# Analyzing Security and Privacy Advice During the 2022 Russian Invasion of Ukraine on Twitter

Juliane Schmüser
juliane.schmueser@cispa.de
CISPA Helmholtz Center for Information Security
Germany

Harshini Sri Ramulu
harshini.sri.ramulu@uni-paderborn.de
University Paderborn
Germany

Noah Wöhler
noah.woehler@cispa.de
CISPA Helmholtz Center for Information Security
Germany

Christian Stransky
christian.stransky@cispa.de
CISPA Helmholtz Center for Information Security
Germany

Felix Bensmann
felix.bensmann@gesis.org
Leibniz Institute for Social Sciences
Germany

Dimitar Dimitrov
dimitar.dimitrov@gesis.org
Leibniz Institute for Social Sciences
Germany

Sebastian Schellhammer
sebastian.schellhammer@gesis.org
Leibniz Institute for Social Sciences
Germany

Dominik Wermke
dominik.wermke@cispa.de
CISPA Helmholtz Center for Information Security
Germany

Stefan Dietze
stefan.dietze@gesis.org
University Düsseldorf
Germany

Yasemin Acar
yasemin.acar@uni-paderborn.de
University Paderborn
Germany

Sascha Fahl
fahl@cispa.de
CISPA Helmholtz Center for Information Security
Germany

## ABSTRACT

The Russian Invasion of Ukraine in 2022 resulted in a rapidly changing cyber threat environment globally and incentivized the sharing of security and privacy advice on social media. Previous research found a strong impact of online security advice on end-user behavior.

Twitter is an important platform for sharing information in crises. We examined 306 tweets with security and privacy advice related to the Ukrainian war, and created a taxonomy of 224 unique pieces of advice in seven categories, targeted at individuals or organizations in Ukraine and elsewhere. While our findings include untargeted and generic advice known from previous research, we identify novel advice specific to the invasion, offers for individual consultation, and misinformation on security and privacy advice as a new threat. Our findings highlight the strengths and shortcomings of the security and privacy advice given online during the invasion and establish areas for improvements and future research.


*CHI '24, May 11–16, 2024, Honolulu, HI*

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642826

## CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing**;

## KEYWORDS

security and privacy advice, ukraine, twitter

**ACM Reference Format:**
Juliane Schmüser, Harshini Sri Ramulu, Noah Wöhler, Christian Stransky, Felix Bensmann, Dimitar Dimitrov, Sebastian Schellhammer, Dominik Wermke, Stefan Dietze, Yasemin Acar, and Sascha Fahl. 2024. Analyzing Security and Privacy Advice During the 2022 Russian Invasion of Ukraine on Twitter. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA*. ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3613904.3642826

## 1 INTRODUCTION

In the early hours of 24 February 2022, Russian President Vladimir Putin announced a "special military operation," launching a large-scale military invasion of neighboring Ukraine. A sudden change in the cyber threat environment accompanied this change in the global threat environment. The invasion was preceded and accompanied by intensified cyber attacks such as malware distribution, distributed denial-of-service (DDoS) attacks, phishing campaigns, and the use of surveillance software. Targets included the Ukrainian government, IT organizations, infrastructure, and the private business sector [67]. In addition, the invasion resulted in a heightened threat environment for companies outside Russia and Ukraine, with

fears that Russian state-sponsored threat actors and aligned cybercrime groups might target critical industries and organizations in the United States and other Western nations or that attacks may spread internationally like the NotPetya attack in 2017 [28] or the SolarWinds incident [4]. This change in threat level was highlighted by several advisories by national agencies, including from the US, UK, Germany, Canada, and Australia [8, 17, 21, 29, 60]. Global impact, high international attention, and direct involvement of multiple nation-state actors that committed cyberattacks with immediate physical consequences as part of their strategy in the conflict differentiate the invasion from previous crises discussed in the literature.

It also led to much security and privacy-related advice for the various affected groups being published on social media platforms and news pages. Similar to prior crises [7, 15, 44, 63, 78], Twitter was a widely used platform to share security and privacy information and advice or link to further resources for individuals and organizations in Ukraine, but also globally. However, the information and advice online were conflated with misinformation and rumors, such as one about Signal, an instant messaging platform, being hacked. Signal dismissed this as part of a coordinated misinformation campaign to encourage users to use less secure communication tools [79]. Hence, while security and privacy information and advice were shared on Twitter, assessing their validity and value seemed challenging. This paper examines the security and privacy advice provided around Russia's 2022 Invasion of Ukraine on the social media platform Twitter and identifies novel opportunities and challenges specific to security and privacy advice in times of war and conflict. This is especially relevant given the connection of cyber attacks, the success of their mitigation, and global physical consequences of the invasion. We base our research approach on the following research questions:

**RQ1.** *"What security and privacy advice was shared on Twitter related to the 2022 Russian Invasion of Ukraine?"* We are interested in what security and privacy advice was shared on Twitter between February and May 2022, primarily related to the heightened cyber threat from the invasion. Here, we analyze tweets and resources provided, such as linked documents and websites, and the targets of the advice, such as companies or individuals, including those in Ukraine and other directly or indirectly affected people.

**RQ2.** *"How does the advice compare to security and privacy advice shared in other contexts?"* By comparing our data with previous studies, we explore whether the advice around the invasion resembles or differs from security and privacy advice collected at different times and contexts. Additionally, we investigate the relationship between advice and its frequency in our data and evaluation and prioritization of advice in prior work. As far as possible, we seek to understand if and how the advice was tailored to the situation.

We create a taxonomy of 224 pieces of advice during the invasion. We find a wide range of advice in seven main categories, including messaging & social media, organizational policies, and meta-advice on sharing security advice. Next to generic advice found in prior research [73, 74], we identify novel advice specific to the invasion, individual support offers as a new, complementary form of advice distribution with unclear impact, and misinformation as a rising threat to security and privacy advice and protection.

This work is structured as follows: After this general introduction (Section 1), we discuss related work in the areas of security perceptions & behavior, social media & information sharing in crises, as well as security & privacy advice (Section 2). We describe our approach (Section 3) and highlight the findings (Section 4). We discuss our findings (Section 5) and conclude our work (Section 6). Finally, we provide information about our replication package in the Availability section.

## 2 RELATED WORK

We present and discuss previous work in three key areas: investigations into security-related user perceptions and behavior, research involving content on social media and information sharing in crises, and security or privacy advice for users. We also contextualize our contributions and highlight the novelty of our work.

**Influences on Security Behavior.** Prior work has investigated how security behavior is influenced in general and in vulnerable populations. Previous studies established connections between user behavior and the user's perception of risk [9, 10, 72], (security) fatigue [82], and social influence effects [31–34]. Factors influencing security decisions include the delivery of security measures to people [48], as well as negative experiences and general perception of and trust in security [96]. Further research into methods for influencing security behavior includes nudges and warnings. Previous studies conducted a literature assessment [2], and investigated security dialog attractors [16, 20]. Vulnerable persons and helpers are often the target of scams and phishing attacks during crises. Egelman et al. examined in a lab study with 60 participants the effectiveness of phishing warnings, finding that 97% participants fell for at least one of the phishing messages [37]. These prior studies on how security behavior is influenced inform our view on and discussion of the advice we collected.

**Social Media & Information Sharing in Crises.** Social media reactions to the events around the 2014 Russian annexation of the Crimea peninsula have been extensively investigated in research [77, 87], specifically, topics [58], hashtags [56], images [65], and memes [98]. Twitter and other social media are a common data source for research, including newcomers' experiences [18], audience perceptions [11], information sharing [25, 88], and rumors [102]. This includes specific user types such as journalists [55] or government departments [36]. Works specifically investigated information aggregation on Reddit [54], and Twitter posts around crises [63] and their comprehension [90]. Specific cases discussed include 2012 Hurricane Sandy [53], the 2013 Gezi Park protests in Turkey [64], and the 2015–2016 Zika virus outbreak [44]. The spread of misinformation during crises was studied concerning the emotional proximity of users [49], and about Russian influence operations within #BlackLivesMatter [7]. In the area of crisis research, multiple publications systematize previous work based on social media data [75, 76, 97]. Imran et al. surveyed the state of the art regarding computational methods to process social media messages and highlight their contributions and shortcomings [50].

Keyword-based filtering is the most dominant approach for retrieving tweets of a targeting topic. Approaches have been proposed for query expansion to improve the coverage of retrieval with synonyms [59], by extracting query terms from initial search

results [42] or Wikipedia and DBpedia [100]. Other works mined latent semantic similarity between the query and candidate terms by applying topic models such as LDA [45] or word embedding techniques [26], considering temporal and spatial information [24, 69, 86]. The TREC 2011–2015 microblog tracks provided datasets for microblog retrieval [91]. Similar to the aforementioned works, which partially used the TREC datasets, the TREC tasks focus on an entity-centric or user-centric search scenario. However, within practical data analysis scenarios, the search intent often reflects broader concepts or social science variables, e.g., "cyber security", or "climate", rather than actual entities [22, 41, 52]. Retrieval for such broader concepts, in contrast to entities such as "Ukraine", have no predetermined keywords, need to deal with the constantly evolving search space of micro posts (evolving at a pace of 8,000 tweets per second [39]), and have to consider an evolving vocabulary and underlying vocabulary drift [6]. Given these challenges, expert-curated seed list terms are still widely used for sampling tweets for social media mining [22, 41, 52] instead of the aforementioned methods. We build on this prior work by combining expert-curated seed lists with a semi-automatic, data-driven approach as described in Section 3.1.

**Security & Privacy Advice.** Previous research investigated security advice in the context of experts vs. users [19, 51], and for older adults [61]. Multiple publications investigated the adoption and impact of security practices [35, 40, 101]. Respondents' security advice sources were investigated in interviews [71] and surveys [68, 70], as well as specific advice for developers [1]. Herley postulates that by evaluating (security) advice solely on benefit, we have implicitly valued user time and effort at zero [46]. This becomes an important aspect in the light of recent studies, which find many advice pieces.

Tahaei et al. qualitatively analyzed 119 privacy-related accepted answers on Stack Overflow, extracting 148 pieces of advice [89]. Reeder et al. collected 152 pieces of advice by asking security experts for the top three recommendations they would give to non-tech-savvy users [74]. Redmiles et al. conducted a measurement study to identify 374 unique recommended behaviors contained within 1,264 documents of online security and privacy advice and evaluated the security advice in a user study with 1,586 users and 41 professional security experts [73]. Boyd et al. collected 41 safety guides distributed during Black Lives Matter (BLM) protests and surveyed 167 protesters, finding that many were unaware of key advice like using end-to-end encrypted messengers [15].

We compare our collection of pieces of advice and online documents shared on Twitter during the 2022 Russian Invasion of Ukraine to these prior studies and provide novel insights on what security and privacy advice is distributed during crises that directly impact the cyber threat environment.

# 3 METHODOLOGY

In this section, we provide an overview of our methodology for assessing online security and privacy advice related to the 2022 Russian Invasion of Ukraine, including data collection from Twitter and documents linked on Twitter in two phases, one covering spring 2022, and one covering February 2022 to February 2023. We also detail our data analysis, including the qualitative codebook and coding process, highlight our ethical considerations, and discuss the limitations of this work. Figure 1 provides an overview of our data collection and analysis procedure.

