevertheless, we will also touch upon noteworthy findings from studies conducted in Latin and North America.

AbuJarour et al. [4] finds well-being and the sense of agency as two goals of social inclusion for refugees in Germany, with ICT supporting by empowering users. The function of empowerment for social inclusion is also mentioned by other researchers [11]. Research on the use of ICT by migrants and asylum seekers with irregular legal status, conducted in places such as Italy or the US, underscores the positive impact of ICT use on well-being and a sense of security, while challenges related to legal status may still arise, including potential surveillance issues [40, 42]. ICT can help them to form and leverage large contact networks, avoid detection by authorities or engage in the underground economy if they are not allowed to work legally [40, 42]. While most privacy concerns within these contexts are related to their fear of detection and are connected to their irregular legal status (which might not be transferable to 'regular' refugees from Ukraine), the role of ICT, especially Facebook for maintaining migrant networks is central. Herbert et al. [44] observe widespread smartphone usage among individuals with a migration background, and note an increased incidence of experiences with cybercrimes, suggesting a heightened vulnerability to such risks. Jauhiainen et al. [49] highlights the role of ICT for transnational digital practices for forced migrants limited in their physical mobility. Ruokolainen and Widén [80] discuss the role of misinformation among asylum seekers and identify the problems of incomplete or inadequate official information, outdated information, the role of trusted gate keepers, unrealistic expectations on the base of rumors and distorted information, e.g., on social media or within asylum seeker networks. Melella [64] also highlight the importance of ICT in facilitating stronger connections for individuals with migration backgrounds. The study revealed that South American migrants in Argentina utilize platforms such as Facebook or Skype for cost-effective and immediate communication with peers in their country of origin. Andonaegui et al. [12] find social networks would enable transnational migrants to communicate with their origin communities, enable them to communicate synchronously and asynchronously and sustain their family role from abroad, an idea we find connected to the idea of the "time capsule" by Khvorostianov [52].

In sum, research has explored ICT and smartphone usage in various conflicts and migration scenarios. Yet, there is a scarcity of research dedicated to the Russo-Ukrainian War and its escalation in 2022, where Ukraine serves as an example of a highly digitalized nation impacted by conflict. Much of the existing research on refugees' ICT use focuses on populations from digitally less advanced countries. Sabie et al. [81] show in their work that while Europe is a major research site for migration and refugee studies in HCI, so far, the research focus has been on migrants and refugees from the MENA region, and European refugee populations had not been studied in their ICT use

behavior when their analysis was conducted. Several HCI researchers interviewed in the paper state that the most significant academic contribution would be to introduce "a politically/economically-motivated but a socially-bearing issue to the HCI field and presenting an understanding of various cultural needs of diverse migrant communities" [81, p. 21]. Furthermore, very few studies have been published that comprehensively examine all stages of displacement [6, 28, 65], with Alencar [8] explicitly mentioning a lack of studies addressing the phase before the flight. Moreover, few studies focus predominantly on interviews with female refugees. This is particularly relevant given the unique circumstances in Ukraine, where the majority of women are leaving due to the "sex-selective military recruiting law", which states that Ukrainian men eligible for military service are not legally authorized to leave Ukraine [67, p. 1]. In other contexts, however, it is primarily men who flee, often due to the perilous nature of the flight routes [25]. Additionally, the research landscape lacks sufficient exploration of refugee ICT usage in the post-pandemic era despite the evident influence of the pandemic on technology adoption and integration.

Our study endeavors to address the identified research gaps by offering thorough and exploratory insights into the use of ICT among Ukrainian refugees in the different stages of flight. We use these results identify relevant case specifics and affordances to analyze collaborative aspects using the Model of Coordinated Action (MoCA) [60].

3 Method

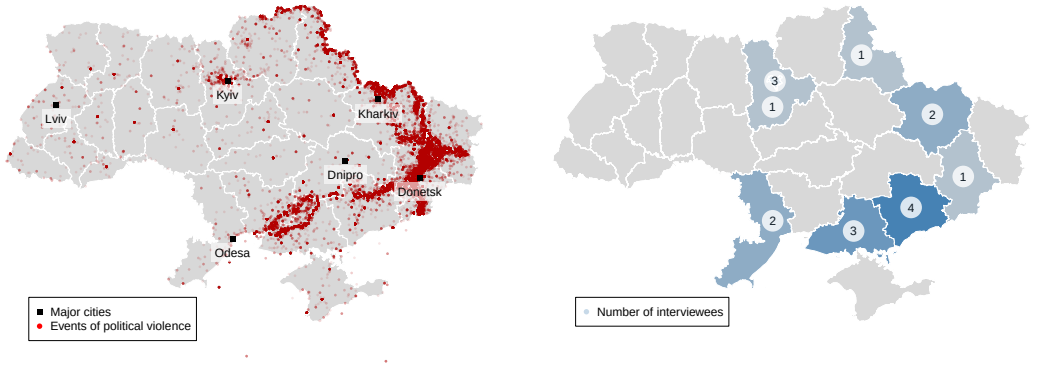
In the following, the methodological procedure will be presented. Due to the sensitive nature of the topic, as also outlined by Sabie et al. [81], we've strictly followed research ethics and do-no-harm principles to safeguard participant well-being [22, 93, 100]. The study received IRB approval by the authors' institution.

3.1 Data Collection

To gain detailed insights in the lived experience of Ukrainian refugees, we conducted qualitative interviews ($t_{\max} = 103$ min, $t_{\min} = 46$ min, $\bar{t} = 73$ min) with Ukrainians that fled from Ukraine to Germany ($N = 17$), following the onset of the full-scale invasion on February 24, 2022. The interviews were carried out between September (2022) and January (2023) in different German cities until we perceived that theoretical saturation had been achieved. We employed multiple strategies for data collection, including collaborating with volunteer workers at refugee contact points in various German municipalities (purposive sampling), contacting administrators of Telegram help channels dedicated to Ukrainian refugees, and then utilizing snowball sampling techniques [36]. Additionally, we engaged in preliminary discussions with professionals collaborating with (Ukrainian) refugees, gaining valuable insights in advance. This process enhanced our understanding of the potential feasibility of conducting a study involving individuals that have potentially experienced trauma.

Prior to the interviews, we prepared a semi-structured questionnaire (see Appendix A) that was developed through an abductive approach, drawing on existing studies on technology use in flight contexts [54, 78, 90]. Overall, we covered several aspects, including (1) information on flight route, (2) relevant apps and general user behavior, (3) communication during the Russian invasion, (4) flight planning and connection with peers in target countries, (5) social media use, trust and information verification, (6) privacy considerations and adaptations of user behavior, and (7) impairment of digital and electrical infrastructure and the impact on user behavior. All respondents were questioned equally on the various aspects.

All interviews, except for one, were carried out face-to-face. For the online interview, we opted for *jitsi* (E2E encrypted and GDPR-compliant) to ensure data security. The face-to-face interviews were conducted at locations selected to ensure the comfort of the participants (e.g., refugee accommodation, café). Before the interviews, participants (18 and older) were provided with comprehensive



(a) Map of events of political violence in Ukraine (explosions, armed clashes, air/drone strikes, violence targeting civilians) based on the publicly available data of the "Ukraine Conflict Monitor" [13] by the Armed Conflict Location & Event Data Project (ACLED) [77].

(b) Origin regions of our interview partners. The number within the circles corresponds to the number of interview partners from the respective region

Fig. 1. Maps of the regions of Ukraine depicting (a) main areas of attacks and (b) origin regions of our interview partners.

information regarding the study's objectives and data processing procedures. Each interviewee provided consent by signing a consent form offered in English, Ukrainian, and Russian. While the majority of interviews were conducted in English, eight interviews involved the use of a translator of which seven were conducted in Russian and translated to German. The translators were not professional interpreters; however, they were also commonly consulted by local municipal administration. In one other instance, an interviewee chose to rely on a trusted friend for the translation process. All interviews were audio recorded using a designated recording device to ensure safe data storage. The participation was voluntary and not financially compensated to avoid false incentives. In case the interviews took place in cafes, the interviewer covered the associated costs.

3.2 Interview Partners and Case Selection

The interview partners (N = 17; 13 females, three males, and one trans-woman) predominantly self-identified as female, mirroring the gender distribution observed among Ukrainian refugees in Germany, which indicates a significant gender imbalance with approximately 80% being women [29]. This gender imbalance is different from most other refugee flows discussed in HCI literature and is in line with literature on refugee movements [56] and can be attributed to compulsory military service in times of war, effecting a ban on leaving the country for healthy male citizens aged from 18 to 60 [27]. Research, like that of Gray and Franck [39], has demonstrated that gender significantly influences the experiences of displaced individuals. Based on estimations by the interviewers the interview partners covered an age range from approximately 20 to 65 in a relatively equal distribution. Many interviewees stated that elderly family members chose to stay in Ukraine.

To grasp potential variations, such as mobile reception, we asked the interviewees about their origin regions in Ukraine (see Fig. 1b). Five of our interview partners fled from regions that had already been occupied by the Russian army. Nearly all of our interview partners reported their area of origin was already under attack when they left or was attacked shortly after (see Fig.1a). We further asked about their first language as Ukraine has a large percentage of Russian speaking

population (29%), although many people are bilingual. We did so because we assumed there could be a greater cultural influence by Russia and Russian media. Of our seventeen interviewees, four spoke Russian as a first language (IP10-13)[1], three spoke Russian at home, but considered themselves bilingual (IP2,8-9), six were bilingual (IP3-7,14), and three spoke Ukrainian as a first language (IP15-17). Moreover, in our effort to minimize the collection of personal data, we did not request further personal information.

In the following, we want to provide context for the case selection, as it is crucial to note that Ukrainian refugees arriving in Germany face(d) different circumstances compared to previous refugee flows. A key factor for this is the activation of the "Temporary Protection Directive" of the EU [92], which simplifies bureaucratic processes and easier access to housing and work allowances [24]. People from Ukraine have been granted visa-free entry to Germany and all other Schengen countries since 2017. They can thus travel to and from their home country without losing entitlements, relieving them of the uncertainty of asylum processes. Other difficulties, e.g., with SIM card registrations for which legal documents are required, did not apply due to Ukraine's digital ID system and the extensive provision of free SIM cards for Ukrainians by several mobile providers. Within the discussion section, we will discuss how these and other contextual factors (e.g., racist resentments) might have affected the results. Some argue that geopolitical considerations have significantly influenced the more positive reception of Ukrainian refugees [41], and that there was an overall favorable perception of them within German society. Brücker et al. [18, p. 397] therefore point out the "need for a more nuanced understanding of the experiences of Ukrainian refugees."

3.3 Data Analysis

The collected audio data was automatically transcribed offline (using OpenAI Whisper [76], an open-source speech-to-text model, in Python), manually corrected and formally anonymized. The resulting transcripts were then analyzed and coded by two researchers, using MAXQDA. The data analysis was inspired by qualitative content analysis [61] and followed different coding steps: Initially, two authors individually openly coded the transcripts sentence by sentence. In a second step, the codes were collectively discussed as recommended by Mayring [61] and grouped in higher-level-categories according to their thematic overlap (see Table 3, Appendix). Overall, 23 core categories (containing 2557 codes) were identified by drawing from both theoretical concepts and building upon the collected empirical data. Given the sensitivity of the research, the audio files were deleted, and the transcripts are anonymously stored in encrypted file containers and can only be accessed by the authors to prevent any possible privacy violations on the base of correlating autobiographical details.

4 Results

In this section, we will organize the findings derived from our interviews, examining ICT use throughout the different phases of our participants' flight experiences.

4.1 Pre-Flight: ICT Use in Ukraine after the Russian Full-Scale Invasion

Our findings indicate that every participant in our interviews owned a smartphone. Some respondents mentioned having a laptop (IP5,7-9,10,15) or tablet (IP7,10,12-13) as well. However, these devices were perceived as less significant. When asked about the importance of smartphones and the internet, interviewees stressed their significant relevance (IP1-3,6-8,14), with some regarding them as the utmost priority (IP12-15).

