ISSN 2421-4442

Sicurezza Terrorismo Società

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

17
2023

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

17

ISSUE 1/2023

Milano 2023

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE 1 – 17/2023

Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISSN: 2421-4442
ISSN DIGITALE: 2533-0659
ISBN: 979-12-5535-127-6

copertina: progetto grafico Studio Editoriale EDUCatt

Sommario

Forms of insurgencies, extremisms and hate crimes

Emerging Threat Ecosystems and Research Methodologies

Exploring the Telegram Hacker Ecosystem

Simone Castagna

Simone Castagna is pursuing a Master's Degree in Public Policies of Security from Catholic University of the Sacred Hearth, and holds a Bachelor's Degree in Sociology and Criminology from "G. d'Annunzio" University. He is currently interning as a research-analyst at ITSTIME (Italian Team for Security, Terroristic Issues and Managing Emergencies) and as cyber-intelligence analyst at InTheCyber Group. His areas of specialisation include digital ethnography, open-source intelligence, social media intelligence, and ethical hacking. He conducts research on hard-to-reach communities, with a particular focus on hacker groups.

Abstract

The study of hacker groups, their activities and the communities they form is becoming increasingly relevant in an even more digitalised world. Historically, academic research has portrayed hackers as solitary, misanthropic, and malevolent figures that reside within the depths of the underground web. This stereotype has led to a research focus only on the activities that occur within underground forums and markets. However, this narrow perspective is not entirely accurate, and it is crucial to understand the interactions and relationships that exist between hackers, even within more accessible and secure platforms such as Telegram. The current study employs a range of research techniques, including non-discriminative snowball sampling and social network analysis to explore the digital ecosystem of hacker groups on the Telegram instant messaging service. The aim of this research is to offer insights into the network's organizational structure and dynamics, as well as to identify key actors, their relationships, and the dissemination patterns of content. The findings of this research provide an original approach to investigating the digital ecosystems of hacker groups, thereby enhancing the understanding of their structures, dynamics, and behaviours, and facilitating the development of effective strategies for monitoring, identifying, and countering their activities.

Lo studio dei gruppi di hacker, delle loro attività e delle comunità che formano sta diventando sempre più rilevante in un mondo sempre più digitalizzato. Storicamente, la ricerca accademica ha dipinto gli hacker come figure solitarie, misantrope e malevole che risiedono nelle profondità del web underground. Questo stereotipo ha portato la ricerca a concentrarsi solo sulle attività che si svolgono all'interno dei forum e dei mercati clandestini. Tuttavia, questa prospettiva ristretta non è del tutto accurata ed è fondamentale comprendere le interazioni e le relazioni che esistono tra gli hacker, anche all'interno di piattaforme più accessibili e sicure come Telegram. Il presente studio impiega una serie di tecniche di ricerca, tra cui il campionamento non discriminatorio a palla di neve e l'analisi delle reti sociali, per esplorare l'ecosistema digitale dei gruppi di hacker sul servizio di messaggistica istantanea Telegram. Lo scopo di questa ricerca è quello di offrire approfondimenti sulla struttura organizzativa e sulle dinamiche della rete, nonché di identificare gli attori chiave, le loro relazioni e i modelli di diffusione dei contenuti. I risultati di questa ricerca forniscono un approccio originale per

indagare gli ecosistemi digitali dei gruppi di hacker, migliorando così la comprensione delle loro strutture, dinamiche e comportamenti e facilitando lo sviluppo di strategie efficaci per monitorare, identificare e contrastare le loro attività.

Keywords

Hacker groups, Social Network Analysis, Telegram, Digital Ecosystems

1. Introduction

The scholarly research conducted over the past forty years has played a significant role in refuting the stereotypical image of hackers as solitary and unsociable actors (Jordan & Taylor, 1998; Turgeman-Goldschmidt, 2005). Through this research, a deeper understanding of the social networks and supportive structures that facilitate hackers' activities has been gained, thus recognising their embeddedness within a community. By acknowledging that hackers are part of a community, a better understanding of the collective motivations and group dynamics that drive their behaviour is allowed. This understanding can assist law enforcement and security professionals in developing more effective strategies for preventing and responding to computer intrusions.