## 3.1 Data Collection

To gain insight into security and privacy advice shared around the 2022 Russian Invasion of Ukraine, we collected and analyzed 8,920 tweets for their relevance and examined 306 posts in detail for security and privacy advice. As we were especially interested in widely shared advice and resources, we studied public data on Twitter. Twitter has been successfully used to analyze the spread of information during crises in several prior studies [7, 15, 44, 63, 78]. We split our data collection into an exploratory and a verifying phase.

**Exploratory Data Collection Phase.** In the exploratory phase, we collected security and privacy advice and resources shared on Twitter during the 2022 Russian Invasion of Ukraine from February to May 2022. We collected the tweets using the official Twitter API for Academic Research [94] and Twitter Streams [95] using the Python library Tweepy [92]. The results were further enhanced by using the unofficial Twitter API and the Python library Twint [66], which allows scraping by hashtags. We compiled an exploratory list of search terms based on our experience[1] and preliminary manual searches for relevant content, to gather as many relevant tweets as possible. As we found more than 20 million collected tweets, we similarly devised a second, more restrictive list of prefiltering terms. The primary goal of using both lists was to explore a widely diverse set of security and privacy advice. We aimed for data diversity and not for completeness or generalizability of the data. Both the exploratory search term and prefiltering term lists are included in our replication package (see Availability section). Applying the prefiltering terms to our tweet collection resulted in 8,920 tweets we manually reviewed. Our manual review process consisted of two rounds: In the first round, we marked all tweets as security or privacy advice if at least one of two coders deemed it relevant. We discarded tweets that did not include or refer to security or privacy advice. In the second round, one coder reviewed if the remaining tweets mentioned Ukraine or the 2022 Russian Invasion of Ukraine in any way. A second coder crosschecked >10% of the tweets, finding no additional relevant tweets. After this manual filtering process, the exploratory data collection resulted in 232 relevant tweets. We extracted any links to external documents from these tweets, resulting in a total of 140 documents. Next, we analyzed both the tweets and the documents (denoted with prefixes T and D, respectively) as detailed in Section 3.2 and depicted in Figure 1.

**Verifying Data Collection Phase.** The second phase of our data collection aimed to verify that we had not missed any relevant topics or themes related to security and privacy advice. Therefore, we used a structured, semi-automatic, and data-driven approach to create search terms. Because some of the resources used for this method are only available in English, we focused on English search terms. We resorted to the long-term Twitter archive, which is the foundation of TweetsKB [39], and based on continuously capturing a data stream of a 1% random sample of Twitter [93]. To identify

[1]To provide context: We are information security and privacy researchers with more than ten years of experience and have worked on analyzing security advice in the past.

suitable search terms that were (a) indicative of relevant tweets for our topic and (b) prevalent in Twitter discourse, we applied a semi-automatic data-driven approach for generating seed lists of relevant terms. We identified three target keywords (*cybersecurity*, *advice*, and *recommend*) that jointly represent the topic under investigation and created corresponding regular expressions (cf. Appendix C) that we used to filter tweets from the TweetsKB archive from February 24, 2022, until February 23, 2023, for each target keyword respectively. We applied part of speech tagging on these three distinct sets of tweets and built four dictionaries of all proper nouns, verbs, and adjectives that co-occur with the target keyword. We discarded stop words and performed lemmatization for all terms in all four dictionaries. For each dictionary, for each entry, we calculated the semantic similarity between the pre-trained fastText word embeddings [38] of the entry and the respective target keyword by calculating the cosine similarity between the corresponding word embedding vectors. We set the similarity to zero if we found no word embedding in the pre-trained embeddings. We discarded all entries with a similarity lower than a similarity threshold set as high as possible while still obtaining sufficiently many terms. We ranked the remaining entries by frequency in their respective initially extracted tweet sets and selected each dictionary's top $n$ terms. N was selected to ensure a large number and variety of terms while excluding rare and irrelevant terms at the bottom. That resulted in three seed lists, which we then examined manually to filter out irrelevant terms and added missing relevant terms that were deemed relevant by domain experts given the exploratory data collection but may have been missing due to biases introduced by our target keyword selection. Finally, we merged the lists for *recommend* and *advice* as they reflect the same aspect of the investigated topic. Appendix C contains exact values of the similarity thresholds, $n$, the performed manual augmentations, and final term lists. We then translated all final terms to Ukrainian and Russian as well and queried the Twitter archive for tweets containing at least one term from each seed list and a reference to Ukraine or Russia implemented as a list of regular expressions (cf. Appendix C). This process resulted in 9,399 possibly relevant tweets between February 24, 2022, and February 23, 2023. We randomly selected a subset of 1,000 tweets for manual inspection of relevance by two independent coders, who determined if the tweets contained security or privacy advice and if they mentioned Ukraine or the 2022 Russian Invasion of Ukraine. The coders met to resolve any conflicts. This process added 74 relevant tweets to our data set, from which we extracted 32 additional linked documents. The tweets and documents were analyzed as detailed in Section 3.2 and depicted in Figure 1.

We found no additional topics or themes in the second phase. Hence, we assumed saturation and stopped the data collection.

**Language Distribution.** Previous work on the language diversity of Twitter tweets illustrated that English, Japanese, and Spanish are the top three languages for tweets [5]. We additionally analyzed the language diversity of the long-term Twitter archive TweetsKB [39] from February 24, 2022, until February 23, 2023. We found that 440,536,989 (30.86%) tweets were written in English, 4,889,877 (0.34%) tweets in Russian, and 1,822,011 (0.13%) tweets in Ukrainian. Correspondingly, Russian and Ukrainian tweets only play a tangential role and barely appeared in our exploratory data collection. For translation, we used automated translation tools and confirmed the quality of the results with a native speaker from outside the research team. We translated the list of search terms from our verifying data collection phase to Russian and Ukrainian and extracted potentially relevant tweets using the same process we used for English search terms. We found nine potentially relevant Ukrainian and two potentially relevant Russian tweets. We translated those tweets to English and coded them for relevance, leaving us with no Ukrainian or Russian tweets containing security or privacy advice. Thus, our analysis is based primarily on English-language tweets.

## 3.2 Data Analysis

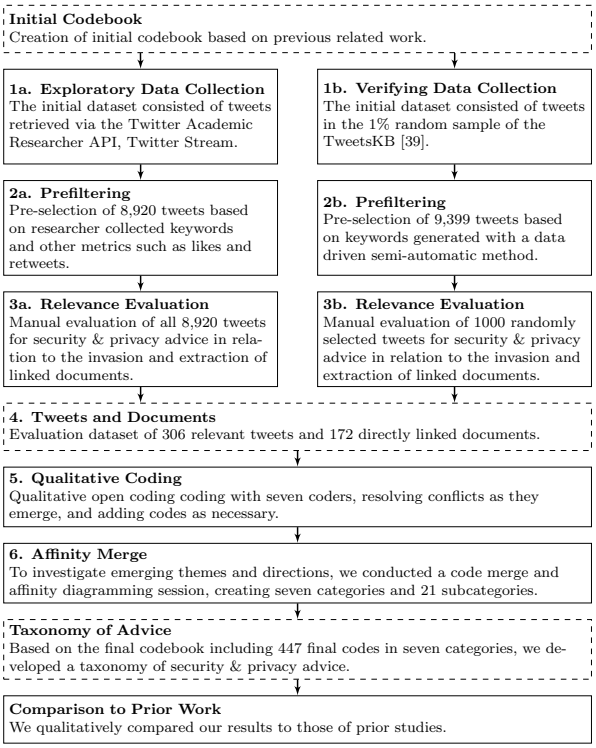


**Figure 1: Illustration of the data analysis pipeline. Based on the final codes, we created a taxonomy of security & privacy advice surrounding the 2022 Russian Invasion of Ukraine, and conducted a comparison with prior work.**

Our goal in analyzing the security and privacy advice was to create a taxonomy of the different types of advice shared during the invasion and to compare it to those prior work has found. To achieve this, we conducted a qualitative analysis of the advice.

We analyzed all collected tweets and documents in an iterative mixed coding approach [23, 27, 85]. All researchers created an initial codebook by categorizing codes from previous work that collected advice from Twitter data and other sources ([68, 73, 74, 101]). Using this initial codebook, each tweet and linked document was then coded by at least two of a total of seven coders. The coders resolved conflicts by consensus decision or expanding the

codebook inductively with new (sub)codes that emerged from the data. This approach does not necessitate the reporting of intercoder agreement because each conflict is resolved as it emerges, resulting in a hypothetical final agreement of 100% [57]. Our final codebook consisted of 458 unique codes. Eleven codes distinguished sources and targets of advice. Of the 447 codes referring to pieces of advice, 224 were assigned at least once. We kept unused codes from prior work at count zero for comparison.

To investigate emerging themes and directions in our codes, we used affinity diagramming [12] on the codes we assigned. In a collaborative affinity diagramming session with five researchers, we iteratively established seven categories and 21 subcategories. An overview is presented in Table 2. The resulting taxonomy can be found in our replication package provided in the Availability section.

To compare our findings with prior work, we manually matched our codebook to theirs. We qualitatively analyzed the top ten corresponding codes from each data set.

### 3.3 Ethical Considerations & Data Protection

Our institutions' ethical review boards did not require ethics approval for our study. However, ethical considerations are essential to the study design, analysis, and reporting when working with data during a crisis. Due to the potential of targeted threats from sophisticated attackers, we focused on ensuring that our reporting would not harm the population as a whole or particular individuals. As such, we do not report potentially compromising data. Out of ethical concerns, we decided against contacting people who live in a war zone or had recently fled one for interviews or other direct interaction to avoid imposing additional stress on recent refugees and focused on publicly available data instead [13]. We stored all data protected from unauthorized access by encryption and access control. While all data was public at the time of collection, we refrain from republishing it alongside this work to preserve people's privacy, control over how their identifiable data is shared, and their ability to delete their data. For reporting in the paper, we de-identified tweets by removing any personal information.

### 3.4 Limitations

Our work includes several limitations typical for this type of measurement study and should be interpreted in context. Given our data collection method, we may have missed some advice or types of advice. Even though Twitter data is commonly used during crises around the world [7, 15, 44, 63, 78] and gave us rich insights into advice targeted at those affected by the invasion, data obtained from Twitter may not be representative of all available advice sources, meaning that our data set may not fully represent the entirety of advice given in the context of the Ukraine war. To mitigate this risk, we only applied very broad filters to our exploratory data collection, and thereafter manually coded data points for their relevance. We conducted a second data collection phase to verify saturation. Additionally, we followed links to advice sources outside of Twitter and included these documents in our data set. Nevertheless, our analysis is qualitative, and generalizability to the entirety of advice cannot be assumed. As described above, we focused our work on tweets in English, introducing a potential language bias to our research. However, we consulted a native speaker to verify that we received useful results from automated translation tools, which we employed in our efforts to evaluate Ukrainian and Russian tweets. Given the prevalence of English on Twitter and the lack of relevant discourse in Ukrainian or Russian, we are confident to have obtained and analyzed meaningful data and can provide valuable and important insights into security and privacy advice shared on Twitter in the Ukraine war. Errors or misunderstandings may have occurred during our manual coding process. We minimized this risk by independently coding each tweet and document by at least two researchers and resolving any emerging conflicts. Finally, a quality evaluation of the advice was out of scope for this paper. Prior work shows that there is no established consensus among experts on what advice is considered important, good, or harmful [73]. In addition, the quality of advice is often relative to the context and situation of the recipient.

