The Use of Private Mobile Phones at War: Accounts From the Donbas Conflict

Irina Shklovski[1,2] and Volker Wulf[2,3]

[1]IT University of Copenhagen
Rued Langgards Vej 7
2300, Copenhagen, Denmark

[2]University of Siegen and
[3]International Institute for Socio-Informatics (IISI)
57068 Siegen, Germany

irsh@itu.dk; volker.wulf@uni-siegen.de

ABSTRACT

Studying technology use in unstable and life-threatening conditions can help highlight assumptions of use built into technologies and foreground contradictions in the design of devices and services. This paper provides an account of how soldiers, volunteers, and civilians use mobile technologies in wartime, reporting on fieldwork conducted in Western Russia and Eastern Ukraine with people close to or participating directly in the armed conflict in the Donbas region. We document how private mobile phones and computers became a crucial but ambiguous infrastructure despite their lack of durability in extreme conditions of a military conflict, and their government and military surveillance potential. Our participants rely on a combination of myths and significant technical knowledge to negotiate the possibilities mobile technologies offer and the life-threatening reality of enemy surveillance they engender. We consider the problems of always-on always-connected devices under conditions of war and surveillance and our responsibilities as HCI practitioners in the design of social technologies.

Author Keywords

Mobile Media; ICT Infrastructures; Field Study; Appropriation; Political Conflict; War

ACM Classification Keywords

H.5.m. Information Interfaces and Presentation (e.g., HCI): Miscellaneous.

INTRODUCTION

The use of mobile communication technologies in crisis situations and armed conflicts is now expected. Research in crisis informatics has addressed situations ranging from natural disasters to terrorist attacks, investigating the dynamics of technology use and theorizing its potential impacts [18,23,39]. Several scholars have also turned their attention to political activism and the role of mobile technologies in armed conflicts [29,41,46]. This work teaches us that the use of mobile technologies has positive aspects in facilitating quick mobilization, getting help and information, and negative aspects in making individuals visible to state or enemy surveillance with potentially life-threatening consequences [25]. Yet there are few in depth accounts of how people live and have to negotiate their survival in on-going armed conflicts, of the opportunities that mobile technologies offer and of the implications of digital surveillance in such circumstances. Studying technology use in unstable and life-threatening conditions can foreground contradictions in design of devices and services, highlight assumptions of use built into technologies and consider the implications of these assumptions. For example, we find that under conditions of war notions of privacy and surveillance are less abstract for people who use social media with the expectation of potential surveillance by their own state and by the enemy.

In this paper we report on fieldwork conducted in Western Russia and Eastern Ukraine with people close to or participating directly in the armed conflict in the Donbas region. We consider the role mobile phones play in this conflict by focusing on their use by the soldiers and volunteers who are directly involved and by affected civilians. We describe how the expectations of state surveillance (and its confirmation through official communication) as well as the technical aspects of enemy targeting through geo-location of active mobile devices are negotiated against the need to remain connected to friends and loved ones beyond the bunkers and dugouts of warfare. Mobile communications and social media enabled soldiers and civilians on both sides of the conflict to leverage civil society in new ways in their efforts to compensate for a disorganized and under-resourced state of military and volunteer fighter groups. These empirical findings let us challenge design assumptions embedded in technologies given our increasingly unstable world.

TECHNOLOGIES OF CRISIS, WAR AND POLITICS

Prior research has examined social media use for political activism [5,31,45], but the events of the "Arab Spring"

CHI 2018, April 21–26, 2018, Montreal, QC, Canada

ACM 978-1-4503-5620-6/18/04…$15.00
https://doi.org/10.1145/3173574.3173960

motivated increasing scholarly attention [1,11,15,31]. The development of digital methods for large-scale quantitative social analysis of media content as well as the popularity of online ethnographic approaches made study of difficult and potentially dangerous locations possible and accessible to scholars worldwide [5,10,39]. For example, Zhou et al. [47] did a quantitative study of Twitter use during the post-election protests in Iran, analyzing over three million tweets of publicly accessible users, thus providing insights into the "dynamics of information propagation that are special to Twitter" ([47], p.123). Al-Ani et al. [1] investigated the Egyptian blogosphere during the "Arab Spring" uprisings in 2011, based on qualitative and quantitative analysis of blog postings. They identified counter-narratives created by Egyptian bloggers to protest against the government's official communication and described the blogosphere as an "alternative public space" [1:25]. Mark et al. [18,19] focused on "war diaries", published by Iraqi bloggers during the war in Iraq. Based on topic modeling and a quantitative analysis of postings, the authors investigated the relationship between war postings and other topics, notably postings about people's everyday life and their daily routines.

The online studies of social media use during crisis and political instability are valuable, but tell us less about the role of social media in political activities in practice. Several studies have gone beyond the focus on information available exclusively online, attempting to engage participants directly. Semaan and Mark [33] examined trust building in disrupted environments, based on (primarily telephone) interviews with Iraqi civilians during the second Gulf war, focusing on public identity. In another study Mark and Semaan [34] focused on collaboration structures and patterns of action during wartime, based on semi-structured telephone interviews with civilians from Iraq and Israel. Given the potentially dangerous nature of field research in politically unstable environments few studies have conducted research in situ. Wulf et al. investigated social media use by political activists 'on the ground' in Tunisia [46], in Republica Srpska [40] and in Palestine [45]. Tufekci [41] researched the use of social media among political activists in Turkey noting creative uses of technology as well as efforts to subvert known government surveillance efforts. Working in the borderlands of the war zone, Rohde et al. [29] interviewed participants in the Syrian civil war. These in-situ studies show that although mobile technologies prove a significant advantage in coordination and information dissemination, these devices also enable increased surveillance and persecution. Our study adds to these efforts to understand the role of social media and mobile technologies in zones of military conflict. We provide an account of mundane uses of mobile technologies and the related social practices around them in a war zone and in the peaceful areas bordering it.

EASTERN UKRAINE: BRIEF SUMMARY OF CONFLICT

The current conflict in the Donbas region in Eastern Ukraine is deeply connected to Ukraine's historical context and its relationships with Russia and Europe [26]. Poverty, the threat of political persecution, voluntary and forced relocations during the Tsarist and Soviet regimes repeatedly reconfigured the composition of the population of Ukraine [2,26]. The Donbas region of Eastern Ukraine, an area rich with coal and iron ore deposits, rapidly industrialized in the late 19th and early 20th centuries. Peasants and miners from other parts of the Russian empire and later the USSR relocated to urban centers such as Donetsk and Luhansk [7,26]. Cities in the Donbas region acquired a significant Russian population, while the rural areas remained extremely ethnically diverse. At the same time many Ukrainians migrated to Russia through forced and voluntary migrations throughout the 20th century. The modern Ukrainian state came into being in its current configuration in 1954 when the Soviet Union added the Crimea peninsula to the Ukrainian SSR. In 1991 Ukraine SSR became a sovereign state, exiting the Soviet Union with a territory stitched together from regions with diverse populations and turbulent histories.

