Learning from Censored Experiences: Social Media Discussions around Censorship Circumvention Technologies

Elham Pourabbas Vafa*†, Mohit Singhal*◇‡, Poojitha Thota†, Sayak Saha Roy†
† *The University of Texas at Arlington*
‡ *Northeastern University*
(exp4529,poojitha.thota,sayak.saharoy)@mavs.uta.edu
m.singhal@northeastern.edu

***Abstract*—During periods of strict internet censorship, maintaining access to online information and communication becomes paramount. However, users must often navigate complicated pathways to find effective censorship circumvention technologies (CCTs). Utilizing real-time data from over 50M posts collected from Twitter and Telegram from September 18th, 2022, to January 31st, 2023, during a peak period of censorship, we examined the impact of CCTs, such as VPNs, proxies, and alternative connectivity solutions, on digital rights, privacy, and internet governance. Through a mixed-method analysis, our findings reveal user resilience and adaptability when the community collaboratively shares and discusses knowledge and resources. First, we developed a codebook for discussions considering English and, for the first time, *Persian* posts, highlighting the main problems users encounter when attempting to bypass the internet restrictions. Several concerns were common across these discourses, such as traceability, identifiability, and accidental use of malicious configurations. Our temporal study, conducted over 20 weeks, showed shifts in VPN preferences due to changing censorship strategies, with the inclusion of more privacy-focused and accessibility features leading to higher adoption. We also found several dedicated popular VPN channels that shared malicious files masked as free VPN services.**

1. Introduction

Digital connectivity is considered a fundamental component of every social progress. Censorship Circumvention Technologies (CCTs), such as Virtual Private Networks (VPNs) and proxies, are more than just a technical convenience; they are essential elements in facilitating unrestricted, secure, and private internet access [1], [2]. These technologies implement various features to effectively bypass restrictions on internet access. Tools like VPNs, proxies, and secure messaging applications employ encryption to protect user communication from surveillance and interception [3], [4]. Technologies like TOR route internet traffic through a network of volunteer-run servers, masking users' IP addresses and enhancing their anonymity [5]. Methods like domain fronting and protocol obfuscation help bypass deep packet inspection [6], [7]. Proxy servers and tunneling protocols, such as SSH and DNS tunneling, enable users to reroute their internet traffic through intermediary servers, bypassing network restrictions and accessing blocked content [8], [9]. Moreover, to adjust to evolving censorship tactics, these tools often employ adaptive strategies involving switching servers, modifying protocols, or utilizing alternative communication channels [10], [11]. Furthermore, much effort has been devoted to making these tools accessible, efficient, and user-friendly [12], [13].

The proposed methods and tools for bypassing censorship are evaluated using various criteria for effectiveness, usability, security, privacy-preserving, and overall performance. However, their evaluation can be challenging. For example, testing their effectiveness often requires access to regions where censorship is prevalent or networks where restrictions are in place [14]. In addition, keeping pace with changing censorship measures and evaluating tools' effectiveness against new tactics can be a continuous and challenging process [15], [16].

In this paper, we propose a social sensing framework for collecting and studying social media discussions to gain insights into the effectiveness of censorship-bypassing tools. As censorship events unfold, users often turn to social media platforms to share their experiences and seek advice on circumvention techniques [17]. These discussions can serve as a rich source of quality data, offering firsthand accounts of individuals attempting to bypass censorship measures. We employed our framework to collect and analyze social media data during the Iran uprisings in 2022-2023, a period marked by stringent internet restrictions and shutdowns [18]. We analyzed Twitter and Telegram conversations over six months and investigated the bypassing technologies utilized, their use cases, and the challenges users encountered. Mainly, this paper aims to investigate the following three research questions:

RQ1: How do users (regular and tech-savvy/ cybersecurity experts) discuss circumvention technologies, such as VPNs, proxies, and Starlink? Exploring these discussions can provide valuable insights into users' concerns, challenges, and expectations about these tools. Regular individ-

*. These authors contributed equally to this work
◇. Work done at The University of Texas at Arlington

© 2025, Elham Pourabbas Vafa. Under license to IEEE.
DOI 10.1109/SP61157.2025.00062

uals' usage patterns and perceptions reflect broader societal concerns and experiences, which can highlight grassroots requirements for these tools. On the other hand, experts' interactions can reveal nuanced technical insights, potentially pointing towards more sophisticated or targeted solutions.

RQ2: How do users' preferences and usage of VPN technologies evolve by shifts in censorship techniques? VPNs are one of the main circumvention tools; thus, we provide an in-depth study of the highly discussed VPN technologies' adaption, effectiveness, and limitations. Insights from this analysis can inform efforts to enhance VPN features and capabilities.

RQ3: How do users navigate the risks and trustworthiness of VPN services distributed through popular Telegram channels? By studying user interactions on popular Telegram channels that share VPN and proxy resources, we obtain insights into the strategies users employ to adopt and use said resources to combat internet censorship.

To answer these research questions, we collected English and Persian posts from September 18th, 2022, to January 31st, 2023, using the Twitter V2 Archive Search endpoint [19], the Telegram API [20] and the Telethon client [21]. We obtained 11M English and 39M Persian tweets from Twitter and 54K posts about VPN and proxy resources on Telegram. To obtain tweets relevant to bypassing censorship, we used keyword-based filtration and fine-tuned RoBERTa [22] and ParsBERT [23] models. As a result, we obtained a novel and unique dataset with 118K posts in English and 762K tweets in Persian. To answer RQ1, we first identified tech-savvy expert users and quantitatively and qualitatively identified major discussion topics, which we present as a code book. To address RQ2, we performed a temporal analysis of a comprehensive list of VPN services mentioned across several platforms over a 20-week period to monitor shifts in their usage over time. Furthermore, we conducted a qualitative analysis of some post samples to understand the technical issues of using VPNs. To address RQ3, we tracked posts in more than 80 Telegram channels to identify and evaluate desktop and mobile executables, IP configuration files, etc., if they had instances of malicious behaviors. Furthermore, we examined comments from these posts to identify how users trusted and adopted these services and exchanged technical knowledge, especially for malicious files.

The contributions of this paper are: (1) We provide a novel and unique dataset gathered from Telegram and Twitter discussions on internet censorship and circumvention strategies. This dataset highlights the main problems users encountered when using CCTs and how the community supported one another in overcoming the restrictions. Our key findings include security concerns about traceability and the use of malicious configurations shared on Telegram channels. (2) For the first time, we presented a security and privacy discussion codebook of English and Persian posts. The codebook highlights discourse on CCTs and covers challenges, such as internet shutdowns, disruptions, and restrictions, reflecting the central issues in internet connectivity. (3) This research offers insights into the discussions on CCTs, like VPNs, proxies, TOR, and Starlink, among novice and tech-savvy users. There is a strong interest in Starlink but concerns over its cost, feasibility, and fake apps. Common topics include account sharing, free and premium CCT access, and technical issues. While users suggested using TOR in the beginning, the number of discussions drastically dropped after 8 weeks to none. One of the major topic points was issues relayed to slow connections, the proliferation of fake Tor, and its security and usability. (4) Our 20-week temporal study tracked changes in user preferences for VPN services in response to evolving censorship. Key findings include a 30% increase in Proton VPN's mentions after releasing a new feature providing free VPN traffic disguise. In contrast, Outline VPN mentions declined, likely due to its ineffectiveness against sophisticated targeting and blocking tactics [24], [25]. (5) Investigating well-known Telegram channels, we found instances of malicious files masked as free CCT services being shared. Users consequently use these, which can damage their personal resources. (6) Analyzing the discussions, we mapped CCT users' concerns into five threat model categories: location monitoring, network traffic monitoring, installing malware and spyware, blocking VPN traffic, and CCT security flaws.

Overall, our work provides an understanding of the state of internet freedom and the continuous fight for digital rights. Our findings show that even with decades of research and development in such technologies, there is a desperate need for more secure, reliable, effective, and accessible solutions. We hope this study's feedback can facilitate rapid adaptation and improvement of CCTs, contributing to the ongoing development and refinement of effective tools for preserving internet freedom.

2. Related Work

Circumventing Internet Censorship: Scholarships have investigated the impact of state-sponsored censorship on users' ability to connect to the internet [2], [26], [27], [28]. Many studies have explored the prevalence and use of various tools to circumvent censorship in multiple countries, including China [1], [17], [29], [30], Iran [31], [32], [33], Russia [27], Egypt [34], Turkmenistan [35], India [36], Japan & Canada [37], and Zambia [38]. Studies investigated people's expectations of CCTs, like VPNs, proxies, etc. For example, Ramesh et al. [4] conducted a quantitative survey with VPN users, concluding that people use VPNs to protect and secure their online activities. They also investigated the adoption and effectiveness of VPNs in Russia [39]. Namara et al. [40] found that people use VPNs for fear of surveillance or for privacy. Dutkowska-Zuk et al. [41] found that university students mainly used VPNs to access restricted content.

Measurements of Bypassing Techniques: Prior work has analyzed the security and privacy risks of VPNs [42], [43], [44], [45], [46]. Ikram et al. [47] identified instances of malware presence, traffic leakages & manipulations in more than 200 Android VPN apps. Zhang et al. [48] probed the security vulnerabilities in 84 OpenVPN-based Android

applications. Works have also investigated the S&P of rogue HTTP proxies [42], [49], [50], [51]. Tsirantonakis et al. [52] found that 5.15% of the tested open HTTP proxies were performing modification or injecting malicious code. O'Neill et al. [53] identified 3,600 cases of malware intercepting a TLS proxy communication. Carnavalet et al. [54] uncovered security vulnerabilities in TLS proxies.

Using Social Media to Understand Discussions around Security and Privacy Topics: Prior work has harnessed social media platforms to understand discussions about users' Security and Privacy (S&P) concerns about various technologies [55], [56], [57], [58], [59], [60], [61], [62]. Li et al. [63] qualitatively analyzed 4K Reddit comments form 180 security- and privacy-related discussions from /r/homeautomation to understand users' concerns and attitudes about smart home Security and Privacy (S&P). Schmidt et al. [64] assessed the S&P of popular baby monitor apps. Singhal et al. [65] showed misinformation posts about the S&P of video conferencing tools, such as Zoom, spread on four social media platforms during the COVID-19 pandemic.

While prior works have either conducted questionnaires or performed network measurement studies to study specific types of CCTs in controlled settings, our work employs an in-depth analysis of social media discussions of users experiencing censorship to learn about their censored experiences.

3. Methodology

Figure 1 illustrates our proposed social sensing framework for data collection and analysis of social media discussions around CCTs. This section explains the data collection, filtering, and classification of discussions about CCT on Twitter and Telegram in detail. Section 4 delves into the methodology of identifying tech-savvy from ordinary users and further addressing our *RQ1*. Section 5 addresses our *RQ2*, and Section 6 investigate the methodology to identify malicious files and addresses our *RQ3*.

Our framework gathers discussions from two widely-used social media and messaging platforms: Twitter and Telegram. Although access to these platforms has been restricted in certain countries during specific time periods [39], [66], they remain among the most popular, with users frequently employing circumvention censorship technologies (CCTs) to bypass these restrictions and maintain connectivity [67], [68], [69]. For example, during our data collection, it has been reported that the use of VPNs has increased by 3000% [70]. Additionally, we manually examined a sample of 100 Twitter accounts in our dataset (50 English and 50 Persian), checking their names, locations, profile descriptions, and timelines. We could confirm that most of them, i.e., 87% are Iranians, of which 26% live outside the country, suggesting that our dataset mainly includes posts by Iranians who discuss the use of CCTs. However, our analysis does not capture the struggles of the population with low or no prior experience and knowledge about CCTs.

3.1. Detecting CCT Discussions on Twitter

3.1.1. Data Collection. Using Twitter, our data collection process began by curating a set of hashtags relevant to the ongoing events, incorporating both English and Persian languages. We used the widely recognized hashtags as a starting point and employed a snowball sampling technique [71] to identify new hashtags that emerged as the protests evolved. To keep pace with the dynamic nature of social media discourse during the protests, our list of hashtags was updated at the end of each month to include any new hashtags that had become relevant. We appended the new hashtags to our existing list and used this updated list to extract tweets for that period. This ensured that our data collection remained comprehensive, reflecting the latest developments in the discussions. A complete list of hashtags can be obtained by contacting the authors.

To collect the tweets, we utilized Twitter V2 Archive Search endpoint [19], which allowed us to access a complete historical archive of public Tweets dating back to the first Tweet in March 2006. Our data collection spanned from September 18th, 2022, to January 31st, 2023, where discussions were heavily centered on security, privacy, and censorship. We used month-specific hashtags to collect data for each month, running separately for both English and Persian. We excluded retweets to prioritize the conversational content, consisting of main tweets and direct replies.