[1]We used interview partners' identifiers (IP = interview partner) for statement sources. If statements could somehow be interpreted as incriminating, we omitted the identifier as an additional privacy measure.

4.1.1 The impact of military attacks on infrastructure and adapting to instability. Smartphones and ICT can only be useful with the necessary infrastructure: electricity or other possibilities to charge batteries, cellphone towers and antennas providing phone reception, WiFi networks, internet infrastructure, and landlines. Media reports indicated these infrastructures were targeted by Russian military attacks [19]. Consequently, we asked our interlocutors, whether and how military attacks affected the infrastructure. Interviewees reported blocked signal, presumably by the Russian military (IP2,7,10-11), no or unstable mobile reception and slow internet (IP2,6,8,10-11,15-17), especially during the attacks in the beginning (IP3,12-13). Complete outages or unstable connection were especially reported by the interviewees from the occupied zone (IP10-11,15-17). Furthermore, TV and cellphone towers were specifically attacked by the Russian military (IP15). In some regions, the connection was quickly reestablished (IP3,8), partly using StarLink satellite internet (IP9,15). The interviews highlighted the crucial role of communication for the Ukrainian population, underscoring the need for a prompt infrastructure reconstruction in case of any damage.

While internet shutdowns and attacks on TV towers had varying impacts on the accessibility of information through TV across different regions (IP7,15-17), only satellite TV remained operational in the occupied zone, as Russian forces were unable to block it (IP15-17). Others used radio as an alternative for information gathering (IP11). In the face of unstable reception, people found personalized solutions to receive messages:

> "*[IP11] always left the phone outside , so that [they] could get information from outside [the occupation] . Because [they] had little reception, so [they] didn't have it in the house. (...) And [IP11] just put the phone in a winter hat and then left it outside. And then, in the morning, they could read messages, if there were any.*" (Translator for IP11)

Given the constraints and unreliability of smartphone communication in certain instances, there was a growing reliance on personal contacts and face-to-face information sharing (IP10-11). IP15 reported that people would bike to the next village and go from house to house to deliver news.

In addition to disruptions to internet and mobile connections, electricity was also impacted in various parts of the country (IP2-3). The extent of the disruption varied depending on the time and the proximity of regions to the front line or areas under more intense attack. Electricity issues caused some routers to stop working, which consequently shut down landlines (IP15) and WiFi internet, and sometimes even mobile internet (IP1-2). At times, electricity issues could be addressed using a generator or by charging phones in the next big supermarket, which had an ensured power supply (IP1). To address electricity shortages, electricity providers have introduced alternating turns for the parts of cities to be supplied. These could be looked up on their website (IP6). This also affected the communication during these times: People posting "*See you after five days for the next turn on electricity*" (IP1). IP1 highlights the importance of asynchronous communication in times of infrastructural uncertainty.

4.1.2 Staying informed in times of war: Connecting on messengers and social media. Following the invasion, obtaining war-related information became crucial for Ukrainians, particularly through messengers or social media. Relevant information included the well-being of beloved ones and getting a realistic assessment of the situation in their own area and elsewhere in the country. Besides getting news directly from peers via chat messages or phone calls, many of the interviewees reported reading news on social media. Particularly Telegram was a common platform, either through channels where only administrators posted, and users received information, or in local public chat groups and self-help chat groups where individuals could also share updates. Even politicians, such as President Zelensky, used their own Telegram channels to keep the public informed (IP4-5).

IP7 stated receiving news "*mostly on Telegram. Because they usually have links to the websites, so I think you can trust them.*" This answer was exemplary for many of our interlocutors. While IP7 trusted in the reliability of information shared on Telegram, mis- and disinformation within Telegram groups were frequently mentioned. The majority of interviewees expressed a belief that Russians had infiltrated these public groups (IP1-2,4,6-16). IP8 stated that they believe recognizing Russians based on the negative remarks they make: "*Sometimes they just talk not really good stuff and they expose themselves by it*". Strategies such as gating the chat groups, for instance, by making them private (IP14) or banning users assumed to be Russian based on their posted content (IP7-9,12-15), were implemented to address these issues. Another approach involved converting the groups into channels where only administrators could post. Individuals seeking to share information had to then contact the administrators, who acted as gatekeepers for publication (IP3-4,12-13).

In addition to infiltrated public chats, IP7 reported the existence of fake news channels where Russian propaganda was shared. Moreover, several deceptive channels attempt to establish credibility by sharing accurate information on specific topics, while also interspersing misleading information (IP14). Many participants had some strategies to check for the trustworthiness of information. Besides checking for credible source links, checking for plausibility, having and estimation of the trustworthiness of the posting user/channel administrator (IP14), personally known contacts were contacted to verify information via the personal network (IP14).

> "*Do you understand that every information channel can do information? They can do information on how they think or how they saw it. When I see it on a different information channel, when I have some people, who can tell me what really happened, I read information from the information channel. I speak with people and then I understand what is the real situation.*" (I6)

Moreover, the Ukrainian military or government would provide lists of reliable news sources (IP10). Several interviewees highlighted the importance of local groups for faster and more accurate information and warnings (IP10,14). "*Actually, so quick news, so actually in the war, the most important is to act in time, okay?*" (IP14). Another ICT-based way to receive critical information on attacks or government warnings is the use of warning apps and air raid siren apps such as *Air Alert* (IP2-3,5,12-14). While normal sirens (IP5-6) or warnings in chat groups (IP12-14) were mentioned as important as well, IP14 highlighted the usefulness of the air raid warning app for individuals working indoors with headphones on so the physical sirens would be overheard. The warning would arrive hours or minutes before strikes would hit, providing time to reach a nearby shelter.

Since a most of our interviewees were fluent or native speakers in Russian, we whether they would read Russian news. Some mentioned ceasing to read it due to its apparent dishonesty, while others continued out of curiosity or to gain insight into Russian perspectives (IP4,8,12-13). IP4 expressed that "*sometimes [the news is] really like ridiculous.*" Several interlocutors reported they stopped using Russian websites or social networks, or listening to Russian podcasts (IP7).

Aside from information sharing among users and receiving news from different channels, users could also provide information, such as details on Russian military activity, directly to the Ukrainian government or military. Although none of the interviewees explicitly admitted to providing such information themselves, they demonstrated awareness of certain tactics. For instance, IP14 stated, that the Telegram bot *e-Voroh* (translated: e-Enemy) could be used. Especially in wooded areas, which could not be well monitored by military drones, user reports were found valuable (IP14). Also, pictures of markings for bomb attacks could be posted (IP2). Later, any pictures would need to be deleted, so it would not be possible to restore them, to not incriminate the person in case of a search or arrest (IP2). In other cases, people could use *Signal* to provide information to the military, e.g., on the position of tanks (IP15).

4.1.3 Privacy considerations during war and foreign aggression. For most participants, personal digital privacy did not stand out as a primary concern. IP4 stated: "*I don't have any secret information which should I worry about.*" Many conveyed the sentiment that they considered themselves ordinary individuals with nothing to conceal (IP2). Nevertheless, there appeared to be an awareness of confidential information that should be safeguarded from falling into the wrong hands, such as the Russian enemy. This awareness was cultivated, in part, by the Ukrainian government's prohibition on disseminating military information and details of attacks. The government conveyed this restriction, often referred to as "information silence", to the population through various information channels. IP5 explained: "*information [such as] photos [and] videos of moving [and] of our technique, of our troops. It's illegal. It's against the law and posting videos of the Russian attacks. (...) Only after the main resources like our president or our people who help him send this to the mass media. After that, you can show what's happening.*" It was evident that the interviewees shared a collective awareness of refraining from posting security-sensitive information and communication details immediately after attacks. This precautionary measure aimed to prevent the potential use of such information by the Russian military to adjust their artillery (IP3).

Another case in which privacy was also relevant and led to privacy-adjusted user behaviors was having contact with the Ukrainian government, military, or authorities, especially from the occupation, where people have to fear life-threatening repercussions for this. Here, one strategy was to avoid a direct communication line: People would contact trusted persons outside of Ukraine, who would then pass on the information to authorities. For this, secure messengers like Signal and VPN clients would be used. Some reported using code language to obfuscate their communication and prevent deciphering without prior knowledge. A similar use of code language was reported outside of the occupation, when talking about attacks to relatives. To adhere to information silence, individuals avoided direct references to streets or places, opting instead for obfuscated information requiring local or interpersonal knowledge. In terms of privacy, individuals in the occupied zone took additional measures beyond following external and internal (reporting) guidelines about the invasion. Some opted for a secondary SIM card (IP10) or a dedicated smartphone (IP15), and they made sure to power off these devices when not in use to avoid localization. Since the occupiers apparently require(d) people to use Russian SIM cards (IP15), probably for surveillance reasons, people tried to use Ukrainian SIM cards for, e.g., accessing their online banking or services that were deemed illegal, were blocked or surveilled (IP15). As sources of knowledge for the aforementioned privacy practices, respondents cited *TikTok* and *YouTube*, along with learning from another or acquiring information through chat groups (IP10-11,15-17).

4.1.4 Importance of using ICT in flight preparation and "Diia" for digital identity management. Many of our interviewees reported having had connections to Germany before coming, either directly via friends (IP2), family living abroad (IP5) or indirectly via contacts of friends (IP8). IP6 mentioned discovering a driver on Instagram, while others coordinated carpooling through group communication on their phones. Due to congested highways, destroyed bridges, and depleted gas stations, interviewees resorted to online checks for road conditions and gas availability along their routes (IP4,10).

Furthermore, having the necessary documents for border crossings was crucial. Many interviewees stressed the vital role of the government's *Diia app* for this — an app serving as a document wallet (e.g., passport), healthcare record repository (IP5), COVID-19 certificates, payment option, government information source, and platform for public surveys. After the invasion, this app was enhanced by many functions, e.g., collecting donations for the military (IP14) or a war game that aims "*to cheer up Ukrainians [by] destroying Russian troops*" (IP3). Since not all people had a passport which needed more processing, they could also get an extemporary "war document" within Diia,

so they could cross the border for flight (IP3). Within the occupied zone, all visits to the authorities had to be replaced by Diia, since the local administration had left (IP15). Overall, a total of 15 interviewees stated that they had actively used Diia before and during their flight.

4.2 Flight: ICT Use in Transit

The means of transportation varied and were often changed for different sections of the journey: Eleven participants used a bus (IP1-5,7,12-13,15-17), eight went by car (IP1,3-4,6,9-11,14), and nine used a train (IP2-3,5-6,10-11,15-17). While most interviewees came from Ukraine via Poland to Germany (IP1-3,5,11-17), some had to take indirect routes via other countries first, e.g., Moldova, Romania, Slovakia, Hungary, and Czech Republic (IP1,4), or took another route via Hungary and Austria (IP6). Due to the necessity of stopovers, some individuals were compelled to seek temporary accommodation in shelters or vehicles (IP4), or alternatively, at the train station (IP6). Five participants had fled from territory occupied by Russian forces (IP10-11,15-17). Given the dynamic circumstances, the flight often involved plan adjustments and continuous re-planning.

4.2.1 Navigation: Planning and adjusting the route to Germany with chat groups. Very important functions during the escape for the interviewees were navigation or proof-checking routes. The majority of interviewees indicated using *Google Maps* (e.g., IP5), with only a few opting for *Apple Maps* (IP7), and *Maps.Me* (IP3). Six mentioned downloading maps for offline navigation to ensure accessibility in case of connectivity issues (IP2,8,10,12-14). Resorting to paper maps (IP6) or relying on road signs (IP7) were mentioned as contingency plans in case of an empty phone battery. In some areas, street signs were deliberately removed to confound Russian soldiers, contributing to the importance of smartphone navigation (IP15-16). Further, local chat groups were also important for proof-checking the routes (IP10,15). Particularly when leaving the occupation, for example, it was possible to organize bus or car rides through the escape corridor, some of which went through mined areas (IP10,15-17).