The events of EuroMaidan

Political protests in Ukraine, known as EuroMaidan, precipitated the current conflict in the Donbas region. In November 2013 Ukrainian President V. Yanukovych refused to sign the Articles of Association Agreement with the EU. The free trade agreement with the EU demanded a change in Ukraine's existing trade relations with Russia. This refusal to sign signaled that government policy was moving to seek closer ties with Russia. In response, EuroMaidan protests began in Kyiv and several cities across the country. On November 30th the Yanukovych government deployed riot police in Kyiv to brutally disperse the protesters, assaulting many participants [14,21]. The next day protests in solidarity with those assaulted exploded across Ukraine and continued for the next three months. These soon turned from peaceful resistance to violent clashes with government forces, which resulted in the deaths of approximately 130 protesters and 18 police officers across Ukraine [4,14]. Although the largest protests and clashes happened in Kyiv, peaceful protests, violent clashes and deaths occurred in other cities in Ukraine, including Donetsk and Luhansk – the epicenters of the current conflict. On February 22 the Ukrainian parliament voted to remove Yanukovych, appointed an interim president and installed a new provisional government. On May 25th 2014, P. Poroshenko was elected as the new president of Ukraine. He follows a policy of western rapprochement and is supported by the EU and the US in return.

Donbas and the conflict in Eastern Ukraine

In Eastern Ukraine support for EuroMaidan was limited. Here voters were strong supporters of the Yanukovich

government [20,26]. Donbas has been one of the more economically troubled regions in Ukraine – although the steel industry fared well, the coal-mining industry that powered the region for nearly a century has been in decline for years [26]. In early April protesters in Donetsk and Luhansk stormed government buildings and raised Russian flags [27]. On April 7 protesters in Donetsk announced the creation of the Donetsk People's Republic (DPR). The Luhansk People's Republic (LPR) was proclaimed on April 27 [7,27]. Both DPR and LPR claimed the need for secession due to anti-Russian sentiment of the EuroMaidan and of the new provisional government.

These actions quickly escalated into a prolonged armed conflict, splitting the country into pro-Ukrainian and pro-Russian supporters. By May armed paramilitary units had taken over most of the region's urban centers, attacking EuroMaidan and interim government supporters [26,27]. The Ukrainian army was initially too weak, disorganized and under-resourced to mount a significant response. This prompted many local residents as well as volunteers from across Ukraine to self-organize into pro-Ukrainian volunteer paramilitary units to engage the pro-Russian fighters in violent clashes. When the Ukrainian army finally entered into the conflict they began to push the pro-Russian paramilitary groups back but both sides sustained heavy losses. Although Russia officially denied any direct involvement in the conflict [51], evidence of Russian artillery installations, regular army and special forces participation has been documented [3,48,49].

In September 2014 the Ukrainian government and the pro-Russian fighters signed a cease-fire deal in Minsk. The agreement was frequently violated and completely collapsed in January 2015. A new cease-fire, Minsk II, was signed in February 2015. Since then more than a dozen cease-fires have been signed with the latest starting on December 22, 2017 [52]. The cease-fires have led to what some call the "frozen conflict" [9] although dozens of soldiers and civilians are killed every month. The military response on both sides has formalized and expanded, with better-equipped and organized soldiers. On the Ukrainian side, most of the self-organized volunteer battalions have now been incorporated into the Ukrainian National Guard. The LPR and DPR have also consolidated and centralized their military operations. The war has had staggering human costs. According to the official statistics, since April 2014 the fighting cost over 10,000 lives, with over 2,000 of them civilians, and over 23,000 wounded [53]. Over 2.5 million have left their homes in the Donbas region, fleeing mostly to Russia or to non-effected parts of Ukraine [50].

Despite the fall of the Soviet Union ties between the central and eastern parts of Ukraine and Russia remained strong due to cultural similarity acquired over centuries of joint political rule and myriad familial connections. The armed conflict in Eastern Ukraine has split friends and families along lines of allegiance and along the borders that had suddenly become far less porous. In Russia the conflict is almost exclusively discussed as one rooted in ethnic differences, while in Ukraine it is seen as rooted in differences in political orientation and as an attack on the independence and sovereignty of a newly created state. Yet to many on both sides of the conflict the war seems senseless and incomprehensible.

Ukrainian EuroMaidan captured the attention of Western media and scholars, generating a significant amount of scholarship and discussion. Research has highlighted the importance of mobile technologies and social media organizing during the protests [5,22,30]. Self-organization and decentralization, enabled by mobile technologies and social media, facilitated cooperation and successful resistance despite government attempts to violently disperse the protesters [14]. Much of the civic organizing relied on neighborhood initiatives as well as on Internet-based news and social media [21,22]. Little research, however, has continued to study the resulting armed conflict in the Donbas region. In the following, we investigate mobile technology use and management by soldiers and civilians involved in the conflict or affected by it.

RESEARCH METHODS

Our method relies on an explorative analysis of narrative interviews and observational data. Narrative interviews are intended to elicit detailed 'stories' and are best understood as reflexive productions by interviewers and interviewees together. They tend not to take the question/answer form associated with traditional social science (see e.g. [6,8]). Our approach to data collection is based on traveling to the conflict zones or as close as security considerations permit. Once in place, we spend time at potentially interesting locations, such as the Maidan square in Kiev, talk to people that we often meet accidentally, and recruit interviewees (see [29, 43]). In the two main field sides, we also drew on initial contacts gained through the authors' networks of acquaintances.

The data collection took place in Russia and in Ukraine in towns bordering the active conflict zones. In November of 2015 we visited Russia for a week, taking an overnight train from Moscow to the city of Belgorod. The Belgorod oblast is situated just across the border from the Ukrainian city of Khrakhiv and northwest of the LPR. This region hosts many Eastern Ukrainian refugees given its proximity to the border. We spent five days in the region, conducting observations, informal conversations and 12 interviews. Interviewees included local volunteers, local residents with family in Eastern Ukraine, refugees from Eastern Ukraine, people directly involved in military action in the region (both volunteers and professionals) and representatives of volunteer organizations organizing unofficial deliveries of humanitarian aid to the LPR. In total we interviewed 19 people in individual and group situations and informally met more. The second author

extended the trip to visit the Crimea peninsula.[1] He flew from Moscow to Simferopol, visiting Sevastopol and Yalta and conducted observations, informal interactions and three interviews with local residents and recent arrivals from Russia and Eastern Ukraine.

In the spring of 2017 we spent a week in Ukraine, visiting the cities of Kiev and Mariupol. After spending 2 days in Kiev we took an overnight train to Mariupol. Mariupol is approximately 20 km from the frontline and 100 km from the city of Donetsk – the main city of the DPR. The DPR and LPR together constitute the Non-Government Controlled Territories (NGCT), in Ukrainian terms. The city of Mariupol saw active military conflict in the spring and summer of 2014, but has remained under Ukrainian control since. We conducted four individual and group interviews in Kiev and 15 in and around Mariupol. In total we obtained extensive interview data from 22 individuals and spent time informally with more. Given the dangerous conditions, we did not enter the NGCT.