## 4 RESULTS

This section presents the results of our qualitative analysis of the final corpus of 306 coded tweets and 172 coded documents. The set of coded tweets has a median number of likes of 39 (sd: 4521) and a median number of retweets of 23 (sd: 2165). We first report on the taxonomy of the advice we created, detailing what advice was shared in connection to the invasion by and for whom (Section 4.1). Secondly, we describe the results of comparing our data to previously collected security and privacy advice and its evaluation (Section 4.2). Given our qualitative methodology, assigned code counts provided in figures and tables in this section and in the appendix are purely descriptive of our sample. They cannot be generalized to the entirety of security and privacy advice shared in the context of the invasion.

### 4.1 Analysis of Advice

Our analysis identified five types of advice sources and distinguished between advice targeted at individuals and organizations. We present an overview in Table 1.

Below, we present our findings in detail. The reporting follows the categories and subcategories of advice we identified through affinity diagramming (see Table 2). For each category, we analyzed advice for individuals and recommendations made to companies and organizations. Where possible, we distinguished between advice directed at individuals or organizations in Ukraine or a specific other country or region. Advice for individuals most commonly did not have a particular audience and was otherwise about evenly distributed between individuals in Ukraine and people elsewhere. Very few resources directly addressed particular groups of individuals, such as people in the conflict zone, journalists, activists, or people looking to donate. About half of the advice targeted at organizations was directed at specific countries or regions, most of which were not Ukraine but the U.S. and its NATO allies. Figure 2 shows an overview of assigned code counts. In cases where the advice for target groups was very similar, we merged the reporting to avoid repetition. In addition, we provide noteworthy insights on advice sources where appropriate.

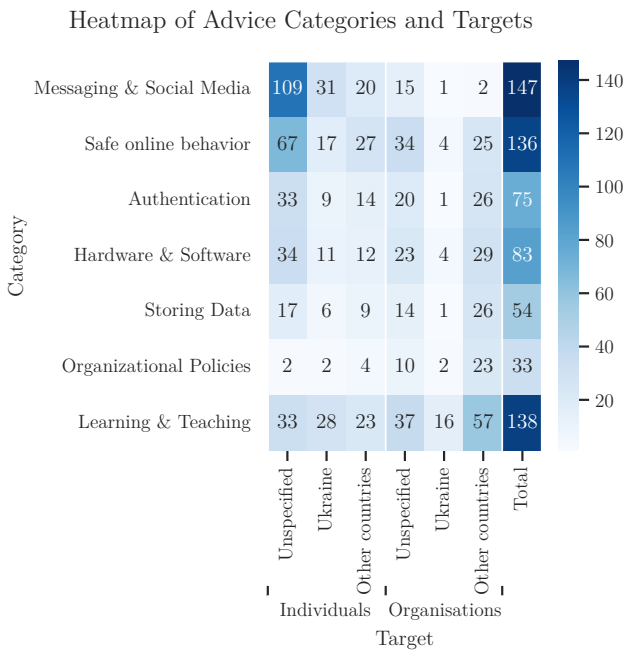


**Figure 2: Heatmap of code categories and the number of times they appeared in advice resources, differentiated by the target group.**

**Table 1: Summary of advice we found, grouped by sources and targets.**

| | Target | | | | | | |
|---|---|---|---|---|---|---|---|
| | Individuals | | | Organizations | | | |
| **Source** | Unspecified | In Ukraine | Other Country | Unspecified | In Ukraine | Other Country | **Total** |
| Company | 37 | 11 | 5 | 21 | 7 | 11 | 70 |
| NPO | 33 | 14 | 9 | 4 | 1 | 8 | 54 |
| Government | 17 | 3 | 9 | 19 | 1 | 39 | 71 |
| News | 36 | 11 | 17 | 20 | 3 | 15 | 80 |
| Individual | 79 | 30 | 17 | 37 | 8 | 15 | 151 |
| **Total** | 197 | 68 | 56 | 97 | 19 | 90 | 478 |

*4.1.1 Messaging & Social Media.* The most considerable portion of advice targeted individuals and dealt with their social lives online. However, most of this advice did not specify a target audience. For the resources that did, more targeted people in Ukraine than outside of it. We identified three key areas of advice on this topic: recommendations regarding secure instant messaging, advice on social media profiles and sharing practices, and pointers regarding misinformation. While some resources also addressed organizations, none gave them this type of advice.

**Secure Messaging.** Recommendations regarding (secure) instant messaging was a category of advice that had a specific target audience more often than most other advice categories. It was directly given to people in Ukraine more often than people in other countries. The recommendations focused on applications one should or should not use, with many resources advocating for or against using at least one specific application. They mainly originated from non-profit organizations (NPOs), news outlets, and individuals and mentioned 13 applications. Some resources warned that phone and SMS services were insecure and not private. Signal and WhatsApp were generally endorsed as secure, but there were also claims of insecurities that both companies called out as false. One individual tweeted that *"@WhatsApp seems to be monitored by Russians,"* (T2745) to which WhatsApp said in their Twitter thread on the Ukraine war that *"As always, your personal messages and calls are protected with end-to-end encryption by default so they cannot be intercepted by any government."* (T4048) Similarly, there were claims that *"Signal Russia has been breached."* (T2766) Signal promptly refuted this: *"This is false. Signal is not hacked. We believe these rumors are part of a coordinated misinformation campaign meant to encourage people to use less secure alternatives."* (T2763)

Telegram was the most discussed application. All advice related to Telegram mentioned risks associated with the default settings of the application, which do not enable encryption of messages. Several also pointed out prevalent user misconceptions regarding this setting, e. g., that through *"misleading marketing and press, most people [in Ukraine] believe it's an encrypted app,"* (T2757) with one person taking it one step further claiming *"that branding may literally cost lives."* (T2745) Outside of highlighting the risks of using Telegram, a few news resources discussed the importance of the app in the distribution of information in Ukraine, both from individuals and government channels, stating that the uses may outweigh security concerns. Unfortunately, only one document provided a step-by-step guide to turning on encryption for chats in Telegram.

In general, the most frequently recommended feature for secure instant messaging was (end-to-end) encryption, followed by self-destructing messages, for which some companies specifically posted guides on how to turn them on. Peer-to-peer messaging applications were promoted as a means of communication in case of internet shutdowns or outages.

**Advice for Social Media.** The advice around social media profiles and sharing practices centered on privacy and controlling what information people share with whom. Individuals and social media companies were the primary sources for this advice; the latter predominantly shared feature descriptions and usage guides for their products. Several resources recommended that people review their privacy settings or tighten visibility on their content. To this end, Meta introduced a region-bound new feature for locking Facebook profiles and hiding their content from the public, which was recommended multiple times. For Twitter users, deactivating their profile to hide old content was suggested. The measures were recommended to anyone in contact with people *"in Ukraine to help protect people from being targeted,"* (T4053) and revealed a general concern that private information already available online may now lead to physical harm.

Advice on sharing practices called for awareness of what is shared. It extended from cautioning against posting sensitive information to war-related specifics, e. g., location information, and its

potentially damaging role in military strategies was a focus. *"Everyone is a target. DO NOT share locations of military operations in #Ukraine in real-time."* (T8925) Accordingly, people were asked not to add metadata to posts, to remove metadata from previous posts, and not to live-tweet. One news article as well as one individual, warned people against sharing videos or pictures of prisoners of war, *"which some experts have argued violates the Geneva Conventions."* (D112)

**Beware of Misinformation.** Misformation was a common topic related to war news and information shared online. Many resources warned that wrong information was frequently shared and must be watched out for, with several specifically mentioning Russian disinformation. While most resources left it at this rather generic warning, some questions for spotting fake claims, such as *"Does it look like Ukraine? Does it look like February time?"* (T1004) could be found, along with the advice not to share anything one had not verified. Some resources recommended reverse image searches to quickly find out if material had been put online previously in other contexts, and a few resources recommended reporting accounts that shared fake information to combat its spread.

**Key Insights: Messaging & Social Media**

- Secure messaging advice focused on the usage of specific applications and was directed at people in Ukraine comparatively often.
- Social media advice focused on features to protect private information.
- Warnings about misinformation were common but often generic.

*4.1.2 Safe Online Behavior.* Most of the advice was on safe online behaviors and being careful with trust online. We divided this advice into three subcategories: phishing, malware, and connections & anonymity. Most of this advice targeted individuals, while some resources addressed organizations and companies. About half of the advice had a specific target audience, with advice for individuals being addressed to both people in Ukraine and elsewhere, while advice for organizations was almost exclusively given to organizations from other countries.

**Phishing.** Phishing was widely considered a significant threat that would become more prevalent as scammers tried to profit from the war, with many resources calling for heightened vigilance of people and organizations. The advice for both groups, in Ukraine and other countries, was very similar, with companies being additionally told to spread the advice to their employees. Most advice came from government institutions, companies, and news outlets.

The most general advice included thinking before clicking, not clicking links from unknown sources, watching out for phishing, and being suspicious of, e. g., unknown people, popups, requests, and things that are too good to be true. Several resources advised to report any phishing attempts to authorities, and some resources cautioned against revealing personal information unless one was certain who was receiving them.

Many resources regarded emails as the most likely medium for phishing. Most generally said to be alert to phishing emails, focusing on links and senders as security-critical elements. Aside from email, resources warned about phishing through instant messages and social media platforms.

**Malware.** We found that a rise in the threat of malicious software was widely reported due to the war. Both individuals and organizations were warned about this threat in very similar ways, and most of the warnings originated from news articles and government institutions, with the latter mainly targeting organizations and companies. Only very few of these resources explicitly addressed people or organizations in Ukraine.

Several resources only generally mentioned malware as a risk to be aware of without providing mitigation strategies. The others focused on two main ways malware could be introduced to a system: email attachments and installing software. The general advice of only installing software from trusted sources was extended in multiple ways specific to the crisis at hand. About half of the resources discouraged the usage of software that came from Russia. A prominent example that most of them referenced was security software from the Russian provider Kaspersky, which multiple Western government agencies spoke out against, recommending *"replacing applications from Kaspersky's portfolio of antivirus software with alternative products over doubts about the reliability of the manufacturer."* (D42) Two resources asked people to beware of offers providing free software, like VPN services, pointing out that scammers may exploit people's acute need for such services to plant malicious software. One news article described how scammers also exploited people's wishes to help Ukraine by *"promot[ing] a fake DDoS tool on Telegram that installs a password and information-stealing trojan."* (D9) This article and one Twitter user generally discouraged people from participating in cyber attacks, as they are illegal and can be a significant risk, especially to non-experts.

**Connections & Anonymity.** Advice regarding internet connection safety and anonymity on the network appeared in many resources, most of which targeted individuals, notably individuals in Ukraine, as often as people in other countries or having no specific audience. Only very few resources directed advice at organizations, with no remarkable differences in the advice for individuals.

A majority recommended using specific types of software to secure connections and preserve privacy. The most common were VPN services. Some of these were advertisements from a company providing VPN services. The others originated from NPOs, news outlets, and individuals. They described two different use cases of VPNs. One was to circumvent local censorship, telling people to *"set up VPN services to help you access blocked sites during a partial [internet] shutdown."* (D129) One person explained how they used *"a VPN to a Western State to avoid Russian censorship."* (T2893) The other was to secure communications and preserve anonymity, explaining that *"When configured correctly, a VPN will secure all of your communications from local interception,"* (D140) and *"It hides your IP address and your location. It also encrypts your data after leaving your device and traveling to whatever website you're visiting."* (D69) Another software that NPOs, news outlets, and individuals commonly recommended for online anonymity was the TOR browser. It was seen as a tool to circumvent censorship, with one user tweeting *"Tor is a means of accessing truth safely. Tor is the equivalent of hidden atenas [sic] in the WWII."* (T6901) Several tweets drew attention to

a particular project offering an uncensored, privacy-protected way to browse Twitter using Tor.