> "*Of course, the most important thing was [Telegram]. All the messages were there. It was particularly important on the road. 'Something happens, something drives.' (...) At once, 30 cars driving and then, when they drive past a place where it's a 'gray zone', so to speak [I: That was this 'escape corridor', right?] Exactly. When they reach a place or gray zone - gray zone, there's nobody in the place — then there are battles and then they always wrote whether it's dangerous. Where mines are, because they drove between mines. Mines should be pushed aside.*" (Translator for IP10)

Another aspect that gained importance for some during their flight was the availability of local support, primarily facilitated through social media groups. In some cases, interviewees mentioned to have accepted such assistance spontaneously. IP3 reported that someone "*came from Germany to Kraków just to pick us up and bring to [city].*" This indicates the presence of volunteers from various nations within these support groups and highlights the provision of transnational assistance. Overcoming the language barrier with volunteers often presented a challenge, highlighting the indispensable role of translation apps in addressing this issue (IP1).

Another important function, that was already essential during the preparation, was finding or booking accommodation (IP3). Challenges mentioned by some interviewees included the lack of familiarity with people that offered accommodation, leading to nights being spent in train stations (IP6), cars (IP4), or communal accommodations (IP4).

4.2.2 Ensuring privacy and data security in transit. A central aspect frequently mentioned was the practice of physical checks of smartphones by border officials or at military checkpoints when

individuals were leaving the occupied territory (IP2,10-13,15-17). While, according to our interviewees, Ukrainian border police or military mainly searched for Russian collaborators, supporters of the Donbas military (IP2), or men aiming to avoid military service, Russian military searched for partisans and soldiers (IP10-11,15-16), or useful information related to the administration (IP15).

> "*(...) 38 'blockposts' [meaning checkpoints] they drove through from [a location within the occupation]. And at every post, at Russian post, they were searched. (...) On the bus, only men were checked. So notebooks and cell phones for men.*" (Translator for IP15)

IP10 and IP11 went through ten checkpoints and reported that every individual underwent thorough searches. Particularly when passing through Russian checkpoints to leave the occupied zone, precautionary measures were taken to ensure that smartphones were as "clean" as possible and did not contain any usable information. According to IP10 and IP11, their smartphones were reset and the memory was repeatedly filled with downloaded videos to prevent data reconstruction. Apps were downloaded to simulate normal use so that the smartphone would not raise suspicion (IP15). Otherwise, devices were hidden from searches and "fake" smartphones were shown (IP10). Important data often was backed up in the cloud before being deleted (IP10,15), however IP10 reported not to have had the time for that. These cleaning measures were acquired through instructional videos on YouTube and TikTok, or via guidance from chat groups or word-of-mouth sources (IP15). However, these procedures were difficult, especially for elderly people (IP11).

4.3 Arrival: ICT Use of Ukrainian Refugees in Germany

The interviewees reported minimal change in smartphone use upon arriving in Germany. Yet, they described adjustment behaviors, reflecting their efforts to adapt to the new country and situation. It is important to note that their behavior may have changed over time, and this only reflects their behavior up to the point of the interviews.

4.3.1 Gathering information and locating (self-) help groups. Overall, the process of gathering information appeared highly complex and many reported to be overwhelmed by bureaucracy and local regulations (IP6-9,11), due to the federal structure of Germany and the differences in rules depending on the municipality. This led to the high importance of local self-help or volunteer help groups, mostly on Telegram, in which refugees and local volunteers exchanged relevant information and hints (e.g., where to find a doctor), could ask questions or ask for help (IP6). IP9 stated: "*But when we arrived in Germany, there are a lot of groups in Telegram where I can find some useful important information about everything.*" These groups existed at different levels of regionality, ranging from groups for towns to federal states, or even nationwide groups. Political discussions were commonly disallowed within these groups (IP9). In summary, interviewees exclusively referred to self-help groups, with no mention of official websites or dedicated apps for refugees (IP1,4).

4.3.2 A virtual bridge to Ukraine: Using ICT to connect two worlds. Numerous interviewees mentioned getting local SIM cards (e.g., by the telecommunication company *Telekom*) upon arrival in Germany, offering free calls to Ukraine for some time: "*When I came here, they give to refugee people free phone cards*" (IP1). Most interviewees expressed using their smartphones to stay connected with beloved ones in Ukraine. For this, messengers (e.g., Telegram, Viber), social networks (e.g., Instagram, Facebook) and Voice-Over-IP apps (e.g., Viber calls, Telegram calls) were mentioned as being relevant for transnational communication. IP6 stressed the importance of video calls, allowing the father of their children, who is unable to leave Ukraine, to see how they grow up: "*We speak with their dad on FaceTime or Telegram and my children kiss the phone. (...) Thank God we have [that] and children can see their dad and dad can see his children are adulting [growing up].*" Video

conference tools, like *Google Classrooms*, were also important for children to continue their studies in Ukraine (IP4).

Several interviewees mentioned that continuous communication with people in Ukraine and frequent exposure to media content were emotionally stressful. IP3 expressed uncertainty about what to share online, feeling a sense of guilt for leading a "normal" life in Germany while their friends in Ukraine are experiencing the realities of war: "*Then I'm texting her [a friend] like 'here, see my hair from this angle. What do you think?' (...) And she's like: 'Sorry for not responding for such a long time. I was collecting water, because there is no water'. I just forgot about it for a second. (...) I just don't know what would be okay.*" Due to the flood of negative reports, IP1, for example, found it necessary to take a step back, distancing themselves, and temporarily blocking certain news.

4.3.3 Advocating for international awareness and informing the world online. In contrast, some people are actively engaged in sharing war-related news. Awareness raising online was considered politically important as it would lead to international solidarity and increase political pressure on other governments to support Ukraine (IP8,12-13). Furthermore, it would document war crimes by Russian troops (IP8,12). IP8 mentioned: "*There are many photos of Russian war crimes and it's shared and shared, and shared.*" The objective of awareness-raising online was to amplify public pressure outside Ukraine and internally, aiming to spotlight political misconduct and corruption (IP15). Translating news to English would be crucial to reach an international audience (IP3). IP14 did not participate in online activism, expressing the belief that effective online protests could only be carried out by more well-known people who reach more individuals online. Some individuals stated that they had been blocked on social media due to the war-related content of their posts (IP6). A different form of online activism targeting Russian society was described by IP3: "*There was another huge Telegram channel of designers. Designers fighting Russia, I believe. Where we were doing posters for social media telling about what is actually going on.*"

4.3.4 Using ICT to handle bureaucracy, the language barrier and integration. By and large, bureaucracy was highlighted as a significant challenge (IP7-8,10-11). German bureaucracy still largely involves paper-based processes, leading multiple interviewees wishing for an application like the Diia app. According to IP6, there are generally more apps in Germany, making it challenging to determine which ones are deemed relevant. With some information being unavailable in Ukrainian or Russian, individuals attempted to utilize online translators to complete e.g., registration forms (IP9). Struggling with the completion of the necessary paperwork hindered people from being allowed to visit an integration course or German class or to find a job. Some interviewees reported using online language courses or apps like *DuoLingo* to learn German (IP6). IP6 praised the opportunity to engage in online German language learning and other educational courses. Without this option, visiting a course would be very difficult, particularly with young children still too young for kindergarten: "*I'm very thankful that we have technologies where I, like [a] mom, can listen different courses. I can learn Deutsch [German] language by myself.*" IP10 reported to avoid groups and networks by Ukrainians in Germany to foster the integration process and learn German faster.

Generally, our interviewees often criticized the lack of digitalization in Germany. German online banking apps were specifically pointed out several times (e.g., IP4). Also, interviewees reported they had payment problems because their Ukrainian bank card or payment via smartphone would not be accepted. Their conclusion was: "*[In Ukraine] it was much better than in Germany. In my opinion, it's like, what you have in Germany, it's like old Ukraine*" (IP9).

5 Discussion

In the following, we will contextualize our results in past research on ICT use by refugees and migrants by discussing case specifics to work out what differentiates this case from other contexts

that have been considered in past research. We then proceed to discuss the relevance of several socio-technical affordances we identified relevant for Ukrainian refugees. Further, we will derive implications for CSCW by positioning our results within current topics of the field.

5.1 Case Characteristics within the Context of HCI Work within Migration Contexts

Within Section 2, we presented several studies particularly relevant to our case. Furthermore, a substantial corpus of HCI and CSCW research examines the utilization of ICT by migrants, asylum seekers, and refugees across various contexts and countries. This is discussed in detail in the review papers that we have referenced [8, 68, 81]. While studies on ICT and migration increasingly focus on refugees, and general ICT access and use is still one of the main issues, many studies now address issues of social inclusion in the host country and access to services [81]. This leads us to believe that the stages before and during the flight still need to be studied in more detail. We have tried to complement this by looking at the use of ICT by refugees at three different stages of displacement. Our findings show similarities with other cases but also some marked differences in contextual factors that we would like to consider in this section. In the following, we will discuss the contextual factors against the background of existing HCI/CSCW research. We have summarized key aspects, provided a comparison with previous research, and offered comparative reflections in Table 2, which can be found in the Appendix.

5.1.1 Refugee population. In contrast to other large refugee movements arriving in Europe, the majority of adult refugees from Ukraine were women (often with children), as most adult men had to stay in the country for military service [67]. Prior research has predominantly focused on male refugees, given that most of the arriving refugees are male [6], as a result of the inherently dangerous nature of the passage (e.g., crossing the Mediterranean Sea). In general, gender appears to play an important role in several areas, such as information needs, particularly during the resettlement process, where some female interviewees reported asking for recommendations for a child's doctor in support groups. Another female interviewee praised an app for language learning since a (young) child had to be cared for at home. However, we did not find any gender differences in access to ICT (everyone had access), as it was found in other refugee populations due to gender discrimination and cultural differences [46, 98]. With the countries of origins sometimes mixed in past research (e.g., [17, 89]), there has been a focus on the MENA region [81], which might lead to differences in cultural user preferences (i.e., the preference for Telegram). Understanding the diverse needs of migrant populations with different cultural backgrounds was identified as a key research contribution for the HCI/CSCW field [81].

5.1.2 Digitalization and digital literacy. Another aspect to consider is the high level of digitalization in the Ukrainian society. Our interviewees reported that their everyday life in Ukraine was characterized by using apps in various areas, such as receiving information, mail, official documents, parking tickets, making doctor's appointments, etc. Partly, local chat and information groups existed and were established before the invasion. They were then repurposed as a hub for information on war developments or help requests. To this extent, this has not been reported in other cases. As a result, even the older interviewees seemed to be comfortable using smartphones to watch YouTube, chat and make internet calls, although not with the same proficiency as the younger interviewees. Overall, many interviewees expressed frustration about the lack of digitalization within Germany, an issue that has not been brought up in the literature before. In other cases from the literature, we see a rather heterogeneous digital literacy. (i.e., [62, 66, 89, 101]). Merisalo and Jauhiainen [65] point to statistics from the International Telecommunication Union, which show that many countries from which refugees flee have a low percentage of internet users[47]. Although further infrastructure development and the effects of the COVID-19 pandemic may have

influenced changes, it remains unlikely that these (conflict-ridden) regions have reached the same level of digitization as Ukraine.

5.1.3 Flight reasons and -context within the country of origin. To understand user behavior, particularly in relation to privacy, it is crucial to be aware of the specific threat scenario they are facing. Most cases considered in literature are characterized by interior conflicts, often involving terrorist or rebel groups, sometimes with additional external forces being involved. Some examples are the Syrian civil war [4, 6, 37], Afghanistan [49, 89], Iraq [37] or Somalia [20]. Further, studies from the US, Canada, or Latin America often conduct research with people fleeing from Latin America [81]. In Central and South America, mass migration is often driven by interior conflicts, gang conflict, organized crime violence, widespread poverty, and frequent kidnapping [5, 81]. This has implications for the obstacles that need to be overcome to leave the country or during the journey, and whether the preparations need to be kept secret. In the case of Ukraine, we found that the threat scenario was different: There was a clear external aggressor and therefore, no political persecution or fear of an oppressive government. Hazards to individuals were often related to attacks (e.g., shelling or air raids) and challenges were mostly related to affected infrastructure. As Ukraine borders the EU and the Temporary Protection Directive was activated, there was no uncertainty about asylum applications and no need to cross borders illegally. Consequently, there was no fear of surveillance. However, this changed for the occupied territories when the external aggressor took over the communication infrastructure and surveillance, searches and censorship followed. This highlights the importance of analyzing the threat model, as it is highly individualized and different threat scenarios can exist within the same conflict scenario. Lastly, it needs to be stated that despite some differences, Ukrainian refugees share common experiences with other refugees who have fled due to war. These include traumatic war experiences and family separation, which are likely to affect their behavior [18].