In Kiev we interviewed people who have close ties or relatives in Eastern Ukraine, volunteers in the Kiev civil defense, refugees from Eastern Ukraine and military personnel on leave from active duty in the Ukrainian army and the National Guard. In Mariupol we interviewed residents who lived in the city during the military conflict in 2014, volunteers helping the Ukrainian army, current and former members of volunteer battalions and of the Ukrainian National Guard, current and former military personnel in the Ukrainian army, refugees from Crimea and Eastern Ukraine and individuals who lived in the NGCT but worked in Mariupol.

Our results are based on empirical data collected from observations, informal conversations and interviews with actors participating in the conflict or living in or near the conflict zones. The interviews lasted between 30 minutes and 2.5 hours. In total, in Belgorod and in Ukraine three interviews were conducted in English with the rest conducted in Russian. The first author synchronously translated all interviews conducted in Russian. On the Crimea peninsula all interviews were conducted in English. Given the sensitive nature of the content of the discussions, none of the interviews were audio recorded but the authors took extensive notes during and after each interview. We do not mention names to maintain confidentiality.

Both authors conducted open and thematic coding on field notes and interview notes throughout the visits and after. We discussed our coding decisions and identified themes. Following the fieldwork, we remained in email and social media contact with some of our informants on both sides. Such contact enabled us to ask for clarifications and further explanations throughout the coding and analytical process. We continue to monitor news media as well as blogs, twitter and social network postings of the individuals we encountered and those whose work and online activity emerged as prominent in our fieldwork.

[1] In March of 2014 the Republic of Crimea signed a Treaty of Accession for immediate admission as part of the Russian Federation after holding a referendum that the international community did not recognize.

EMPIRICAL FINDINGS

"*It's a strange kind of war*," a volunteer soldier tells us in a café in Belgorod. He explains that he has recently returned from "*helping to keep the fascists at bay*" in the Luhansk region now that the fighting is settling into something more organized and the new people's republics – LPR and DPR are formalizing their military units. The war is "*strange*" he said because while the two sides are trying to kill each other, mobile phone reception is doing just fine and there is electricity and water available in those structures that are not too damaged. Mobile technology, as it turns out, has become key to both sides of the conflict for coordinating their lives at war as well as for identifying and targeting concentrations of enemy fighters. Throughout our fieldwork themes of the capabilities of mobile phones, their function as a life-line in crisis and as a way to work around brittle official structures, their ability to document the goings on, their lack of durability in extreme conditions of a military conflict, and their government and military surveillance potential consistently came up regardless of which side we spoke to.

In what follows we discuss the themes that emerged across conversations and battle lines. We begin by considering the military significance of the visibility of mobile phone signals in the field conditions of a military conflict. We then describe how the use of mobile phones supported keeping in touch with family and friends away from the front lines, enabled connections and informal support between the soldiers and the civilian residents in or near the areas of fighting, and offered ways for soldiers to cope with the rigors and boredom of military service. Finally, we discuss how expectations of state surveillance seemed to shape the use of mobile technologies among the refugees, their relatives and the soldiers themselves.

Telecom infrastructures as military assets

The capability to geo-locate private mobile phones became an important element of military systems in the Donbas conflict. During our fieldwork in Russia in 2015, civilians and paramilitary volunteers told us how they avoided using their mobile phones too often in conflict zones. One of the professional soldiers we interviewed explained the reason: "*When you hear a drone, you have about five seconds to leave your position and run. The rocket will fly in that fast."* He noted that drones were easier to recognize at night because of their in-flight navigation lights. Locating them in daylight is more difficult, especially when they fly very high. Soldiers on the Rus-

sian side told us that the Ukrainian army was using "*American drones*" to search for active mobile phone signals to assist targeting[2].

When we interviewed military personnel and volunteers in Ukraine in 2017, the use of mobile phones signals as targeting beacons for enemy fire was a constant theme. Ukrainian military personnel freely admitted that location triangulation is used for targeting by both sides. This is not to say that military coordination and action relies on mobile phones exclusively. Ukrainian military field deployments also use secure radio communications and wired communication field equipment, acknowledging that a mobile signal is easy to intercept.

It is technically possible to locate active devices that are exchanging data with the cell tower infrastructure of a mobile network. However, even smartphones that are switched off can potentially be tracked, depending on software and model. Only when the battery is removed is there a guarantee that the phone is truly off. Our data suggest that the information gained from geo-locating mobile phone signals could be used as rocket and artillery targeting information. Prior work has reported that satellite phones can be easily geo-located when in use, noting that such knowledge was often acquired by civilians and activists through potentially life-threatening experience in conflict zones [25,29]. Regular mobile phone communications are similarly vulnerable especially with the cooperation of the telecom operators. At the start of the war many soldiers on both sides did not realize this capability was present, but quickly learned from personal experience and the mistakes of others. Here the type of device plays a curious role. Smartphones and tablets turn out to be terrible wartime devices for two reasons. First these devices are relatively fragile given the field conditions of trenches. As the mother of a young solder in the Ukrainian National Guard tells us – "*he used to have an iPhone but the screen got busted by a blast wave the first time his position got shelled.*" Second, the fact that the battery in many flagship devices cannot be removed means that turning them off does not necessarily guarantee safety.

The problem of visibility to the enemy through mobile digital activity is acute and omnipresent. We were told that some military positions deploy "*glushilki*" - devices that block phone signal – but these are ineffective because they cover a small radius and the batteries run out quickly so the military errs on the side of less connectivity as part of soldier responsibility. Despite the problems, the military recognizes the value of mobile phones, issuing simple non-feature mobile phone devices to all personnel to be carried turned off and with battery taken out until necessary and in case of emergency.

Soldier, if you want to survive:
1. Leave your own SIM card at home.
2. The best place to get a SIM card is in the zone of conflict itself.
3. If you plan to make a phone call, walk at least 400-500 m away from squad positions.
4. Don't walk away alone, take an armed friend with you to cover you.
5. The best place to make a phone call is in locations with a lot of civilians, preferably in recently liberated towns.
6. Always keep your phone off. Your life depends on it. Grad missiles will hit your whole squad.
7. Do not accept refill codes or cards from the locals. The young woman that brought you a refill card from the neighboring village may be working for the enemy. Right now FSB and SBU have to process enormous amounts of data to identify the mobile phones of our own people and of the enemy. Do not make their job easier.
8. Watch over your comrades – a friend calls his girlfriend and an hour or so later your position gets shelled or attacked.
9. Remember, the enemy could be listening to your conversations regardless of which SIM card or which telecom operator you are using.

Table 1. Selection of points from an official military order to Ukrainian soldiers.