3.1.2. Initial Keyword Filtration and Cleaning. Upon collecting data for each month, we obtained nearly 40M tweets across both languages. Direct sampling could be an initial approach to understanding the major discussion topics within this vast dataset. However, this method often results in capturing a large number of irrelevant posts, highlighting the need for a more targeted approach. To address this issue, we implemented a preliminary keyword-based filtration system to filter tweets relevant to security and privacy using a predefined set of keywords, such as cybersecurity, privacy, anonymous, etc., in both English and Persian. The complete list, comprising 280 Persian and 256 English keywords, can be found at: https://tinyurl.com/5nkfjaxh.

While maintaining the original set of keywords, we encountered some false positives, leading to iterative refinements. After each filtration iteration, we randomly sampled 100 tweets to identify keywords that frequently led to irrelevant tweets. Based on these insights, we introduced a layer of context-sensitive filtering to eliminate false positive instances effectively. For instance, terms like 'virus' were only considered relevant when paired with cybersecurity-related terms, excluding matches with 'deadly virus,' 'corona virus,' or other non-security contexts. Similarly, 'risk' and 'code' were targeted only in contexts directly associated with digital security and privacy, avoiding broader or unrelated uses such as 'political risk' or 'dress code.' This approach of context-specific filtering ensured that the tweets retained in our dataset were related to S&P discussions.

Tweets were then lemmatized using NLTK WordNet Lemmatizer [72] to standardized words for effective key-

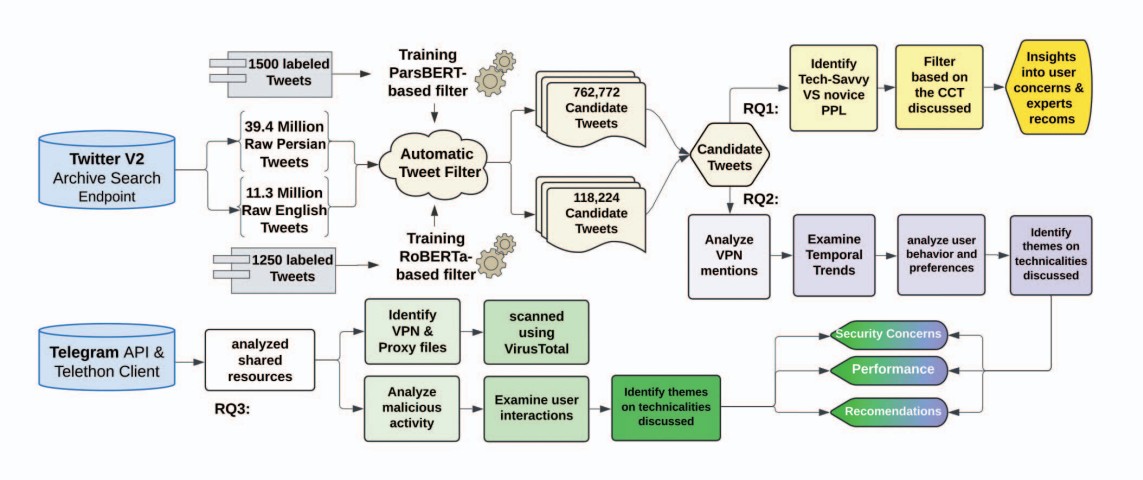

Figure 1: Data analysis pipeline

word matching. A similar process was applied to Persian tweets, which involved using both English and Persian keywords along with PersianStemmer [73] to accommodate the bilingual nature of Persian tweets. During keyword filtering, we also noticed hashtags like 'VPN' or 'server' often included unrelated commercial or irrelevant discussions about VPNs in China. To refine the dataset further, only tweets with protest-related hashtags were retained.

3.1.3. Codebook Creation. We used the refined dataset to develop a codebook for categorizing security and privacy topics in the tweets. To ensure the codebook captured the diversity of discussions, we proportionately sampled 1000 posts from the filtered tweets each week relative to their total volume. We obtained a similar sample for Persian as well. This method ensured that our sample accurately reflected the weekly discussion volume and topic fluctuations.

We assessed these samples to determine their relevance to our research criteria. We found 80% of the English posts and 46% of the Persian posts were relevant. Based on these relevant posts, we created a hierarchical codebook of security and privacy posts in English and Persian, applying the open coding process [74]. Following this process, two coders for English and two coders for Persian coded the security and privacy posts identified in the previous subsection until no new categories emerged. The inter-coder reliability for this process, measured by the Cohen Kappa score, was 0.78 for English and 0.86 for Persian. To improve the quality of the categories, we used an iterative process [75] so that new categories were added or existing ones were reorganized. To create the codebook, we followed certain guidelines: (1) Read through the post and identify themes and sub-themes; (2) While creating the categories, identify the motive and meaning of the post; and (3) Consider various features that can help in the identification of categories.

Figure 2 shows the codebook. Orange denotes the main classes. Yellow boxes were only in our English dataset, and blue boxes were only found in our Persian dataset.

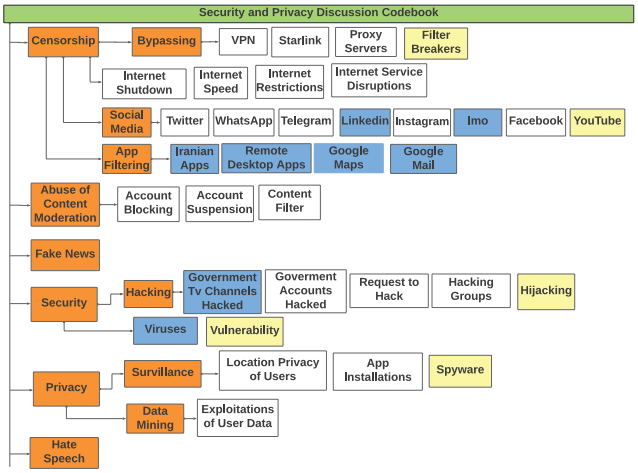

Figure 2: Security and Privacy hierarchical codebook.

After identifying a wide range of discussion categories, in this paper, we focus on two categories from our codebook, *Censorship Bypassing* and *Censorship*, to concentrate on discussions most relevant to the core aspects of our research. Among the English posts analyzed, the *Censorship* category comprised nearly 55% of tweets, making up the majority of relevant discussions, and *Censorship Bypassing* comprised about 4% of tweets. Among English censorship bypassing tweets, the percentage of VPN, Starlink, Proxy, and TOR tweets were 50%, 20%, 15%, and 15%, respectively. Whereas, for Persian posts, *Censorship* constituted 31% and *Censorship Bypassing* constituted 7% of tweets. Among Persian censorship bypassing tweets, the percentage of VPN, Starlink, Proxy, and TOR tweets were 66.66%, 12.82%, 10.26%, and 10.26%, respectively. Appendix B provides further information on the main topics and their subclasses.

3.1.4. Obtaining Censorship Relevant Tweets and Groundtruth Creation. To obtain a dataset for the cen-

English and Persian Keyword List
Internet shutdown, internet restrictions, internet speed, censor, bypassing, VPN, starlink, Proxy server, internet filtering, tor, server, internet, net, network, censorship, bypass فیلتر - فیلترینگ - قطع شدن اینترنت -دور زدن - استارلینک - مشکل اینترنت - نت قطع - قطع‌شدن اینترنت - وی‌پی‌ان - وی پی ان - نت وصل - فیلترشکن - افت سرعت - کاهش سرعت - پروکسی - اینترنت قطع - سرعت اینترنت - فیلتر شکن

Figure 3: Keywords list for obtaining relevant tweets.

sorship category, we conducted a second round of filtration using relevant keywords, including 'VPN,' 'Proxy,' 'Internet Shutdown,' etc. Figure 3 shows the list of keywords.

During the codebook generation phase, we noted that keyword-based filtration was somewhat effective, capturing 80% of the posts as relevant when we manually labeled them. However, the remaining 20% of irrelevant posts highlighted the need for a more refined approach to improve accuracy. Thus, we decided to build classifiers supported by a robust ground truth. To achieve this, we initially created a new set of censorship-related keywords and filtered the tweets using the same methods and cleaning procedures described in Section 3.1.2. The tweets that met these criteria formed our "filtered" dataset, and the remaining tweets formed our "unfiltered" dataset. We utilized both of them to establish ground truth for our classifiers. Moreover, recognizing that keyword filtration could exclude some relevant tweets not employing the targeted terms, we also included posts from the unfiltered dataset in our manual labeling process. This approach was necessary to mitigate biases and ensure that relevant tweets not captured by new keywords were still considered in the ground truth dataset.

To establish the ground truth dataset, two coders manually labeled each tweet as either *Relevant to Censorship* or *Irrelevant*. We extracted 1000 tweets from the Persian filtered dataset, labeling 888 as *Relevant* and 112 as *Irrelevant*. To address this imbalance, we further labeled 1000 unfiltered tweets, finding 15 as *Relevant* and 985 as *Irrelevant*. From these, we randomly selected 750 *Relevant* and 750 *Irrelevant* tweets to compose the Persian ground truth dataset. We extracted 1000 from the English-filtered dataset, resulting in 580 *Relevant* and 420 *Irrelevant*. To address a slight imbalance, we additionally labeled 250 tweets from an unfiltered dataset, identifying 26 *Relevant* and 224 *Irrelevant*, leading to a combined total of 606 *Relevant* and 644 *Irrelevant* tweets for the English ground truth dataset. To assess the inter-rater agreement, Cohen's kappa score was calculated. The score was 0.85 for English and 0.94 for Persian tweets, showing near-perfect agreement between the coders.

3.1.5. Preprocessing Labeled Data. The preprocessing stage involved several steps. **English tweets preprocessing:** We preprocessed by applying text normalization and noise elimination of stop words, HTML tags, URLs, usernames, hashtags, and emojis [65]. Additionally, tweets were truncated to match the model's maximum length requirements. **Persian tweets preprocessing:** Preprocessing Persian tweets requires a different approach due to the language's unique characteristics. Additionally, some users might be using Arabic keywords mistakenly or because their operating systems do not support Persian keyboards. Therefore, we eliminated Arabic diacritical marks, which can create inconsistencies in text processing, e.g., a diacritical mark that appears as a small circle above a letter, indicating the absence of a vowel sound, was removed. Later, Character Normalization was performed, where Arabic equivalents such as 'kaf' were converted to their Persian equivalents. We also adjusted the zero-width non-joiners and standardized numerals to preserve linguistic accuracy. This approach ensured consistency in Persian and helped prevent ambiguity or confusion during text processing.

TABLE 1: Twitter's filtering and classification results.

	Raw Posts	Filtered Posts	Classified Posts
English	11,264,108	88,154	118,224
Persian	39,375,975	154,218	762,772

3.1.6. Model selection for Tweets Classification:. To classify tweets as either "Relevant" or "Irrelevant" in English and Persian, we used BERT-based models (RoBERTa [22] for English and ParsBERT [23] for Persian) rather than traditional machine learning algorithms as they often require many features and large datasets to perform optimally [76].

Training details: Leveraging the pre-trained capabilities of RoBERTa and ParsBERT, we fine-tuned these models on English and Persian datasets. Both models underwent training using a stratified k-cross validation ($k = 5$) to ensure each data point was evenly represented across the training and validation sets. The English model achieved 98% for both F1 score and accuracy, and the Persian model achieved 99% for both F1 score and accuracy. Table 1 demonstrates the effectiveness of our classifiers compared to keyword filtering. Initially, keyword filtering reduced the number of relevant posts to 88,154 for English and 154,218 for Persian posts from the raw dataset. However, after applying our fine-tuned RoBERTa and ParsBERT classifiers, the number of relevant posts identified increased to 118,224 for English and 762,772 for Persian, showing the effectiveness in capturing posts that keyword filters were missing.

3.1.7. Descriptive Statistics. Figure 4 shows the monthly posting activity and number of unique users in both English and Persian datasets. As we can observe, initially, there were many unique users in our English dataset; however, that started to decrease in October; on the other hand, the number of unique users in our Persian dataset increased from September to October before we observed the downward shift. We see a similar pattern for the number of hashtags in both English and Persian, wherein there is a downward pattern observed from October onwards. Figure 4 shows a sharp declines in the number of posts after October, corresponding to the periods with high incidences of internet shutdowns [66]. This huge drop shows how these interruptions affected the flow of information and the conditions under which the users struggled to use these platforms. We obtained 38,995 and 168,700 unique users in our English and Persian datasets, respectively. Table 2 shows the descriptive statistics of our dataset.