Additionally, it was recommended to turn off network features, including WiFi, mobile internet, and Bluetooth, whenever they were not used, as they may still disclose one's location. A situation-specific advice that appeared twice was to hide Star Link ground stations Ukrainians received to ensure internet access and use them sparingly, as they might become targets for military attacks.

**Key Insights: Safe Online Behavior**

- There were many warnings about intensified phishing and malware distribution but few actionable imperatives.
- To preserve confidentiality and anonymity, VPNs and Tor Browser were common suggestions.

*4.1.3 Organizational Policies.* We found several resources advising about policies that only applied to organizations, targeted again majorly at organizations in Western countries, and grouped them into two categories: incident response and recovery plans and access and network policies. About two-thirds of the resources gave advice coming from government organizations.

**Incident Response & Recovery Plans.** Most resources that dealt with organizational policies contained information about responding to security incidents and having plans for recovery from such incidents. Of these, multiple recommended developing an incident response plan or advised to verify that a plan existed and was up to date. Regarding the plan's content, some resources said it should be known and actionable, and some stressed the importance of having contact information for essential personnel available. A few resources mentioned that routes of an incident response plan should be accessible even if systems had been shut down. Some resources suggested practicing the response plan in the organization, i. e., the US agency CISA recommended to *"Conduct a tabletop exercise to ensure that all participants understand their roles during an incident."* (D89)

**Access & Network Policies.** A majority of resources made recommendations regarding access control and network policies. Several resources advised that the principle of least privilege access should be followed for internal access. Keeping track of authorization and timely removing leavers' and unused accounts was also recommended. In addition to general network security measures, the US agency CISA included isolation and extra careful inspection of traffic from Ukrainian organizations and blocking activity from VPN or Tor connections in their situation-specific recommendations.

**Key Insights: Organizational Policies**

- Advice focused on up-to-date, properly communicated incident response and recovery plans.
- Isolating networks and strict authorization were recommended defenses.

*4.1.4 Learning & Teaching.* Advice on the usage and distribution of security information, learning, and teaching was prevalent in our data collection, as various entities offered, referenced, and commented on advice resources, targeting individuals and organizations in Ukraine and elsewhere. They had diverse sources, the most common being government agencies and individuals, followed by NPOs and companies. We identified four subcategories: meta advice about sharing security advice during crises, awareness and resources, learning, and building a threat model.

**Recommendations for Sharing Advice During Crises.** Some of the tweets dealt with sharing security advice during crises, wherein the authors gave other professionals who may want to share advice guidance on how to prioritize classes of advice and what topics or phrasings to avoid. A few authors of advice resources asked that the readers pass on the advice to friends and family. Advice givers should do their due diligence and refrain from recommending single tools while drastically overstating their efficacy concerning security or privacy, especially during the current situation in Ukraine. One Twitter user pointed out that giving digital security advice was a major responsibility and that *"[one should not] encourage people to entrust their safety to one thing. Especially not in conflict."* (T504)

In line with this, some resources encouraged others to give realistic as well as actionable advice that takes into account that security and privacy priorities may be different for people in Ukraine and that is more specific than, e. g., following all the advice that has been reiterated for years. Correspondingly, one individual focused on actionable advice and called on companies to prioritize a fast roll-out of basic security measures in the face of emerging cyber threats: *"We need to make things BETTER, NOW! We can tweak and harden later when we have the basics deployed."* (D112) Multiple resources, which were shared mainly by companies citing government institutions or by government institutions themselves, also recommended that companies raise awareness for increased risks by, e. g., performing employee training. However, the resources mainly pointed to conveying current security best practices without going into further detail.

**Awareness & Resources.** Many resources did not offer advice but rather raised awareness for resources provided by others. Several resources offered help in the form of technical guidance or support, often directly to Ukrainian companies. Government institutions were most notable here, followed by fellow companies and NPOs. For the former, this took the form of, e. g., accepting forwarded websites, emails, and texts to support Ukraine by not falling victim to attacks (T8889). Companies offered free services like firewalls and VPNs. Offers for individual consulting on security were common as well. In some resources, the advice givers warned that *"there'll be well-intentioned twitter connectivity advice. Some great. Some not."* (T504) Others reported advice they had come across that might be impractical or even actively damaging to the individual's or company's security: *"[...]Lots of great info but please don't follow their mitigation advice for ICS. It's not practical & in some cases dangerous."* (T617)

A few resources advocated that companies and organizations follow current best practices in security without giving specifics, and some government institutions set up newsletters for companies to receive updates on emerging threats and advisories. In contrast to the efforts around offering support, two Twitter users told companies and organizations that the steps to protect from cybercrime had not changed: *"Contrary to the marketing emails that'll flood your inbox in the coming days inviting you to a webcast on how to protect against Russian attacks, the measures to protect your org haven't changed a bit since the war started."* (T3978)

**Learning.** General advice related to learning about security appeared in a couple of resources.

Staying up-to-date with security and privacy developments and to keep learning was shared in documents from companies, NPOs, government institutions, and news sites. D139, as a security guide for journalists, is an example of a learning resource that became highly applicable again in light of the invasion. It dedicates an entire section to technology security in conflict areas, ranging from threat modeling and secure communications over mobile device security to malware, data integrity, and secure credentials. Written by a NPO with a target group of journalists in general, it was shared again on Twitter by the NPO, specifically mentioning reporters in Ukraine.

A few documents, mostly targeted at companies, endorsed learning and getting advice from security experts and professionals. In two, government institutions pointed to their services, while a news site indicated urgency but stayed vague: *"If you don't have a competent security team to help (and most don't), you absolutely must find a reputable security partner immediately."* (D17)

**Threat Modeling.** In multiple resources, advice on building threat models as a foundation for choosing security advice to apply appeared. It was a category with notable distinctions between advice targeted at individuals and advice for organizations.

Of the advice targeting individuals, the majority generally recommended considering threats when making security choices and came from individuals and NPOs. More specific pointers, such as that ordinary people may be targeted by advanced persistent threats or scammers and bots, were rare and mainly came from news outlets and government institutions. One individual stressed: *"To a human scammer or a bot, they/it don't care who you are, you're just a vulnerable victim. Practice safe computing."* (T4098)

For organizations, general pointers to think about threats were less prevalent. Instead, most of the resources were more specific, with several referring to advanced persistent threats and some to the software supply chain as a potential attack vector, scammers and bots, and overseas attackers. Most of this information originated from government institutions and was shared by news, individuals, NPOs, and the government itself.

**Key Insights: Learning & Teaching**

- Several resources called for giving advice responsibly and making it actionable.
- Offers for free individual support and consulting were extended to affected people and organizations.
- There was a disagreement between people calling for immediate measures and people saying the measures had not changed.
- Having a threat model was sometimes recommended, but there was no actionable guidance on prioritizing advice.

*4.1.5 Other Advice Types.* Finally, we aggregate findings of the three remaining advice categories: authentication, hardware and software, and storing data in this section.

**Authentication.** Advice on authentication targeted individuals and organizations without notable distinction between regions and commonly originated from government agencies, companies, and individuals. It mostly concerned passwords and multi-factor authentication (MFA). For passwords, most resources recommended strong passwords or password policies, often with no specific criteria for what makes a password strong. Advice further mentioned using unique passwords and password managers: *"Have a strong, unique password that you store in a password manager."* (D124) Advice to enable MFA was common from companies operating services that offer MFA. Government institutions advised organizations to enable or enforce MFA, especially for privileged accounts. One tweet addressed the general public: *"Implementing multi-factor authentication on your accounts makes it 99% less likely you'll get hacked."* (T1138) In this case, the exaggerated claim of effectiveness might be an attempt to increase adoption, although data from Microsoft support it [3].

**Hardware & Software.** Advice related to hardware and software mainly consisted of recommendations to apply updates and security patches, to use security software such as anti-virus applications, and to lock devices. Resources recommended regular updates and installation of security software to individuals and organizations alike, suggesting automatic updates, and conveying a sense of urgency: *"I cannot emphasize enough. Everyone, all your companies, all your phones, everything, update your virus protection and download your security patches IMMEDIATELY."* (T4064) Device security advice often addressed individuals in Ukraine and Russia. While some of it only generically recommended locking devices, other resources detailed how to disable biometrics to prevent police from using one's finger or face to unlock a device without consent. In addition, some resources advised turning off location services and other connectivity features to disable device tracking.

**Storing Data.** Backups were the most prevalent topic in advice on storing data. The recommendations for organizations were mostly tailored to professional data handling, suggesting to test backup and restore processes and isolate backups from the network: *"Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections."* (D89) By contrast, backup advice for individuals was more diverse and often focused on specific actions rather than a broader strategy. Examples include *"Scan or take photos of all important docs and send them to your own email account."* (T534) Advice on data storage also included recommendations for logging key functions, network activity, authentication activity, personnel information access, and security-enabled group changes in organizations. Finally, mainly NPOs advised mostly individuals in Ukraine to prevent unwanted access to data by minimizing how much data was stored and encrypting stored data.

**Key Insights: Other Advice Types**

- Authentication advice focused on strong passwords and MFA.
- Advice on software primarily addressed anti-virus software and updates.
- Device security was centered around preventing unwanted access and tracking.
- Advice on storage focused on preservation and access control, and had a stark contrast between professional strategies for organizations and quick-and-easy actions recommended to individuals.

## 4.2 Comparison with Prior Work

To answer our second research question, we compare our findings for advice targeting individuals to those of two other papers that have investigated this kind of advice sharing: Reeder et al. collected advice by asking experts to name the top three pieces of advice they would give non-tech-savvy users in 2017 [74], Boyd et al. investigated advice shared on Twitter in the context of the BLM protests in 2020 [15]. Additionally, we evaluate the advice from our data collection that was targeted at individuals using data from Redmiles et al. on advice priority as well as uselessness and harmfulness of advice [73]. While we use the top ten pieces of advice for the comparison to focus on advice that was frequent in the respective data sets, we note that neither our nor the related work's sample generalizes to the entirety of advice. The comparison is meant to highlight similarities and differences in advice content, and not draw quantitative conclusions.

*4.2.1 Comparing Data Collections.* In this section, we present the comparison of our data to that of prior work. The top ten most frequent pieces of advice from each data set can be found in Table 3.

**Advice for Non-tech-savvy Users.** In their analysis of advice for non-tech-savvy users Reeder et al. collected and coded 231 expert responses for the advice they contained, using 152 unique codes. Of these, 56 match codes from our codebook. All pieces of advice from their top ten were present in our data collection. Our top ten pieces of advice included their top four and one other of their pieces of advice. Of our top ten pieces of advice, those on misinformation, pointers to support with cyber security, insecurity of Telegram messenger, and VPN usage were not part of the data collected by Reeder et al.. The similarities between the two sets of advice, especially in how they contain a high number of individual pieces of advice, show that the authors call for a limited, prioritized set of advice to provide to end users has not been answered, even though it could have been beneficial during the invasion.