5.1.4 Impact of war on ICT infrastructure, and connectivity. Within HCI/CSCW literature, the impacts of armed conflicts on ICT infrastructure from a civil user perspective are rarely considered explicitly. Rohde et al. [79] considered this for the civil war in Syria and found a fragmentation of infrastructure. With connectivity being quickly reestablished in regions that were under Ukrainian control even after attacks, fragmentation and unreliability were also reported from the front line regions. Additionally, our study shows how the Russian takeover of communication infrastructure (which included censorship and surveillance) sparked extensive privacy protection behaviors. In regions bordering Ukrainian territory, there were unreliable attempts to connect to Ukrainian mobile phone towers, while other parts remained completely cut off. Our findings reflect the results of Jain et al. [48], who found connectivity is inversely related to the presence of Russian troops in Ukraine. In addition, frequent power cuts affected the use of ICTs, underscoring the necessity for asynchronous communication. Despite all this, we conclude that access and connectivity were remarkably high due to the successful efforts of the Ukrainian government. Other issues known from other cases, such as limited connectivity due to the difficulty of purchasing SIM cards for several countries [26, 58, 89] or a lack of financial resources[98], was not applicable as roaming was cheap and SIM cards were sometimes handed out at borders. This is in stark contrast to cases as reported by Gillespie et al. [37], in which an interviewee reported having had 13 SIM cards to get to Europe. This is often even more difficult (and illegal) as in most countries, legal documents and sometimes even biometric information[46] are required to register a number [37].

5.1.5 Relevance of privacy. Past research has often highlighted privacy protection as an important requirement for ICT use [26, 40, 58, 89]. As this is sometimes not possible or risky, it can lead to smartphone use being abandoned [73, 89], deletion of data, and general avoidance of the system [57].

In previous research, this seemed to be strongly associated with the risk scenario: surveillance by government [73, 98], a vulnerability to data leaks, e.g., by NGOs, in the cases of political persecution [58, 83], the avoidance of authorities due to irregular immigration or illegal border crossings [37], or the passing of physical inspection by terror groups or other criminal organizations [89]. In the context of our study, we see a marked difference between people from the unoccupied parts of Ukraine and people fleeing the occupied zone. In the former, privacy concerns only manifested themselves in relation to Russian services (i.e., the social network VK) or in the form of information silence. While this information silence was sometimes reported to be held up in social media groups and private phone conversations, this points to a heightened but to the threat scenario adjusted privacy awareness. Within the occupied zone, in which Russian checkpoints had to be passed to escape, and in which Russia took over the communication infrastructure, participants reported a very pronounced privacy behavior, which is congruent with reports from people fleeing (semi-)authoritarian regimes, as found in past research (e.g., the use of VPNs [49, 89], second SIM cards and phones [89], hiding the smartphone for physical checks[83, 89]).

5.1.6 Differences of the journey. With populations arriving in central European countries in other cases from literature originating mostly from the MENA region or other African countries [81], they had either to cross the Mediterranean Sea or to move via Turkey and the Balkan countries [37, 58]. As this often involves crossing borders illegally and traveling through several countries, authorities are avoided to avert arrest. It is often necessary to contact people-smugglers, so the planning is clandestine [6, 26, 37, 58, 89]. Dekker et al. [26] mention the uncertainty of destination countries, as it is often difficult for asylum seekers to assess whether they will be granted a residence permit. The flight route would often be sensitive to the Dublin Regulation, contributing to further privacy protection strategies [17, 37], which is not applicable for Ukrainians.

For most Ukrainians, the journey to Germany was much easier (and legal) once the occupied zone or areas under attack were left. Then, public transportation or private cars could be used to pass an EU border, which involved a simple border control that was primarily described as unproblematic. Before, for those who fled the occupation, the journey was highly critical and dangerous due to unsafe humanitarian corridors or landmines on roads. Numerous Russian military checkpoints with physical checks in search of valuable information or militia associations had to be passed. This mirrors reports from refugees fleeing the Syrian civil war with terrorist or military checkpoints with cellphone checks having to be passed [79, 83, 89, 102]. Due to the legality of border passage and certainty about the legal protection status, the planning of the journey could be organized publicly in open groups on social media or messengers, including pickups at the border by volunteer helpers. In summary, while the journey was not necessarily safe, depending heavily on whether the region was already under attack or occupied, the threat scenario for Ukrainian refugees was somewhat different, allowing for much more public planning of the journey and greater online collaboration.

5.1.7 Reception by German civil society. . In comparison to other large refugee movements, such as the 2015/2016 influx of mainly Syrians and Iraqis, the reception of Ukrainians by German civil society has generally been more positive. Reception in 2015 has been mixed, with some media outlets reporting very positively (making 'refugees welcome' the 'anglicism of the year' [99]) and many civil society volunteers helping out. However, there already were racist sentiments, especially in certain regions of Germany, like the Islamophobic PEGIDA (acronym for "Patriotic Europeans against the Islamization of the West", a right-wing extremist organization) demonstrations [15]. Social attitudes also deteriorated over time. As a result, it can be said that overall, there seems to have been less resentment within the population towards Eastern European women than, for example, towards Arab men. One participant even reported that a member of her German host

family made an explicit comment to this effect. The provision of ICT access also differed, as several German mobile providers provided free SIM cards to each Ukrainian with valid documents, which was less of a problem due to Diia and certainty about the refugee status.

In addition, the activation of the Temporary Protection Directive by the EU has allowed the German government to provide a less bureaucratic registration process, allowing Ukrainians to find accommodation outside of designated housing facilities, access language courses, and provide a work allowance. Some interviewees also reported that they were able to enter the country on a tourist visa, which would probably not be possible in many other cases. In our view, all of this provided more security in terms of residency status than other refugee cases in the literature, making the tasks of integration and orientation in the new society more comparable to those of other regular transnational migrants. This may also have influenced the focus of the self-help groups on tasks such as finding work and housing. The importance of jobs in building social capital was highlighted by Almohamed et al. [10], indicating advantages for Ukrainians to integrate.

5.2 Identified Affordances within the Different Stages of Flight

Based on our results, we identified eight high-level socio-technical affordances [96] of ICT, which are already partly known from the literature on ICT use during wartime, flight, and migration. Often, these reflected the contextual differences identified within the previous subsection, leading to different aspects being important compared to other contexts known from research. The identified affordances are depicted in Table 1 together with different sub-aspects and explanations relevant to the case of our study. The importance of the affordance varied depending on the phase of the flight, with occasional shifts in content, such as which type of information was predominantly gathered. Additionally, we provide the findings of past research (second column of Table 1) to draw parallels and find differences that differentiate our results from past research. We will present the affordances in the following subsections.

5.2.1 Privacy protection. The predominant absence of privacy concerns outside the occupation also had implications for the organization of flight: In contrast to the clandestine planning of escape reported in other cases, the planning of escape from unoccupied parts of Ukraine could take place openly in public groups, in which a large group size could be leveraged to find help. This was much more difficult for participants fleeing from the occupation, as humanitarian corridors were not safe and information was only available in numerous closed local groups (to avoid infiltration) or face-to-face. This underscores the significance of understanding the local context and conducting thorough threat modeling, which involves assessing the capabilities of potential attackers to comprehend the ICT usage behavior of refugees.

5.2.2 Gathering information. Information gathering was one of the most crucial aspects. In contrast to the findings of previous studies, our research indicates that Telegram is the most frequently used network for information and communication functions, rather than Facebook (groups) and WhatsApp [89]. This is most likely due to the high adoption rate already before the invasion and might reflect cultural preferences. Many interviewees reported using different apps to get information and highlighted the importance of timely and locally relevant information, e.g., about bombings. Local chat groups and channels on Telegram proved to be a convenient and pragmatic tool for this in each phase of the flight. As described by Alencar [8], the information-gathering process serves to deal with uncertainty. However, instead of a lack of information, some of our interviewees mentioned an overload of information, making it hard to process or to judge which was true. This leads to new uncertainty, and in a way to "information precarity" [98] by information overload. This relates to the problem of misinformation in refugee groups, already brought up by

Borkert et al. [17]. Collective and individual processes were used to debunk false information and find trustworthy sources.

Table 1. Relevant affordances identified in comparison to other cases from HCI/CSCW literature

Affordances	Findings	Other Cases from Literature	Comparative Reflections
1. *Privacy protection*	• VPN use in occupied zone • Second SIM card/phones • Hiding of data storages/phones, deletion of data to pass checkpoints • Transferring personal data to cloud • Selective communication, face-to-face if necessary • "Information silence" • Use of code-language	• Use of VPNs to hide online behavior [89] • Second SIM cards/phones [89, 98] • Renouncement of phone use • Deletion of contacts/data to pass checkpoints • Selective communication [89, 98] • Use of code language [89]	• Privacy behavior comparable in occupied zone comparable to privacy measures of refugees trying to avoid authorities [37] or oppressive regimes [98] • Circumvention of censorship • Hetergenous privacy behavior due to different threat scenarios
2. *Gathering information*	• Information via personal networks or public or closed Telegram self-help groups (different scales and regionality) • Reliance on established platforms (Telegram, Viber, Instagram) • Identifying Russian actors and misinformation channels	• Information via personal connections [98], migrant networks, facebook groups • Reliance of established platforms (WhatsApp, Facebook) [89] • Misinformation due to lack of correct official sources [80]	• Higher relevance of deliberate disinformation / information warfare • Misinformation is a general problem [80, 98, 102] • Verification of information via personal networks [6, 98] or additionally in Ukraine via large scale groups (can happen in the open)
3. *Providing information*	• Specific apps, Telegram bots or Signal are used to provide information on war to authorities	• No reports of information provision to government • Only online exchange in groups [58]	• Population siding with government, fast app development, high digitalization • People-to-government information stream
4. *Personal communication*	• Often intertwined with information gathering/ verification • Personal support • Contact to friends/family abroad to organize flight in advance	• Emotional comfort often highlighted, verification of information [98] • Contact with people smugglers [37, 89]	• Despite difference in contact to people smugglers, very similar findings • Instead contact to other helpers abroad to organize logistics of flight
5. *Navigation*	• Important in dynamic situations (i.e., street signs demounted, attacks on bridges) • Partly offline maps for countries on the way • Otherwise "normal" use • Orientation in new country	• Highly relevant for orientation and flexible route planning, use of GPS • Orientation in new country [3, 4]	• Facilitation of movement, as mentioned before by many other studies [9, 26, 89] • Less relevance in many cases, access to public transportation • Related to threat scenario
6. *Awareness raising*	• Posting photos/videos of what is happening, documentation of war crimes to people outside of Ukraine • People posting TikToks for morale • Fund raising for help and to support the army	• Awareness raising (i.e., in Syria for people outside) and documentation of war crimes [79, 102]	• Different threat model because people are not afraid of documenting crimes because own government is not the aggressor • Fund raising for army is specific for Ukraine

Continued on the subsequent page

Affordances	Findings	Other Cases from Literature	Comparative Reflections
7. *Handling the language barrier*	• Use of translation apps (e.g., DeepL, Google Translate) • Reports of "advanced" functions like Google Lens or speech-to-text for translation • Language learning via app (Duo Lingo) from home due to kids	• Use of translation apps in Germany [5] and other European countries, the US, Canada or other contexts (i.e., [70])	• Translation apps often relevant in Europe (language variety) • Advancements for translating documents or conversations via STT, but often inaccurate for Ukrainian • Some languages privileged for linguistic capital [70]
8. *Bridge to old life / time capsule*	• (Video) calls, messenger apps and social media to stay connected • Digital class room for school children/university • VPN to access remote networks/data	• Video calls and messenger apps to keep transnational contact with relatives and friends [12, 101]	• Strong bridge, possibly based on assumption that war is temporary and men staying • Measures like schooling online facilitated due to implementations during COVID-19 pandemic

5.2.3 Personal communication. Given the dynamic wartime scenario, this significantly influenced user behavior, often intertwining with information gathering as peers became key sources. Additionally, checking on friends and family and seeking comfort were vital aspects heavily dependent on ICT, as highlighted in various studies [7, 52, 86]. While the infrastructure was mostly good, some connectivity issues (especially in the occupied zone or during attacks) aligned with findings from previous studies like [79]. This affected communication, leading to more asynchronous communication due to outages.

