WORKING PAPER: A Comparison of pro-Hamas and pro-Ukraine Crowdsourced Cyber Attack Coordination on Telegram

Ian Kloo[0000−0002−0829−3341] and Kathleen M. Carley[0000−0002−6356−0238]

Carnegie Mellon University, Pittsburgh, PA 15213, USA
iankloo@cmu.edu

Abstract. Crowdsourcing cyber attacks on social media presents a low-cost opportunity for bad actors to create effects far beyond their home-grown capabilities. In particular, distributed denial of service (DDoS) attacks are easy to crowdsource, requiring only simple code and a list of targets. Using two case studies, we found that bot activity with built-in redundancy was used when coordinating DDoS attacks on Telegram in both pro-Hamas and pro-Ukraine communities. The pro-Hamas groups better employed this redundancy, resulting in networks that were much more robust to potential mitigation from de-platforming individual users or channels.

Keywords: cybersecurity · social cybersecurity · social media coordination.

1 Introduction

Cyber attacks are a major component of modern armed conflict. Unlike kinetic attacks, cyber activities can be conducted by sympathetic parties without the need to be physically present and pose little immediate personal risk to the attackers. Nations with robust cybersecurity forces can directly support their militaries, but less-capable actors are at a major disadvantage. To even the playing field, some international actors have turned to crowdsourcing cyber attacks. This approach allows for large-scale mobilization of cyber actors, but because each attacker is essentially untrained, these crowdsourced attacks tend to be low-sophistication. For example, DDoS (distributed denial of service) attacks are easy to crowdsource because they require only simple code to execute.

DDoS attacks are performed by making repeated requests to a server with the goal of overwhelming it into a state of unresponsiveness. These attacks range in sophistication and are most effective when a server faces requests from many different nodes [5]. A single, sophisticated user can execute this kind of attack by automating the distribution of requests across a number of different machines, but the same thing can be accomplished by simply having a large number of users make repeated requests at the same time. The code to execute such an attack from a single machine is as easy as writing an infinite loop that continues to make

requests to a domain or IP address. As a result, coordinating these cyber attacks is quite simple: a coordinator just needs to share IP address targets and possibly simple code (if the user is unable to write their own loop) to a community with access to basic computers who are willing to assist in executing the attacks.

Social media is an effective means for the coordination of activities such as protests [6], and it has similar utility when crowdsourcing cyber activities. This is subject to censorship from platforms that forbid the coordination of illegal activities. While other types of crimes can be coordinated using private messages, these types of cyber attacks require rapid dissemination to the largest number of people possible. As a result, coordination in this domain is most effective when done on platforms with a large reach that are not subject to censorship. In today's information environment, Telegram fits both of these requirements in that it is almost completely uncensored and is globally popular. As a result, this study will focus on Telegram as the coordinating platform.

This study seeks to study crowdsourced cyber attacks from a social cybersecurity perspective, focusing on the ways in which social media was used to coordinate these activities. Specifically, we will examine the following questions:

1. To what extent were bots used in the coordination of cyber attacks?
2. What is the structure of the network of coordinating users/channels, and how does this impact potential mitigation strategies?

We will focus on two recent cases in which crowdsourced cyber attacks were used to support Hamas in their war with Israel and Ukraine during the Russian invasion. Both datasets capture online activity for the first week of open conflict. Because these cases are so temporally close (Israel and Hamas began open fighting in October 2023, and Russia invaded Ukraine in February 2022), they allow for a comparison that is less likely to be confounded by major changes to the platform or its user base.

The rest of this paper will describe related work, present an overview of the cases that will be used, explain how the data was collected and preprocessed, describe the methodology for detecting bots and creating coordination networks, present results, and describe a future course of related research.