To help soldiers cope with realities of active deployment the Ukrainian military issues formal military orders for limiting technology use (see excerpt in Table 1). Acknowledging that there is little chance new soldiers will leave their personal mobile phones at home, the main suggestion is to bring non-feature phones that allow only calling and texting and that have a long battery life (there are few power sources in the trenches). Mobile phone use has become the digital version of carelessly lighting a cigarette at night and revealing a position to the enemy in a combat zone. Where before soldiers were instructed to obscure the visual marker of the cigarette, now they are told to walk away from the trenches and take a friend along to make a phone call. Mobile phones, however, can reveal far more than the glowing ember of a cigarette. The military order leaflet not only clearly acknowledges the fact of surveillance of all communications by both sides of the conflict but also instructs how to obstruct it.

Social uses of mobile phones in war-time

Despite the very real risks represented by mobile devices and the efforts of the commanding structures to limit their use, their proliferation among the regular soldiers was expected and acknowledged for a range of reasons, some of which are detailed below.

Mobile phones as life-lines in war

Mobile devices represented very real risks due to potential for enemy surveillance, but they were also necessary for soldiers to manage their participation in under-resourced military infrastructures. On both sides, the start of the

[2] In 2017 OECD announced termination of their drone monitoring program to observe cease fire violations because the expensive machines were shot down by both sides too frequently [16].

conflict was rife with disorganization and confusion where equipment was hard to come by. Our participants told us how many heavily relied on their local networks to equip themselves and for support throughout. In Russia a volunteer soldier, who had fought on the pro-Russian side in LPR in late 2014 and early 2015, explained that he always kept his phone with him despite the acknowledged risk just in case he needed to call for help. He had been injured in action after stepping on a mine and ended up in a hospital in Luhansk. The wound was too difficult to treat at that hospital so he phoned his contacts in Belgorod who managed to organize an ambulance for a transfer across the border to a hospital in Belgorod.

In Ukraine mobile phones also offered a way to leverage local networks in shoring up the brittle and uncertain formal infrastructures. Consider the following example: We met K and M, local Mariupol volunteers who organize support for the army and paramilitary units in the vicinity. One afternoon they took us along when a soldier had gotten in touch after his detachment was shelled by the enemy the previous day. He had ended up in a military hospital with a concussion and was asking for some legal advice as well as support. K and M first went to the grocery store and then headed to a used goods store to get a pair of pants and a t-shirt – the soldier would need clean clothes that the hospital was unlikely to provide. We drove for some time on bumpy roads through checkpoints, eventually arriving in a small village where a building has been converted into a field hospital. The soldier walked out to the gates to speak to us and to receive the care-package. He explained his situation – his concussion was quite bad and he had lost hearing in his left ear entirely, but he still had a year of his draft left to serve. His commander initially did not believe he was hurt badly enough to warrant a hospital, but when the medics diagnosed a severe concussion, he pragmatically called to ask where to ship the belongings. The soldier was worried about retaining access to military resources given the extent of the injury. M, who has a legal background, gave extensive advice on the best course of action.

On the way back K and M explained that although the Ukrainian army is much better organized and equipped now, the equipment is still low quality and insufficient. K told us that the previous winter had been very cold, so they used social network sites to organize people in Mariupol to knit sweaters for the soldiers. The names of these volunteers are known and their phone numbers get passed along to soldiers in military detachments stationed in the vicinity. Soldiers call to ask for help and advice as the volunteers leverage their contacts through Facebook and phone calls to respond. Partly this happens because the Ukrainian army is under-resourced, partly because of the lack of trust in the government that is considered to be corrupt and has been repeatedly accused of attempting to limit paying out benefits. Mobile phones and social media help knit an alternative safety net linking soldiers with local civilian supporters.

Keeping in touch with family and friends

We asked the Ukrainian soldiers whether they used their mobile phones given the dangers and everyone replied that of course they kept in touch. After all, mothers, partners, relatives and friends worry for good reasons and want regular contact. A young soldier in the National Guard tells us that he calls his mom every day either in the morning or in the evening. Others call to chat with girlfriends or friends (but not too long). At the beginning of each interview in Ukraine, we are dutifully told that soldiers only use the basic military-issued phones, but as the conversation progresses we often learn that they also have tablets and smartphones. They tell us then that indeed they also use social network sites to talk to friends (because otherwise it is possible to go mad).

This ability to stay in touch allows soldiers to keep in contact with what life looks like away from the conflict zone. Yet remaining connected with friends, family and local civilian volunteers can also occasionally lead to terrible outcomes, as soldiers must deal with both military realities and civilian concerns. In Ukraine, we heard a story about a soldier whose friend told him via messenger that the soldier's girlfriend has decided to dump him. The soldier had served two of his three years and was by all accounts a reasonable man, but in this case he got sad. His commander took away the gun, but the bottle of vodka was there and grenades tend to be strewn around the compounds. So he drank the vodka and then pulled the pin out of a grenade as his friends slept nearby.

This story suggests that perhaps soldiers, while facing harsh military realities, remain too reachable for civilian life. Their everyday experiences in the conflict zone are so different from that of their friends that they are likely to be incomprehensible. Yet their updates appear in the feed just like everyone else's. This can potentially normalize both the soldier's digital presence and their availability to friends and family connected to them. The impact of such communication can inadvertently have powerful effects. The use of private mobiles, however, has become an essential part of the life at war. As one soldier commented: "*If they* [military command] *tried to take away mobile phones, there would probably be a riot*."

Pragmatic negotiations across battle lines

The ability to connect across distance and borders also spawned creation of stories about the possibilities mobile technologies and social media might offer. In a war being able to negotiate with the enemy soldier to soldier, outside the official command structures, can be helpful. One commander told us a curious story of a village store located in the middle between the positions of the two armies where the soldiers negotiated the days on which they can go to the store and buy vodka lest they get shot at from

the other side. He explained that of course they didn't call each other - such phone calls would be easily visible to the security forces and would count as treason. There are other ways to connect, for example using the social network platform VKontakte or finding people in common through people they know who have moved around and have civilian contacts in the vicinity. There are, after all, many whose friends and families that have been physically separated by the battle lines but still maintain contact. Somehow they negotiated this very specific non-aggression agreement, he told us, because vodka was purchased and nobody got shot. Mobile technologies, social media and personal connections allowed such stories where the absurdities of war are made banal as people work around expectations of surveillance and violence.

The basic reality of war is boredom

The cease-fire agreements mean that the Donbas conflict is essentially a positioning war – where frontlines rarely move and focus is on managing existing positions. This also means that much of the time soldiers deployed on the front lines are spending time monitoring each other rather than in active engagements. Mostly, the soldiers tell us that being on the front line is a lot of waiting occasionally punctuated by moments of terror. Waiting is boring.

In nearly all of our interviews and conversations in Ukraine the first response we received about social media and mobile phone use by soldiers was in line with the official policy. The military has taken steps to limit information leakage through social media. Our informants told us that the Ukrainian military requires all military personnel to sign a document that commits them to disabling their social media accounts for the duration of active deployment. According to recent media reports Russia is considering a similar move [35].