**Advice Shared in the Context of BLM Protests.** Of the 193 unique codes Boyd et al. assigned, only 26 matched codes in our codebook, which in part stems from them coding specifically for rationales of advice, while we did not. Of our top ten pieces of advice, only two occurred in their data. Of the advice that matched, all that belonged to the top ten during the BLM protests were present in our data collection, but only one was among our top ten most frequent pieces of advice, with the others having low counts in our data collection. Despite the overall differences, it is noteworthy that most of the top ten pieces of advice during the BLM protests come from categories more often directly addressed at people in Ukraine in our data set than others: secure messaging, online anonymity, and device security. This suggests that the two events and the corresponding advice were considered similar for individuals in dangerous positions while varying drastically in international scope and impacting companies and organizations.

**Key Insights: Comparing Data Collections**

- The most frequent advice in our sample was similar to that Reeder et al. found for non-tech-savvy users.
- There were few similarities between the advice around the invasion and that shared during the BLM protests.

*4.2.2 Evaluation of Advice.* In their paper "A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web", Redmiles et al. provide detailed insights into how end users and security experts evaluate security advice for end users from internet sources [73]. We mapped 241 pieces of advice from their data set to 458 of our unique codes. 102 of their advice imperatives matched one of our 224 assigned codes that refer to advice content. An overview of the top ten pieces of advice can be found in Table 4.

**Priority Rankings.** With their replication package, Redmiles et al. provide separate priority rankings of advice for expert and end-user evaluation, which combine their more fine-grained ratings. We analyze the overlap and differences in the top ten advice pieces from each of the rankings and our sample (see Table 4).

Nine out of the top ten advice pieces from the expert ranking were present in our data collection. Two of them, namely *"Use different passwords for each account"* and *"Use strong passwords"*, were among our top ten most frequently shared advice.

Seven of the top ten advice pieces from the user priority rankings occurred in our data collection, albeit in much smaller quantities than those from the expert rankings. None could be found in our top ten most frequent pieces of advice.

In our top ten advice pieces, six were rated by users and experts. As expected, given the description above, they have relatively high ranks in the expert ranking, with the highest being first and the lowest at rank 53. By contrast, they are spread out through the user ranking, with the highest at 22 and the lowest at 190. The other four top pieces of advice deal with misinformation, instant messenger recommendations, and pointers to sources of support. These topics are notably absent from the data Redmiles et al. collected via user search queries and expert recommendations for advice sources in 2017. The low ranks in the user ranking, which Redmiles et al. based partly on user-perceived actionability of advice, aligns with our general finding that advice we collected was often very generic.

**Key Insights: Evaluation of Advice**

- Advice that frequently appeared in our sample was given high priority by experts in the study of Redmiles et al. [73].
- Much of the advice frequent in our sample scored low on a user priority ranking based on, i.e., perceived actionability and time consumption.

# 5 DISCUSSION

We analyzed 306 tweets and 145 linked documents shared around the 2022 Russian Invasion of Ukraine regarding the security and privacy advice they contained. In 224 unique pieces of advice, we found a large variety of recommendations that five different types of sources gave to individuals and organizations. We derive the following discussion points from our findings, illustrate their novelty and significance, and make actionable recommendations for researchers, organizations, and future work:

**Contextualizing our Findings.** Our work provides novel insights into security and privacy advice shared during war and conflict. Previous work focused on general security and privacy advice for end-users [73, 74] and in the context of political and social movements [15]. They did not investigate the specifics of a crisis like the 2022 Russian Invasion of Ukraine, which had global effects,

attracted high international attention, and had direct involvement of multiple nation-state actors that used cyberattacks with immediate physical consequences as part of their strategy in the conflict. While much of the security and privacy advice shared in general or during political and social movements was also present in this context, we identify novel advice content and dissemination channels specific to the 2022 Russian Invasion of Ukraine that are not discussed in previous work. Extending the call for general advice prioritization [73], we find that extraordinary circumstances call for tailored guidelines, yet advice shared concerning the invasion was rarely specific to times of war and conflict. We identify individualized support offers as a promising new avenue to be further investigated. We find that next to being a generic threat, misinformation on security and privacy advice can introduce immediate security and safety risks to individuals and organizations during war and conflict.

**Specific Security and Privacy Advice Needed in Times of War and Conflict is Rare.** While prior work finds a general lack of security and privacy advice prioritization [73, 74], our findings highlight how advice is not more specific or tailored to the target audience even in times of war or conflict, which poses multiple risks and necessitate different measures than other situations. The 2022 Russian Invasion of Ukraine has significantly altered peoples' and organizations' digital security and privacy protection resources. Like other high-stress situations, security and privacy compete with different needs such as physical and financial safety [30, 80]. However, in cyber warfare, they also directly influence these. The few war-zone-specific guidelines we found highlighted the intersection between digital security and physical safety through, e.g., warning about the location of targets by transmissions of people's devices or recommending the protection of power plant networks to avoid destruction of critical infrastructure through cyberattacks. Protection during war is vital and time-critical, yet we found more pieces of advice than people can be reasonably expected to process or implement, and most of them were generic and unactionable despite claiming relevance to the invasion. The many different actors who posted this advice largely appeared well-intentioned but contributed to a flood of unsorted information with the potential to drown out any specific shared security and privacy guidelines. This finding demonstrates a need for effective, actionable, and comprehensive guidelines with specific advice adapted to war or conflict situations that people and organizations can turn to and share. We recommend developing such guidelines by collaborating with security and privacy researchers and experts on safety and security in times of war and conflict, involving people with first-hand experience. One example of tailored advice that could be adapted to other target groups is guidelines for journalists in conflict zones, such as chapter four of D140 [81].

**Individual Security and Privacy Consultation and Support Offers as a New Type of Advice.** In addition to written security and privacy advice in tweets and guidelines, we identified offers for individual security and privacy consultation and support by governments, non-governmental and private organizations, and individuals. While this advice has not been discussed in the security and privacy research literature, individual consultation and support offers are an exciting complement to broadcasting written security and privacy advice and guidelines. We did not further evaluate the quality and value of these offers to avoid drawing resources from organizations or burdening providers and recipients during the war. However, we believe such offers could have both the potential to effectively address the security and privacy needs of organizations and individuals, and drawbacks such as limited scalability or varying quality. Therefore, we recommend future work to investigate the availability and quality of such offers, as well as the specific needs and expectations of their recipients.

**Security and Privacy Misinformation is a Threat.** Misinformation and its dissemination via social media has been studied before [47, 49, 83] and is often one of the first weapons deployed in a war [14]. However, our findings provide novel insights for incorrect and misleading security and privacy advice in times of war and conflict and its potential impact on the cyber- and physical security of people affected by the 2022 Russian Invasion of Ukraine. In times of war or conflict, it is particularly critical to identify misinformation [49, 84]. Given the potentially disastrous consequences of implementing incorrect security and privacy advice in times of war, distinguishing misinformation from legitimate and helpful advice is even more critical. For example, the claim that the end-to-end encrypted Signal messenger was breached (T2766) at the beginning of the 2022 Russian Invasion of Ukraine aimed to confuse Ukrainian Signal users and push them toward using less secure messaging apps such as Telegram [62]. Telegram is less secure, not end-to-end encrypted by default, and allows attackers to track the real-time geolocation of any Telegram user [99]. This example illustrates the potentially life-threatening consequences of following misinformation in times of war. Unfortunately, our data set also included multiple pieces of conflicting security and privacy advice, contributing to user uncertainty. While very few resources discussed the existence of bad or false security and privacy advice, many generically warned about misinformation on the war. However, few provided strategies to mitigate the challenges around misinformation or how users can verify legitimate information [43]. While identifying misinformation is generally challenging, the time-consuming verification of information details and sources or reverse-searching images is even more unlikely to be adopted in times of war or conflict. Based on our findings, we make multiple recommendations: Our community should put more effort into better understanding the impact of security and privacy misinformation on end-user security and privacy in crises and conflicts, as well as developing mitigation strategies and technologies. Platform providers like Twitter (now X) should continue fighting misinformation dissemination to protect their users better. Trustworthy actors such as governments or non-governmental organizations should develop and disseminate adequate, easy-to-understand security and privacy advice tailored to particular situations.

## 6 CONCLUSION

We studied security and privacy advice that was shared around the 2022 Russian Invasion of Ukraine. Specifically, we analyzed 306 tweets and 172 linked documents using qualitative open coding. We distinguished advice targeted at individuals and organizations, as well as five types of sources: companies, NPOs, government agencies, news outlets, and individuals. Using affinity diagramming,

we created a taxonomy containing 224 unique pieces of advice, clustered into seven categories. We then compared our findings to those of three prior studies, confirming findings in previous work and identifying topics and phenomena novel to the 2022 Russian Invasion of Ukraine. Unfortunately, we confirmed previous findings that overwhelming amounts of advice are shared and labeled high priority. In addition, we found novel advice specific to the invasion and offers for individual support and consultation with unclear impact on the security and privacy of recipients. Security and privacy misinformation aimed to degrade the security and privacy of individuals and organizations to make them easier targets for cyberattacks. We recommend the development of effective, actionable, and comprehensive guidelines with specific advice adapted to times of war or conflict, further exploration of individualized support offers for security and privacy, and investigation of the impact and mitigation of security and privacy misinformation.

## AVAILABILITY

To support the replication and transparency of our work, we make our study material available at https://osf.io/uc2gm/?view_only=925b38062eac4530a1b97c7f01ad6e9a. It includes the search queries we used for data collection and the full taxonomy.

## REFERENCES


[1] Yasemin Acar, Christian Stransky, Dominik Wermke, Charles Weir, Michelle L Mazurek, and Sascha Fahl. 2017. Developers need support, too: A survey of security advice for software developers. In *2017 IEEE Cybersecurity Development (SecDev)*. IEEE, Cambridge, MA, USA, 22–26. https://doi.org/10.1109/SecDev.2017.17

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 1–41. https://doi.org/10.1145/3054926

[3] Alex Weinert. 2019. Your Pa$$word doesn't matter. https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/your-pa-word-doesn-t-matter/ba-p/731984. Accessed 2022-08-18.

[4] Rahaf Alkhadra, Joud Abuzaid, Mariam AlShammari, and Nazeeruddin Mohammad. 2021. Solar winds hack: In-depth analysis and countermeasures. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, Kharagpur, India, 1–7. https://doi.org/10.1109/ICCCNT51525.2021.9579611

[5] Thayer Alshaabi, David Rushing Dewhurst, Joshua R. Minot, Michael V. Arnold, Jane L. Adams, Christopher M. Danforth, and Peter Sheridan Dodds. 2021. The growing amplification of social media: measuring temporal and social contagion dynamics for over 150 languages on Twitter for 2009–2020. *EPJ Data Science* 10 (2021), 15. https://doi.org/10.1140/epjds/s13688-021-00271-0

[6] Spurthi Amba Hombaiah, Tao Chen, Mingyang Zhang, Michael Bendersky, and Marc Najork. 2021. Dynamic Language Models for Continuously Evolving Content. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining* (Virtual Event, Singapore) *(KDD '21)*. Association for Computing Machinery, New York, NY, USA, 2514–2524. https://doi.org/10.1145/3447548.3467162

[7] Ahmer Arif, Leo Graiden Stewart, and Kate Starbird. 2018. Acting the Part: Examining Information Operations Within #BlackLivesMatter Discourse. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 20 (Nov. 2018), 27 pages. https://doi.org/10.1145/3274289

[8] Australian Cyber Security Center (ACSC). 2022. Australian organisations encouraged to urgently adopt an enhanced cyber security posture. https://www.cyber.gov.au/acsc/view-all-content/alerts/australian-organisations-encouraged-urgently-adopt-enhanced-cyber-security-posture. Accessed 2022-06-02.