2 Existing Work

Several existing studies examined the intersection of social media and cybersecurity, with a nearly exclusive focus on Twitter. Khandpur et al. presented and demonstrated a methodology for detecting evidence of cyber attacks using the text content of Tweets in an event detection framework [2]. Our work differs from this approach in that Khandpur et al. were not looking for direct coordination of cyber attacks but were instead using social media as a sensor to identify cyber attacks in general.

More similar to our approach, Mahaini et al. developed a machine learning classifier to label Twitter accounts into several cybersecurity-specific classes [3]. One of the classes identified in this work is "hackers," which could ostensibly

be used to help locate crowdsourced cyber attacks. Mahaini et al. demonstrate their model's utility on Twitter, but the machine learning feature generation required restricts its usefulness to other social media platforms. In particular, their model relies on robust user-level features that are not available on more privacy-focused platforms (like Telegram) by design.

One notable study moves beyond Twitter to describe crowdsourced cyber attacks on Telegram during the Russian invasion of Ukraine. Juhani Merilehto's paper characterized the activities of a single, highly active pro-Ukraine Telegram account that crowdsourced cyber attacks during the first year of the invasion [4]. This study characterized how DDoS attacks were sourced by the account, as well as several other cyber activities, such as port scans. Our study seeks to expand upon this previous work by focusing on more than one Telegram account so that we can study collaboration in the larger communities conducting these attacks.

3 Data

Unlike social media studies on other platforms, Telegram data is not freely searchable using keywords. As a result, a common practice for acquiring Telegram data is to start with a curated list of channels of interest before snowball sampling any channels mentioned in the initial list. This snowball sampling can be iterated until the full community structure has been captured.

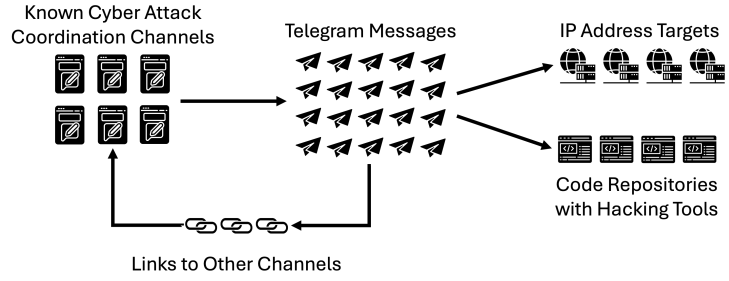

Fig. 1. Data collection strategy

To acquire data for this study, we started with a crowd-sourced list of channels for each case (Hamas and Ukraine) generated by Reddit communities reporting on the conflicts. To capture channels that were left off the curated lists, we performed a one-hop snowball sample using channel forwards. This sampling approach is depicted in Figure 1. We tested a second-level snowball sample but found that the one-hop approach captured more applicable data. A manual review of the two-hop approach found many channels that were posting content about the conflicts but were not related to cyber attacks (e.g., major news networks).

Interestingly, we could not find similar curated lists channels performing pro-Israel and pro-Russian attacks. While it is possible that this is due to the bias of those curating the lists, we also did not find links to these counter-stance attacks in our snowball sampling. Previous Telegram work has demonstrated that opposing communities regularly forward content to/from each other, so we would have expected to see these pro-Israel and pro-Russian attack channels if they were popular. We believe that this discrepancy may stem from the fact that Russia and Israel both have sophisticated cyber organizations, which removes the need to perform low-sophistication crowdsourced attacks.

The final dataset is described in Table 1. Notably, the Hamas dataset is much larger than the Ukraine dataset. Given the similar data ranges and methodologies used to capture the data, we believe this difference depicts the fact that crowdsourcing cyber attacks was much more popular with pro-Hamas actors than pro-Ukraine actors.

Table 1. Data Overview

	Hamas Data	**Ukraine Data**
Channels	273	68
Messages	1,100,000	194,000
Dates	October 7 - 14, 2023	February 22 - 29, 2022

After the snowball sampling process, we were left with a set of messages related to cyber attack coordination. We used regular expressions to extract the specific IP address targets and code repositories used to coordinate attacks.