5.2.4 Providing information. While in other conflicts with an internal threat by a state actor the main information stream often only happened between citizens (e.g., during the thawra/Arab Spring), in Ukraine we found that citizens were involved in providing information to the Ukrainian military and the government using ICT, establishing an additional citizens-to-government information stream. This was enabled by the use of governmental apps (e.g., Diia) or even within messenger apps. Additionally, chat groups established a citizen-to-citizen information stream, and official channels or information, e.g., in the Diia app, established a government-to-citizen information channel. For the government, this has the advantage to have eyes and ears everywhere, and to get information even from areas that were remote, difficult to monitor or occupied, as described by our interview partners.

5.2.5 Navigation. While other research often highlighted the use of GPS for navigation, using offline and online maps, the interviewees especially highlighted the route checking and planning based on information that could be sourced from chat groups. This relates to smartphone use for the facilitation of movement, as mentioned before by many other studies [9, 26, 89]. The aspect of GPS orientation seemed to be more relevant escaping the approaching Russian troops or the occupied zone. As the flight itself was not criminalized and borders could be passed regularly, no border police had to be avoided as in other cases[40, 42], and public transportation networks could be used. Those driving with a personal car could rely on highway signs (at least further away from the front line and the occupied zone) or built-in GPS navigation. Consequently, it appeared to us that navigation functions of the phone were important (all interviewees reported using it), for many it was not as crucial as reported within the literature.

5.2.6 Awareness raising. While few interviewees engaged in awareness raising themselves, some also mentioned friends to be actively engaging in it. Many highlighted social media's importance in documenting war crimes to increase international political pressure. This is in line with findings

by Wulf et al. [102]. We also identified the sub-aspect of calls for donations online, which some interviewees responded to, aiming for fundraising actions or the collection of relief supplies. Last but not least, social media was not only used to protest online, but also to organize protests offline in and outside of Ukraine.

5.2.7 Handling the language barrier. Just as in other studies [5, 23], translation software or online dictionaries were highly relevant, especially for the arrival in the new host country when confronted with forms and paperwork. While not being directly part of the interviews, the translator lamented that the translation apps were often inaccurate for Ukrainian, leading him to be incessantly called on by municipal institutions.

5.2.8 Bridge to old life / Time capsule. This function, as outlined by Khvorostianov [52], pertains to preserving a sense of continuity from one's previous life. In our case, this includes identity management, like having the personal administrative documents in Diia and preserving personal documents and images. The digital continuation of the old life also included other aspects, as online schooling, being in touch with the family and maintaining business connections, with transnational calling via VoIP functions of messengers, digital classrooms, and Zoom providing functions to actualize this affordance. In general, user behaviors within Germany resembled strongly individual and collective behaviors already found by other research for regular migrants, e.g., transnational communication via VoIP calls and social networks, liaising in local (self-) help groups of other refugees [9], the use of translation apps [5], and more reliance on navigation apps.

5.3 Reflections and Implications for CSCW

The results of our study have several connections to current CSCW issues, which we discuss in this subsection. Certain features of the Ukrainian case that make it particularly interesting for CSCW research, most notably the high level of collaboration and bottom-up community formation that could take place freely due to fewer privacy concerns. As many of the identified affordances are based on user collaboration or at least interaction, they can be analyzed by using typical frameworks of CSCW, i.e., Johansen's time-space matrix for a rough analysis [51], or extended to the Model of Coordinated Action (MoCA) [60]. These help to describe the collaborative situations on a spectrum of synchronicity (asynchronous vs. synchronous), physical distribution (same location vs. different location), and for the MoCA also on the dimensions of scale (number of participants), the number of community practices, the nascence of these (routine vs. developing), planned permanence (short-term vs. long-term) and turnover (low vs. high, in terms of actors). Even if certain functions reported by our participants (e.g., navigating with a mapping app) were not based on collaboration between users, the use was often enriched by additional information from local or large-scale groups in which users could contribute information (e.g., which gas stations ran out of gas). This shows that the affordances we have identified are often complex and multifaceted and should not be reduced to single functionalities of a device. Further, the example also shows the importance of considering the continuum of synchronicity, as the communication in a dynamic scenario has to be asynchronous, as people providing information will not necessarily be able to interact in a synchronous way (possibly due to infrastructural outages or bad reception), but at the same time, information cannot be too old as it might be outdated quickly (e.g., a gas station could be refilled). Hence, interactions often had to be asynchronous but timely.

With regard to physical distribution, it should be noted that a lot of the usefulness of ICT-based collaborations within migration and war contexts is based on the physical distribution of interaction partners. This applies to information gathering within groups, for which we have seen in the results that different levels of local granularity can be desirable, but also to informing authorities (having volunteer vigilantes everywhere), raising awareness (showing the outside world what is going on),

maintaining a bridge (living in a new country while maintaining social and sometimes professional ties to Ukraine). Other dimensions from the MoCA varied a lot for different affordances, or even within. Just as information gathering happened in groups of localities, there were also different group sizes. While large, public groups could be used to find information and help easily, they were also more prone to infiltration and had to be administered very actively. This also led to different community practices appearing (e.g., kicking out members on the basis of suspicious postings), serving as a real-life case for (self-)moderating communities in CSCW [84]. While debunking of misinformation in groups as a crowd effort was reported by our interview partners, they also reported using small groups of personally known peers or a number of direct contacts to assess credibility and verify information. Again, this shows that aspects like the verification of information happened on several layers. Not being part of the MoCA, the additional dimension of familiarity of interaction partners seemed to be a highly relevant aspect, since groups could be infiltrated by bad or unreliable actors.

In the context of information gathering in groups, other dimensions of the MoCA are much more difficult to describe, as an analysis of the information groups were not the primary objective of this study. However, the change of group activity depending on the location (in Ukraine vs. in Germany) points to a high turnover and a low planned permanence. More CSCW research could be conducted within this context in the future and provide valuable insights into these crowd processes. The re-purposing of existing and the formation of new (self-) help and news groups could also be relevant case study for the CSCW research on community formation [43].

5.4 Limitations

In our study, some research design decisions and challenges led to some limitations. While the sample size aligns with exploratory research conventions, it is insufficient for any generalizations. Instead, our goal is to explore user behaviors in detail within the specific context. Additional concerns arise regarding representativeness: Despite our interviewees coming from different regions and covering a wide age range, most of them identified as female. As previously mentioned, this mirrors the predominantly female refugee population from Ukraine in Germany. Moreover, our focus on refugees arriving in Germany calls for comparisons with results from other host countries. Policies and conditions of the respective host country may influence the challenges identified during the arrival process. Another challenge in our study revolved around the language barrier, as the authors speak neither Ukrainian nor Russian. Initially, we looked for interviewees who speak English or German, aiming for a more natural conversational atmosphere without needing a translator, but this approach entailed difficulties as many refugees felt insufficiently proficient in these languages to engage in an interview. This led us to opt for the help of a translator. While we later cross-checked the Russian statements for any overlooked nuances, the use of a translator might have influenced the conversations. Also, we acknowledge a potential bias, given that about half of the interviewees were English-speaking, thus possibly excluding valuable perspectives.

Additionally, it's essential to recognize that our results are time-bound, capturing the initial stages of the 2022 conflict. As the war has persisted, with refugees returning to safer regions, our findings may not reflect the current situation. The disorder and "information precarity" [98] observed during the early attacks may have influenced results, affecting aspects like the threat model for privacy measures. When this paper was written, many men were involuntarily being drafted for the military even on the street [97], pointing to a potential incentive to be more secretive toward the government.

As Sabie et al. [81, 18] outline, failing to grasp the cultural nuances of a community—such as hierarchies, local norms, and privacy practices—is a common issue highlighted by many scholars in this sensitive area of research. We acknowledge that this challenge is also present in our own

work due to the homogeneous background of all authors. In response, we took proactive measures by engaging in conversations with Ukrainians and volunteers both before and during the study to deepen our understanding of the challenges and subtleties experienced by Ukrainian refugees and to ensure the ethical conduct of our research. Recognizing the significance of minimizing power imbalances and steering clear of data extractivism, we strongly recommend collaborative teamwork with individuals from Ukraine in the future.

6 Conclusion

This study contributes to existing HCI and CSCW research on how refugees use ICT before, during, and after their flight by examining the ICT use of 17 Ukrainian refugees who fled to Germany in response of the Russian invasion in 2022. We conducted semi-structured interviews, surveying the user behavior in different phases of the flight, as well as, relevant contextual factors, like the impairment of communication infrastructures. Overall, technology has played a crucial role in supporting refugees' resilience, autonomy, and resettlement. Due to Ukraine's advanced digitalization, many Ukrainians used digital technologies in many aspects of life prior to the invasion. This has facilitated the transition to using technology for gathering war-, flight-, and resettlement-related information (e.g., in Ukraine for air alerts, in Germany for application processes), planning the flight, and maintaining communication. While we identified eight socio-technical affordances of ICT, a comparison of our findings with existing literature revealed significant disparities in contextual factors between the country of origin and the flight, underscoring the importance of context-specific analyses for a comprehensive understanding of ICT use. Discussing these factors, we highlight how our results are contrasting numerous studies focusing on less digitalized countries. Digital tools like the Diia app, which was actively promoted by the Ukrainian government and centralizes important documents and services, help(ed) Ukrainian refugees to coordinate their flight, and support, amongst others, initiatives back home through donation options via the app. This level of government involvement and the provision of official, reliable digital resources is so far less common in other flight and migration settings. Unlike studies in regions such as MENA, interviewees often expressed little concern about privacy, due to the possibility of legal migration and Ukraine's distinctive situation of being under attack by Russia, which lessened apprehensions about any government measures. With regard to the use of ICT after flight, translation and language learning apps, along with self-help and volunteer groups on Telegram, have further supported their arrival by providing quick answers and connecting them with people in Germany. As Germany has initiated rapid and large-scale integration efforts for Ukrainian refugees, including providing access to free SIM cards, calling to Ukraine and train tickets, the political and social context in Europe, including Germany, has generally been more supportive of Ukrainian refugees. This potentially facilitated the resettlement compared to other cases and affected user behaviors. Of the eight identified affordances, information gathering and communication stand out in particular and we discuss different dimensions of user collaboration within the context of our study in light of the Model of Coordinated Action [60].

While the exploratory findings exclusively capture a limited segment of reality, making it inappropriate to generalize these results, the study offers an in-depth understanding of diverse individual experiences in the initial months following the Russian invasion. Considering the intricate situations individuals face when fleeing, this empirical study underscores the importance of recognizing ICT in conflict-affected contexts as a component of a nuanced and complex environment. This perspective aims to consider cultural aspects, social structures, and the extent of digitalization, among other factors, which we consider crucial since each scenario is unique, and no universal technical solution applies to all cases when deriving design implications. Overall, our results can contribute by providing contextual insights for technology development and serve as a base for

future CSCW research, by providing empirical results connected to the topics of ICT use and privacy in migration and war contexts, as well as online group formation and self-moderating communities for information gathering. Moreover, the results could help policymakers or NGOs to find suitable ways to provide assistance and information. Generally, future research endeavors should focus on conducting and comparing empirical studies on refugees' ICT use to gain insights into the contextual technological requirements of people who (have to) flee.