Despite the fact that soldiers are officially forbidden from using private mobile devices on the front lines, most of them still do. As one Ukrainian army soldier told us: "*you've got to understand, sitting out there in the dug-outs, trenches and bunkers for days and even weeks with nothing to do, people start going out of their heads. You need something to take your mind off of things.*" Here social media offer a welcome distraction, the threat of being located by the enemy becoming less an acute concern despite its very real potential.

Boredom can lead even the most cautious to do things they say they will never do. A military investigator told us: "*Sometimes everyone in the dug-out is using their devices - if a mine or an artillery shell hits and some of them live, they abstain for only so long*." Story after story we heard that many spend considerable amount of time on social media, eventually admitting that many post about where they are and what they do as the genre of social media demands. As a military incident investigator confirmed: "*the commanders know, everyone knows but what are you going to do?*" Social media is excellent at relieving boredom, downgrading the very real risks of becoming visible to enemy surveillance.

Keeping up to date with news and information

We found that Ukrainian civilians and soldiers widely shared the opinion that Russian and Ukrainian mass media are biased and unreliable in the information they provide. Instead, our interviewees tended to rely on social media to better understand the political context and events in the war. Civilians pointed to particular journalists and media figures they followed on Facebook or smaller-scale online media projects. A member of the National Guard explained that he gets the best of his information from VKontakte groups and other sites where volunteer soldiers are active: "*People at the front line know what is going on*." Groups on social network sites were common sources of information. As many interviewees explained: "*There are people in these groups whom you trust*."

Social media made possible a broader implementation of a kind of "samizdat" – an old tradition of creating alternatives to state news in the Soviet times. For example, when speaking about ongoing railway blockades by Ukrainian veterans an interviewee stated that he preferred to find information via the internet about the new law which rendered the blockade legal [13,54]. He claimed that the official information was biased and only online was it possible to find a more balanced view. Two of our interviewees, having previously served in private and locally organized battalions, took part in this blockade. They felt that the Ukrainian state TV had misrepresented the veterans as violent outlaws. They stated that the media manipulated the display of violence: "*On TV it looked like the protesters were attacking the army, in reality the army had beaten up the protesters.*" They showed us their own webpages and Facebook groups that were oriented towards disseminating information that they felt was more legitimate.

On both sides of the divide we encountered explicit discussions of bias in government-sanctioned media, often pointing to the radical difference in interpretation of the same events by different news outlets. In many conversations, people carefully explained the sources of their information, sometimes listing regular media, social media and various news sites and discussing the discrepancies between these. Several soldiers noted that being able to tell others what was really going on was an important reason to use their mobile technologies.

State surveillance and mobile phone use practices

Without exception everyone we spoke to expected that their phone conversations and internet activities were under at least some surveillance by their own state or by the enemy. Our participants did not express outrage or concern for this state of affairs. They merely noted its existence with statements such as: "*of course 'they' know*

who you talk to or what you are posting" and *"of course 'they' are watching*." This expectation of surveillance shaped their decisions in what types of mobile phones they purchased and what channels of communication they chose to use for various different purposes. They constructed stories of myth and fact to back up their decisions, similar to what Wash termed "folk stories" [43].

For example, when we asked a local civilian organizer of refugee support and humanitarian aid in Belgorod why she was using a simple non-feature mobile phone she explained this was her way of ensuring that her phone does not get tracked. "*It does not get tracked because it does not have an Internet connection*" she said, convinced that this was an important aspect of tracking and locating. Her reasons for this concern were not directed towards the Russian government but towards the Ukrainian security services (SBU). She was worried that SBU might find out where she has been and how often she has traveled into the Luhansk oblast' and create problems for her relatives living in Ukraine. Despite being quite central to the local efforts to support refugees and families still living in Eastern Ukraine, she never used the Internet for any of her organizing activities because she felt that the Internet was even easier to monitor for the SBU.

Nearly everyone we spoke to both in Russia and in Ukraine (the aid organizer included) who had relatives still living in the Eastern Ukraine conflict zones used Skype or Viber to communicate because calling on the phone had become both expensive and unreliable. Skype, by virtue of being a western-owned resource, was often seen as safer from surveillance than mobile phones. An artist from Donetsk, now living in Mariupol as a refugee, explained that she expected phone lines to be monitored for conversations with people in the zone of conflict. She used Skype to speak with her mother because "*the Internet in Donetsk is much better than even in Mariupol*" and, she confided, it is "*safer*."

Expectations of state surveillance among the regular population are of no surprise as both governments have been clear about their capabilities. For example, in January 2014 all mobile phone subscribers who were near the scene of the Maidan protests in Kiev received a text message from the Ukrainian government informing them that they had been registered as participants in a "mass riot" and suggesting they disperse [12]. The Russian state communication oversight agency, RosComNadzor, routinely issues notices of which websites have been blocked as well as who had been observed accessing these [38].

Those we spoke to on the Russian side were relatively sanguine about being monitored by the Russian state. Instead, they worried about their Ukrainian friends and family being affected if the Ukrainian state was able to track their interactions across the border. Those on the Ukrainian side were equally concerned about both Russian and Ukrainian state surveillance especially if they had relatives living either in Russia or in the conflict zone. The expectation of monitoring extended to social media resources as well.

A former soldier and volunteer in Mariupol working with children orphaned by the conflict explained that his life was basically about three or four social media networks. He used Facebook, VKontakte and Line intensively but in different ways. While Facebook was about his daily life and for friends and contacts his age, he had a different personality and a different network of friends on VKontakte: "*I have a different life there, basically speaking about ideas*". On VKontakte, he explained, there are more young people he can mentor. Using Line, he discussed political strategies with his network, laughing he joked "*how to take over the Rada* [Ukrainian Parliament]*, that sort of thing*." Then there are people he talks to on Telegram but those are not frequent conversations. Telegram is the only app in his list that offers encryption but he ignored our mentioning of this as if he didn't quite understand what we were talking about.

When asked why this proliferation of methods of communication, he notes that different people are on different resources and then mentions that Facebook is harder for "them" to track because it is American. VKontakte on the other hand is a Russian social network site and was extremely popular among Russian-speaking youth since its inception.[3] Despite the public take over of the company by owners loyal to the Russian government [38], most users remained on the social network. VKontakte users were responsible for posting content that inadvertently confirmed Russian military involvement early on in the conflict in Eastern Ukraine and postings on the network on this topic have been routinely publicized and then swiftly removed [38,42]. The young Russian-speaking soldiers and civilians on both sides of the conflict continue to actively use it. When asked why VKontakte, he says "*of course the Russian government knows everything that happens on VKontakte but that's where all the young ones are who are on both sides of this conflict, that's where they were when it all started!*"

Studies in Post-Soviet states show that there is often an expectation of internet blocking and surveillance among the population [36]. At the same time, there is also acquiescence to the actions of the state complete with post-hoc explanations and justifications of its actions [24]. To most our participants state surveillance is a logical move on the part of the state and they used their communication technologies with this in mind.