[9] Kregg Aytes and Terry Conolly. 2003. A research model for investigating human behavior related to computer security. In *Proceedings of the Ninth Americas Conference on Information Systems (AMCIS)*. Association for Information Systems, Tampa, FL, USA, 260.

[10] Odette Beris, Adam Beautement, and M Angela Sasse. 2015. Employee rule breakers, excuse makers and security champions: mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop*. Association for Computing Machinery, New York, NY, USA, 73–84. https://doi.org/10.1145/2841113.2841119

[11] Michael S Bernstein, Eytan Bakshy, Moira Burke, and Brian Karrer. 2013. Quantifying the invisible audience in social networks. In *Proceedings of the SIGCHI conference on human factors in computing systems*. Association for Computing Machinery, New York, NY, USA, 21–30. https://doi.org/10.1145/2470654.2470658

[12] Hugh Beyer and Karen Holtzblatt. 1997. *Contextual Design: Defining Customer-Centered Systems*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[13] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M. Redmiles, and Angelika Strohmayer. 2022. Ethical Practices for Security Research with At-Risk Populations. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, Genoa, Italy, 546–553. https://doi.org/10.1109/EuroSPW55150.2022.00065

[14] Tulika Bose and Sophie Bushwick. 2023. How Misinformation Spreads through Conflict. https://www.scientificamerican.com/podcast/episode/how-misinformation-spreads-through-conflict/. Accessed 2023-12-12.

[15] Maia J Boyd, Jamar L Sullivan Jr, Marshini Chetty, and Blase Ur. 2021. Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–18. https://doi.org/10.1145/3411764.3445061

[16] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/2501604.2501610

[17] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2022. Einschätzung der aktuellen Cyber-Sicherheitslage in Deutschland nach dem russischen Angriff auf die Ukraine. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement.html?nn=1025778. Accessed 2022-08-09.

[18] Moira Burke, Cameron Marlow, and Thomas Lento. 2009. Feed me: motivating newcomer contribution in social network sites. In *Proceedings of the SIGCHI conference on human factors in computing systems*. Association for Computing Machinery, New York, NY, USA, 945–954. https://doi.org/10.1145/1518701.1518847

[19] Karoline Busse, Julia Schäfer, and Matthew Smith. 2019. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 117–136.

[20] Karoline Busse, Dominik Wermke, Sabrina Amft, Sascha Fahl, Emanuel von Zezschwitz, and Matthew Smith. 2019. Replication: Do We Snooze If We Can't Lose? Modelling Risk with Incentives in Habituation User Studies. In *Proceedings of the 2019 Workshop on Usable Security (USEC), USEC 2019, San Diego, CA, USA, February 24, 2019*. The Internet Society, San Diego, CA, USA, 10 pages. https://doi.org/10.14722/usec.2019.23001

[21] Canadian Centre for Cyber Security. 2022. Cyber threat bulletin: Cyber Centre reminds Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-reminds-canadian-critical-infrastructure-operators. Accessed 2022-08-09.

[22] Junyeop Cha, Seoyun Kim, and Eunil Park. 2022. A lexicon-based approach to examine depression detection in social media: the case of Twitter and university community. *Humanities and Social Sciences Communications* 9 (12 2022), 325. Issue 1. https://doi.org/10.1057/s41599-022-01313-2

[23] Kathy Charmaz. 2014. *Constructing Grounded Theory*. Sage, Thousand Oaks, CA, USA.

[24] Wen-Haw Chong and Ee-Peng Lim. 2019. Fine-grained geolocation of tweets in temporal proximity. *ACM Transactions on Information Systems (TOIS)* 37, 2 (2019), 1–33. https://doi.org/10.1145/3291059

[25] Emily Christofides, Amy Muise, and Serge Desmarais. 2012. Hey mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science* 3, 1 (2012), 48–54. https://doi.org/10.1177/1948550611408619

[26] Abu Nowshed Chy, Md Zia Ullah, and Masaki Aono. 2019. Query expansion for microblog retrieval focusing on an ensemble of features. *Journal of Information Processing* 27 (2019), 61–76. https://doi.org/10.2197/ipsjjip.27.61

[27] Juliet Corbin and Anselm Strauss. 1990. Grounded theory research: Procedures, canons and evaluative criteria. *Qualitative Sociology* 19, 6 (1990), 418–427. https://doi.org/10.1007/BF00988593

[28] Matteo Crosignani, Marco Macchiavelli, and André F Silva. 2021. Pirates without borders: The propagation of cyberattacks through firms' supply chains.

[29] Cybersecurity and Infrastructure Security Agency (CISA). 2022. SHIELDS UP. https://www.cisa.gov/shields-up. Accessed 2022-06-02.

[30] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G Bardas. 2021. Defensive technology use by political activists during the Sudanese revolution.

In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 372–390. https://doi.org/10.1109/SP40001.2021.00055

[31] Sauvik Das, Laura A Dabbish, and Jason I Hong. 2019. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 97–115.

[32] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 143–157.

[33] Sauvik Das, Adam DI Kramer, Laura A Dabbish, and Jason I Hong. 2014. Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. Association for Computing Machinery, New York, NY, USA, 739–749. https://doi.org/10.1145/2660267.2660271

[34] Sauvik Das, Adam D. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The role of social influence in security feature adoption. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*. Association for Computing Machinery, New York, NY, USA, 1416–1426. https://doi.org/10.1145/2675133.2675225

[35] Louis F DeKoven, Audrey Randall, Ariana Mirian, Gautam Akiwate, Ansel Blume, Lawrence K Saul, Aaron Schulman, Geoffrey M Voelker, and Stefan Savage. 2019. Measuring security practices and how they impact security. In *Proceedings of the Internet Measurement Conference*. Association for Computing Machinery, New York, NY, USA, 36–49. https://doi.org/10.1145/3355369.3355571

[36] Nic DePaula and Ersin Dincelli. 2018. Information strategies and affective reactions: How citizens interact with government social media content. *First Monday* 23, 4 (2018). https://doi.org/10.5210/fm.v23i4.8414

[37] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1065–1074. https://doi.org/10.1145/1357054.1357219

[38] Facebook. 2022. fastText Word Embeddings. https://fasttext.cc/docs/en/english-vectors.html Accessed 2024-02-20.

[39] Pavlos Fafalios, Vasileios Iosifidis, Eirini Ntoutsi, and Stefan Dietze. 2018. TweetsKB: A Public and Large-Scale RDF Corpus of Annotated Tweets. In *The Semantic Web*. Springer International Publishing, Cham, 177–190. https://doi.org/10.1007/978-3-319-93417-4_12

[40] Michael Fagan and Mohammad Maifi Hasan Khan. 2016. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*. USENIX Association, Denver, CO, 59–75.

[41] Max Falkenberg, Alessandro Galeazzi, Maddalena Torricelli, Niccolò Di Marco, Francesca Larosa, Madalina Sas, Amin Mekacher, Warren Pearce, Fabiana Zollo, Walter Quattrociocchi, and Andrea Baronchelli. 2022. Growing polarization around climate change on social media. *Nature Climate Change* 12 (12 2022), 1114–1121. Issue 12. https://doi.org/10.1038/s41558-022-01527-x

[42] Mehrdad Farokhnejad, Raj Ratn Pranesh, and Javier A Espinosa-Oviedo. 2020. Classifying Micro-text Document Datasets: Application to Query Expansion of Crisis-Related Tweets. In *International Conference on Service-Oriented Computing*. Springer International Publishing, Cham, 444–456. https://doi.org/10.1007/978-3-030-76352-7_41

[43] Christine Geeng, Savanna Yee, and Franziska Roesner. 2020. Fake News on Facebook and Twitter: Investigating How People (Don't) Investigate. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA). Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376784

[44] Loni Hagen, Thomas Keller, Stephen Neely, Nic DePaula, and Claudia Robert-Cooperman. 2018. Crisis communications in the age of social media: A network analysis of Zika-related tweets. *Social science computer review* 36, 5 (2018), 523–541. https://doi.org/10.1177/0894439317721985

[45] Malek Hajjem and Chiraz Latiri. 2017. Combining IR and LDA topic modeling for filtering microblogs. *Procedia Computer Science* 112 (2017), 761–770. https://doi.org/10.1016/j.procs.2017.08.166

[46] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*. Association for Computing Machinery, New York, NY, USA, 133–144. https://doi.org/10.1145/1719030.1719050

[47] Shandell Houlden, Jaigris Hodson, George Veletsianos, Darren Reid, and Chris Thompson-Wagner. 2021. The health belief model: How public health can address the misinformation crisis beyond COVID-19. *Public Health in Practice* 2 (2021), 100151. https://doi.org/10.1016/j.puhip.2021.100151

[48] Adele E Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. 2012. The psychology of security for the home computer user. In *2012 IEEE Symposium on Security and Privacy*. IEEE, San Francisco, CA, USA, 209–223. https://doi.org/10.1109/SP.2012.23

[49] Y. Linlin Huang, Kate Starbird, Mania Orand, Stephanie A. Stanek, and Heather T. Pedersen. 2015. Connected Through Crisis: Emotional Proximity and the Spread of Misinformation Online. 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, 969–980. https://doi.org/10.1145/2675133.2675202

[50] Muhammad Imran, Carlos Castillo, Fernando Diaz, and Sarah Vieweg. 2015. Processing social media messages in mass emergency: A survey. *ACM Computing Surveys (CSUR)* 47, 4 (2015), 1–38. https://doi.org/10.1145/2771588

[51] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. '... No one Can Hack My Mind': Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 327–346.

[52] Nicole E. Kogan, Leonardo Clemente, Parker Liautaud, Justin Kaashoek, Nicholas B. Link, Andre T. Nguyen, Fred S. Lu, Peter Huybers, Bernd Resch, Clemens Havas, Andreas Petutschnig, Jessica Davis, Matteo Chinazzi, Backtosch Mustafa, William P. Hanage, Alessandro Vespignani, and Mauricio Santillana. 2021. An early warning approach to monitor COVID-19 activity with multiple digital traces in near real time. *Science Advances* 7 (3 2021), eabd6989. Issue 10. https://doi.org/10.1126/sciadv.abd6989

[53] Alex Leavitt and Joshua A Clark. 2014. Upvoting hurricane Sandy: event-based news production processes on a social news site. In *Proceedings of the SIGCHI conference on human factors in computing systems*. Association for Computing Machinery, New York, NY, USA, 1495–1504. https://doi.org/10.1145/2556288.2557140

[54] Alex Leavitt and John J Robinson. 2017. The role of information visibility in network gatekeeping: Information aggregation on Reddit during crisis events. In *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*. Association for Computing Machinery, New York, NY, USA, 1246–1261. https://doi.org/10.1145/2998181.2998299

[55] Jayeon Lee. 2015. The double-edged sword: The effects of journalists' social media activities on audience perceptions of journalists and their news products. *Journal of Computer-Mediated Communication* 20, 3 (2015), 312–329. https://doi.org/10.1111/jcc4.12113

[56] Mykola Makhortykh and Yehor Lyebyedyev. 2015. #SaveDonbassPeople: Twitter, propaganda, and conflict in Eastern Ukraine. *The Communication Review* 18, 4 (2015), 239–270. https://doi.org/10.1080/10714421.2015.1085776

[57] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 72 (Nov. 2019), 23 pages. https://doi.org/10.1145/3359174

[58] Alan Mishler, Erin Smith Crabb, Susannah Paletz, Brook Hefright, and Ewa Golonka. 2015. Using structural topic modeling to detect events and cluster Twitter users in the Ukrainian crisis. In *International conference on human-computer interaction*. Springer, Cham, 639–644. https://doi.org/10.1007/978-3-319-21380-4_108

[59] Vidya Nakade, Aibek Musaev, and Travis Atkison. 2018. Preliminary research on thesaurus-based query expansion for Twitter data extraction. In *Proceedings of the ACMSE 2018 Conference*. Association for Computing Machinery, New York, NY, USA, 1–4. https://doi.org/10.1145/3190645.3190694

[60] National Cyber Security Centre (NCSC). 2022. UK organisations encouraged to take action in response to current situation in and around Ukraine. https://www.ncsc.gov.uk/news/uk-organisations-encouraged-to-take-action-around-ukraine-situation. Accessed 2022-08-09.