All data used in this study comes from public Telegram channels, and no efforts have been made to extract information beyond what is freely made publically available on the Telegram platform. Furthermore, we discarded any potentially identifiable information about users that was in the public data, using non-attributional user IDs for our study.

4 Methodology

4.1 Bot Detection

The first step of our methodology was to identify inauthentic accounts (which we will refer to as "bots," though we do not intend to claim that the account is entirely automated). Previous work has identified that repeater bots are a common type of inauthentic account that can be used to send a message to various user groups [1]. Given that crowdsourcing DDoS attacks requires widespread dissemination of IP address targets, repeater bots would be particularly useful for this coordination.

Modern bot-finding methods often rely on machine learning, but repeater bots are especially easy to detect using rule sets. In particular, we labeled any

account as a bot if they posted the same message in more than two Telegram channels within five seconds.

4.2 Network Analysis

The main networks used in this study were built by first constructing node sets from the users and channels in the raw Telegram data. We also considered the IP addresses and links to hacking tools (that were extracted from the Telegram messages using regular expressions as described in section 3) as nodes. Next, we defined edges between tools and IP addresses and the channels in which they were posted. We also constructed user-focused networks by defining an edge between a user and a channel if an IP address target was shared in that channel.

To evaluate each network's susceptibility to mitigation strategies, we first calculated the number of components in each network. Next, we iteratively removed each node and recalculated the number of components. The percentage increase in components from removing a single node serves as a measure of how sensitive each network is to potential mitigation strategies that could de-platform important actors.

5 Results and Discussion

After running our simple bot detection method, we found that most of the accounts actively sharing IP address targets and tools were inauthentic. Specifically, 93% and 88% of user accounts were identified as repeater bots in the Ukraine and Hamas data, respectively. This is strong evidence of the widespread use of bots in crowdsourced cyber attack coordination. While bot activity is common on Telegram in general, bots are mainly used within single channels. So, it is surprising to find that bots are responsible for the majority of cross-community target coordination in these cases.

Next, we examined the networks linking channels/groups to IP targets and tools shown in Figure 2. The Ukraine networks show that IP targets and tools were typically posted by a single channel/group. In contrast, the Hamas networks show that channels/groups regularly posted targets and tools that were also posted in other channels/groups. This suggests heightened coordination between channels/groups in the Hamas case.

In addition to supporting much more interaction between channels, the Hamas data also shows that channels were mainly used to post IP targets, while tools were shared mostly in groups. Examining the specific posts, we found that tools were often provided in user-to-user discussions (in groups) in response to questions from other users who did not know how to execute the cyber attacks. This kind of hacking technical support was not provided in channels. Interestingly, we did not see the same behavior in the Ukraine data where tools and targets were both shared by channels and groups.

To identify differences in user behavior, we then created networks to study how users interacted with different groups shown in Figure 3. The Ukraine network shows that five users who posted in nine groups were responsible for the