Acknowledgments

First, we would like to thank all the interviewees who shared their experiences with us. We would also like to thank the organizations, translators, and volunteers who helped throughout our study with their (context) specific advice and support and who played a crucial role in shaping the outcome of our study, particularly Artem Kolesnikov. Further, we would like to thank Dr. Kateryna Zarembo and Olga Sanina for translating and proofreading our translated documents and giving feedback. Finally, we would like to thank the anonymous reviewers for their reviewers for their insightful suggestions, which greatly enhanced this this work. This work has been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) (251805230/GRK2050), the German Federal Ministry of Education and Research (BMBF) within the framework of TraCe, the Regional Research Centre on Transformations of Political Violence (01UG2203E), and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

References

[1] Konstantin Aal, Anne Weibert, Reem Talhouk, Vasilis Vlachokyriakos, Karen Fisher, and Volker Wulf. 2018. Refugees & Technology: Determining the Role of HCI Research. In *Proceedings of the 2018 ACM International Conference on Supporting Group Work (GROUP '18)*. Association for Computing Machinery, New York, NY, USA, 362—-364. doi:10.1145/3148330.3152160

[2] Ruba Abu-Salma, Reem Talhouk, Jose Such, Claudia Aradau, Francesca Meloni, Shijing He, Syed Ishtiaque Ahmed, Cansu Ekmekcioglu, Dina Sabie, Rikke Bjerg Jensen, Jessica McClearn, Anne Weibert, Max Krüger, Faheem Hussain, and Rehema Baguma. 2023. Diverse Migration Journeys and Security Practices: Engaging with Longitudinal Perspectives of Migration and (Digital) Security. 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 345, 7 pages. doi:10.1145/3544549.3573800

[3] Safa'a AbuJarour. 2019. Smartphone app adoption at home and on the move: The case of Syrians. In *Conference paper at the 3rd AFU International Conference: Towards Advanced Scientific Knowledge (TASK2019) in Business Sciences*. Dubai, UAE, 1–10. https://www.researchgate.net/publication/332835399_Smartphone_App_Adoption_at_Home_and_on_the_Move_The_Case_of_Syrians

[4] Safa'a AbuJarour, Haya Ajjan, Jane Fedorowicz, and Antonia Köster. 2021. ICT Support for Refugees and Undocumented Immigrants. *Communications of the Association for Information Systems* 48, 1 (2021), 40. doi:10.17705/1CAIS.04840

[5] Safa'a AbuJarour, Cora Bergert, Jana Gundlach, Antonia Köster, and Hanna Krasnova. 2019. Your home screen is worth a thousand words": Investigating the prevalence of smartphone apps among refugees in Germany. In *25th Americas Conference on Information Systems, AMCIS 2019, Cancún, Mexico, August 15-17, 2019*. Association for Information Systems, Atlanta, GA, USA, 1–10. https://aisel.aisnet.org/amcis2019/social_inclusion/social_inclusion/3

[6] Safa'a AbuJarour, Lama Jaghjougha, and Mohammed AbuJarour. 2021. The Impact of Digitizing Social Networks on Refugee Decision Making – The Journey to Germany. In *Innovation Through Information Systems: Volume I: A Collection of Latest Research on Domain Issues*. Springer, Springer International Publishing, Cham, 331–345. doi:10.1007/978-3-030-86790-4_23

[7] Safa'a Abujarour, Antonia Köster, Hanna Krasnova, and Manuel Wiesche. 2021. Technology as a Source of Power: Exploring How ICT Use Contributes to the Social Inclusion of Refugees in Germany. *Proceedings of the 54th Hawaii International Conference on System Sciences* (2021), 2637–2646. doi:10.24251/HICSS.2021.322

[8] Amanda Alencar. 2020. Mobile communication and refugees: An analytical review of academic literature. *Sociology Compass* 14, 8 (2020), 1–13. doi:10.1111/soc4.12802

[9] Amanda Alencar, Katerina Kondova, and Wannes Ribbens. 2019. The smartphone as a lifeline: An exploration of refugees' use of mobile communication technologies during their flight. *Media, Culture & Society* 41 (2019), 828–844. Issue 6. doi:10.1177/016344371881348

[10] Asam Almohamed, Arindam Dey, Jinglan Zhang, and Dhaval Vyas. 2019. Extended reality for refugees: Pragmatic ideas through ethnographic research with refugees in Australia. In *2019 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*. IEEE, 422–425. doi:10.1109/ISMAR-Adjunct.2019.00046

[11] Asam Almohamed and Dhaval Vyas. 2016. Designing for the Marginalized: A Step Towards Understanding the Lives of Refugees and Asylum Seekers. In *Proceedings of the 2016 ACM Conference Companion Publication on Designing Interactive Systems* (Brisbane, QLD, Australia) *(DIS '16 Companion)*. Association for Computing Machinery, New York, NY, USA, 165–168. doi:10.1145/2908805.2909415

[12] Isabel Pavez Andonaegui, Cecilia Claro, and Julián Andrés Burgos Suárez. 2020. El uso de redes sociales en migrantes Colombianos en Chile. *Signo y Pensamiento* 39, 76 (2020), 1–16. doi:10.11144/Javeriana.syp39-76.ursm

[13] Armed Conflict Location & Event Data Project (ACLED). 2023. Ukraine Conflict Monitor. https://acleddata.com/ukraine-conflict-monitor/ [Accessed Jan 13th, 2023].

[14] Jennifer Baranoff, R. Israel Gonzales, Jay Liu, Heidi Yang, and Jimin Zheng. 2015. Lantern: Empowering Refugees Through Community-Generated Guidance Using Near Field Communication. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15)*. Association for Computing Machinery, New York, NY, USA, 7–12. doi:10.1145/2702613.2726950

[15] BBC. 2015. Germany Pegida protests: Rallies over 'Islamisation'. *BBC News* (Jan. 2015). https://www.bbc.com/news/world-europe-30685842 [Accessed on 15th Jul 2024].

[16] Maarten P Bolhuis and Joris Van Wijk. 2021. Seeking asylum in the digital era: social-media and mobile-device vetting in asylum procedures in five European countries. *Journal of refugee studies* 34, 2 (2021), 1595–1617.

[17] Maren Borkert, Karen E Fisher, and Eiad Yafi. 2018. The best, the worst, and the hardest to find: How people, mobiles, and social media connect migrants in (to) Europe. *Social Media + Society* 4, 1 (2018), 1–11. doi:10.1177/2056305118764428

[18] Herbert Brücker, Andreas Ette, Markus M Grabka, Yuliya Kosyakova, Wenke Niehues, Nina Rother, C Katharina Spieß, Sabine Zinn, Martin Bujard, Adriana R Cardozo Silva, et al. 2023. Ukrainian Refugees in Germany: Evidence From a Large Representative Survey. *Comparative Population Studies* 48 (2023).

[19] Matt Burgess. 2022. The last cell tower in Mariupol. *Wired* (Mar 2022). https://www.wired.com/story/mariupol-ukraine-war/ [Accessed Jan 13th, 2023].

[20] Houssein Charmarkeh. 2012. Social media usage, tahriib (migration), and settlement among Somali refugees in France. *Refuge* 29 (2012), 43.

[21] Kyle Chayka. 2022. Ukraine Becomes the World's "First TikTok War". *The New Yorker* (March 2022). https://www.newyorker.com/culture/infinite-scroll/watching-the-worlds-first-tiktok-war [Accessed 15th Jul 2024].

[22] Christina Clark-Kazak. 2017. Ethical considerations: Research with people in situations of forced migration. *Refuge* 33, 2 (2017), 3–17. doi:10.7202/1043059ar

[23] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Reem Talhouk. 2018. In a New Land: Mobile Phones, Amplified Pressures and Reduced Capabilities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montréal, Québec, Canada,) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3173574.3174158

[24] European Commission. [n. d.]. Temporary protection. https://home-affairs.ec.europa.eu/policies/migration-and-asylum/common-european-asylum-system/temporary-protection_en [Accessed on 15th Jul 24].

[25] Sabine Damir-Geilsdorf and Martina Sabra. 2018. *Disrupted Families: The Gendered Impacts of Family Reunification Policies on Syrian Refugees in Germany.* United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), New York, NY, USA. 1–40 pages.

[26] Rianne Dekker, Godfried Engbersen, Jeanine Klaver, and Hanna Vonk. 2018. Smart refugees: How Syrian asylum migrants use social media information in migration decision-making. *Social Media + Society* 4, 1 (2018), 1–11. doi:10.1177/2056305118764439

[27] Maciej Duszczyk and Paweł Kaczmarczyk. 2022. Poland and war refugees from Ukraine–Beyond pure aid. In *CESifo Forum*, Vol. 23. ifo Institut - Leibniz-Institut für Wirtschaftsforschung an der Universität München, Munich, 36–40. http://hdl.handle.net/10419/263863

[28] Martin Emmer, Marlene Kunst, and Carola Richter. 2020. Information seeking and communication during forced migration: An empirical analysis of refugees' digital media use and its effects on their perceptions of Germany as their target country. *Global Media and Communication* 16, 2 (2020), 167–186. doi:10.1177/1742766520921905

[29] Federal Institute for Population Research. 2023. How do refugees from Ukraine live in Germany? https://www.bib.bund.de/EN/News/2023/2023-02-16-New-Study-How-do-refugees-from-Ukraine-live-in-Germany.html [Accessed Jan 13th, 2023].

[30] Karen E Fisher. 2022. People first, data second: A humanitarian research framework for fieldwork with refugees by war zones. *Computer Supported Cooperative Work (CSCW)* 31, 2 (2022), 237–297. doi:10.1007/s10606-022-09425-8

[31] European Union Agency for Fundamental Rights. 2023. *Fleeing Ukraine: Displaced people's experiences in the EU. Ukrainian Survey 2022.* Publications Office of the European Union, Luxembourg, Luxembourg. doi:10.2811/39974

[32] Department for Media Affairs and Information. 2022. Russian Armed Forces will continue special operation in Ukraine until the set goals are achieved. https://eng.mil.ru/en/special_operation/news/more.htm?id=12411177 [Accessed Jan 13th, 2023].

[33] Bram Frouws, Melissa Phillips, Ashraf Hassan, and Mirjam Twigt. 2016. Getting to Europe the WhatsApp way: The use of ICT in contemporary mixed migration flows to Europe. *Regional mixed migration secretariat briefing paper* (2016), 1–16. https://mixedmigration.org/wp-content/uploads/2018/05/015_getting-to-europe.pdf [Accessed Jan 13th, 2023].

[34] Jim Garamone. 2023. Biden: 'Ukraine will never be a victory for Russia. never'. *U.S. Department of Defense (DOD News)* (Feb 2023). https://www.defense.gov/News/News-Stories/Article/Article/3304356/biden-ukraine-will-never-be-a-victory-for-russia-never/ [Accessed Jan 13th, 2023].

[35] Maria Garbielsen Jumbert, Rocco Bellanova, and Raphaël Gellert. 2018. *Smart Phones for Refugees. Tools for Survival, or Surveillance?* Peace Research Institute Oslo (PRIO), Oslo, Norway.

[36] Sara L. Gill. 2020. Qualitative Sampling Methods. *Journal of Human Lactation* 36, 4 (2020), 579–581. doi:10.1177/0890334420949218

[37] Marie Gillespie, Souad Osseiran, and Margie Cheesman. 2018. Syrian refugees and the digital passage to Europe: Smartphone infrastructures and affordances. *Social media+ society* 4, 1 (2018), 1–12. doi:10.1177/2056305118764440

[38] gov.ua - State sites of Ukraine. 2023. Digital transformation. https://www.kmu.gov.ua/en/yevropejska-integraciya/coordination/cifrova-transformaciya [Accessed Jan 13th, 2023].

[39] Harriet Gray and Anja K Franck. 2019. Refugees as/at risk: The gendered and racialized underpinnings of securitization in British media narratives. *Security Dialogue* 50, 3 (2019), 275–291.

[40] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal, Québec, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–15. doi:10.1145/3173574.3173688

[41] Simon B Haack. 2023. *What are the underlying reasons for the differing treatment of Ukrainian and Syrian refugees in Europe identifiable in the debates within the European Parliament?* Master's thesis. University of Twente.