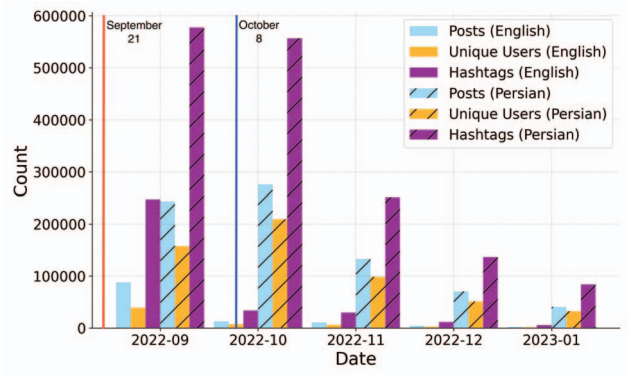

Figure 4: The number of monthly Persian/English posts, unique users, and hashtags. According to [18], [66], red line denotes the first incident of shutdown, and the blue line denotes the second incident of shutdown.

TABLE 2: Descriptive statistics of Twitter datasets.

	English dataset/ Persian dataset			
Feature	Mean	Min	Max	Med.
Followers	3.7K/1.0K	0/ 0	10M/ 8M	106/ 162
Following	517/ 565	0/ 0	275K/ 126K	416/ 171
Tweets	8.3K/ 5.8K	1/ 1	3.4M/ 2.1M	4.9K/ 1.6K
Verified	0.009/ 0.009	0/0	1/1	-

4. RQ1: Qualitative analysis of CCT discussions by tech-Savvy vs. other users

Based on our codebook (Figure 2), we found that users repeatedly echoed the need for CCTs, in particular, 59% and 38% in our English and Persian datasets, respectively. Our datasets' most frequently discussed CCTs were Virtual Private Networks (VPNs), Proxy servers, TOR, and Starlink. Hence, we focused our analysis on posts related to these technologies to understand users' discussions around them.

4.1. Identifying tech-savvy/ expert users

Identifying tech-savvy users on social media is not a trivial task. Previous works have used various methods to differentiate between user types by performing surveys on the profile descriptions [77], [78], by linguistic features [79], or by using the *list* feature provided by Twitter [80]. We examined the author's profile description to detect *tech-savvy/ expert* users on Twitter. We built a comprehensive list of keywords, in both English and Persian, that people usually use to describe their technology-related profession or knowledge. To build this list, we started with a broad set of security, privacy, and technology-related terms and their combinations, such as 'Cybersec,' 'Security expert,' 'tech-savvy,' 'Developer,' etc. Then, we used the snowball sampling technique [71] by filtering the author biographies and finding additional keywords that were added to this initial list. This was done iteratively until no new keywords were found. Figure 9 in the appendix lists 21 distinct keywords.

Using these, we identified 1,065 unique tech-savvy/ expert users. We validated our keyword-based filtration by employing a stratified sampling approach, randomly selecting 50 author profile descriptions from a pool of 1,065 unique expert users and 500 from a pool of 167,664 other users, and two coders manually labeled these 550 descriptions. The Kappa score was 0.99, which shows near-perfect agreement. We found an accuracy rate of 99% between the manual label and labels obtained by the filtering approach. Two instances were incorrectly classified as experts, while one was incorrectly not classified as an expert. Our keyword selection process aimed to balance identifying as many experts as possible while minimizing false positives. The low false positive rate and high accuracy indicate that our filtration method successfully achieves this balance, making it effective for the purposes of this study despite potentially missing a small number of experts.

We then distinguished tweets related to four circumvention technologies, i.e., Starlink, proxies, TOR, and VPNs. Since the relevant posts had already been obtained, we used keyword filtering to find the posts about each CCT. Keywords consisted of the terms related to these tools and their equivalent in Persian were used. We found 69 tweets from *tech-savvy/expert* users about proxies, 144 about Starlink, and 544 about VPNs, compared to higher counts from *other* users: 3,925 for proxies, 12,037 for Starlink, and 72,901 for VPNs. To qualitatively analyze these tweets, we obtained all the tweets that were posted by expert users (757) across all three circumvention technologies and obtained a random sampled ordinary users' tweets: 1,300, 400, and 300 for VPN, Starlink and proxies, respectively from the Persian dataset and aggregated that with all the other users' tweets in English, totaling 2,438, 1900, and 666 for VPNs, Starlink, and proxies. To identify major topics in English and Persian, the open coding process was conducted [74]. This was done iteratively so that new themes were added or existing ones were reorganized. After the process ended, similar themes in English and Persian were merged together.

In the next sections, we present a qualitative analysis of the three CCT tools, organized according to their mentions' volume. Note that we translated Persian tweets into English for ease of understanding. For each identified topic of discussion, we also report the number of posts we identified in all 5,761 posts, indicating the prevalence of that theme.

4.2. Discourse regarding VPN

Other user's queries on VPNs: Due to the restrictive internet policies and shutdowns, people increasingly relied on VPNs as a bypassing tool, leading to a variety of inquiries, and the following themes were identified: (1) **VPN performance inquiries and recommendations (n= 672):** The majority of the questions consist of the ones in which users asked questions from others about the effectiveness of VPNs. Users were asking about the best and most effective ones that were working and, in some cases, were asking for

VPNs to connect to various social media platforms: "Which VPN do you use to access Instagram? My VPNs barely connect and often drop," or "tried more than 10 VPNs, then I'm twitting now." We found in our English dataset that some users were often providing a list of free VPNs that are working. (2) **VPN usage inquiries (n= 156):** We found that users were proactively asking companies to provide free, premium VPN: "ProtonVPN. I was wondering if you could give Iranian people a free premium account." The process of purchasing, installing, and setting up a VPN was a frequently discussed topic, e.g., "How can I install a VPN if I don't have a VPN to download it in the first place?" (3) **Providing configurations (n= 102):** Interestingly, we found users were sharing configurations to the VPN they opened, e.g., "I have opened a VPN in Turkey, via vpngate: aa.bb.cc.dd." (4) **Security concerns (n= 63):** Many users were concerned about the security of VPN services. They either asked for VPNs that others were confident about their security or inquired about the security of the VPN that they were using at that time. Some examples are: "How can we know if the VPN we are using is secure?" or "Is Argo VPN really safe?" Additionally, we saw some users were asking for secure download links for the VPNs, which was mostly observed in our Persian dataset. (5) **Device specific issues (n = 46):** We observed that users had different experiences with different devices. While a VPN may work well on one of their devices, it might not work as expected on the other one, which leads them to ask questions to understand this problem. In some cases, users were even aware of this compatibility issue, so they looked for VPNs compatible with their device or operating system. For example, a user had asked: "What VPNs work on iPhones?" "What VPN are you using for Windows? I've been trying everything for two days, and it's not working." (6) **Collective solution seeking (n= 13):** Some users discussed the possibility of purchasing and sharing a VPN. For instance, in Persian dataset, a query that illustrates this scenario is, "Can a single VPN account be shared among multiple users, or is one needed per individual?" This is because not everyone could afford the premium version of VPNs, and most conventional credit card payment methods are prohibited [81]. Hence, users with access to the premium versions were asking if they could share their VPN account, showing community resilience and support. Additionally, there was a significant interest of Iranians living abroad in providing help which was evident in both datasets, asking questions such as: "Can we (Iranians outside) buy VPNs so Iranians inside the country can use them? Do you know which VPN is best to use?"

Tech-savvy/experts insights on VPNs: Experts' pivotal role in guiding the general public using VPNs manifests in their tweets and reflects their deep understanding of both technical and socio-political aspects of VPN use. (1) **Server management (n= 44):** We encountered instances in our Persian dataset where experts emphasized the importance of having and managing personal servers to avoid being detected or banned. For example, an expert user suggested, "Running your VPN on personal servers on port 443 reduces the chance of being blocked significantly, especially with protocols like v2ray," (2) **Support from companies & community (n= 43):** We observed experts tagging VPN companies and echoing the need for free VPNs. This phenomenon has been exemplified in the following tweet, "This is the time we need major #VPN providers allow users get their services for free to bypass filtering: NordVPN, surfshark, expressvpn, CyberGhost_EN." Additionally, experts were asking users to donate funds for purchasing VPNs and providing them for free. Experts were asking users to transfer bitcoin. Interestingly, this was only observed in our English dataset, (3) **Providing configurations and educational outreach (n= 41):** In Persian dataset, we found that experts were proactive by providing configurations to VPNs and also providing users with resources to setup their VPNs, and suggesting effective VPNs, "Here's how to build your personal VPN using servers abroad to ensure it functions effectively," "... give ProtonVPN a try; its new protocol currently cannot be blocked," "Proton VPN has a mode called Stealth. When you set it to this mode it becomes more stable and disconnects less often. It also has lower ping, automatic switch, and higher security." Additionally, experts were echoing that users could buy premium VPN using bitcoin: "Dear friends who are familiar with crypto, you can use the Windscribe VPN. The Pro account accepts crypto payments," and (4) **Security risks associated with downloading VPNs from unverified sources and ISP blocking (n= 27):** We found that experts were warning about the installation of unauthorized VPN services that might carry malware. One expert strongly advised, "Be cautious and only install original VPN software from reliable sources like Google Play," in another instance, an expert mentioned that "Our people have been affected by the spread of unofficial and harmful software, such as GB WhatsApp and fake VPNs ...," "Beware of the Instagram page [USERNAME], selling VPNs; they are actively deceiving people. I fell victim myself." Interestingly, this was only observed in our English dataset, where experts were warning people of Instagram pages that are deceiving. Additionally, unusual changes in the filtering status of some VPNs raised suspicion among experts, as they posted tweets to make aware of these suspicious changes, e.g., "...OpenVPN has been unexpectedly unblocked, raising suspicions about potential surveillance," Additionally, tweets from experts were echoing how some ISPs used sophisticated detection and throttling techniques to identify and slowed down VPN traffic, which was evident in Persian dataset: "[A cellphone provider]'s bandwidth has decreased drastically today and most of the VPNs have been disconnected."

4.3. Discourse regarding Starlink

Other user's queries regarding Starlink: (1) **Dire need of Starlink (n= 1,030):** Users were proactively echoing the need for Starlink because of the massive internet shutdown. Users were tagging *Elon Musk* to activate Starlink and seeking news and updates on internet accessibility, demonstrating a level of anticipation for the launch

of Starlink. (2) **Connectivity discussions (n= 164):** Conversations around connecting to Starlink and exploring its features reflected a curiosity to understand and utilize the technology effectively. One query in this realm was, "How can we connect to Starlink? Share if you have insights." Interestingly, in both datasets, users were celebrating that Starlink is active: "Want to give a shout out to elonmusk for allowing the Iranians to use #Starlink. With this device, they can keep fighting for freedom," (3) **Questions about infrastructure, connectivity, and cost (n= 102):** We found that users were actively seeking information about the status and process of acquiring Starlink equipment, showing an interest in embracing technology and addressing concerns. For instance, one user mentioned, "Mr elonmusk we are ready to pay with $USDT cryptocurrency. Provide us with #Starlink equipment." Additionally, they were discussing how they connect to Starlink, reflecting a curiosity to understand and utilize the technology effectively, (4) **Concerns about feasibility (n= 59):** Some skeptics doubted the feasibility of implementing Starlink and hinting at restrictions on usage. Tweets were also suggesting that Starlink would not work because either it is too expensive or the equipment would eventually be caught this was observed in both the datasets, and (5) **Detection and security (n= 34):** Users seemed to be wary of the surveillance risks associated with using Starlink, expressing concerns about the tracking. Users often asked, "Can Starlink devices be traced?," "Hello, Mr. Elon Musk Please try to make Starlink satellites undetectable and its radiation undetectable..."