Specifically, the research conducted about this topic suggests that hackers form closely-knit online communities that encourage collaboration and sharing of specialised skills (Dupont et al., 2017; Leukfeldt et al., 2017a). This social embeddedness often leads to social hierarchies within the group, where members strive to establish their status and reputation through their hacking exploits (Décary-Hétu et al., 2012). This insight is crucial for understanding how these communities function, and for developing effective strategies to disrupt their activities.

However, while much research has been conducted on individual hackers and their behaviour, there remains a gap in the understanding of the groups to which they belong (Perkins et al., 2022). Specifically, to gain a comprehensive understanding of the individual proclivities among hackers, it is necessary to examine their social dynamics at the group level. As a result, greater insight can be gleaned for designing effective interventions to disrupt these groups. Moreover, by examining the group-level dynamics, researchers can identify key factors that contribute to the formation and maintenance of these groups, such as shared ideologies, specialised skills, or access to resources (McGloin & Nguyen, 2013; Tremblay et al., 2019).

The presented study builds upon prior research about hacker communities by focusing on the digital connections among hacker groups and the

structural dynamics of the Telegram ecosystem in which they are increasingly becoming active. Specifically, this study aims to provide a more in-depth understanding of the intricate relationships that exist between hacker groups, as well as their interactions within the broader context of the Telegram platform. This study is guided by the following research questions: (1) How does the illicit ecosystem of hacker groups operate within the Telegram platform? (2) What are the primary activities and functions of hacker groups within this ecosystem? By addressing these research questions, this study aims to contribute to the existing literature on hacker groups and their activities on social media platforms.

The paper is organised into four sections. The next section provides a comprehensive review of the latest literature on hacker groups and the most recent studies of hard-to-reach communities on Telegram. The second section argues in favour of using snowball sampling and social network analysis methodologies to explore the intricate ecosystem of hacker groups on Telegram, while describing the retrieved data. The third section presents the findings of the performed analyses and critically discusses them. Finally, the fourth section presents an in-depth discussion of the observations, situating them within the broader context of prior research on hacker groups and offering insights into possible avenues for future research.

2. Related Work

The academic literature on cybercrime ecosystems has devoted significant attention to understanding the social networks surrounding online offenders, such as hackers. In general, hackers can be defined as individuals who exploit computer systems and Internet technologies to gain unauthorised access to other computer systems (Grabosky, 2016; Oliver & Randolph, 2022). Contrary to the popular stereotype of the isolated and misanthropic hacker (Holt & Kilger, 2008; Steinmetz, 2015; Turgeman-Goldschmidt, 2005), recent research has revealed that hackers operate within online communities that are structured hierarchically stratified by skill, expertise, and social standing (Dupont et al., 2016; Holt, 2013; Lu et al., 2010). These meritocratic communities foster the formation of small, cohesive groups that maintain social connections with the broader community through various means, such as personal interactions and online forums (Abbasi et al., 2014; Holt, 2007; Holt & Kilger, 2008). The culture of these communities is focused on sharing information, acquiring specialized knowledge, and disseminating expertise among new members (Dupont et al., 2017; Holt, 2007; Leukfeldt et al., 2017a). In particular, a growing corpus of research has used network analysis approaches to map out and measure the social interactions that hackers establish in order

to acquire a deeper understanding of these social systems. Overall, this research has revealed that hackers tend to be highly connected within their social networks, and their activities are often characterized by pockets of tight-knit groups. Specifically, the importance of social relationships to hackers' online activities has been observed across various data sources, including social media platforms such as Twitter (Aslan et al., 2020) and Facebook (Howell et al., 2019), online discussion forums (Macdonald & Frank, 2017; Paracha et al., 2023; Pete et al., 2020), and police records (Décary-Hétu & Dupont, 2012; Leukfeldt et al., 2017b).