[42] Nicholas Harney. 2013. Precarity, affect and problem solving with mobile phones by asylum seekers, refugees and migrants in Naples, Italy. *Journal of Refugee Studies* 26, 4 (2013), 541–557. doi:10.1093/jrs/fet017

[43] Alexa M. Harris, Diego Gómez-Zará, Leslie A. DeChurch, and Noshir S. Contractor. 2019. Joining Together Online: The Trajectory of CSCW Scholarship on Group Formation. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 148 (nov 2019), 27 pages. doi:10.1145/3359250

[44] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou, and M Angela Sasse. 2023. Digital Security—A Question of Perspective. A Large-Scale Telephone Survey with Four At-Risk User Groups. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, IEEE Computer Society, Washington, DC, USA, 27–27. doi:10.1109/SP54263.2024.00027

[45] Roman Horbyk. 2022. "The war phone": mobile communication on the frontline in Eastern Ukraine. *Digital War* 3, 1-3 (2022), 9–24. doi:10.1057/s42984-022-00049-2

[46] Faheem Hussain, Abdullah Hasan Safir, Dina Sabie, Zulkarin Jahangir, and Syed Ishtiaque Ahmed. 2020. Infrastructuring Hope: Solidarity, Leadership, Negotiation, and ICT among the Rohingya Refugees in Bangladesh. In *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development* (Guayaquil, Ecuador) *(ICTD '20)*. Association for Computing Machinery, New York, NY, USA, Article 12, 12 pages. doi:10.1145/3392561.3394640

[47] International Telecommunication Union. 2024. Statistics. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx [Accessed Jul 14th, 2024].

[48] Akshath Jain, Deepayan Patra, Peijing Xu, Justine Sherry, and Phillipa Gill. 2022. The ukrainian internet under attack: An NDT perspective. In *Proceedings of the 22nd ACM Internet Measurement Conference*. Association for Computing Machinery, New York, NY, USA, 166–178. doi:10.1145/3517745.3561449

[49] Jussi S Jauhiainen, Davood Eyvazlu, Johanna Junnila, and Ada Virnes. 2022. Digital divides, the Internet and social media uses among Afghans in Iran. *Technology in Society* 70 (2022), 1–10. doi:10.1016/j.techsoc.2022.102057

[50] Rikke Bjerg Jensen, Lizzie Coles-Kemp, and Reem Talhouk. 2020. When the Civic Turn Turns Digital: Designing Safe and Secure Refugee Resettlement. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. doi:10.1145/3313831.3376245

[51] Robert Johansen. 1988. *Groupware: Computer support for business teams.* The Free Press, New York, NY, USA.

[52] Natalia Khvorostianov. 2023. "Is everyone alive?": Smartphone use by Ukrainian refugee children. *New Media & Society* (2023), 1–17. doi:10.1177/14614448231173657

[53] Ida Kjeøy and Guri Tyldum. 2022. *Assessing future migration among Ukrainian refugees in Poland and Norway.* Fafo, Oslo, Norway. 1–4 pages. https://www.fafo.no/images/pub/2022/brief-assesing_future_migration.pdf

[54] Kilian Kleinschmidt. 2016. *Las TIC, claves para los refugiados.* Vol. 51. Estudios de Política Exterior S.A., Madrid, Spain. 58–60 pages. https://www.iemed.org/wp-content/uploads/2021/01/Las-TIC-claves-para-los-refugiados.pdf

[55] Judith Kohlenberger, Konrad Pędziwiatr, Bernhard Rengs, Bernhard Riederer, Ingrid Setz, Isabella Buber-Ennser, Jan Brzozowski, and Olena Nahorniuk. 2022. What the self-selection of Ukrainian refugees means for support in host countries. *London School of Economics European Politics and Policy (EUROPP) Blog* (2022). https://blogs.lse.ac.uk/europpblog/2022/09/07/what-the-self-selection-of-ukrainian-refugees-means-for-support-in-host-countries/

[56] Egon F. Kunz. 1973. The Refugee in Flight: Kinetic Models and forms of Displacement. *International Migration Review* 7, 2 (1973), 125–146. doi:10.1177/019791837300700201

[57] Mark Latonero, Keith Hiatt, Antonella Napolitano, Giulia Clericetti, and Melanie Penagos. 2019. Digital identity in the migration & refugee context. *Data & Society* 4 (2019). https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf

[58] Mark Latonero and Paula Kift. 2018. On digital passages and borders: Refugees and the new infrastructure for movement and control. *Social Media + Society* 4, 1 (2018), 1–11. doi:10.1177/205630511876443

[59] Mark Latonero, Danielle Poole, and Jos Berens. 2018. *Refugee connectivity: a survey of mobile phones, mental health, and privacy at a Syrian refugee camp in Greece.* Report. Harvard Humanitarian Initiative, Data & Society Research Institute. https://apo.org.au/node/139581 [Accessed Dec 18th, 2023].

[60] Charlotte P. Lee and Drew Paine. 2015. From The Matrix to a Model of Coordinated Action (MoCA): A Conceptual Framework of and for CSCW. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) *(CSCW '15).* Association for Computing Machinery, New York, NY, USA, 179–194. doi:10.1145/2675133.2675161

[61] Philipp Mayring. 2022. *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (13 ed.). Beltz, Weinheim/Basel.

[62] Katherine T McCaffrey and Maisa C Taha. 2019. Rethinking the digital divide: Smartphones as translanguaging tools among middle eastern refugees in New Jersey. *Annals of Anthropological Practice* 43, 2 (2019), 26–38. doi:10.1111/napa.12126

[63] Jenna McLaughlin. 2023. Ukrainian hacktivists fight back against Russia as cyber conflict deepens. *NPR* (Nov. 2023). https://www.npr.org/2023/11/21/1214170140/ukraine-hacktivists-cyber-russia-war [Accessed 15th Jul 2024].

[64] Cecilia Eleonora Melella. 2017. Prensa digital, espacio público y migraciones: Crónicas del chivo expiatorio. *INTERIN* 22, 1 (2017), 149–167. http://hdl.handle.net/11336/44021

[65] Maria Merisalo and Jussi S. Jauhiainen. 2020. Digital Divides among Asylum-Related Migrants: Comparing Internet Use and Smartphone Ownership. *Tijdschrift voor Economische en Sociale Geografie* 111, 5 (2020), 689–704. doi:10.1111/tesg.12397

[66] Maria Merisalo and Jussi S. Jauhiainen. 2021. Asylum-Related Migrants' Social-Media Use, Mobility Decisions, and Resilience. *Journal of Immigrant & Refugee Studies* 19, 2 (2021), 184–198. doi:10.1080/15562948.2020.1781991

[67] Tony Blomqvist Mickelsson. 2023. Safety, Shame, and Ambiguity — The Case of Ukrainian Male Refugees. *International Migration Review* (2023), 1–11. doi:10.1177/01979183231216075

[68] Claire Moran. 2023. The 'connected migrant': A scoping review. *Convergence* 29, 2 (2023), 288–307. doi:10.1177/13548565221090480

[69] Anatoly Motkin. 2020. Ukraine in a smartphone: Zelenskyy's Digital Dream. https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-in-a-smartphone-zelenskyys-digital-dream/

[70] Gina Netto, Lynne Baillie, Theodoros Georgiou, Lai Wan Teng, Noraida Endut, Katerina Strani, and Bernadette O'Rourke. 2022. Resilience, smartphone use and language among urban refugees in the Global south. *Journal of Ethnic and Migration Studies* 48, 3 (2022), 542–559. doi:10.1080/1369183X.2021.1941818

[71] Bryce Clayton Newell, Ricardo Gomez, and Verónica E. Guajardo. 2016. Information seeking, technology use, and vulnerability among migrants at the United States–Mexico border. *The Information Society* 32, 3 (2016), 176–191. doi:10.1080/01972243.2016.1153013

[72] UN News. 2022. Ukraine: Security Council urged to "put aside" divisions, end "senseless war". https://news.un.org/en/story/2022/04/1116512 [Accessed Jan 13th, 2023].

[73] Matthew E. Opas and David A. McMurray. 2015. Under the Gaze of the State: ICT Use and State Surveillance of Eritrean Refugees in Italy. *Refugee Survey Quarterly* 34, 4 (10 2015), 105–125. doi:10.1093/rsq/hdv013

[74] Saknicte Piste Beltran and Araceli Mendieta-Ramírez. 2022. Apropiación de la información y uso de las TIC en un campamento migrante. In *Política en red: acción social y agenda pública en la era digtal*, Rodrigo Vera Vázquez (Ed.). El Colegio de Tamaulipas, Tamaulipas, México, 241–273. doi:10.54511/IELCOL16

[75] Steffen Pötzschke, B Weiß, A Hebel, JP Piepenburg, and O Popek. 2022. Geflüchtete aus der Ukraine–Erste deskriptive Ergebnisse einer Onlinebefragung in Deutschland und Polen. *Gesis Blog* 6 (2022). doi:10.34879/gesisblog.2022.60

[76] Alec Radford, Jong Wook Kim, Tao Xu, Greg Brockman, Christine Mcleavey, and Ilya Sutskever. 2023. Robust Speech Recognition via Large-Scale Weak Supervision. In *Proceedings of the 40th International Conference on Machine Learning (Proceedings of Machine Learning Research, Vol. 202)*, Andreas Krause, Emma Brunskill, Kyunghyun Cho, Barbara Engelhardt, Sivan Sabato, and Jonathan Scarlett (Eds.). PMLR, 28492–28518. https://proceedings.mlr.press/v202/radford23a.html

[77] Clionadh Raleigh, Andrew Linke, Håvard Hegre, and Joakim Karlsen. 2010. Introducing ACLED-Armed Conflict Location and Event Data. *Journal of Peace Research* 47 (2010), 651–660. Issue 5. doi:10.1177/0022343310378914

[78] Claudia Vargas Ribas. 2018. La migración en Venezuela como dimensión de la crisis. *Pensamiento propio* 47 (2018), 91–128. http://www.cries.org/wp-content/uploads/2018/09/009-Vargas.pdf [Accessed Jan 13th, 2023].

[79] 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. doi:10.1080/10447318.2016.1177300

[80] Hilda Ruokolainen and Gunilla Widén. 2020. Conceptualising misinformation in the context of asylum seekers. *Information Processing & Management* 57, 3 (2020), 102127. doi:10.1016/j.ipm.2019.102127

[81] Dina Sabie, Cansu Ekmekcioglu, and Syed Ishtiaque Ahmed. 2022. A decade of international migration research in HCI: Overview, challenges, ethics, impact, and future directions. *ACM Transactions on Computer-Human Interaction (TOCHI)* 29, 4, Article 30 (mar 2022), 35 pages. doi:10.1145/349055

[82] 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. doi:10.1145/2556288.2557357

[83] Emrys Schoemaker, Dina Baslan, Bryan Pon, and Nicola Dell. 2021. Identity at the margins: data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. *Information Technology for Development* 27, 1 (2021), 13–36. doi:10.1080/02681102.2020.1785826

[84] Joseph Seering. 2020. Reconsidering Self-Moderation: the Role of Research in Supporting Community-Based Models for Online Content Moderation. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 107 (oct 2020), 28 pages. doi:10.1145/3415178

[85] Marina Sharpe. 2018. Mixed Up: International Law and the Meaning(s) of "Mixed Migration". *Refugee Survey Quarterly* 37, 1 (2018), 116–138. doi:10.1093/rsq/hdx021

[86] Irina Shklovski and Volker Wulf. 2018. The Use of Private Mobile Phones at War: Accounts From the Donbas Conflict. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3173574.3173960

[87] Statista. 2023. Smartphone user penetration rate in Ukraine from 2019 to 2028. https://www.statista.com/statistics/1134646/predicted-smartphone-user-penetration-rate-in-ukraine/ [Accessed Jan 13th, 2023].

[88] Statista Research Department. 2023. Estimated number of refugees from Ukraine recorded in Europe and Asia since February 2022 as of September 12, 2023, by selected country. https://www.statista.com/statistics/1312584/ukrainian-refugees-by-country/ [Accessed Jan 13th, 2023].