Tech-savvy/experts' insights on Starlink: (1) **Announcements of Starlink activities (n= 34):** Reports on Starlink's progress were reported, indicating efforts by the company to make the service available. Experts amplified this in the following tweet: "Around 100 Starlink terminals are now active in Iran." (2) **Privacy risks of using Starlink (n= 28):** Experts advised that using Starlink to browse websites could potentially expose users' identities through traceable IP addresses which we mostly observed in the Persian dataset. For instance, a tweet from an expert stated, "Connecting to sites via Starlink could reveal your IP and personal information." Experts also urged vigilance when dealing with sellers and impostors advising, "Starlink does not operate through dealerships; refrain from disclosing details." Additionally, experts echoed that fake and malicious Starlinks apps are widely available and emphasized the dangers of downloading apps claiming to offer Starlink access as they could be Trojans: "My antivirus detected threats after attempting to connect with Starlink. Beware of trojans!" Additionally, clarifying that the presence of Starlink satellites did not guarantee service availability, e.g., "Active satellites visible do not indicate service availability in Iran." (3) **Urgent need for Starlink (n= 26):** Due to heavy Internet censorship, experts called on Elon Musk and the international community to activate Starlink faster. This is a common theme in both ordinary and tech-savvy users and across both the datasets, showing the depth at which users needed Internet access. The following tweet exemplifies this: "Dear Mr. Elon Musk, we ask you to activate the Starlink Internet for us because the Internet may be cut off soon." (4) **Providing technical information on Starlink (n= 21):** Experts echo the possible speed reductions of Starlink mentioning that at that point, Starlink only accommodated around 25,000 to 30,000 subscribers in Tehran, and speed could decrease as new subscribers join the network.

4.4. Discourse regarding Proxies

Other user's queries regarding proxies: Through our qualitative analysis, we found the following broader topics that ordinary users were asking about proxies: (1) **Crowdsourcing Proxies (n= 212):** We found that users were frequently calling on others and VPN companies to help them by providing proxies. Additionally, they were echoing the need for platform-specific proxies, such as: "Please explain how this Twitter proxy works?" Moreover, many users were praising people who successfully setup a Signal proxy, which was seen exclusively in the English dataset. (2) **Creating and providing configurations for proxies (n= 129):** The development and application of proxies were areas of interest among individuals. A technical question originating from a user and exemplifying this is: "How can secure proxies be created? What are the expenses?." (3) **Technical issues with proxies (n= 90):** Users sometimes encountered technical issues that hampered them from using the proxies properly. These problems were voiced through questions like, "Why doesn't the Telegram proxy work without a VPN?" Additionally, users were mentioning switching proxies in hopes of achieving faster speed or stability. However, there was a possibility of losing connection entirely when connecting to a new proxy. (4) **Security and Privacy concerns (n= 34):** Many individuals had doubts about the security and reliability of proxies, e.g., "Are these paid proxies safe, or should I not buy them?" Additionally, in the English dataset, we found that users were telling people not to share proxies on social media but rather to DM people and ask for them. Additionally, warnings related to fake VPNs and proxies were being echoed by the community. (5) **International Support Queries (n= 32):** We observed that people overseas were greatly interested in helping, but they often lacked the knowledge on how to do so, e.g., "Does anyone know an effective way to set up proxies for our friends and family?" is a heartfelt question from overseas.

Tech-savvy/Expert's insights on proxies: The following themes were obtained from analyzing expert's tweets: (1) **Instructional guidance on proxy setup and usage (n= 40):** Experts provided detailed instructions, configurations, and guidance on how to set up a proxy, and sometimes yielding list of free proxies that people can use. For example, "Overseas friends, please set up a server in Iran and one in Turkey, and then run the following command on the Iran server. This way, you provide us with a SOCKS5 proxy that works in browsers and Telegram. For Android, just use the AndProxy app," (2) **Built-in messaging platforms proxies (n= 15):** Experts constantly highlighted the importance of platform-specific built-in proxies, sharing their feedback: "...

Users could now connect to WhatsApp over a proxy. Update your iPhone if you have one, and use the instructions and file I've posted in the Telegram channel if you have an Android device," (3) **Utility and reliability (n= 11):** Experts emphasized the importance of proxies, especially during times of complete internet restrictions. One expert shared their experience: "During internet completele shut down, we used one of our company's technological networks to establish a tunnel and proxy to the outside world." Experts were echoing and encouraging improvements to the current proxy technologies, e.g., the current need for a secure in-build proxy messaging apps. (4) **Security and Safety Warnings (Posts= 6):** Experts warned users about the risks and dangers associated with using proxies, especially in terms of security and the possibility of being monitored, as one expert gave advice stating that "When someone introduces a proxy, proceed with extreme caution and ideally, avoid using them if you don't know them."

Summary & Discussion of RQ1: Our examination of tweets from tech-savvy/expert users and other users revealed that their consideration of various circumvention techniques consisted of S&P concerns as well as finding effective solutions. In our examination regarding *VPNs*, the public's questions mainly revolved around the best and most effective VPNs (n= 672). On the other hand, tech-savvy/experts stressed the importance of managing servers (n= 44) and providing configurations, and educational outreach (n= 41). Additionally, regarding *Starlink* indicated a community that is enthusiastic about potential connectivity solutions (n=1,056); however, concerns regarding its cost (n=102), feasibility (n=59), and traceability (n=62) of Starlink were of paramount concern. Moreover, we discovered that discussions around *Proxies* highlight the need for community support in addressing S&P and reliability issues (n=212). Based on our findings, we provide the following recommendations: (1) **Mining social media for obtaining real-time user feedback is paramount in times of severe internet censorship**, which can provide important feedback about S&P concerns of users, as well as integrate the concerns into their design process, can help users effectively bypass censorship. (2) **Transparency of S&P of various bypassing tools is essential**, given the fact that all users echod the issues around S&P of using *VPNs*. It is crucial that companies inform the users about the strengths and how their tool protects them from possible surveillance in a transparent way, echoing the recommendation by [63]. (3) **Proactive detection and moderation of malware and misinformation about the use of CCT tools is crucial**, especially when social media platforms lack such moderation [65]. Hence, online communities, social media platforms, and credible third parties could help mediate S&P discussion to detect malicious VPNs/proxies, provide credible sources, and moderate the content to stop their spread on social media [76].

5. RQ2: In-depth analysis of Twitter discussions about VPN services

In a constant battle between internet freedom and censorship, users constantly searched for VPNs that work properly. In this section, we analyze this phenomenon by understanding which VPNs saw a surge in use and which VPNs saw a downward trend. Additionally, we aim to determine the causes of such variations and the specific technical aspects that users discuss.

5.1. VPN Names Collection

To systematically identify different VPN services mentioned on Twitter, we integrated four distinct data sources. This multi-source approach assures a broad capture of VPNs, covering English and Persian languages and reducing biases related to any single data collection method. These sources are: (1) **Twitter dataset:** We initiated a targeted search on our Twitter dataset for VPNs' names, applying the use of pattern-matching techniques for the selection of tweets discussing VPNs. We retrieved 103 English and 14 Persian VPN names, (2) **VPN-Dedicated websites:** We searched for websites dedicated to discussing and reviewing VPNs, such as CNET [82], Bleeping News [83], etc. We identified another 25 English VPN names. (3) **Reddit threads:** Using "r/VPNTorrents," which provides in-depth guides, a regularly updated VPN list, and resources for VPNs, we gained an additional 97 English VPN names, and (4) **Telegram channels:** We used popular Telegram channels ($\sim$100k followers), focusing on sharing VPN/Proxy resources, along with channels with similar utility whose URLs were embedded in the tweets in our dataset.

In total, our extensive search yielded 396 different VPNs. However, we found some duplicates, as one VPN can have different versions in English and Persian. Therefore, we removed duplicates by consolidating them into one entry. This process yielded 107 different VPNs, which can be found at: https://tinyurl.com/5nkfjaxh.

Analysis of VPN Mentions: We analyzed the VPN mentioned in our dataset. Figure 5 shows the distribution of VPNs discussed among users. We found that 11 different VPNs were mentioned more than 100 times, with Proton (15.3%), Argo (10.6%), and Express (11.0%) VPNs being the highest-mentioned VPNs across our dataset. We also observed that about 67 VPNs (62.62%) were only mentioned between the range of 1–10 times. However, in total, they contributed to 19.4% of the VPN mentions, shown as "others." Some VPNs' higher mention counts—especially those that receive hundreds of mentions—indicate that a tiny subset of VPN services once dominated the conversation. This suggests that these VPNs were more popular than others, which could be due to their being more reliable, effective, or accessible compared to other technologies. We study this matter in more detail.

Temporal Trends in VPN Service Discussions: Figure 6 provides a segmented depiction of the percentage of

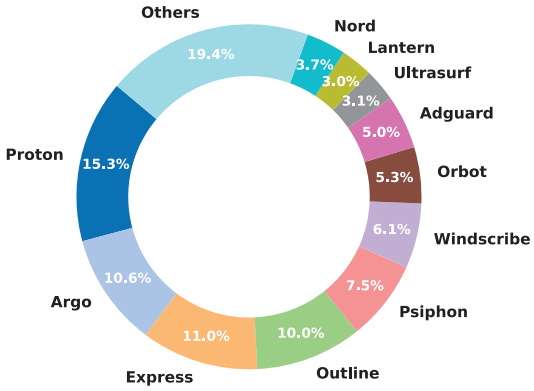

Figure 5: VPN usage distribution

VPN mentions in our dataset compared to total mentions, providing insight into the weekly changes of conversations surrounding VPNs. We could not do the weekly analysis for our English dataset due to a small number of posts. To guarantee that the services we analyze were heavily discussed, Figure 6 only illustrates VPNs with over 90 mentions, including Windscribe, Argo, Ultrasurf, Psiphon, Express, Adguard, Lantern, Proton, Orbot, and Outline. Interestingly, *Proton* saw a 30% increase in the number of mentions in the early months of October. This coincides with the fact that Proton VPN created a new feature to disguise VPN traffic, and this stealth feature was provided for free [84], [85]. At the same time, we observed an opposite trend in *Outline* VPN, as there was a significant decrease, which can be attributed to the sophisticated tactics to block and target Outline VPN [24], [25]. Additionally, we observed that *Ultrasuf* had a variable interest change, where the VPN mentioned saw almost a 5% increase in the number of mentions in the week of September 26th and a sudden decrease the next week with a constant rate of mention in the subsequent weeks, furthermore *Orbot* saw a sudden jump in the mentions in the later week of January.

We qualitatively analyzed the tweets to further examine trends for all VPNs. We randomly sampled 20 tweets from the top ten most discussed VPNs for 20 consecutive weeks, i.e., 4K tweets in total, in our Persian dataset, and analyzed 180 tweets in total that mentioned Nord, Express, Proton, and Outline VPNs in our English dataset.

Case study: Proton and Outline VPN: Figure 6 shows that there was a sharp increase in the week of October 3rd, 2022, for Proton and an initial sharp increase for Outine in the week of September 26th, 2022, followed by a sudden drop. Analyzing the tweets from these dates provides more insights into the sudden jump and shift of these two VPNs.

Proton VPN: Initially, we observed users were discussing the reliability of ProtonVPN. Users were attesting to its efficacy and even urging others to buy ProtonVPN subscriptions. An example from week 3:"ProtonVPN is good, friends. It connects easily for now," and an example from week 4: "Use ProtonVPN. They have a free plan that allows you to send and receive data anonymously." However, that suddenly changed when users echoed and reported outages in ProtonVPN. An example from week 12:"Strong VPNs like Express and Proton have stopped working," and an example from week 13:"Guys, can you recommend a few good VPNs? Proton has burst," This shows that not all the time many mentions of VPNs show their reliability, but sometimes users discuss their limitations and ineffectiveness, e.g., "I used Proton for a while, but it's completely destroyed. Speedify is working for now." ProtonVPN's mentions in conversations significantly declined following this peak, on week 15, suggesting that the community might have stopped using it, evident from users' posts on Proton VPN's official Reddit page.◇ The qualitative examination of these conversations shows the community's flexibility in seeking fresh answers to shifting conditions.

Outline VPN: Figure 6 shows a sharp increase in the number of mentions for Outline VPN in the week of September 26th. We found that users initially posted positive tweets about it: "Google has activated Outline VPN on its front page!" Some users were also posting information on how to make OutlineVPN servers more resilient against blocking: "(1) Use a domain name and rotate IPs (2) Use a 2-hop system (3) Do packet manipulation to confuse the censor Follow along." But this excitement was quickly destroyed by an obstacle that they encountered. They needed an international credit card to pay for Outline VPN services. However, Iranians do not have access to these banking services because of the sanctions: "Outline VPN has a few limitations: only someone with access to a valid credit card can set up the server..." We observed a decline in Outline VPN's mentions in the preceding weeks.

Users preferences in VPNs: In our qualitative analysis of 4K VPN-related tweets from the Persian dataset and 180 VPN-related tweets from the English dataset, we labeled the reasoning, concerns, advice, and preferences of users and obtained their frequency. Figure 7 shows the different preferences that users seek in VPN, the common issues & concerns with VPNs, the community effort, and how users overcome financial challenges. As we can observe, users seek *affordable* (119) and *fast* (93) VPNs as the main key features. Additionally, one of the most prominent problems that users encountered was *connection failure* (179), and hence, we observed that users were frequently inquiring about the *connectivity* (103). Furthermore, users were echoing companies and other users to provide them with *free versions* (103). We also observed that many tweets shared information about *servers* (179).