The significance of this study lies in its focus on the Telegram ecosystem and its use and abuse by hacker groups. Specifically, Telegram is a freemium, privacy-oriented, and cloud-based instant messaging service launched in 2013. The app boasts a variety of privacy-enhancing features, including end-to-end encryption, self-destructing messages, and the possibility to create private channels and groups (*Telegram FAQ*, n.d.). These features have made it a popular choice among a variety of users, including political dissidents, journalists, and human rights activists, who require secure communication channels to protect their privacy and safety. However, these same features have also made Telegram an attractive platform for terrorists, online-extremists, and criminals who seek to evade detection and carry out their illicit activities anonymously (Bucher & Helmond, 2018; Rogers, 2020; Shapiro, 2013; Urman & Katz, 2022). Specifically, Telegram offers a to the security versus efficiency trade-off that illicit communities encounter as they attempt to balance their operational activities with their efforts to remain secure (Morselli et al., 2007). These groups are drawn to Telegram due to its ability to create and maintain private groups and channels, which allows them to communicate, trade for illicit goods and services, and share information without fear of being detected by law enforcement or other authorities. Moreover, the end-to-end encryption and self-destructing messages features make it difficult for authorities to track their activities and gather evidence for prosecution.

It is here considered that hacker groups, much like terrorist, extremist, anarchist, subversive, and conspiracy groups, can be classified as hard-to-reach communities. Thus, reviewing the limited literature about hard-to-reach communities' studies on Telegram can provide a framework for understanding the complexities of such communities and assist in identifying effective methodologies for researching hacker groups. Specifically, the literature on researching hard-to-reach communities on Telegram suggests that snowball sampling is the most common approach for exploring their complex social networks. While some scholars prefer to use an exponential discriminative snowball sampling approach (Peter et al., 2022; Simon et al., 2022; Urman & Katz, 2022), others opt for a more straightforward

snowballing technique (Krona, 2020; Zehring & Domahidi, 2023). Some research may even go as far as interacting with administrators and key actors in the network to gain access to closed groups and channels (Fisher & Prucha, 2022). After mapping the network, researchers commonly employ the framework of (participant and non-participant) covert observation to study the contents and materials produced by individual groups (Fisher & Prucha, 2022; Krona, 2020). This approach enables researchers to access and analyse their activities without disrupting their operations. The presented approaches are reasonably effective for facing the hard-to-reach nature of hacker groups and their activities on Telegram.

The presented studies have distinctly aided the advance of hacker groups ecosystems studies and the investigation of hard-to-reach communities on Telegram. However, it is suggested that a research gap exists regarding the study of hacker communities, which should not be limited to mainstream social media platforms and underground forums. This limitation exists because mainstream social media platforms and traditional social networks are easily accessible to all and are subject to censorship in cases of unethical or illegal activities. Meanwhile, underground forums are difficult to access, require specific technical expertise, have limited participation, and are self-referential. Therefore, it is argued the necessity to explore the dynamics of different hacker groups on Telegram, an ecosystem that is an intermediate point between traditional platforms and underground forums and has a more balanced security-efficiency tradeoff (Morselli et al., 2007), to gain a more comprehensive understanding of their activities and dynamics.

3. Data and Methodology

3.1 Data Collection

The complexity of data sampling on Telegram is more challenging than on other platforms, since it does not provide simple data scraping functions and its privacy-oriented structure presents difficulties in identifying connections between groups and channels. Furthermore, Telegram's third-party plugins and encryption features create a unique data environment that requires specific technical expertise to navigate. To overcome these challenges, it was necessary to begin with a precompiled seed list and gradually expand the sample using a non-discriminative snowball sampling approach (Atkinson & Flint, 2001; Cohen & Arieli, 2011).

The selection and initial access to channels and groups in the seed list was accomplished through invitations extended by a network of researchers and analysts, along with reviewing available information from open

sources. Channels and groups requiring peer-to-peer vetting in private chats were deliberately avoided in favour of those with no such vetting procedures. Finally, data of each accessed channel or group are collected through Telegram's integrated 'export chat history' function. This approach helps the recognition of other public and partially closed channels and groups that would have otherwise been difficult to access, while still guaranteeing an acceptable level of ethicality and scientificity of the research.