[89] Enno Steinbrink, Lilian Reichert, Michelle Mende, and Christian Reuter. 2021. Digital Privacy Perceptions of Asylum Seekers in Germany: An Empirical Study about Smartphone Usage during the Flight. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 382 (oct 2021), 24 pages. doi:10.1145/3479526

[90] Nicole Stremlau and Anna Tsalapatanis. 2022. Social media, mobile phones and migration in Africa: A review of the evidence. *Progress in Development Studies* 22, 1 (2022), 56–71. doi:10.1177/14649934211043615

[91] Reem Talhouk, Syed Ishtiaque Ahmed, Volker Wulf, Clara Crivellaro, Vasilis Vlachokyriakos, and Patrick Olivier. 2016. Refugees and HCI SIG: The Role of HCI in Responding to the Refugee Crisis. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 1073–1076. doi:10.1145/2851581.2886427

[92] The Council of the European Union. 2001. COUNCIL DIRECTIVE 2001/55/EC. L 212/12 (2001). http://data.europa.eu/eli/dir/2001/55/oj

[93] The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. 1978. *The Belmont Report. Ethical Principles and Guidelines for the Protection of Human Subjects of Research.* Department of Health, Education, and Welfare, Washington, D.C., USA.

[94] UNHCR. 2023. Ukraine refugee situation. https://data2.unhcr.org/en/situations/ukraine [Accessed Jan 13th, 2024].

[95] United Nations in Ukraine. 2022. "The war has caused the fastest and largest displacement of people in Europe since World War II". https://ukraine.un.org/en/175836-war-has-caused-fastest-and-largest-displacement-people-europe-world-war-ii [Accessed Jan 13th, 2023].

[96] Ravi K. Vatrapu. 2009. Towards a Theory of Socio-technical Interactions. In *Learning in the Synergy of Multiple Disciplines*, Ulrike Cress, Vania Dimitrova, and Marcus Specht (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 694–699. doi:10.1007/978-3-642-04636-0_70

[97] Shaun Walker and Jamie Wilson. 2023. Bribes and hiding at home: The Ukrainian men trying to avoid conscription. https://www.theguardian.com/world/2023/aug/15/bribes-and-hiding-at-home-the-ukrainian-men-trying-to-avoid-conscription [Accessed Jan 13th, 2023].

[98] Melissa Wall, Madeline Otis Campbell, and Dana Janbek. 2017. Syrian refugees and information precarity. *New Media & Society* 19, 2 (2017), 240–254. doi:10.1177/1461444815591967

[99] Deutsche Welle. 2016. 'Refugees Welcome' is Germany's Anglicism of the year. https://www.dw.com/en/refugees-welcome-is-germanys-anglicism-of-the-year/a-19004440 [Accessed on 15th Jul 2024].

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

[101] Shane Worrell. 2021. From Language Brokering to Digital Brokering: Refugee Settlement in a Smartphone Age. *Social Media + Society* 7, 2 (2021), 20563051211012365. doi:10.1177/20563051211012365

[102] Volker Wulf, Kaoru Misaki, Konstantin Aal, and Markus Rohde. 2017. Mobile Media Use in the Zone of Conflict Findings from Early Phases of the Syrian Civil War (2011–2013). *International Reports on Socio-Informatics (IRSI)* 14 (2017), 1–15. Issue 2.

[103] Ying Xu, Carleen Maitland, and Brian Tomaszewski. 2015. Promoting participatory community building in refugee camps with mapping technology. In *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development (ICTD '15)*. Association for Computing Machinery, New York, NY, USA, 1–4. doi:10.1145/2737856.2737883

[104] Kateryna Zarembo, Michèle Knodt, and Jannis Kachel. 2024. Smartphone resilience: ICT in Ukrainian civic response to the Russian full-scale invasion. *Media, War & Conflict* (2024), 1–20. doi:10.1177/17506352241236449

Received January 2024; revised July 2024; accepted October 2024

Appendix

A Semi-structured interview guideline

(1) Information on flight route
- When did you arrive in Germany? How did you get to Germany and which route did you take?
- Did you know anyone in Germany before you came here? Did you contact them?
- Do you own a smartphone, a simple mobile phone, a tablet or a computer? Which of these devices do you own?

(2) Relevant apps and general user behavior
- Did you always have access to your phone during your flight?
- How important was the internet / your smartphone when the Russian invasion started?
- Did you use the internet for collecting information on the situation in Ukraine when everything started?
- Which platforms and websites did you use to get information and to stay in contact with friends and family?

(3) Information and communication when the Russian invasion started
- Was your region already under attack when you left?
- Was the telephone, TV, and internet connection affected by the attacks? Was the internet connection stable?
- While escaping, did you always have internet? If not, why didn't you have internet?
- Did you have to use mobile internet or did you use WIFI hotspots?
- Were you dependent on using a smartphone from another person, for example, because your smartphone ran out of battery?
- Has your social media consumption changed because of the war?
- If you had to say, which functions of your phone or apps or websites for your computer were the most important for you after all of this started, what would it be?

(4) Planning of flight and connection with peers in target countries

(5) Use of social media and group chats / channels, trust and verification of information

(6) Privacy considerations and adaptations of user behavior
- Did you switch to another messenger app in the last few weeks? If so, why?
- Do you know what digital privacy means? [if not, provide explanation]
- Was digital privacy relevant for you when using your smartphone?
- Did you have concerns regarding which data you share?
- Did you take any measures to protect your data?

(7) Impairment of digital and electrical infrastructure and the impact on user behavior
- You decided to share/not to share information, how did you decide with whom you share information, how did you decide who you can trust?
- Was the information you found online reliable during that time?
- How did you get your information and how did you decide whether it is trustworthy?
- Did you try to verify information?
- After arriving in another country, how did you use your phone then?
- Do some applications help you to arrive in the new country?
- Could you use any specific websites or apps for refugees?
- How do you do that? What apps/functions do you use?

B Comparison of contextual factors

Table 2. Identified contextual factors in comparison to cases discussed within HCI/CSCW literature

Contextual factors	Findings	Other cases from literature	Comparative reflections
Refugee population (origin, gender)	Predominantly female Ukrainians; most adult males had to stay due to military obligations	In Europe research often mixed in Gender [81] with ratio not specified; majority of refugees arriving male due to dangerous passage; origin countries often mixed with focus on MENA region [81]	gender might impact information gathering (i.e., relevant information for mothers, search for doctor for children, ...), and integration efforts (i.e., use of apps for language learning from home); no reported instances of racism
Digitalization in country of origin, digital literacy	high digitalization (i.e., DIIA app, digital administration procedures, air alert apps…); relatively high digital literacy even for older interview partners	low digitalization in many countries [65], very heterogeneous digital literacy [62, 89]	used to digital every day life and administrative procedures, high proficiency with smartphones; bottom-up organization within Telegram groups, already very common in Ukraine; higher frustration because of lacking digitalization in Germany
Flight reasons / context	Russian-Ukrainian war, external aggressor	In Europe mainly civil war in Syria / Iraq (i.e., [79]), terror and war in Afghanistan (i.e., [89]), different wars / civil wars in Africa, political persecution (i.e., [89]); in Latin America often violence by organized crime [81], drug wars, armed interior conflicts	Clear external aggressor for the case of Ukraine, opposed to multiple interior actors or authoritarian regimes
Impact of war on ICT infrastructure	Destruction of infrastructure at frontlines and in occupied zone, partly replacement by Russian communication infrastructure w. surveillance, censorship; unreliable access to Ukrainian networks in bordering areas; power outages impact connectivity; generally quick reestablishement of connectivity	Fragmentation of infrastructure in Syrian civil war, heterogenity of connectivity [79]	Reports from Ukraine reflect the findings of [48], presence of Russian troops correlates with lower connectivity; findings reported from occupied zone / front line reflect infrastructural fragmentation reports [79] from Syria; in most of Ukraine quick restablishment of connection, despite power outages or attacks on network towers.
Journey	Passing military checkpoints, orderly passing borders by car or public transportation; help for organization by people online	Crossing borders (partly secretly to get to Europe), using services of people smugglers [37, 79, 89], passing military or terrorist checkpoints [89, 98]	orderly border passing requires less clandestine planning and contacts; more organization within public groups or on social media; help from civil society organized online (pick-ups at the border), which would have in been illegal in other cases
Reception in Germany	Positive, many voluntary helpers from civil society; picking up at Polish border; barely reports of racism; easier procedure due to Temporary Protection Directive by EU; more support with supply of SIM cards; free calling to Ukraine; sentiment got slightly worse over time, but remained generally positive	In Germany 2015 and after mixed, initially positive with many voluntary helpers [99], but with islamophobe, right-wing extremist resentments prevalent in some areas (i.e., PEGIDA [15]); sentiment worsened over time; limited supply of SIM cards, laws had to be adjusted first	easier for Ukrainian refugees to get housing outside of designated facilities, work allowance; might lead to other focus within self-help groups (finding jobs, housing, ...); tasks more comparable to regular migrant populations; jobs are vital factor for integration and rebuilding social capital [10], which advantages Ukrainians
Relevance of digital privacy & security	fear of persecution within occupied zone based on online actions; effort not to provide information to the enemy ("information silence") or russian companies; no other heightened need for privacy expressed	fear of persecution within country of origin based on online actions; fear of extorsion (by smugglers or corrupt officers) [58, 89]; privacy measures to avoid physical checks [89, 98]; privacy needs within refugee help programs; surveillance threat of political opponents [98]; threat by surveillance of European authorities [58] and system avoidance [40, 42, 58]	within occupied zone in Ukraine similar reports to refugees fleeing from authoritarian countries or system avoidant; "information silence" specific to war scenario: selective privacy concerns due to external aggressor; no system avoidance, no surveillance threat by migration authorities to prevent passage for Ukrainians

C Hierarchical code categories

Table 3. Excerpt of the hierarchical code categories for qualitative data analysis. The 23 categories covered a total of 2557 codes. Categories, sub-categories, and codes within the table are exemplary. The complete code book is provided as supplemental material online and can be found under with the doi [to be added].

Category	Subcategory	Codes
• Security & Privacy	- Location and GPS	Not sharing exact location/GPS, GPS not a problem, Location maybe sensitive
	- Additional measures	Support to hide information, Self-deleting messages, ...
	- Privacy Awareness and Relevance	Increased privacy efforts, Personal privacy not relevant, ...
	- Renouncement of apps	Switch of messenger, Deleted Apps from Russia
	- Security and security measures	Data security not common, Checking connected Telegram devices, ...
	- Anonymity, identity disclosure	Using Ukrainian phone number for Viber, anonymity, Use of pseudonym, ...
	- Sensitive information	Private information, Confidentiality of information for security of country, ...
	- Self-censoring, selective communication	Adapting Communication: Leaving out information, Use of code language, ...
	- Data Storage	No time to protect data, Use of cloud storage, Hiding of storage device, ...
	- VPN	Use of international VPN providers, VPN for access (geoblocking), ...
	- SIM cards / phone provider	Change of SIM cards, Not switching SIM card
	- Occupied zone	Blocking of Services, Physical device checks, Switching off smartphone, ...
• Protest	- Donations to military or for humanitarian aid	Support for and by artists, Humanitarian aid, Collecting money
	- Awareness raising	Information sharing in English, Sharing information about war crimes, ...
	- Protests on the street	Use of Viber to organize protests in occupied zone, ...
	- Online protest	Designers fighting Russia, Using SM to protest, Heard of protests online, ...
	- Content	Protesting against Russians / Making fun of soldiers, ...
• Information gathering	- Difficulty in handling information	Overwhelmed by information, Difficult to find info about specific issues, ...
	- Social Media	Following news links in groups / channels, Search function on SM, ...
	- Fake news / Misinformation / Propaganda	Increase / No increase, Misinformation by Russians, Countermeasures, ...
	- Information on government websites / official information	Newsletter from city, Looking for information on official websites
	- Reading news	Always checked news/alarms, news mostly on SM, Telegram channels, ...
Categories omitted: Change of User Behavior, Side notes, Information Warfare, Interview / Research related remarks, Navigation General Aspects / Problems / Challenges in Germany, Emotions, Demographic Properties, Ukraine - Russia Exchange / Peacebuilding, Digitalization, ICT Use, ICT use in Germany, Situational Factors, Affordance, Media Consumption, Gender perspective, Safety and Warning Infrastructure, Providing war related information, Infrastructure, Flight		