5.2. Exploration of VPNs' technical aspects

To further investigate the discussed technical aspects of VPNs, we first used keyword matching to identify tweets relevant to *access keys*, *bridges*, *protocols*, *configurations*, and *servers* in the VPN ecosystem. It is quintessential to investigate these components, as in our qualitative analysis of tweets, we found that users often shared these five topics.

◇. The thread can be accessed here: https://tinyurl.com/yx2cn7bv

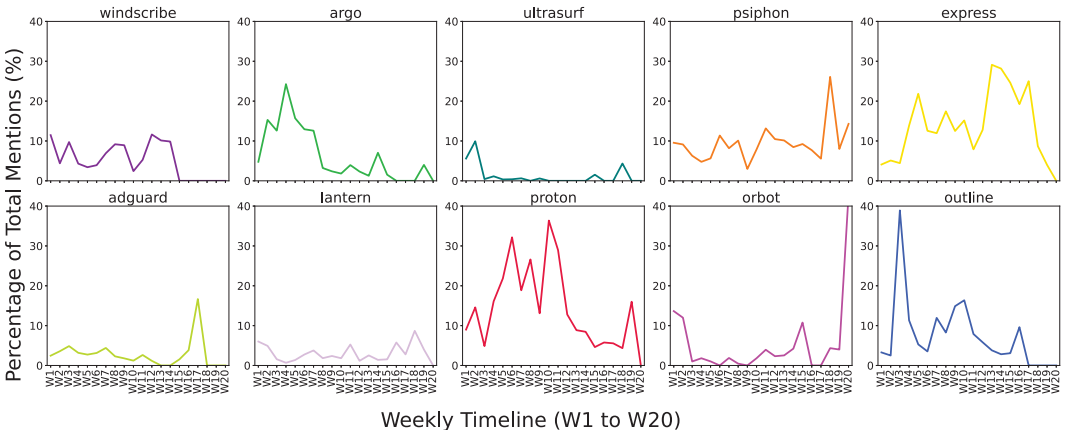

Figure 6: Weekly percentage of popular VPN mentions relative to total mentions

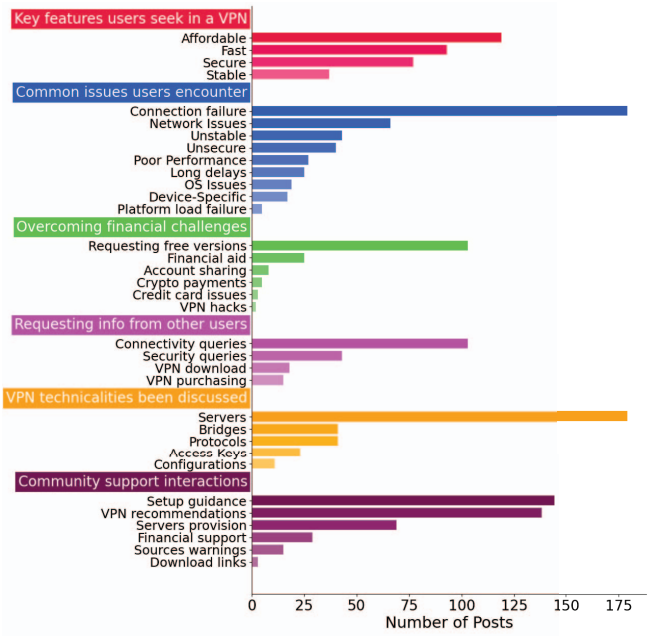

Figure 7: Tweet volume by VPN theme: features, challenges, and solutions

Definitions for each component are given in Section C in the Appendix. The keyword matching retrieved *access keys* (n=139), *bridges* (n=295), *protocols* (n=596), *configurations* (n=372), and *servers* (n=3,255) related tweets. To validate the accuracy of the keyword matching, we conducted a manual analysis on a random sample of 100 tweets for each component and found an accuracy of more than 90% for all the components, indicating that the retrieved tweets were indeed relevant to their respective technical aspects. We then analyzed all the retrieved tweets to identify three critical themes and understand their role in maintaining Internet freedom. Due to the large number of tweets related to *servers*, we analyzed a random sample of 500 tweets. Note that TOR relays are public, but can be blocked by governments or ISPs. However, TOR bridges are relays in the network that are not listed in the public TOR directory, which makes it harder for ISPs and governments to block them [86]. A popular example of this is Snowflake [87].

(1) **Security concerns (n= 291):** Users often worried about the security of their data and unauthorized access. They discussed the challenges of finding trustworthy and reliable *bridges* and the security dangers associated with using bridges from unverified sources. In a tweet, a worried user writes, "...is it safe to take bridges from an anonymous source, or will they steal our IP and information?". Additionally, an emphasis on strong encryption algorithms to protect user data and ensure anonymity in the existing *protocols* and *configurations* was observed. Additionally, concerns extended to the distribution of *access keys* for VPNs like Outline. Despite the official advice against sharing these keys [88], some users manipulate this guidance to foster a sense of exclusivity and safety. For example, a tweet suggests, "Make sure to install the Outline software yourself from the store to ensure its safety. Only get the activation code from me." This example shows that users might trust these people rather than the official guidelines, as they feel safe getting access keys from these users, hence adding exclusivity for these users. Moreover, reflecting an acute awareness of these security concerns, one user expressed the desire to enhance security by inquiring about the feasibility of acquiring a personal dedicated *server* outside Iran.

(2) **Performance & Troubleshooting (n= 353):** Users shared a positive experience using stealth *protocols*, by actively promoting it: "Set the protocol to stealths on 443 in windscribe. It functions quickly and effortlessly." They also discussed the performance and reliability of *configurations*, sharing their experiences with the ones that provide maximum speed and dependability. We observed that there was a special focus on *servers* in which countries provided the best connection quality. The performance of *bridges* was a key topic of discussion among users, "Since yesterday, the speed has really slowed down, and only the orbot snowflake bridge is working." This aligns with the findings from [39], [66]. In discussions about *access keys*, variations in performance

emerged. Users reported varied connectivity levels, with some noting weak connections despite successful setups and asking if others had different experiences.

(3) **Recommendation & community sharing (n=291):** We identified three primary methods users employed to provide *access keys*: (a) posting direct links to websites, (b) encouraging users to join specific Telegram channels or send emails, and (c) direct messaging (DM) the user. In addition, users offer links to Telegram channels where *bridges* and *configurations* can be found. They also actively and regularly distribute and recommend hard-to-block *protocols*, such as WStunnel [89]. An example of such sharing is: "Use WStunnel on your VPNs (including Windscribe). It's hard to block..." Furthermore, there is a notable practice of community members updating and sharing new *server* information beneath their posts, enabling others to access more current and potentially uncensored resources.

Summary & Discussion of RQ2: Findings from RQ2 reveal how users' discussion around VPN usage and preferences evolves in response to challenges and security concerns. Figure 6 shows users' preferences are not static but dynamic due to the shift toward more reliable and effective VPNs. Significant patterns emerged from the qualitative analysis of VPN-related discussions, highlighting user preferences, the issues and concerns they faced when using those services, and their impact on end users. Furthermore, technicalities discussed regarding VPN services (n=353) and security (n=291) of VPN emerged as the prominent concern, wherein users echoed the dangers associated with using configurations from unverified sources and the need for strong encryption standards. Towards this, we provide the following recommendations: (1) **Transparency is vital for VPN service providers**, especially given users' concerns about S&P. Companies must clearly inform users about how their tools ensure protection against potential surveillance. (2) **Providing trustworthy resources for furnishing configurations is pivotal**, as these collaborative efforts from various credible third parties, researchers, and companies can help users access secure and reliable information. This can help bridge S&P information of users online and provide a platform for companies to share important security and privacy information on time, e.g., patches, secure and free access keys, etc.

5.3. Twitter discussions about TOR

TOR is one of the most well-studied CCT tools in the security and privacy community. While Tor is not explicitly designed to circumvent censorship, it is often used for that purpose due to its ability to mask users' identities and access restricted content. Its primary focus is on providing anonymity and privacy, but many users leverage its features to bypass internet restrictions. The first publicly available version of TOR was released, originally known as "The Onion Routing Project [90]." The project aimed to provide anonymous online communication by routing traffic through multiple volunteer-run servers to obscure users' IP addresses. Over the years, TOR has continuously

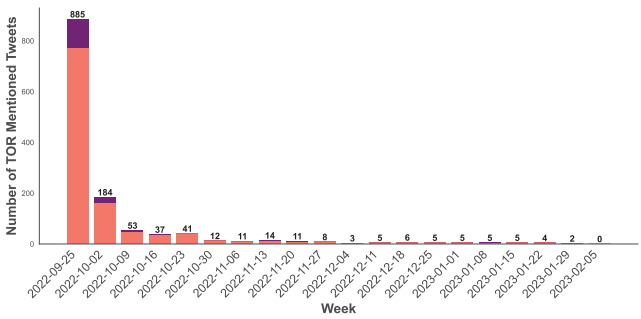

Figure 8: No. of TOR tweets by week. Purple represents English, and orange represents Persian

evolved to address security vulnerabilities and improve performance [91], [92], [93]. Today, TOR is considered a key player in the broader privacy ecosystem, collaborating with other privacy-enhancing technologies like VPNs and decentralized platforms. To identify TOR-related tweets, we employed keyword-matching filtering using "TOR" and its equivalent in Persian and identified 1,296 tweets.

Figure 8 shows the number of tweets that mention TOR on a weekly basis. In the first week, we observed that 60.3% (534 out of 885) of the tweets either recommend TOR, explain how to use it, or report successful connections. Conversely, 9% (80 out of 885) report it not working, mainly from the second day onward. Interestingly, 6.5% (58 out of 885) requested help from Iranians abroad to donate bandwidth and data as TOR proxies using Snowflake. We found 5.6% (50 out of 885) mentioned TOR was working but with poor performance, while 3.9% (35 out of 885) complained about difficulty in downloading, installing, or configuring TOR, sometimes noting confusion about which TOR-related app to use. Only 1.5% (13 out of 885) discussed about TOR's security. From the second week onward, we observed increased negative sentiments about TOR, with recommendations dropping to 24% (44 tweets). Of 184 tweets this week, 15% (27) reported it not working and its inaccessibility, and 15% (28) complained about its poor performance. Two instances mentioned that TOR only works for web browsers, not for other apps. Four instances note it is not user-friendly, and three mention difficulties downloading it safely due to Google Play and App Store being filtered. Interestingly, there is mention of someone from abroad offering assistance. In the third week, a further decline in TOR-related tweets (down to 53, with only four recommending it) is seen. Notably, 21% (11 tweets) discussed the spread of a fake TOR app that traces users' device apps. Eleven tweets (21%) reported TOR being completely blocked. Complaints about poor performance persisted, accounting for 17% of tweets. In weeks 5 and 8, some users began associating TOR with hackers and the dark web, expressing security concerns. Since December, users reported the blocking of public TOR bridges and the inability to share multimedia, only accessing text-based news. At this point, tweets drastically decreased to 4-5 per week and eventually disappeared altogether.

In summary, this shows a progression from initial enthusiasm to disappointment as technical and security challenges mount. To maintain its reputation and efficacy, TOR must continue evolving, not only to meet technical demands but also to provide clear and accessible user support.

6. RQ3: Monitoring Telegram channels

6.1. Detecting CCT discussions on Telegram

From our Twitter data analysis, we noticed several posts that asked users to visit Telegram channels to download various CCTs. Thus, to get a better idea of how the flow of adopting these services continues on Telegram, we focused on evaluating the content shared on VPN-focused Telegram channels and their corresponding discourse and adoption by users. We utilized the Telegram API [20] and Telethon client [21] to collect posts from 34 unique Telegram channels mentioned in tweets from our Twitter dataset, as well as 47 popular Telegram channels (∼100k followers) compiled from Telemetr.io [94] that are frequently used for sharing CCT resources. Telemetrio is an online database of Telegram channels across various languages and categories, and for our purposes, we specifically looked for channels whose primary language was Persian and contained the term "VPN" in either their channel name or description. Additionally, we manually verified the first ten posts of each channel to make sure they met our criteria for VPN channels. Table 3 shows

TABLE 3: Descriptive statistics Telegram dataset.