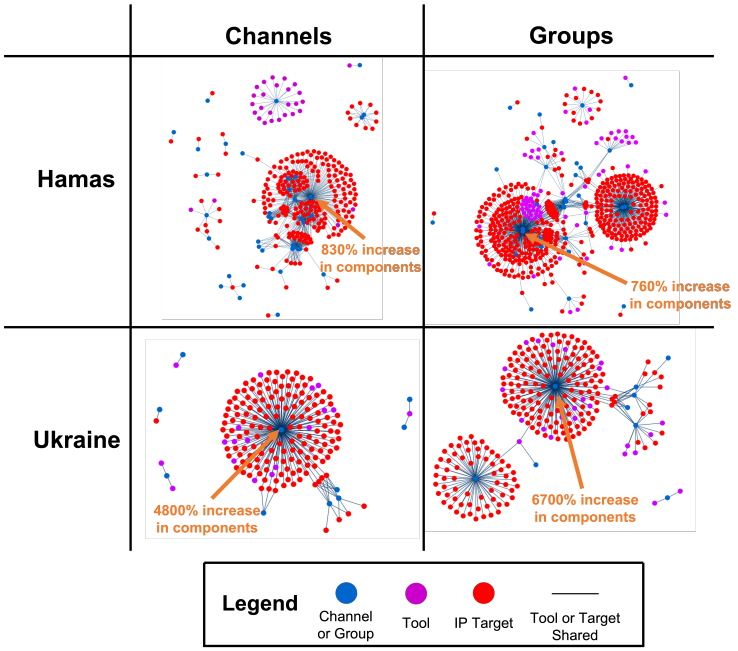

Fig. 2. Networks of channels to the IP addresses and hacking tools they shared. Blue nodes are channels, purple nodes are tools, and red nodes are IP addresses. An edge denotes that a channel shared a tool or IP address in a message.

majority of cross-group IP target sharing. By contrast, many more users posted in more than one group in the Hamas data.

We note that both the Ukraine and Hamas networks demonstrate multi-account coordination (indicated by the orange circles in Figure 3). In the Ukraine network, we can see two users posting large numbers of IP addresses to a single group, while the Hamas network shows two users posting large numbers of IP targets to two different groups. In both cases, we see that bots are being used to further amplify a specific set of IP targets or to create redundancy to ensure these targets are attacked.

Finally, we identified the potential increase in components (effectively a measure of network degradation). In both Figures 2 and 3, orange arrows denote which node should be removed for maximum network degradation, while the orange text shows the percent increase in components that would result from removing that specific node.

Unsurprisingly, the Hamas networks featuring more duplicative IP targets and tool sharing were less susceptible to degradation from removing a single node than the Ukraine networks. This finding is even more obvious when looking at the user-to-channel networks. Again, the structure of the Hamas networks does not depend on single users to spread information, which creates much more redundancy. This redundancy translates to resilliance to potential mitigation.

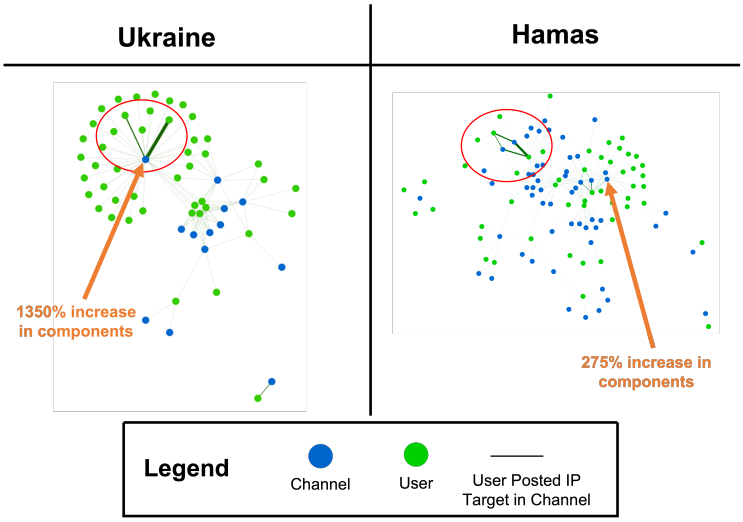

Fig. 3. Bipartite networks showing users posting IP targets to different channels. Blue nodes are channels and green nodes are users. Edges correspond to the number of IP address targets a user posted to a specific channel.

6 Limitations and Future Work

As an early entry to the study of crowd-sourced cyber attack coordination on Telegram, this work has significant limitations that indicate potential avenues for future work. First, this paper only focused on a single type of cyber attack. While DDoS attacks are some of the most conducive to crowdsourcing, it is possible that other types of attacks are also being coordinated on social media platforms.