In this research, a comprehensive dataset of 47 public and partially closed channels and groups is collected, spanning a period ranging from July 2019 to March 2023, for the purpose of constructing a citation-based network. Specifically, the network is assembled by extracting all forwards from the retrieved channels and groups messages. Forwards are defined as direct reposts from other channels or groups, without considering the sentiment of the referred content. The resulting network is comprised of 1669 nodes, with 2 edges weighted by the number of forwards between channels. The total number of forwards (unweighted edges) is found to be 2647.

3.2 Methodology

The methodological framework for this research draws on a combination of different methodological approaches, an unavoidable condition for studying the dynamics and activities of hacker groups on Telegram. The use of exponential non-discriminative snowball sampling allows for network mapping, while social network analysis techniques are performed to analyse the dynamics of the network.

Regarding sampling methodology, a more straightforward snowballing approach has been preferred in order to be able to explore the context as a whole, with the aim of identifying affiliations, interests, and ideologies of hacker groups in their digital relations with other different communities on Telegram. Specifically, discriminative snowball sampling approaches involve the inclusion specific individuals or groups in the sample and excluding others basing on predetermined characteristics. These approaches have a limited scope, as they can effectively examine the internal dynamics of a specific community, but do not account for the broader ecosystem that surrounds and interacts with it, still remaining distinct from it.

Concerning the network, it is modeled through the process of extracting and aggregating all messages that have been forwarded from the channels and groups that have been accessed. Therefore, the nodes within the network are the channels and groups that have been accessed. The connections within the network are represented through forwarded messages,

as they indicate both the source of the information and its distribution. Specifically, the nature of forwarded data presents two different roles, that of the forwarder and the forwarded, which in turn forms a directed network structure. Furthermore, the temporal dimension of the network will be ignored in this analysis, thus being collapsed into a single snapshot.

Following the application of a community detection algorithm (Blondel et al., 2008), descriptive network metrics are examined to address the first research question, which focused on understanding the dynamics of the hacker group ecosystem and its key actors. Specifically, the community detection algorithm is employed to partition the network into clusters of nodes that are more closely related within a particular community of hacker groups than with nodes outside of it. This approach enables the identification of hacker groups that are more likely to forward and receive forwarded messages from other hacker groups within that community.

3.3 Research Limitations and Ethical Considerations

The outlined methodologies are crucial for gathering insightful information on how hacking groups act and interact on Telegram. However, it is also necessary to consider the limitations and ethical implications of these approaches.

First, since the seed list is not compiled through a random process, the nature of the sampling procedure introduced some distortions in the data collection. Specifically, the use of a non-random sampling technique in the compilation of the seed list can introduce various distortions, such as over-representation of certain groups, under-representation of others, and the failure to capture the diversity of the population of interest. Second, the research is limited to a subset of hacker groups active on the Telegram platform. Therefore, the findings might not fully reflect the interactions and connections between hacker groups and other communities because of insufficient network coverage. Specifically, it is possible that these communities may utilise other similar platforms or mediums to engage within each other's and other communities (e.g., Element, Matrix.org, Signal, Tox). Furthermore, the challenges of identifying and accessing small or closed channels and groups adds to the limitation of having an incomplete network, as their interactions, dynamics and the valuable information they share are not accessible. It can be defined 'Unknown Recommendation Problem' (Peter et al., 2022).

4. Results and Discussion

The visualization of the mapped hacker groups' digital ecosystem on Telegram based on forwarded messages is presented in Figure 1, providing a visual representation of the network's structure and properties. The ForceAtlas algorithm implemented in Gephi is used to generate the network's representation (Bastian et al., 2009). Specifically, the illustration captures the interconnections and the direction of information exchange, without considering the time component. Considering the nature of the research, for security reasons no labels will be included in the graphical representations and no mention will be made of specific chats, groups or users.