	Shared Channel/ Popular Channel			
Feature	Mean	Min	Max	Med.
Views	62K/61K	205/ 35	2.4M/ 4.5M	145K/ 250K
Forwards	274/ 308	0/ 0	174K/ 50K	1.0K/ 733
Followers	341K/ 714K	2/ 98K	6.8M/ 4.7M	2.3K/ 200K

the descriptive statistics. We obtained 39,876 posts from *shared* channel and 14,531 posts from *popular* channels. Note that, unlike Twitter conversations, most communication in Telegram channels is unidirectional, i.e., the admin posts content that members can react to and forward but cannot reply to, except in select instances where replies are enabled.

Overall, the 81 channels shared 1,459 unique VPN installation files, with an average of 71 files shared per channel ($Med. = 9$). Most of these files (89%) were executable installers specifically designed for Android devices (.apk). This focus on Android is logical given the high prevalence of Android devices in Iran [95]. In addition to VPN files, the channels distributed over 2,453 files, enabling direct connections to proxy servers through the Telegram app. Among these, 1,763 (72%) were HTTP Injectors, and 690 were VPN configuration files, facilitating easier setup and use. Furthermore, 168 text files were shared, each containing several proxy addresses ($Med. = 180$) that users can configure to access the internet. Interstingly, 55% (n=807) of these shared files were "cracked" or "free" versions of commercial VPNs. In addition to copyright infringement issues [96], such jailbroken tools often contain malicious software embedded [97], [98], which can cause harm to the user. Similarly, malicious proxy servers/network gateways are often used by attackers for constructing botnets [99]. Considering the large number of users who access these channels, it was paramount that we also explored the presence of malicious activity in these channels.

6.2. Malicious activity in shared resources

To identify if a shared file/IP (as part of a proxy) was malicious, we used the VirusTotal API [100]. VirusTotal is an online tool that aggregates detection scores from 80 security tools. For both malware and malicious IP detection, we utilize a detection score of 2 or more for labeling, a threshold which has been established in prior literature [101]. We found 125 (8.5%) files were malicious, with an average detection rate of 3.7 engines ($Med. = 2$). Overall, these files targeted 53 unique VPN services, such as Outline VPN, Argon VPN, and 28 were detected as keygen/cracked software, 62 were detected as spyware/keyloggers, and the remaining were detected as malware. Conversely, out of the 28,988 unique proxy addresses (IPs) shared through 168 *.txt* files, 1,730 IPs (5.9%) were detected as malicious. On the other hand, 31 out of 690 VPN configurations were malicious (4.4%), and the HTTP Injections were 221 out of 1,763 (12.5%). Thus, our findings indicate that while popular VPN/Proxy-focused channels on Telegram provide users with resources for bypassing internet censorship, a significant portion of the content shared is malicious and can harm users. Several factors can contribute to malicious content appearing in these popular VPN/Proxy-focused channels on Telegram. A primary cause may be the lack of rigorous vetting or oversight of the legitimacy of the shared software. Also, given the tendency of these channels to distribute "cracked" or free versions of VPNs, distinguishing between a genuine threat to users and an exploit can prove challenging. This can inadvertently lead to a scenario where hundreds of thousands of subscribers can be accidentally exposed to malicious software. In more closely examining the impact of malicious files shared in Telegram channels, we concentrated on user interactions under posts shared with the reply feature enabled. We analyzed 20 such cases. In total, out of the 20 posts, interactions occurred under two channels, with one of them receiving the highest number of interactions of 19,198 replies, which highlights the widespread use and potential impact of the malicious file among a large group of users. 1 "Post: [MASK]": This threat received the highest number of responses, i.e., 19,198; 5% of the responses were echoing that the shared malicious file was being used by the users. 2. "Post: [MASK]": This thread had 114 replies, and among these, 17 contributors specifically described the installation of the VPN. Most shared their experience with the VPN's performance, meaning it had been actively used, and there was initial satisfaction with the software. On the other hand, the remaining 16 channels did not receive many or any reactions from users.

6.3. VPNs' technical aspects in Telegram

We found 475 aggregated posts directly related to VPNs on Telegram channels. We took a random subsample of 20 and obtained the first 100 replies for each, adding all responses with fewer than 100 replies. We found the following technical aspects, i.e., *injectors* (77), *access keys* (1,213), *modded VPNs* (19), *backups* (51), *Falcon* (2,700), and *bridges* (921). After analyzing the posts about these, we identified three themes similar to those obtained on Twitter:

(1) **Security concerns (n= 184).** VPN discussions in Telegram channels frequently emphasize security, with frequent inquiries about the safety features of *injector* tools. Questions like "Is this HTTP Injector safe?" Concerns about the safety and legality of using *modded VPNs* are prevalent, with a user expressing caution about potentially malicious APKs disguised as free or modded VPNs. User's concerns regarding security extend to the *Falcon* configurations, wherein Falcon can be used for hacking. For instance, a user warns: "Don't use Falcon, it hacks everything; only use a bridge." We found that members actively inquired about the security of the tools such as *bridges*, exemplified by questions such as, "If you have a secure bridge, please send it." Additionally, *access keys*, are often exchanged within the Telegram community, much like they were previously shared on Twitter. Security & safety concerns related to *VPN backups* were identified in community discussions.

(2) **Performance & troubleshooting (n= 588).** Discussions often cover troubleshooting and performance optimization on *injectors*, such as: "I've been connected with this injector for a week now, its speed is great, you need to give it a new code." The performance of *modded VPNs* is also a significant topic of discussion. Whenever a modded version of a VPN gets shared, feedback often centers on its efficacy. Feedback from users about the quality of *backups* is also frequent. Ranging from positive feedback: "Best filtering and backup..." to negative ones, "... yours none connected, but I tried three backups myself, and they worked." Similarly, users have expressed mixed opinions on *Falcon's* performance. In addition, the efficacy of *bridges* is a recurring topic, with community members discussing the performance and reliability of different bridge configurations. Users provide real-time feedback on the effectiveness of bridges, which informs others about which bridges to use and when to seek alternatives. Furthermore, discussions around the performance of shared *access keys* are prevalent, focusing mainly on speed and responsiveness.

(3) **Recommendation & community sharing (n= 351).** Users frequently explore *injector* tools' use and specific recommendations, endorsed as "HTTP Injector is better for you." *Modded VPNs* are praised for their enhanced features, such as additional server options and removed bandwidth limits. Users often share their knowledge on creating and updating the *backups*, posting: "Friends, today I will put up a tutorial on making Thunder backups." Additionally, detailed tutorials and steps for setting up *Falcon* are prominent in discussions, providing a step-by-step process and helping new users navigate the setup more effectively. We have also observed that users not only exchange links and codes but also provide insights into managing and updating *bridge configurations* to ensure continued access.

Summary & Discussion of RQ3: We found that 8.5% of files that were shared on Telegram channels about VPNs were malicious, showing how Telegram is one of the popular ways for malicious users to draw their targets to this often unmoderated and closed environment [102], [103]. Additionally, we found that users are using malicious VPN files shared on the channels. We also closely observed the overall responses to the files shared on those channels and discovered that they had similar themes of performance feedback, recommendations, and security concerns as in *RQ2*; however, the technicalities discussed were different, e.g., users' echoed not to use *Falcon* configurations due to its S&P concerns. We provide the following recommendation: **Official channels of VPN providers are crucial**, as they can mitigate the issues associated with malicious sharing of configurations, APK files, etc. Additionally, this will provide the end user with a sense of security and can help the companies acquire customer feedback, helping them to provide better functionalities.

7. Threat Model obtained from users' concerns

Finally, based on all our analysis of discussions, we categorized threat models that CCT users are concerned about: **Location Tracking: (Section 4.3)** Concerns have been raised by the users on the traceability of CCTs, especially for technologies such as Starlink and the chances of authorities tracking the place of origin via IP addresses. **Network Traffic Surveillance: (Section 5.2)** A primary concern is the ability of authorities to eavesdrop on the network traffic, making users look for ways of encrypting and obscuring their activities online. This concern is reflected in user observations like "...OpenVPN has been unexpectedly unblocked, raising suspicions about potential surveillance." **Malware and Spyware Installation (Sections 4.2, 4.3, and 6.2):** Users are concerned with fake and malicious apps and configurations. They often inform and warn other users and ask questions about the safety of CCT tools. For example, "Our people have been affected by the spread of unofficial and harmful software, such as GB WhatsApp and fake VPNs ..." **Blocking the VPN traffic (Section 4.2):** Users describe elaborate techniques used by Internet Service Providers (ISPs) to detect and throttle VPN traffic, revealing that there is a constant cat-and-mouse hunt between Internet censors and CCT users. **Exploitation of security vulnerabilities in CCTs: (Sections 4.2 and 6.3)** There are frequent discussions and inquiries about the security of various CCTs and their configurations, indicating user awareness of potential vulnerabilities that could be exploited by adversaries.

8. Limitations & Future Work

Our analysis has some limitations. We used two data sources, i.e., Twitter and Telegram; however, we acknowl-

edge that using other sources, such as Facebook, Reddit, etc., could also be beneficial in providing newer insights. We acknowledge the limitation of not capturing all the expert users because not all experts have indicators in their biographies. We acknowledge the possible biases in our Twitter and Telegram datasets because they might only represent a certain section of the population who already use CCTs to access social media platforms. Additionally, our work does not consider discussions around other popular circumvention technologies, such as Psiphon, refraction networking, and V2Ray. Future scholarships can conduct longitudinal studies to monitor the long-term effectiveness and adaptability of these tools. This could involve tracking the evolution of censorship techniques and the corresponding responses of the bypassing technologies. Additionally, future work can investigate the use and effectiveness of these tools in other regions experiencing censorship and also other popular circumvention technologies that our work did not investigate.

9. Conclusion

This research showcases how security, privacy, and online discourse intersect by studying the utilization of tools to circumvent censorship during internet disruptions. It emphasizes the role of VPNs, proxies, TOR, and other potential connectivity options, such as Starlink, in ensuring communication in restricted settings. Furthermore, it highlights the impact on internet governance, user privacy, and the advancement of VPN technologies. The community's collaborative sharing of resources and shifting preferences for VPN services demonstrate user resilience and adaptability. Nonetheless, the discovery of malicious content in Telegram channels stresses the significance of user awareness and reliable information sources. Through insights into user behavior, preferences, and the socio-political backdrop of VPN usage, this research enhances our comprehension of resilience and the ongoing struggle for internet freedom in regulated environments.

References

[1] Y. Mou, K. Wu, and D. Atkin, "Understanding the use of circumvention tools to bypass online censorship," *New Media & Society*, vol. 18, no. 5, pp. 837–856, 2016.

[2] R. Ensafi, P. Winter, A. Mueen, and J. R. Crandall, "Analyzing the great firewall of china over space and time," *Proceedings on privacy enhancing technologies*, 2015.

[3] R. Ramesh, "Investigating the vpn ecosystem through the lens of security, privacy, and usability," Ph.D. dissertation, 2023.

[4] R. Ramesh, A. Vyas, and R. Ensafi, ""' all of them claim to be the best": Multi-perspective study of {VPN} users and {VPN} providers," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 5773–5789.

[5] R. Dingledine, N. Mathewson, P. F. Syverson *et al.*, "Tor: The second-generation onion router." in *USENIX security symposium*, vol. 4, 2004, pp. 303–320.

[6] L. Dixon, T. Ristenpart, and T. Shrimpton, "Network traffic obfuscation and automated internet censorship," *IEEE Security & Privacy*, vol. 14, no. 6, pp. 43–53, 2016.

[7] D. Fifield, C. Lan, R. Hynes, P. Wegmann, and V. Paxson, "Blocking-resistant communication through domain fronting," *Proceedings on Privacy Enhancing Technologies*, 2015.

[8] A. Mani, T. Vaidya, D. Dworken, and M. Sherr, "An extensive evaluation of the internet's open proxies," in *Proceedings of the 34th Annual Computer Security Applications Conference*, 2018, pp. 252–265.

[9] N. Weaver, C. Kreibich, M. Dam, and V. Paxson, "Here be web proxies," in *International Conference on Passive and Active Network Measurement*. Springer, 2014, pp. 183–192.

[10] M. J. Freedman, E. Freudenthal, and D. Mazieres, "Democratizing content publication with coral." in *NSDI*, vol. 4, 2004, pp. 18–18.

[11] T. Koponen, K. Amidon, P. Balland, M. Casado, A. Chanda, B. Fulton, I. Ganichev, J. Gross, P. Ingram, E. Jackson *et al.*, "Network virtualization in multi-tenant datacenters," in *11th USENIX symposium on networked systems design and implementation (NSDI 14)*, 2014, pp. 203–216.