[61] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3290605.3300579

[62] Kate O'Flaherty. 2022. Signal Confirms Hack Claims Are Part Of Misinformation Campaign. https://www.forbes.com/sites/kateoflahertyuk/2022/03/01/signal-confirms-hack-claims-are-part-of-misinformation-campaign/. Accessed 2023-12-12.

[63] Alexandra Olteanu, Sarah Vieweg, and Carlos Castillo. 2015. What to expect when the unexpected happens: Social media communications across crises. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*. Association for Computing Machinery, New York, NY, USA, 994–1009. https://doi.org/10.1145/2675133.2675242

[64] Ozge Ozduzen and Aidan McGarry. 2020. Digital traces of "twitter revolutions": Resistance, polarization, and surveillance via contested images and texts of occupy Gezi. *International Journal of Communication* 14 (2020), 2543–2563.

[65] Mervi Pantti. 2019. The personalisation of conflict reporting: Visual coverage of the Ukraine crisis on Twitter. *Digital Journalism* 7, 1 (2019), 124–145. https://doi.org/10.1080/21670811.2017.1399807

[66] Twint Project. 2023. Twint. https://github.com/twintproject/twint Accessed 2024-02-20.

[67] Jakub Przetacznik. 2022. Russia's war on Ukraine: Timeline of cyber-attacks. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/

EPRS_BRI(2022)733549_EN.pdf
[68] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1 (2015), 121–144. https://doi.org/10.1093/cybsec/tyv008
[69] Jinfeng Rao and Jimmy Lin. 2016. Temporal query expansion using a continuous hidden markov model. In *Proceedings of the 2016 ACM international conference on the theory of information retrieval*. Association for Computing Machinery, New York, NY, USA, 295–298. https://doi.org/10.1145/2970398.2970424
[70] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2016. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, New York, NY, USA, 666–677. https://doi.org/10.1145/2976749.2978307
[71] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. 2016. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 272–288. https://doi.org/10.1109/SP.2016.24
[72] Elissa M Redmiles, Michelle L Mazurek, and John P Dickerson. 2018. Dancing pigs or externalities? Measuring the rationality of security decisions. In *Proceedings of the 2018 ACM Conference on Economics and Computation*. Association for Computing Machinery, New York, NY, USA, 215–232. https://doi.org/10.1145/3219166.3219185
[73] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, USA, 89–108.
[74] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy* 15, 5 (2017), 55–64. https://doi.org/10.1109/MSP.2017.3681050
[75] Christian Reuter, Amanda Lee Hughes, and Marc-André Kaufhold. 2018. Social media in crisis management: An evaluation and analysis of crisis informatics research. *International Journal of Human–Computer Interaction* 34, 4 (2018), 280–294.
[76] Christian Reuter and Marc-André Kaufhold. 2018. Fifteen years of social media in emergencies: a retrospective review and future directions for crisis informatics. *Journal of contingencies and crisis management* 26, 1 (2018), 41–57. https://doi.org/10.1111/1468-5973.12196
[77] Alexander Ronzhyn. 2014. The use of Facebook and Twitter during the 2013-2014 protests in Ukraine. In *Proceedings of the European Conference on Social Media*. Academic Conferences and Publishing International Limited, UK, 442–449.
[78] Rob Schroeder, Sean Everton, and Russell Shepherd. 2012. Mining Twitter Data from the Arab Spring. http://hdl.handle.net/10945/53058 Combating Terrorism Exchange 2.4 (2012): 54-64.
[79] Shikhar Mehrotra. 2022. Russia-Ukraine War: Signal Says Hack Claims Part Of 'coordinated Misinformation Campaign'. https://www.republicworld.com/world-news/russia-ukraine-crisis/russia-ukraine-war-signal-says-hack-claims-part-of-coordinated-misinformation-campaign-articleshow.html. Accessed 2022-07-27.
[80] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. 2018. Computer security and privacy for refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 409–423. https://doi.org/10.1109/SP.2018.00023
[81] Frank Smyth. 2012. Journalist Security Guide. https://cpj.org/wp-content/uploads/2020/05/guide.pdf
[82] Brian Stanton, Mary F Theofanos, Sandra Spickard Prettyman, and Susanne Furman. 2016. Security fatigue. *It Professional* 18, 5 (2016), 26–32. https://doi.org/10.1109/MITP.2016.84
[83] Kate Starbird. 2019. Disinformation's spread: bots, trolls and all of us. *Nature* 571 (07 2019), 449–450. https://doi.org/10.1038/d41586-019-02235-x
[84] Kate Starbird, Jim Maddock, Mania Orand, Peg Achterman, and Robert Mason. 2014. Rumors, False Flags, and Digital Vigilantes: Misinformation on Twitter After the 2013 Boston Marathon Bombing. In *IConference 2014 Proceedings*. IConference, Berlin, Germany. https://doi.org/10.9776/14308
[85] Anselm Strauss and Juliet M Corbin. 1997. *Grounded theory in practice*. Sage, Thousand Oaks, CA, USA. 288 pages.
[86] Haifeng Sun, Zhaoyu Wang, Jianhui Wang, Zhen Huang, NichelleLe Carrington, and Jianxin Liao. 2016. Data-driven power outage detection by social sensors. *IEEE Transactions on Smart Grid* 7, 5 (2016), 2516–2524. https://doi.org/10.1109/TSG.2016.2546181
[87] Mikhail D Suslov. 2014. "Crimea Is Ours!" Russian popular geopolitics in the new media age. *Eurasian geography and economics* 55, 6 (2014), 588–609. https://doi.org/10.1080/15387216.2015.1038574
[88] Sue Yeon Syn and Sanghee Oh. 2015. Why do social network site users share information on Facebook and Twitter? *Journal of Information Science* 41, 5 (2015), 553–569. https://doi.org/10.1177/0165551515585717
[89] Mohammad Tahaei, Tianshi Li, and Kami Vaniea. 2022. Understanding Privacy-Related Advice on Stack Overflow. *Proceedings on Privacy Enhancing Technologies* 2 (2022), 114–131. https://doi.org/10.2478/popets-2022-0038
[90] Irina Temnikova, Sarah Vieweg, and Carlos Castillo. 2015. The case for readability of crisis communications in social media. In *Proceedings of the 24th international conference on world wide web*. Association for Computing Machinery, New York, NY, USA, 1245–1250. https://doi.org/10.1145/2740908.2741718
[91] TREC. 2020. TREC. https://trec.nist.gov/data/microblog2015.html Accessed 2024-02-20.
[92] Tweepy. 2023. Tweepy. https://github.com/tweepy/tweepy Accessed 2024-02-20.
[93] Twitter. 2022. Twitter 1 % Stream. https://developer.twitter.com/en/docs/twitter-api/tweets/volume-streams/introduction Accessed 2023-08-20.
[94] Twitter. 2022. Twitter API for Academic Research. https://developer.twitter.com/en/products/twitter-api/academic-research Accessed 2023-07-07.
[95] Twitter. 2022. Twitter Streams. https://developer.twitter.com/en/docs/tutorials/stream-tweets-in-real-time Accessed 2023-07-07.
[96] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. 'I Knew It Was Too Good to Be True': The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 1–25. https://doi.org/10.1145/3274445
[97] Zheye Wang and Xinyue Ye. 2018. Social media analytics for natural disaster management. *International Journal of Geographical Information Science* 32, 1 (2018), 49–72. https://doi.org/10.1080/13658816.2017.1367003
[98] Bradley E Wiggins. 2016. Crimea River: Directionality in memes from the Russia-Ukraine conflict. *International Journal of Communication* 10 (2016), 35.
[99] XIT. 2023. How to Track Realtime Location of ANY Telegram User — 2 Methods. https://x-it.medium.com/how-to-track-realtime-location-of-any-telegram-user-2-methods-ec09d873b839. Accessed 2023-12-12.
[100] Meriem Amina Zingla, Latiri Chiraz, and Yahya Slimani. 2016. Short query expansion for microblog retrieval. *Procedia Computer Science* 96 (2016), 225–234. https://doi.org/10.1016/j.procs.2016.08.135
[101] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3313831.3376570
[102] Arkaitz Zubiaga, Ahmet Aker, Kalina Bontcheva, Maria Liakata, and Rob Procter. 2018. Detection and resolution of rumours in social media: A survey. *ACM Computing Surveys (CSUR)* 51, 2 (2018), 1–36. https://doi.org/10.1145/3161603

# A TAXONOMY

Table 2 shows the categories and subcategories of our taxonomy, as well as the two most frequently assigned codes as examples. The column *count* contains the total number of resources a code was assigned to. The count is an aggregate of all codes they contain for the categories and subcategories. The columns under *Individuals* and *Organizations* contain the number of resources that were assigned the respective code as well as this target, where we further distinguished between being addressed at people and organizations in Ukraine, in another, specific country or region, and resources that did not specify their audience. For the full taxonomy version, please refer to our replication package (see Availability section).