Figure 1 - Network layout of the hacker groups' ecosystem on Telegram

In analysing the entire network, it is crucial to examine the density of the network as a metric that reflects the general level of connectivity among the constituent nodes. This measure is calculated by dividing the total number of actual connections by the maximum number of possible connections, resulting in a proportion that ranges from 0 to 1. In the context of the present research, the computed density is 0.001, indicating a relatively low degree of interconnectivity among the hacker groups' network. This implies that information transmission between individual channels and groups within the network may be suboptimal, since many potential paths for information flow may not exist. Nonetheless, the network is likely to be more resilient to disruptions and damage than net-

works with higher densities values. Specifically, the removal of few nodes would not significantly impair the overall functioning of the network, given that there are relatively few connections to begin with.

Furthermore, to deepen the dynamics at the node level, degree centrality measures are examined to quantify the number of connections incident upon a node (i.e., the number of ties that a node has). Specifically, in the case of a directed network, such as in the current research, it is necessary to perform two separate measures of degree centrality, namely, outdegree and indegree. Accordingly, outdegree refers to the number of relationships originating from a node to other nodes, while indegree refers to the number of relationships directed towards the node from other nodes. It is important to note that a high degree centrality score does not necessarily indicative of a leadership position, but rather demonstrates that the node has an extensive number of direct connections with other nodes.

Figure 2 and Figure 3 represent the hacker groups' digital ecosystem on Telegram by respectively scaling the node size and colour to emphasise the weighted outdegree and indegree values. Specifically, a larger node size indicates a higher weighted outdegree or indegree score. Moreover, to support the interpretation, the values are also scaled according to the legend displayed in both Figure 2 and Figure 3: nodes with higher weighted outdegree or indegree values are coloured with a tone closer to red, while nodes with lower values tend towards blue. This colour scheme is likewise applied to the relative edges of the nodes. The nodes or clusters of nodes that emerge as most relevant from the degree measures have been identified by numbers both in Figure 2 and Figure 3.

Figure 2 - Weighted outdegree of the hacker groups' ecosystem on Telegram

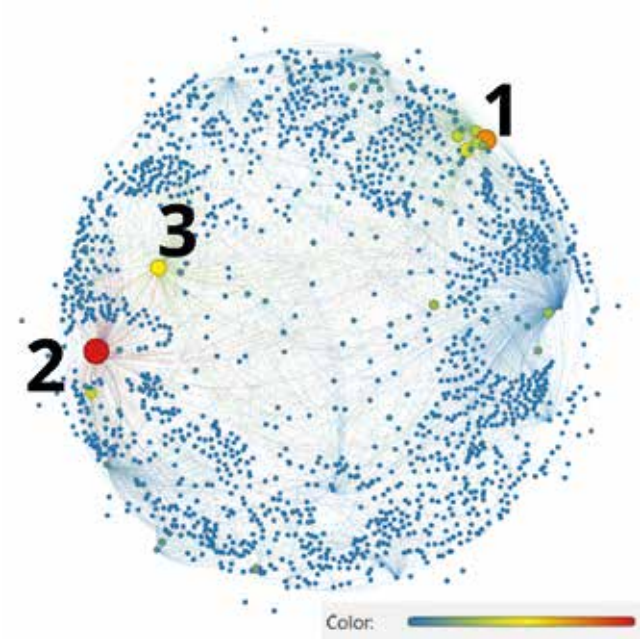
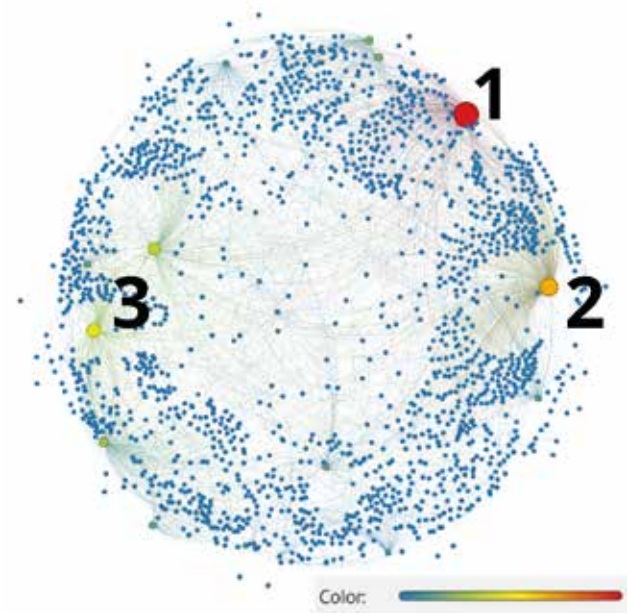