Additionally, this paper only focused on Telegram as a means of coordination. We point out that previous work was limited by a myopic focus on Twitter, but we also only focused on a single platform. Future research should focus on a cross-platform analysis. In particular, identifying coordinated attacks using multiple platforms would be impactful. Another possible approach would be to compare the coordination methods used on different platforms.

Another key limitation of this work is that we did not attempt to quantify the effectiveness of any of these cyber attacks. It is possible, for example, that the Hamas-supporting attacks were less effective than those sourced by the pro-Ukraine community in spite of the relatively enhanced resilience of the Hamas network. This is an especially difficult problem because measuring the impact of these attacks would require the victims to publicly state how much their servers were degraded, which could make them more likely to be attacked in the future. Without victim participation, researchers would need to send requests to the target servers and check for a response - but this would amount to participating

in the DDoS attack. Future work should identify creative ways to characterize DDoS effectiveness in non-intrusive ways.

Finally, this paper only considered simple mitigation strategies when testing the networks' vulnerability to countermeasures. This was sufficient for this paper as the Hamas networks included much more redundancy than the Ukraine networks, but it is easy to imagine future cases that are not as clear-cut. Future work should implement a more realistic set of countermeasures that mirror those implemented by platforms in the real world to more realistically evaluate coordination network susceptibility.

7 Conclusion

This study demonstrated that bots were the main drivers of crowdsourced cyber attack coordination in two distinct case studies. Additionally, we detected similar tradecraft in both cases, where multiple bot accounts were used to spam the same IP address targets to the same communities. However, while Telegram was used by both Hamas-supporting and Ukraine-supporting users to share the tools and IP address targets needed to facilitate DDoS attacks, we found that the Hamas community contained much more redundancy that left it less prone to mitigation when compared with the Ukraine community. The generalizability of these findings should be tested with future work with an expanded methodology, but this study provides a critical first step to understanding a potentially geopolitically impactful method for cyber attack coordination that is available to even the most unsophisticated actors.

Acknowledgments. This work was supported in part by the Army (W911NF20D0002) and the Office of Naval Research (N000142112749) through grants and the Center for Computational Analysis of Social and Organization Systems (CASOS). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Army, the Office of Naval Research, or the U.S. government.

References

1. Jacobs, C.S., Ng, L.H.X., Carley, K.M.: Tracking china's cross-strait bot networks against taiwan. In: Thomson, R., Al-khateeb, S., Burger, A., Park, P., A. Pyke, A. (eds.) Social, Cultural, and Behavioral Modeling. pp. 115–125. Springer Nature Switzerland, Cham (2023)
2. Khandpur, R.P., Ji, T., Jan, S., Wang, G., Lu, C.T., Ramakrishnan, N.: Crowdsourcing cybersecurity: Cyber attack detection using social media. In: Proceedings of the 2017 ACM on Conference on Information and Knowledge Management. p. 1049–1057. CIKM '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3132847.3132866, https://doi.org/10.1145/3132847.3132866
3. Mahaini, M.I., Li, S.: Detecting cyber security related twitter accounts and different sub-groups: a multi-classifier approach. In: Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. p. 599–606. ASONAM '21, Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3487351.3492716, https://doi.org/10.1145/3487351.3492716
4. Merilehto, J.: Ukraine's it army–crowdsourced ddos hammer in telegram. Available at SSRN 4733858 (2024)
5. Nazario, J.: Ddos attack evolution. Network Security **2008**(7), 7–10 (2008). https://doi.org/https://doi.org/10.1016/S1353-4858(08)70086-2, https://www.sciencedirect.com/science/article/pii/S1353485808700862
6. Ng, L.H.X., Carley, K.M.: Online coordination: Methods and comparative case studies of coordinated groups across four events in the united states. In: Proceedings of the 14th ACM Web Science Conference 2022. p. 12–21. WebSci '22, Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3501247.3531542, https://doi.org/10.1145/3501247.3531542