**Table 2: Taxonomy.**

| Category | Code | Count | Individuals | | | Organizations | | |
|---|---|---|---|---|---|---|---|---|
| | | | Unspecified | In Ukraine | In other country | Unspecified | In Ukraine | In other country |
| **Messaging & Social Media** | | 147 | 109 | 31 | 20 | 15 | 1 | 2 |
| Secure Messaging | | 47 | 35 | 17 | 7 | 2 | 1 | 1 |
| | Don't use Telegram/Telegram is insecure | 15 | 13 | 5 | 2 | 1 | 0 | 0 |
| | Use (end-to-end) encryption for communication | 11 | 7 | 6 | 3 | 1 | 0 | 0 |
| Advice for Social Media | | 39 | 25 | 10 | 8 | 2 | 0 | 0 |
| | Review privacy settings | 13 | 6 | 7 | 4 | 0 | 0 | 0 |
| | Be aware of what you share | 12 | 10 | 0 | 2 | 1 | 0 | 0 |
| Misinformation | | 83 | 67 | 8 | 9 | 13 | 0 | 1 |
| | Disinformation | 39 | 32 | 4 | 2 | 9 | 0 | 0 |
| | Beware of Russian disinformation | 36 | 28 | 3 | 7 | 4 | 0 | 1 |
| **Safe online behavior** | | 136 | 67 | 17 | 27 | 34 | 4 | 25 |
| Phishing | | 74 | 44 | 6 | 12 | 19 | 1 | 11 |
| | Be alert to phishing email | 21 | 10 | 3 | 5 | 4 | 1 | 1 |
| | Be suspicious of emails asking you to click links | 13 | 7 | 2 | 3 | 4 | 1 | 2 |
| Malware | | 55 | 21 | 2 | 13 | 20 | 3 | 17 |
| | Beware of Malware | 28 | 9 | 2 | 5 | 10 | 3 | 8 |
| | Don't use software from Russia | 14 | 6 | 0 | 2 | 7 | 0 | 5 |
| Connections & Anonymity | | 38 | 18 | 11 | 11 | 4 | 1 | 2 |
| | Use a VPN | 19 | 13 | 5 | 1 | 3 | 0 | 0 |
| | Use anonymity systems (Use TOR/Psiphon) | 12 | 4 | 1 | 7 | 1 | 1 | 1 |
| **Authentication** | | 75 | 33 | 9 | 14 | 20 | 1 | 26 |
| Passwords | | 51 | 24 | 7 | 12 | 10 | 0 | 17 |
| | Use strong passwords | 44 | 19 | 7 | 10 | 10 | 0 | 15 |
| | Use different passwords for each account | 24 | 14 | 1 | 6 | 7 | 0 | 5 |
| Recovery | | 6 | 3 | 2 | 1 | 1 | 0 | 2 |
| | Require email and phone number for a password reset | 4 | 3 | 2 | 1 | 0 | 0 | 0 |
| | Enable timeouts and lock-outs for failed log-in attempts | 2 | 0 | 0 | 0 | 1 | 0 | 2 |
| Multi-Factor Authentication | | 59 | 23 | 9 | 12 | 16 | 1 | 23 |
| | Use MFA | 44 | 18 | 6 | 8 | 9 | 0 | 18 |
| | Enforce MFA for privileged accounts/services/systems | 21 | 5 | 3 | 5 | 8 | 1 | 11 |
| **Hardware & Software** | | 83 | 34 | 11 | 12 | 23 | 4 | 29 |
| Software & System Updates | | 53 | 20 | 1 | 7 | 18 | 1 | 25 |
| | Keep systems/software up to date | 45 | 16 | 1 | 6 | 16 | 1 | 23 |
| | Update devices and device firmware | 14 | 7 | 0 | 2 | 3 | 0 | 6 |
| Security Software | | 35 | 10 | 1 | 5 | 10 | 2 | 19 |
| | Use anti-virus software | 13 | 5 | 0 | 3 | 3 | 0 | 7 |
| | Use anti-malware software | 7 | 2 | 0 | 1 | 2 | 0 | 4 |
| Device and Hardware Security | | 24 | 13 | 9 | 3 | 2 | 1 | 3 |
| | Turn off location devices | 11 | 4 | 8 | 2 | 0 | 0 | 0 |
| | Lock devices | 3 | 3 | 0 | 0 | 0 | 0 | 0 |
| **Storing Data** | | 54 | 17 | 6 | 9 | 14 | 1 | 26 |
| Backups | | 35 | 9 | 2 | 7 | 9 | 1 | 21 |
| | Backup your data | 28 | 8 | 2 | 7 | 7 | 1 | 17 |
| | Test backup/restore | 15 | 3 | 0 | 2 | 5 | 0 | 9 |
| Logging | | 20 | 4 | 0 | 1 | 5 | 0 | 13 |
| | Ensure logging is done, storage, retention periods | 8 | 0 | 0 | 0 | 1 | 0 | 8 |
| | Log network activity and monitor for suspicious activity | 6 | 0 | 0 | 0 | 2 | 0 | 5 |
| Preventing Access | | 12 | 7 | 4 | 2 | 2 | 0 | 1 |
| | Don't store data if you don't need to | 6 | 3 | 3 | 1 | 2 | 0 | 0 |
| | Encrypt your device data | 5 | 3 | 1 | 1 | 0 | 0 | 1 |
| **Organizational Policies** | | 33 | 2 | 2 | 4 | 10 | 2 | 23 |
| Incident & Recovery Plans | | 30 | 2 | 2 | 4 | 7 | 1 | 23 |
| | Incident Response Plans | 14 | 2 | 0 | 2 | 4 | 0 | 10 |
| | Verify an incident response plan exists and is up to date | 10 | 0 | 1 | 1 | 2 | 1 | 8 |
| Access & Network Policies | | 19 | 0 | 0 | 0 | 8 | 1 | 13 |
| | Track authorization and access, remove leavers | 10 | 0 | 0 | 0 | 3 | 0 | 8 |
| | Apply least privilege access | 9 | 0 | 0 | 0 | 4 | 1 | 7 |
| **Learning & Teaching** | | 138 | 33 | 28 | 23 | 37 | 16 | 57 |
| Recommendations for Sharing Advice During Crises | | 27 | 10 | 2 | 2 | 12 | 1 | 10 |
| | Alert users about increased risks | 17 | 3 | 0 | 2 | 8 | 0 | 10 |
| | Share advice with friends and family | 5 | 3 | 1 | 0 | 1 | 0 | 0 |
| Awareness & Resources | | 85 | 16 | 21 | 15 | 19 | 10 | 36 |
| | Support pointers | 52 | 11 | 19 | 11 | 8 | 9 | 18 |
| | Guidelines | 26 | 1 | 3 | 4 | 8 | 1 | 15 |
| Learning | | 10 | 3 | 1 | 2 | 3 | 0 | 4 |
| | Seek professional help for cyber security issues | 6 | 1 | 0 | 1 | 2 | 0 | 3 |
| | Always keep learning about security and privacy | 4 | 2 | 1 | 1 | 1 | 0 | 1 |
| Threat Modeling | | 45 | 10 | 5 | 8 | 15 | 5 | 21 |
| | Advanced persistent threat groups | 11 | 1 | 1 | 2 | 5 | 2 | 4 |
| | Threat model | 10 | 4 | 3 | 2 | 2 | 1 | 4 |

# B COMPARISON TABLES

Tables 3 and 4 show the top ten pieces of advice from the datasets we compared, and the advice evaluation data, respectively.

# C SEED LIST GENERATION DATA

## C.1 Regular expressions for target keywords

- \b**cyber secur***\b
- \b**advice**\b
- \b**recommend***\b

## C.2 Parameters

Table 5 lists the values for the parameters used in the seed list generations. *Seed list* denominates the respective seed list, $s_{min}$ is the minimum similarity threshold and $n$ is the target length of the seed list.

## C.3 Final Seed Lists

In the following, we list the final seed lists with individual terms. The terms can contain regular expressions and are matched as whole words. A superscript a indicates a manually added term.

**Advice + recommend.** adopt[a], advice, advice-, advices, advise, advised[a], advises[a], advising[a], advisor, advisors, advisory[a], alert[a], assistance, avoid, best practice[a], beware[a], bolster[a], consider, consult, consultation, consultations[a], consulted[a], consulting, counsel, counseled[a], counselling, encourage, endorse, entrust[a], guidance, guide, guided[a], guides[a], guiding[a], help, helped[a], helpful,

**Table 3: Top ten pieces of advice compared to the frequency of appearance in Reeder et al. [74] and Boyd et al. [15].**

| # | Our Data | Reeder et al. [74] | Boyd et al. [15] |
|---|---|---|---|
| 1 | Beware of disinformation | Keep systems and software up to date | Disable biometric unlocking |
| 2 | Support pointers | Use unique passwords | Use E2EE messaging app |
| 3 | Use strong passwords | Use strong passwords | Use Signal |
| 4 | Use multi-factor authentication | Use multi-factor authentication | Turn off location |
| 5 | Keep systems and software up-to-date/patched | Use antivirus software | Avoid identifiable people (in social media posts) |
| 6 | Use a VPN | Use a password manager | Remove metadata (from social media posts) |
| 7 | Beware of Russian disinformation | Use HTTPS | Encrypt device |
| 8 | Be alert to phishing email | Use only software from trusted sources | Turn off Bluetooth and WiFi |
| 9 | Telegram is insecure | Use automatic updates | Use a strong password |
| 10 | Use different passwords for each account | Be careful/think before you click | Disconnect cellular data |

**Table 4: Top ten pieces of advice compared to user and expert priority rankings in Redmiles et al. [73].**

| # | Our Data | Expert Priority [73] | User Priority [73] |
|---|---|---|---|
| 1 | Beware of disinformation | Use different passwords for each account | Never give your credentials to third parties |
| 2 | Support pointers | Update devices and device firmware | Buy devices with security-focused platforms |
| 3 | Use strong passwords | Use anti-malware software | Don't open unnecessary attachments |
| 4 | Use multi-factor authentication | Scan attachments you open for viruses | Use anti-virus software |
| 5 | Keep systems and software up-to-date/patched | Never give your credentials to third parties | Don't click random or unfamiliar links from unknown senders |
| 6 | Use a VPN | Use unique passwords for different accounts | Verify suspicious emails, senders, and email contents |
| 7 | Beware of Russian disinformation | Use (end-to-end) encryption for communication | Not open email from unknown senders |
| 8 | Be alert to phishing email | Keep anti-virus software installed and up-to-date | Don't friend/put in your contacts people you don't know |
| 9 | Telegram is insecure | Use strong passwords | Be suspicious if something is too good to be true |
| 10 | Use different passwords for each account | Turn on automatic updates for devices | Set your antivirus/anti-malware to run periodic full scans |

**Table 5: Parameters for seed list generation.**

| Seed list | $s_{min}$ | n |
|---|---|---|
| advice | 0.4 | 50 |
| recommend | 0.4 | 50 |
| cyber security | 0.4 | 100 |

helping[a], helps[a], ideas, insight, insightful, insights, invaluable, practical, protect[a], recommend, recommendation, recommendations, recommended, recommending, reconsider, refrain[a], safe[a], safeguard[a], secure[a], sensible, stay, step[a], steps[a], strengthen[a], suggest, suggested[a], suggesting[a], suggestion, suggestions, tip[a], tips, warn[a], wisdom

**Cyber security.** antivirus[a], authentication[a], breach[a], breaches, cisa[a], ciso[a], cissp[a], cloud computing, cloudcomputing, cryptography, cyber, cyber attack, cyber attacks, cyber crime, cyber crimes, cyber criminal, cyber criminals, cyber risk, cyber risks[a], cyber safety, cyber security, cyber space, cyber threat[a], cyber threats, cyber war, cyberattack, cyber-attack[a], cyberattacks, cyber-attacks, cybercrime, cybercrimes[a], cybercriminal, cybercriminals, cyberrisk, cybersafety[a], cybersecurity, cyberspace, cyberthreat, cyberthreats[a], cyberwar[a], data breach, data privacy, data protection[a], dataprivacy[a], dataprotection[a], ddos, disinformation[a], dns[a], encrypt[a], encrypted[a], encryption, firewall[a], gchq, gdpr, hack.*[a], homeland security, info security[a], information security[a], information technology, informationsecurity, infosec, infosecurity, iso27001, malware, misinformation, national security, ncsam, ncsc, oscp[a], osint, password[a], passwords[a], penetration test[a], penetration tester[a], penetration testing, pentest, pentester, pentesting, phishing, privacy[a], ransomware, scams[a], securi, security, social engineering, social media[a], spyware[a], surveillance, vulnerabilities, vulnerability[a]

**Ukraine + Russia.** ukrain.*, russia.*, ukran.*