Figure 3 - Weighted indegree of the hacker groups' ecosystem on Telegram



Regarding Figure 2, it can be observed that certain nodes play a leading role in producing the most widely shared material within the network. Specifically, nodes identified with number 1 consist of pro-Russian groups and information channels involved in news spreading and propaganda around the ongoing Ukrainian-Russian conflict. Meanwhile, nodes identified with number 2 consist of groups and channels associated with a well-known pro-Russian hacker collective known for launching DoS[1] and DDoS[2] attacks against government institutions and private companies since the beginning of the Ukrainian-Russian conflict. Lastly, node identified with number 3 corresponds to a channel related to and probably run by members of the hacker collective previously described and identified with number 2, which disseminates wide-ranging material ranging from informative to satirical.

On the other side, Figure 3 identifies the nodes that forward a considerable amount of content, encompassing material, news, and user messages in other channels or groups. Similar to Figure 2, node identified with number 1 corresponds to a specific pro-Russian information channel, which is actively involved in spreading news and propaganda regarding the ongoing Ukrainian-Russian conflict. Meanwhile, node identified with number 2 relates to a less-known pro-Russian hacker group affiliated with the aforementioned better-known hacker group, with which has also participated in DoS and DDoS attacks against government institutions and private companies since the onset of the Ukrainian-Russian conflict. Lastly, nodes identified with number 3 comprise groups and channels associated to a well-known pro-Russian hacker collective, known for launching DoS and DDoS attacks against government institutions and private companies since the beginning of the Ukrainian-Russian conflict. Overall, it is possible to observe that some nodes present a relevant degree score both in Figures 2 and Figure 3. Specifically, it can be stated that certain channels, groups, or users perform a dual function in the network by generating a substantial amount of original content that is shared by other nodes while concurrently serving as a connector between different

[1] Denial of Service (DoS) is a type of cyber attack that involves overwhelming a network or server with traffic or requests in order to make it unavailable to users. The goal of a DoS attack is to disrupt the normal functioning of a system, either to cause inconvenience or to extort money from the target.

[2] Distributed Denial of Service (DDoS) is a type of cyber attack that is similar to a DoS attack, but involves multiple sources of traffic or requests, often from a network of compromised computers or devices, known as a botnet. The goal of a DDoS attack is to overwhelm a target with traffic or requests from multiple sources, making it more difficult to mitigate and defend against.

nodes. These observations lead to the conclusion that these prominent nodes have a central role in shaping the network's dynamics and may be the main participants of the network itself.

Analysing the subgroups of the network, Figure 4 represents the hacker groups' digital ecosystem on Telegram basing on the modularity class values. Specifically, the network is color-coded based on each node's modularity class, and the edges are correspondingly coloured. The modularity score of the hacker groups' network is found to be 0.66, which indicates the presence of distinct communities within the network. As posited by Newman and Girvan (2004), elevated modularity scores are indicative of greater community structure in a network. Nevertheless, in the present study, the modularity score of 0.66 does not attest to a distinctly delineated community structure.

Figure 4 - Community layout of the hacker groups' ecosystem on Telegram

Specifically, Table 1 provides an overview of the distribution of the eight different communities detected in the network. The size of each community is expressed as a percentage of the total nodes in the network. To support the interpretation of the data, a reference system has been implemented in the form of a 'community number' column. This column allows for each community's location within the network to be easily matched to the corresponding colour legend presented in Figure 4.