[3] The Ukrainian government banned the use of Russian SNS VKontakte in the armed forces in May 2017. We report on data collected prior to the ban: https://tinyurl.com/l8rk9qg

DISCUSSION

In this paper we offer an account of the role mobile technologies play for soldiers and civilians involved in or affected by an armed conflict. Such an in situ investigation carried out on both sides of the frontline helps us understand the mundane social practices at war and how they are shaped by technological devices and infrastructures, civilian as well as military ones. Though the conflict has changed, becoming more organized and formalized over time, the soldiers continued to rely on local volunteers for sweaters in winter and legal advice when in trouble. From the beginning, private mobile phones were a key infrastructure in this war. Existing in parallel with the army communication infrastructure, private mobiles allowed soldiers to link with different actors in civil society. As the war unfolded soldiers predictably used mobile media in creative ways for information gathering and even local enemy negotiations but they also relied on these devices to relieve the boredom of active duty. This continued despite the fact that these devices critically endangered them when in use.

The war in Eastern Ukraine engulfs population centers where civilians continue to live between the frontlines. There is then motivation to maintain infrastructures regardless of military goals although infrastructure integrity is quite uneven. For example, there is considerable concern that water infrastructures are nearing collapse in some of the populated areas [32]. Yet people in Mariupol frequently commented that Internet connectivity was so much better in Donetsk (DPR) than in Mariupol. Infrastructures function differently in every military conflict. In the Donbas conflict, mobile infrastructures were important enough that we heard unbidden third-hand reports of military orders to avoid damaging the cell towers in combat. In contrast, in the Syrian civil war, in rebel-controlled areas the network infrastructure was immediately switched off by the Syrian government [29].

Our narrative demonstrates how the rise of new forms of military surveillance technology capitalizes on pre-existing communication infrastructures and on the proliferation of civilian communication devices that are part of the fabric of daily life. The stories we heard suggest that there are military technologies, which can use mobile phone connections with cell towers for location triangulation rapidly providing targeting coordinates for artillery and rocket installations. While there is considerable data on how this can be done with satellite phones, we have been unable to find solid technical information on how regular telecommunications have been integrated into such systems. Given our data, we can speculate that this technology is able to differentiate local and non-local callers (soldiers typically bring their private SIM card from places where they have been before). This situation is fundamentally different from conditions of natural disasters where mobile infrastructures and localization technologies can be of help to first responders and to those affected. Surveillance technologies under the conditions of war have particular implications for the design of always-on always-connected devices.

The problem of 'always-on always-connected' devices

Given the dangers of the geolocalization of private devices and the surveillance of content generated on social media platforms all soldiers of the Ukrainian army had to sign an agreement to delete or deactivate their social media accounts when deployed to the frontline. Predictably, we found that the soldiers did not follow this order. Officers, we talked to, either did not want to comment on this fact or acknowledged that they could not stop the soldiers' use of private mobile devices. HCI research on civilian work in office settings has demonstrated that formal rules are often bypassed in practice (e.g. [17,44]). Clearly, the local reinterpretation of rules happens in command line organizations under life-threatening conditions as well. Though the risks are high and rarely fully understood, the breach of commands and orders is tolerated by the military hierarchy for the sake of local needs and habits.

For good reasons soldiers remain connected to civilian life through their smartphones and tablets even as they engage the enemy in combat. Such connectivity can at times lead to normalization of combat experience as it gets slotted in between cat videos and vacation pictures in the news feed. Connection to normal experience is a draw for the soldiers and yet social media use can also mean detection by the enemy with tragic consequences. Contemporary devices increasingly do not give users the ability to really turn them off. Perhaps hardware producers of mobile devices should be required to implement an 'OFF' button, which effectively switches off technical opportunities to locate the device. Such a design would considerably increase the security and self-determination of their consumers – not only in situations of an armed high-tech conflict.

Social media platforms and their responsibilities

Social media platforms connect us inexorably with our social ties and create expectations of reachability and connectivity, generating significant stores of personal information. These data stores represent important assets from a strategic military point of view. Surveillance is a common expectation of war. Soldiers know they are being tracked and watched, by both sides and by security services. They realize the dangers and yet we are told that while talking on the phone is definitely tracked, Skype and Viber may be better despite the fact that neither are more secure in reality. What are the obligations and responsibilities of platforms such as Facebook, Microsoft (Skype) or VKontakte to their users who are involved in or merely end up in the midst of military combat operations and to their governments, embroiled as they are in geopolitical conflicts?

Social practices on social media platforms are great at alleviating boredom but these rely on infrastructures of surveillance that are pervasive and easily used. The data stores these platforms amass are a basis for extensive advertising services, but such infrastructures also offer convenient ways of identifying and targeting individuals of interest by governments and secret services too [29,45,46].

Most of the people we spoke to used social media for personal connections and relief from boredom, fear and pressure of being part of an active military conflict. For those that were of a more activist orientation, social media provided a way to keep track of sentiment, to engage those who might listen, to lead by example and to push their ideas forward. They carefully selected channels of communication for the kinds of messages they disseminated, considering the problems of surveillance and visibility these channels represented. Yet we observed that the actual social media use that could be construed as radical or even political was relatively infrequent. Our study suggests that use of social media channels is a complex intertwining of the practical and the political and these need to be considered together to be understood. While large-scale analyses of social media activity can identify networks and influences, more in-depth studies are desperately needed to really delve into the role these media have in how people live their lives, accomplish their goals and, occasionally, engage in politics within environments where state surveillance and real threats to personal safety are constantly present [36].

Such questions cannot be considered without addressing the role of the platforms themselves. Platform providers have a responsibility to be open about the way they amass and collect personal data, with whom they share these data, and what access is allowed by government agencies. Ideally, platforms need decentralized architectures, distributed data storage and better security mechanisms. People will use social media regardless of surveillance and social media platforms will continue to capitalize on the personal data they collect. Clarifying the responsibility for communicating how personal data may be used is crucial for users in all contexts to be able to better balance the risks. Designing services that make such communication with end-users possible is crucial.

Mobile and social media surveillance

The practices of our informants seemed to rely on a curious mix of myth and technical understanding combined with expectations based on where the servers are and who might have access to data. For the most part, the people we spoke to did not have significant technical training but all seemed to be much more aware of the dangers of personal data leakage enabled by mobile technologies than the average western consumer [37]. Our participants worried about their own exposure through state surveillance (on both sides) for very real reasons and were extremely motivated to engage in what some Western privacy activists have termed "digital self defense" [28]. Their knowledge and understanding of data flows and expectations of whether and how the media companies whose services they used might behave were logical, despite being potentially wrong. The concept of self-defense, whether physical or digital, is about survival and people develop folk wisdom and "folk models" [43] for acting with technologies to manage personal visibility and risk, to survive and to accomplish their goals.