[12] M. Pudelko, P. Emmerich, S. Gallenmüller, and G. Carle, "Performance analysis of vpn gateways," in *2020 IFIP Networking Conference (Networking)*. IEEE, 2020, pp. 325–333.

[13] G. Norcie, J. Blythe, K. Caine, and L. J. Camp, "Why johnny can't blow the whistle: Identifying and reducing usability issues in anonymity systems," in *Workshop on Usable Security*, vol. 6, 2014, pp. 50–60.

[14] S. Khanvilkar and A. Khokhar, "Virtual private networks: an overview with performance evaluation," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 146–154, 2004.

[15] H. Roberts, E. Zuckerman, and J. G. Palfrey, "2011 circumvention tool evaluation," *Berkman Center Research Publication*, no. 2011-08, 2011.

[16] H. Abbas, N. Emmanuel, M. F. Amjad, T. Yaqoob, M. Atiquzzaman, Z. Iqbal, N. Shafqat, W. B. Shahid, A. Tanveer, and U. Ashfaq, "Security assessment and evaluation of vpns: A comprehensive survey," *ACM Computing Surveys*, vol. 55, no. 13s, pp. 1–47, 2023.

[17] W. R. Hobbs and M. E. Roberts, "How sudden censorship can increase access to information," *American Political Science Review*, vol. 112, no. 3, pp. 621–636, 2018.

[18] Netblocks, "Internet disrupted in iran amid protests over death of mahsa amini," 2022. [Online]. Available: https://netblocks.org/reports/internet-disrupted-in-iran-amid-protests-over-death-of-mahsa-amini-X8qVEwAD

[19] "Twitter v2 api," 2021, https://developer.twitter.com/en/docs/twitter-api/tweets/search/introduction.

[20] Telegram, "Telegram apis." [Online]. Available: https://core.telegram.org/

[21] Lonami, "Telethon's documentation," 2017-2019, revision 7325718f. [Online]. Available: https://docs.telethon.dev/en/stable/

[22] Y. Liu, M. Ott, N. Goyal, J. Du, M. Joshi, D. Chen, O. Levy, M. Lewis, L. Zettlemoyer, and V. Stoyanov, "Roberta: A robustly optimized bert pretraining approach," *arXiv preprint arXiv:1907.11692*, 2019.

[23] M. Farahani, M. Gharachorloo, M. Farahani, and M. Manthouri, "Parsbert: Transformer-based model for persian language understanding," *Neural Processing Letters*, vol. 53, pp. 3831–3847, 2021.

[24] T. R. Mosley, "Google has a new tool to outsmart authoritarian internet censorship," 2023. [Online]. Available: https://www.technologyreview.com/2023/09/13/1079381/google-jigsaw-outline-vpn-internet-censorship/

[25] H. Kiros, "Big tech could help iranian protesters by using an old tool," 2022. [Online]. Available: https://www.technologyreview.com/2022/11/11/1063107/big-tech-iran-protests-domain-fronting/

[26] S. Aryan, H. Aryan, and J. A. Halderman, "Internet censorship in iran: A first look," in *3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13)*, 2013.

[27] D. Xue, B. Mixon-Baca, ValdikSS, A. Ablove, B. Kujath, J. R. Crandall, and R. Ensafi, "Tspu: Russia's decentralized censorship system," in *Proceedings of the 22nd ACM Internet Measurement Conference*, 2022, pp. 179–194.

[28] M. Wu, J. Sippe, D. Sivakumar, J. Burg, P. Anderson, X. Wang, K. Bock, A. Houmansadr, D. Levin, and E. Wustrow, "How the great firewall of china detects and blocks fully encrypted traffic," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 2653–2670.

[29] Y. Chen and D. Y. Yang, "The impact of media censorship: 1984 or brave new world?" *American Economic Review*, vol. 109, no. 6, pp. 2294–2332, 2019.

[30] F. Shen and Z. Zhang, "Do circumvention tools promote democratic values? exploring the correlates of anticensorship technology adoption in china," *Journal of Information Technology & Politics*, vol. 15, no. 2, pp. 106–121, 2018.

[31] A. Dal and E. C. Nisbet, "Walking through firewalls: Circumventing censorship of social media and online content in a networked authoritarian context," *Social Media+ Society*, vol. 8, no. 4, p. 20563051221137738, 2022.

[32] R. Deibert, J. Oliver, and A. Senft, "Censors get smart: Evidence from psiphon in iran," *Review of Policy Research*, vol. 36, no. 3, pp. 341–356, 2019.

[33] V. Ververis, S. Marguel, and B. Fabian, "Cross-country comparison of internet censorship: A literature review," *Policy & Internet*, vol. 12, no. 4, pp. 450–473, 2020.

[34] P. M. Lutscher, "When censorship works: Exploring the resilience of news websites to online censorship," *British Journal of Political Science*, vol. 53, no. 4, pp. 1342–1350, 2023.

[35] S. Nourin, V. Tran, X. Jiang, K. Bock, N. Feamster, N. P. Hoang, and D. Levin, "Measuring and evading turkmenistan's internet censorship: A case study in large-scale measurements of a low-penetration country," in *Proceedings of the ACM Web Conference 2023*, 2023, pp. 1969–1979.

[36] T. K. Yadav, A. Sinha, D. Gosain, P. K. Sharma, and S. Chakravarty, "Where the light gets in: Analyzing web censorship mechanisms in india," in *Proceedings of the Internet Measurement Conference 2018*, 2018, pp. 252–264.

[37] L. Moore and T. Mori, "Vpn awareness and misconceptions: A comparative study in canadian and japanese contexts."

[38] L. Parks and R. Mukherjee, "From platform jumping to self-censorship: Internet freedom, social media, and circumvention practices in zambia," *Communication and Critical/Cultural Studies*, vol. 14, no. 3, pp. 221–237, 2017.

[39] R. Ramesh, R. S. Raman, A. Virkud, A. Dirksen, A. Huremagic, D. Fifield, D. Rodenburg, R. Hynes, D. Madory, and R. Ensafi, "Network responses to russia's invasion of ukraine in 2022: a cautionary tale for internet freedom," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 2581–2598.

[40] M. Namara, D. Wilkinson, K. Caine, and B. P. Knijnenburg, "Emotional and practical considerations towards the adoption and abandonment of vpns as a privacy-enhancing technology," 2020.

[41] A. Dutkowska-Zuk, A. Hounsel, A. Xiong, M. Chetty, N. Feamster, M. Roberts, and B. Stewart, "Practicing safe browsing: Understanding how and why university students use virtual private networks. arxiv preprint, cs," *HC, February*, 2020.

[42] J. Appelbaum, M. Ray, K. Koscher, and I. Finder, "vpwns: Virtual pwned networks," in *2nd USENIX Workshop on Free and Open Communications on the Internet. USENIX Association*, 2012, p. 106.

[43] N. M. Al-Fannah, "One leak will sink a ship: Webrtc ip address leaks," in *2017 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2017, pp. 1–5.

[44] M. T. Khan, J. DeBlasio, G. M. Voelker, A. C. Snoeren, C. Kanich, and N. Vallina-Rodriguez, "An empirical analysis of the commercial vpn ecosystem," in *Proceedings of the Internet Measurement Conference 2018*, 2018, pp. 443–456.

[45] V. C. Perta, M. Barbera, G. Tyson, H. Haddadi, A. Mei *et al.*, "A glance through the vpn looking glass: Ipv6 leakage and dns hijacking in commercial vpn clients," 2015.

[46] R. Ramesh, L. Evdokimov, D. Xue, and R. Ensafi, "Vpnalyzer: systematic investigation of the vpn ecosystem," in *Network and Distributed System Security*, vol. 10, 2022.

[47] M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson, "An analysis of the privacy and security risks of android vpn permission-enabled apps," in *Proceedings of the 2016 internet measurement conference*, 2016, pp. 349–364.

[48] Q. Zhang, J. Li, Y. Zhang, H. Wang, and D. Gu, "Oh-pwn-vpn! security analysis of openvpn-based android apps," in *International Conference on Cryptology and Network Security*. Springer, 2017, pp. 373–389.

[49] S. Chakravarty, G. Portokalidis, M. Polychronakis, and A. D. Keromytis, "Detecting traffic snooping in tor using decoys," in *Recent Advances in Intrusion Detection: 14th International Symposium, RAID 2011, Menlo Park, CA, USA, September 20-21, 2011. Proceedings 14*. Springer, 2011, pp. 222–241.

[50] P. Winter, R. Köwer, M. Mulazzani, M. Huber, S. Schrittwieser, S. Lindskog, and E. Weippl, "Spoiled onions: Exposing malicious tor exit relays," in *Privacy Enhancing Technologies: 14th International Symposium, PETS 2014, Amsterdam, The Netherlands, July 16-18, 2014. Proceedings 14*. Springer, 2014, pp. 304–331.

[51] T. Chung, D. Choffnes, and A. Mislove, "Tunneling for transparency: A large-scale analysis of end-to-end violations in the internet," in *Proceedings of the 2016 Internet Measurement Conference*, 2016, pp. 199–213.

[52] G. Tsirantonakis, P. Ilia, S. Ioannidis, E. Athanasopoulos, and M. Polychronakis, "A large-scale analysis of content modification by open http proxies." in *NDSS*, 2018.

[53] M. O'Neill, S. Ruoti, K. Seamons, and D. Zappala, "Tls proxies: Friend or foe?" in *Proceedings of the 2016 Internet Measurement Conference*, 2016, pp. 551–557.

[54] X. d. C. de Carnavalet and M. Mannan, "Killed by proxy: Analyzing client-end tls interception software," in *Network and Distributed System Security Symposium*, 2016.

[55] R. Bellini, E. Tseng, N. McDonald, R. Greenstadt, D. McCoy, T. Ristenpart, and N. Dell, "" so-called privacy breeds evil" narrative justifications for intimate partner surveillance in online forums," *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW3, pp. 1–27, 2021.

[56] T. Li, E. Louie, L. Dabbish, and J. I. Hong, "How developers talk about personal data and what it means for user privacy: A case study of a developer forum on reddit," *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW3, pp. 1–28, 2021.

[57] M. Tahaei, K. Vaniea, and N. Saphra, "Understanding privacy-related questions on stack overflow," in *Proceedings of the 2020 CHI conference on human factors in computing systems*, 2020, pp. 1–14.

[58] E. Tseng, R. Bellini, N. McDonald, M. Danos, R. Greenstadt, D. McCoy, N. Dell, and T. Ristenpart, "The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums," in *29th USENIX security symposium (USENIX Security 20)*, 2020, pp. 1893–1909.

[59] J. B. Whiting, R. D. Olufuwote, J. D. Cravens-Pickens, and A. Banford Witting, "Online blaming and intimate partner violence: A content analysis of social media comments," 2019.

[60] J. Parsons, M. Schrider, O. Ogunlela, and S. Ghanavati, "Understanding developers privacy concerns through reddit thread analysis," *arXiv preprint arXiv:2304.07650*, 2023.

[61] E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes," in *thirteenth symposium on usable privacy and security (SOUPS 2017)*, 2017, pp. 65–80.

[62] A. Preece, D. Shaw, and P. Haynes, "Perspectives of non-expert users on cyber security and privacy: An analysis of online discussions on twitter," *Computers in Human Behavior*, vol. 131, p. 107169, 2022.

[63] J. Li, K. Sun, B. S. Huff, A. M. Bierley, Y. Kim, F. Schaub, and K. Fawaz, ""it's up to the consumer to be smart": Understanding the security and privacy attitudes of smart home users on reddit," in *IEEE Symposium on Security and Privacy (SP)(SP)*. IEEE Computer Society Los Alamitos, CA, 2023, pp. 380–396.

[64] L. Schmidt, H. Hosseini, and T. Hupperich, "Assessing the security and privacy of baby monitor apps," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 303–326, 2023.