Table 1 - Distribution of communities in the network by share of nodes

Community number	Share of nodes	Brief description
11	25.22%	Lesser-known pro-Russian hacker groups
8	21.21 %	Most notorious pro-Russian hacker groups
99	10.25%	Pro-Russia news spreaders on the ongoing conflict
69	7.67%	Other hacker groups involved in the ongoing conflict
97	6.47%	Bottom-up propaganda related to PMC Wagner
104	5.15%	Pro-Russia news spreaders on the ongoing conflict
112	4.43%	Russian language bot chatroom
46	4.13%	Iranian anti-regime hacker groups

The concept of modularity class extends beyond the dentification of specific communities within the network, as it can also provide an introductory understanding of their behaviour and ideologies basing on the common ground of the content they disseminate.

Communities identified with numbers 11 and 8 have been identified as pro-Russian hacker groups whose constituent appear to be motivated by political motives rather than being driven by profit-oriented goals. Specifically, community number 8 is composed of highly skilled groups whose names have also come to the public's attention on more than one occasion., whereas community number 11 is composed by groups considered lesser-known due to the lack of evidence to suggest that they have independently executed cyberattacks against public or private institutions of national strategic importance. However, this does not necessarily mean that they do not have the internal competencies to conduct such complex cyberattacks. On the other side, while the communities identified with numbers 11 and 8 appear to have close affiliations with the Kremlin and other pro-Russia entities, the community, the community identified with number 69 seems to be comprised of more technically and organisationally prepared groups than those in the former two communities. Furthermore, the groups belonging to community identified with number 69 appear not to be homogeneous in supporting one or the other side in the ongoing Ukrainian-Russian conflict, even committing with different levels of involvement.

Communities identified with numbers 99 and 104 have been identified as pro-Russian news spreaders, mainly concerning the Ukrainian-Russian conflict (Aleksejeva & Mammadova, 2023). Disseminating news articles, photographs, and videos that portray the conflict from a pro-Russian per-

spective, these actors aim to control the information environment on Telegram and influence public opinion and legitimise Russia's involvement in the conflict. Specifically, they employ various techniques to reinforce their narratives, such as spreading disinformation and propaganda, highlighting conspiracy theories, and discrediting opposing views.

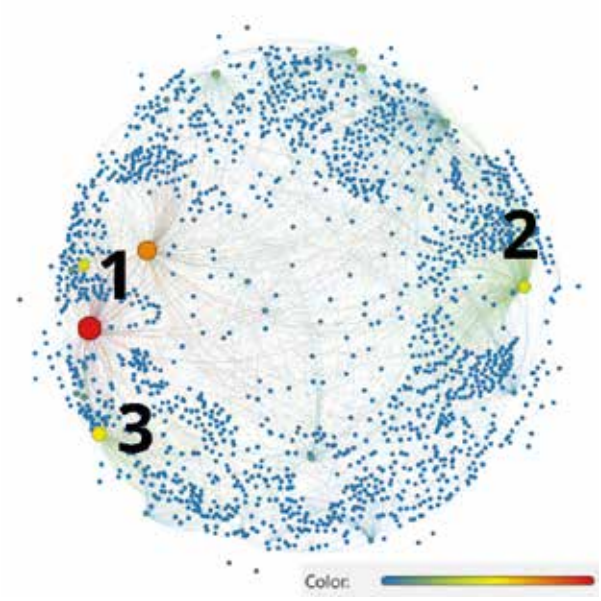
Community identified with number 97 has been associated with the Private Military Company (hereinafter, PMC) Wagner's grassroots propaganda efforts, which are disseminated by Wagner members themselves (Porrino & Borgonovo, 2023).[3] These individuals draw inspiration from the official top-down repertoire and generate a plethora of content that primarily revolves around war bulletins and enlistment-encouraging imagery. It is worth noting that these actors are also involved in financial support operations. Typically, these individuals, who are often mercenaries, attempt to establish a sense of membership within the war context by showcasing guitars, flags, and weapons while functioning as primary recruiters.