It is perhaps tempting to think of such unstable conditions as a unique environment for the use of social media where restrictions, risks and benefits become ambiguous. We argue, however, that extreme situations, such as war, make the problems of surveillance and exposure of social media and mobile technologies unignorable. This demonstrates the need for better information sources to enable actors to better judge the inherent dangers. However, our data also point to limitations of efforts to educate users about protecting their data. After all, if the clear threats of open state surveillance and death do not limit disclosure of sensitive information on Facebook, what hope is there for mere nudges?

CONCLUSION

Our study demonstrates that in considerations of mobile technologies two points are important from the point of view of HCI research and design. First, any mobile technology-based solution relies on availability of infrastructures supporting telephony, and must consider who owns and controls these. Second, data sent across mobile infrastructures is always vulnerable and makes visible its producers and consumers. Such visibility can have significant and even life-threatening consequences, calling for a rethinking of design objectives for consumer communication devices. Given the rapid development of military surveillance technologies in an increasingly unstable world, what does it mean to be digitally visible? We argue that users of social media and communication technologies have a right to an understanding of surveillance practices by the state, the platforms and the military industrial complex. It is crucial to ask: How might HCI help make surveillance detection a mundane, everyday practice? How might we enable people to respond in ways that can protect and support them?

ACKNOWLEDGEMENTS

We are indebted to all of our respondents for their generous participation in our study. We thank D. Struthers and anonymous reviewers for constructive commentary. This research was supported by the German Science Foundation in the Context of the Collaborative Research Centre 'Media of Cooperation' (DFG-SFB 1187).

REFERENCES

1. Ban Al-Ani, Gloria Mark, Justin Chung, and Jennifer Jones. 2012. The Egyptian Blogosphere: A Counter-

narrative of the Revolution. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (CSCW '12), 17–26. https://doi.org/10.1145/2145204.2145213

2. Kate Brown. 2005. *A Biography of No Place: From Ethnic Borderland to Soviet Heartland*. Harvard University Press, Cambridge, Mass.
3. Uri Friedman. 2014. Russia's Slow-Motion Invasion of Ukraine. *The Atlantic*. Retrieved January 7, 2018 from https://tinyurl.com/y8yra4un
4. Katya Gorchinskaya. He Killed for the Maidan. *Foreign Policy*. Retrieved September 18, 2017 from https://foreignpolicy.com/2016/02/26/he-killed-for-the-maidan/
5. Anatoliy Gruzd and Ksenia Tsyganova. 2015. Information Wars and Online Activism During the 2013/2014 Crisis in Ukraine: Examining the Social Structures of Pro- and Anti-Maidan Groups. *Policy & Internet* 7, 2: 121–158. https://doi.org/10.1002/poi3.91
6. Jaber F. Gubrium and James A. Holstein. 2002. *Handbook of Interview Research: Context and Method*. SAGE.
7. John-Paul Himka. 2015. The History behind the Regional Conflict in Ukraine. *Kritika: Explorations in Russian and Eurasian History* 16, 1: 129–136. https://doi.org/10.1353/kri.2015.0008
8. James A. Holstein and Jaber F. Gubrium. 2000. *Constructing the Life Course*. AltaMira Press, Dix Hills, N.Y.
9. Patrick Jackson. 2014. "Frozen conflicts" and the Kremlin. *BBC News*. Retrieved September 19, 2017 from http://www.bbc.com/news/world-europe-29078541
10. Andrea Kavanaugh, Steven D. Sheetz, Riham Hassan, Seungwon Yang, Hicham G. Elmongui, Edward A. Fox, Mohamed Magdy, and Donald J. Shoemaker. 2013. Between a Rock and a Cell Phone: Communication and Information Technology Use during the 2011 Uprisings in Tunisia and Egypt. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)* 5, 1: 1–21. https://doi.org/10.4018/jiscrm.2013010101
11. Andrea Kavanaugh, Steven D. Sheetz, Hamida Skandrani, John C. Tedesco, Yue Sun, and Edward A. Fox. 2016. The Use and Impact of Social Media During the 2011 Tunisian Revolution. In *Proceedings of the 17th International Digital Government Research Conference on Digital Government Research*, 20–30. https://doi.org/10.1145/2912160.2912175
12. Shaun Walker Oksana Grytsenko in Kiev. 2014. Text messages warn Ukraine protesters they are "participants in mass riot." *The Guardian*. Retrieved September 19, 2017 from https://tinyurl.com/mxc5lks
13. Andrew E. Kramer. 2017. Ukraine 'Blockaders' Try to Cut Off Rail Traffic From Rebel Areas. *The New York Times*. Retrieved January 7, 2018 from https://www.nytimes.com/2017/03/02/world/europe/ukraine-blockaders-cut-off-rail-traffic-from-rebel-areas.html
14. Svitlana Krasynska and Eric Martin. 2017. The Formality of Informal Civil Society: Ukraine's Euro-Maidan. *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations* 28, 1: 420–449. https://doi.org/10.1007/s11266-016-9819-8
15. Gilad Lotan, Erhardt Graeff, Mike Ananny, Devin Gaffney, Ian Pearce, and Danah Boyd. 2011. The Arab Spring| The Revolutions Were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolutions. *International Journal of Communication* 5, 0: 31.
16. Alec Luhn. 2017. Ukraine blocks popular social networks as part of sanctions on Russia. *The Guardian*. Retrieved September 19, 2017 from http://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war
17. Peter Mambrey and Mike Robinson. 1997. Understanding the Role of Documents in a Hierarchical Flow of Work. In *Proceedings of the International ACM SIGGROUP Conference on Supporting Group Work: The Integration Challenge* (GROUP '97), 119–127. https://doi.org/10.1145/266838.266881
18. Gloria Mark, Mossaab Bagdouri, Leysia Palen, James Martin, Ban Al-Ani, and Kenneth Anderson. 2012. Blogs As a Collective War Diary. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (CSCW '12), 37–46. https://doi.org/10.1145/2145204.2145215
19. Gloria Mark and Bryan Semaan. 2009. Expanding a Country's Borders During War: The Internet War Diary. In *Proceedings of the 2009 International Workshop on Intercultural Collaboration* (IWIC '09), 3–12. https://doi.org/10.1145/1499224.1499228
20. David Marples. 2016. Ethnic and social Composition of Ukraine's Regions and Voting Patterns. In *Ukraine and Russia: People, Politics, Propaganda and Perspectives*, Agnieszka Pikulicka-Wilczewska and Richard Sakwa (eds.). E-International Relations, Bristol, UK, 9–18.