[65] M. Singhal, N. Kumarswamy, S. Kinhekar, and S. Nilizadeh, "Cybersecurity misinformation detection on social media: Case studies on phishing reports and zoom's threat," *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 17, no. 1, pp. 796–807, Jun. 2023. [Online]. Available: https://ojs.aaai.org/index.php/ICWSM/article/view/22189

[66] OONI, "Technical multi-stakeholder report on internet shutdowns: The case of iran amid autumn 2022 protests," 2022. [Online]. Available: https://ooni.org/post/2022-iran-technical-multistakeholder-report

[67] D. Kılıç and A. N. Chúláin, "How iranians are hopping between vpns to stay connected and break through internet censorship," 2022. [Online]. Available: https://www.euronews.com/next/2022/11/06/iran-protests-vpn-use-soars-as-citizens-seek-way-around-internet-censorship

[68] R. Browne, "Vpn use skyrockets in iran as citizens navigate internet censorship under tehran's crackdown," 2022. [Online]. Available: https://www.cnbc.com/amp/2022/10/07/vpn-use-skyrockets-in-iran-as-citizens-navigate-internet-censorship.html

[69] M. Salami, "Internet filtering in iran boosts vpn business – much of it government-owned," 2023. [Online]. Available: https://www.stimson.org/2023/internet-filtering-in-iran-boosts-vpn-business-much-of-it-government-owned/

[70] CNET, "Vpn demand surges," 2022. [Online]. Available: https://www.cnet.com/tech/services-and-software/vpn-demand-surges-in-iran-as-protests-continue-study-shows/

[71] L. A. Goodman, "Snowball sampling," *The annals of mathematical statistics*, pp. 148–170, 1961.

[72] "Source code for nltk.stem.wordnet," 2022, https://www.nltk.org/_modules/nltk/stem/wordnet.html.

[73] H. Taghi-Zadeh, M. H. Sadreddini, M. H. Diyanati, and A. H. Rasekh, "A new hybrid stemming method for persian language," *Digital Scholarship in the Humanities*, vol. 32, no. 1, pp. 209–221, 2017.

[74] B. G. Glaser and A. L. Strauss, *Discovery of grounded theory: Strategies for qualitative research*. Routledge, 2017.

[75] J. M. Corbin and A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative sociology*, vol. 13, no. 1, pp. 3–21, 1990.

[76] M. Singhal, C. Ling, P. Paudel, P. Thota, N. Kumarswamy, G. Stringhini, and S. Nilizadeh, "Sok: Content moderation in social media, from guidelines to enforcement, and research to practice," in *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, 2023, pp. 868–895.

[77] C. Wagner, V. Liao, P. Pirolli, L. Nelson, and M. Strohmaier, "It's not in their tweets: Modeling topical expertise of twitter users," in *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*. IEEE, 2012, pp. 91–100.

[78] Q. V. Liao, C. Wagner, P. Pirolli, and W.-T. Fu, "Understanding experts' and novices' expertise judgment of twitter users," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2012, pp. 2461–2464.

[79] B. Horne, D. Nevo, J. Freitas, H. Ji, and S. Adali, "Expertise in social networks: How do experts differ from other users?" in *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 10, no. 1, 2016, pp. 583–586.

[80] N. K. Sharma, S. Ghosh, F. Benevenuto, N. Ganguly, and K. Gummadi, "Inferring who-is-who in the twitter social network," *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 4, pp. 533–538, 2012.

[81] Exotigo, "Cash or credit? what you need to know about iranian credit cards," 2020. [Online]. Available: https://exotigo.com/blog/credit-card-and-debits-cards-in-iran-guide/

[82] CNET, "Best vpn service 2024: Vpns tested by our experts," 2024. [Online]. Available: https://www.cnet.com/tech/services-and-software/best-vpn/

[83] J. Milin-Ashmore, "The best vpns to stop your isp from tracking your activity," 2023. [Online]. Available: https://www.bleepingcomputer.com/vpn/guides/stop-isp-tracking-internet-activity/

[84] M. Eddy, "https://www.pcmag.com/opinions/proton-vpns-new-stealth-feature-helps-fight-censorship-in-iran-and-russia," 2022. [Online]. Available: https://www.pcmag.com/opinions/proton-vpns-new-stealth-feature-helps-fight-censorship-in-iran-and-russia

[85] I. National, "Proton sees whopping 6,000% surge in vpn sign-ups in iran," 2022. [Online]. Available: https://www.iranintl.com/en/202307274303

[86] T. Project, "Types of relays on the tor network." [Online]. Available: https://community.torproject.org/relay/types-of-relays/

[87] ——, "What is snowflake?" [Online]. Available: https://support.torproject.org/censorship/what-is-snowflake/

[88] Outline, "Using an access key more than once," 2019. [Online]. Available: https://support.getoutline.org/s/article/multiuse-access-key?language=en_US

[89] "Wstunnel," 2024, https://windscribe.com/knowledge-base/articles/what-is-the-wstunnel-protocol/.

[90] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing," *Communications of the ACM*, vol. 42, no. 2, pp. 39–41, 1999.

[91] M. AlSabah and I. Goldberg, "Performance and security improvements for tor: A survey," *ACM Computing Surveys (CSUR)*, vol. 49, no. 2, pp. 1–36, 2016.

[92] Z. Ling, J. Luo, W. Yu, X. Fu, D. Xuan, and W. Jia, "A new cell counter based attack against tor," in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 578–589.

[93] R. Snader and N. Borisov, "A tune-up for tor: Improving security and performance in the tor network." in *ndss*, vol. 8, 2008, p. 127.

[94] Telemetrio, "Telemetrio: Telegram channels of the world," 2024. [Online]. Available: https://telemetr.io/en/catalog/global

[95] Statcounter, "Mobile operating system market share islamic republic of iran," 2024. [Online]. Available: https://gs.statcounter.com/os-market-share/mobile/iran

[96] M. A. Lemley and R. A. Reese, "Reducing digital copyright infringement without restricting innovation," *Stan. L. Rev.*, vol. 56, p. 1345, 2003.

[97] R. Rivera, P. Kotzias, A. Sudhodanan, and J. Caballero, "Costly freeware: a systematic analysis of abuse in download portals," *IET Information Security*, vol. 13, no. 1, pp. 27–35, 2019.

[98] P. O'Kane, S. Sezer, and K. McLaughlin, "Obfuscation: The hidden malware," *IEEE Security & Privacy*, vol. 9, no. 5, pp. 41–47, 2011.

[99] A. Tosun, M. De Donno, N. Dragoni, and X. Fafoutis, "Resip host detection: identification of malicious residential ip proxy flows," in *2021 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2021, pp. 1–6.

[100] "VirusTotal API," https://support.virustotal.com/hc/en-us/articles/115002100149-API, 2020.

[101] P. Peng, L. Yang, L. Song, and G. Wang, "Opening the blackbox of virustotal: Analyzing online phishing scan engines," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 478–485.

[102] A. Urman and S. Katz, "What they do in the shadows: examining the far-right networks on telegram," *Information, communication & society*, vol. 25, no. 7, pp. 904–923, 2022.

[103] M. La Morgia, A. Mei, A. M. Mongardini, and J. Wu, "Uncovering the dark side of telegram: Fakes, clones, scams, and conspiracy movements," *arXiv preprint arXiv:2111.13530*, 2021.

[104] M. Iqbal and I. Riadi, "Analysis of security virtual private network (vpn) using openvpn," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 1, pp. 58–65, 2019.

[105] D. Bateyko, "Censorship-circumvention tools and pluggable transports," *Geo. L. Tech. Rev.*, vol. 6, p. 335, 2022.

[106] P. Winter, "Measuring and circumventing internet censorship," Ph.D. dissertation, Karlstads universitet, 2014.

[107] S. Saleh, J. Qadir, and M. U. Ilyas, "Shedding light on the dark corners of the internet: A survey of tor research," *Journal of Network and Computer Applications*, vol. 114, pp. 1–28, 2018.

[108] M. O. Akinsanya, C. C. Ekechi, and C. D. Okeke, "Virtual private networks (vpn): A conceptual review of security protocols and their application in modern networks," *Engineering Science & Technology Journal*, vol. 5, no. 4, pp. 1452–1472, 2024.

Appendix A. keywordlist

Figure 9 shows the list of keywords that were used for filtering Twitter authors' biographies and identifying experts from others.

Keywords
'privacy', 'infosec', 'digital security', 'امنیت شبکه' , 'امنیت وب', 'tech-savvy', 'network security', 'cryptography', 'Cyber Security', 'Cyber Security', ' network & security', 'security manager', 'security researcher', 'IT security', 'متخصص امنیت', ' Security Enthusiast', 'Security expert', 'برنامه نویس', 'Developer', 'CyberSec', 'Security exploits'

Figure 9: Keywords list used for identifying experts.

Appendix B. Codebook

We discovered 6 main topics. The main classes were: (i) *Censorship*: subdivided into 3 sub-classes discussing about the ways to bypass censorship using VPN, Starlink etc., how users are facing censorship i.e., Internet being shutdown, restrictions etc., how different social media such as Facebook, Twitter are censoring and filtered users' voices, (ii) *Abuse of Content Moderation*: posts talking about how various social media are abusing the content moderation guidelines to block, suspend accounts or filtering users' content, (iii) *Fake News*: posts describing the spread of fake news, (iv) *Security*: subdivided into 1 sub-class, of posts discussing about security vulnerability in internet connectivity tools, and discussing about Government accounts being hacked, or requesting hacking groups to hack websites, also posts discussing about viruses and vulnerabilities in applications, (v) *Privacy*: subdivided into 2 sub-classes, where posts discussing about tools that are spyware, or doing surveillance on the user, or where user data is being exploited to identify users', and (vi) *Hate Speech*: posts talking about how some users are spreading hateful rhetoric. These classes describe the data, and a post might fit multiple classes. For example, a post can be about how Facebook is censoring some important accounts and blocking or filtering content.

As one can see, some of the categories are the same for both our English and Persian datasets, however, some are only in one dataset. In *Censorship*, we found a subclass, "App Filtering", in which posts were discussing about how certain Iranian apps are filtered. *Fake News* and *Hate Speech* were the classes that were only observed in our Persian dataset. Interestingly, we can also observe that in *Security*, people were discussing how some tools are viruses and advising people not to download them.

We observed that users' were expressing their concerns about hateful rhetoric on social media and how it is affecting them. These tweets are marked by a tone characterized by aggression and disapproval due to the usage of insulting Most notably *Arzeshi* an extremely derogatory Persian term, which appeared 12,278 times. Such words convey a deep hatred for people who are thought to disagree with particular viewpoints or behaviors.

Appendix C. VPN Ecosystem

Access Keys. Access keys are crucial credentials that allow users to securely connect to VPN servers [104]. Access keys can be passwords, digital certificates, or a pre-shared key (PSK), allowing only authorized users to access the VPN network.

Bridges. Bridges have intrinsic usefulness in contexts where direct Tor access and traditional VPN usage are restricted [105], [106]. Bridges serve as VPN intermediary relays or secret Tor network entry points [107], making them critical to the free movement of information, maintaining privacy, and opposing widespread surveillance.

Protocols. VPN protocols are essential to the operation of VPN services. They are responsible for regulating the data transfer mechanism between the user's device and the VPN server [108].

Configurations. VPN configurations (configs) are crucial for controlling how VPN software operates, including server connections, protocol use, data encryption, etc.

Servers. VPN servers play a huge and important role as intermediaries between users and the internet. User's IP addresses can be hidden and data is encrypted with the help of using these servers to route internet traffic.

Appendix D.
Meta-Review

The following meta-review was prepared by the program committee for the 2025 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

D.1. Summary

This paper examines online discussions on Twitter and Telegram about censorship circumvention technologies (CCT) during the 2022 protests in Iran. The paper explores 3 research questions: First, it explores how normal and tech-savvy users discuss three specific circumvention-related topics – VPNs, Starlink, and proxies – using filtering and NLP models to extract relevant English and Persian tweets. The paper finds that users frequently post regarding VPN and proxy recommendations, security and privacy aspects, and the ability to use Starlink for censorship circumvention. Second, the paper dives deep into VPN technology, focusing on discussion around popular VPN providers. Finally, the paper investigates well-known Telegram channels, finding that users share recommendations, configurations, and even VPN software, some of which are malicious. Overall, the paper provides recommendations for improving circumvention technologies based on social media discussions.

D.2. Scientific Contributions

- Independent Confirmation of Important Results with Limited Prior Research.
- Addresses a Long-Known Issue.
- Provides a Valuable Step Forward in an Established Field.
- Establishes a New Research Direction.

D.3. Reasons for Acceptance

1) The paper provides important insight to circumvention technology developers and operators on issues users are facing during censorship events.
2) The paper is the first to process social media posts directly related to censorship circumvention technology and the inclusion of Persian posts provides an important level of thoroughness.
3) The data gathered for this paper is a valuable contribution in its size and focus.

D.4. Noteworthy Concerns

1) The paper uses two data sources (Twitter and Telegram) that have been blocked for a while in the Iran, which may affect how Internet users in Iran are able to participate in discussions on these platforms.
2) The paper does not consider discussions around other popular circumvention technologies, such as Psiphon, refraction networking, and V2Ray.