21. Olga Onuch. 2014. Who Were the Protesters? *Journal of Democracy* 25, 3: 44–51. https://doi.org/10.1353/jod.2014.0045

22. Olga Onuch. 2015. EuroMaidan Protests in Ukraine: Social Media Versus Social Networks. *Problems of Post-Communism* 62, 4: 217–235. https://doi.org/10.1080/10758216.2015.1037676

23. Leysia Palen, Kenneth M. Anderson, Gloria Mark, James Martin, Douglas Sicker, Martha Palmer, and Dirk Grunwald. 2010. A Vision for Technology-mediated Support for Public Participation & Assistance in Mass Emergencies & Disasters. In *Proceedings of the 2010 ACM-BCS Visions of Computer Science Conference* (ACM-BCS '10), 8:1–8:12. Retrieved September 19, 2017 from http://dl.acm.org/citation.cfm?id=1811182.1811194

24. Katy Pearce. 2014. Two Can Play At That Game: Social Media Opportunities In Azerbaijan For Government And Opposition. *Demokratizatsiya* 22, 1: 39–66.

25. Robert Young Pelton. Kill the Messenger. *Foreign Policy*. Retrieved September 18, 2017 from https://foreignpolicy.com/2012/03/03/kill-the-messenger/

26. Serhii Plokhy. 2017. *The Gates of Europe: A History of Ukraine*. Basic Books, New York.

27. Andrii Portnov. 2016. How 'eastern Ukraine' was lost. *openDemocracy*. Retrieved September 18, 2017 from https://www.opendemocracy.net/od-russia/andrii-portnov/how-eastern-ukraine-was-lost

28. B. Reinicke, J. Cummings, and H. Kleinberg. 2017. The Right to Digital Self-Defense. *IEEE Security Privacy* 15, 4: 68–71. https://doi.org/10.1109/MSP.2017.3151324

29. 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: 515–531. https://doi.org/10.1080/10447318.2016.1177300

30. A. Ronzhyn. 2016. Social Media Activism in Post-Euromaidan Ukrainian Politics and Civil Society. In *2016 Conference for E-Democracy and Open Government (CeDEM)*, 96–101. https://doi.org/10.1109/CeDEM.2016.17

31. Saqib Saeed, Markus Rohde, and Volker Wulf. 2011. Analyzing Political Activists' Organization Practices: Findings from a Long Term Case Study of the European Social Forum. *Computer Supported Cooperative Work (CSCW)* 20, 4–5: 265–304. https://doi.org/10.1007/s10606-011-9144-0

32. United Nations News Service Section. 2017. UN News - Clashes near vital infrastructure in eastern Ukraine may have "grave" impact on population, UN warns. *UN News Service Section*. Retrieved January 8, 2018 from https://tinyurl.com/ybxtktsz

33. Bryan Semaan and Gloria Mark. 2011. Creating a Context of Trust with ICTs: Restoring a Sense of Normalcy in the Environment. In *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work* (CSCW '11), 255–264. https://doi.org/10.1145/1958824.1958863

34. Bryan Semaan and Gloria Mark. 2011. Technology-mediated Social Arrangements to Resolve Breakdowns in Infrastructure During Ongoing Disruption. *ACM Trans. Comput.-Hum. Interact.* 18, 4: 21:1–21:21. https://doi.org/10.1145/2063231.2063235

35. Damien Sharkov. 2017. Russia military bans Facebook as soldiers' battlefield selfies reveal secret locations. *Newsweek*. Retrieved December 21, 2017 from https://tinyurl.com/ya72lvyv

36. Irina Shklovski and Nalini Kotamraju. 2011. Online Contribution Practices in Countries That Engage in Internet Blocking and Censorship. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11), 1109–1118. https://doi.org/10.1145/1978942.1979108

37. Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '14), 2347–2356. https://doi.org/10.1145/2556288.2557421

38. Andrei Soldatov and Irina Borogan. 2017. *The Red Web: The Kremlin's Wars on the Internet*. PublicAffairs, S.l.

39. Kate Starbird and Leysia Palen. 2012. (How) Will the Revolution Be Retweeted?: Information Diffusion and the 2011 Egyptian Uprising. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (CSCW '12), 7–16. https://doi.org/10.1145/2145204.2145212

40. Borislav Tadic, Markus Rohde, Volker Wulf, and David Randall. 2016. ICT Use by Prominent Activists in Republika Srpska. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), 3364–3377. https://doi.org/10.1145/2858036.2858153

41. Zeynep Tufekci. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press, New Haven ; London.

42. Dmitry Volchek and Claire Bigg. 2015. Ukrainian bloggers use social media to track Russian soldiers fighting in east. *The Guardian*. Retrieved September 19, 2017 from https://tinyurl.com/o68ekz4

43. Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (SOUPS '10), 11:1–11:16. https://doi.org/10.1145/1837110.1837125

44. Volker Wulf. 1997. Storing and Retrieving Documents in a Shared Workspace: Experiences from the Political Administration. In *Human-Computer Interaction INTERACT '97*. Springer, Boston, MA, 469–476. https://doi.org/10.1007/978-0-387-35175-9_72

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

46. Volker Wulf, Kaoru Misaki, Meryem Atam, David Randall, and Markus Rohde. 2013. "On the Ground" in Sidi Bouzid: Investigating Social Media Use During the Tunisian Revolution. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work* (CSCW '13), 1409–1418. https://doi.org/10.1145/2441776.2441935

47. Zicong Zhou, Roja Bandari, Joseph Kong, Hai Qian, and Vwani Roychowdhury. 2010. Information Resonance on Twitter: Watching Iran. In *Proceedings of the First Workshop on Social Media Analytics* (SOMA '10), 123–131. https://doi.org/10.1145/1964858.1964875

48. 2015. Ukraine captures "Russian soldiers." *BBC News*. Retrieved January 7, 2018 from http://www.bbc.com/news/world-europe-32776198

49. 2015. The Avalanche that Went from Russia to Ukraine. *bellingcat*. Retrieved January 7, 2018 from https://www.bellingcat.com/news/uk-and-europe/2015/05/31/avalanche/

50. 2017. UNHCR Ukraine Refugees and Asylum Seekers, June 2017. *ReliefWeb*. Retrieved September 19, 2017 from https://reliefweb.int/report/ukraine/unhcr-ukraine-refugees-and-asylum-seekers-june-2017

51. Putin Claims Russia Was 'Forced To Defend Russian-Speaking Population In Donbass.' Retrieved September 18, 2017 from http://www.interpretermag.com/day-968/

52. Ukraine, Separatists Agree To Cease-Fire. *RadioFreeEurope/RadioLiberty*. Retrieved January 7, 2018 from https://www.rferl.org/a/ukraine-separatists-agree-cease-fire-christmas-new-years-holidays/27444120.html

53. UN Reports on Human Rights Situation in Ukraine - United Nations in Ukraine. Retrieved September 19, 2017 from http://www.un.org.ua/en/publications-and-reports/un-in-ukraine-publications/3592-un-reports-on-human-rights-situation-in-ukraine

54. Grey Zone: Eastern Ukraine Blockade. Retrieved January 7, 2018 from https://tinyurl.com/ycy6uazq