Community identified with number 112 has been associated with a chat of Russian hackers who employ a bot to relay user messages and maintain anonymity in the conversations. Specifically, rather than writing directly to the chat, users compose messages to a chatbot that masks their unique identifier before forwarding the message to the chat as if sent directly. The chatroom appears to serve as an unrestricted venue for discussing topics and issues pertaining to the underground cybercrime world, as well as anonymous discourse between users on non-digital matters. Community identified with number 46 has been identified as Iranian anti-regime hacker groups. These groups appear to be politically motivated and have been observed encouraging to target government and military institutions in Iran. Specifically, the goals of these groups include disrupting government operations and exposing sensitive information, as well as promoting anti-regime sentiment. Furthermore, these groups are observed exchanging materials and instructional resources pertaining to the perpetration of cyberattacks, as well as discussing the development of the online cybercriminal community. Figure 5 represents the hacker groups' digital ecosystem on Telegram scaling the node size and colour basing on the PageRank algorithm measurement. Specifically, a larger node size corresponds to a higher PageRank value. Furthermore, the va-

[3] The Wagner Group is a Russian PMC that has been linked to several conflicts around the world. The group has been described as a "shadow army" that operates in a grey area between the Russian military and private enterprise and is also believed to be closely linked to the Russian government and to have ties to Russian President Vladimir Putin's inner circle.

lues are colour-scaled according to the legend presented in Figure 5: a node with a higher PageRank value is coloured with a tone closer to red, while a node with a lower value tends towards blue. This colour scheme is also applied to the edges of the nodes.

Figure 5 – PageRank measurement of the hacker groups' ecosystem of Telegram



PageRank measurement shows how important a node is to other important nodes. Specifically, the PageRank algorithm calculates the importance of a node based on the number and quality of connections it has with other nodes in the network. The algorithm assigns a score to each node, with higher scores indicating greater importance within the network.

As previously assumed, certain nodes with relevant weighted outdegree and indegree scores are also identified in Figure 5 as the most important nodes of the network. Specifically, nodes identified by the numeral 1 correspond to groups and channels associated with a well-known pro-Russian hacker collective recognised for its involvement in DoS and DDoS attacks against governmental institutions and private enterprises since the commencement of the Ukrainian-Russian conflict. Meanwhile, node denoted with number 2 relates to a lesser-known pro-Russian hacker group that has collaborated with the previously mentioned prominent hacker group in carrying out DoS and DDoS attacks against government entities and private companies since the beginning of the Ukrainian-Russian conflict. Lastly, node identified with number 3 pertains to a national fringe of an international activist

and hacktivist movement that has gained recognition for its multiple cyberattacks targeting various governmental institutions and private companies. This group is siding with the Kremlin in the ongoing Ukrainian-Russian conflict and has mobilised alongside the hacker collective previously described and identified with number 1.

5. Conclusions

In this research, a first attempt is made to reconstruct the digital ecosystem of hacker groups on Telegram using a seed list of channels and groups compiled from open-source and third-party information, and then expanded through a non-discriminatory snowball sampling approach. The network is constructed by using the forwarding of a message as an indicator of a connection between nodes. This approach allowed for a comprehensive analysis of the structure and content of the network, which yielded valuable insights into the interactions and activities of the hacker groups.

Performing a social network analysis, it is observed that nodes comprising the hacker groups' network are not extensively interconnected, which suggests a certain level of closedness within the different groups. It is also shed light on the dynamics between different nodes within the network, highlighting those that produce a greater amount of original content and those that act primarily as disseminators of material produced by others. Notably, some nodes emerge as playing a dual role, serving as both significant disseminators of original content and relayers of material produced by other nodes. Furthermore, the network is also analysed at the subgroup level using a community detection algorithm to identify the common constituents of each community present in the network. Lastly, the study identified the main nodes in the network by computing the PageRank measurement of each node, which results identify a similarity with nodes that held a dual role in the network. It must be highlighted that those profit-oriented hacker groups that use Telegram to sponsor and sell leaked datasets obtained from their cybercriminal activities do not emerge as important nodes in the network. This result may be attributed to their lack of interest in formally interacting with other hacker groups, as their objectives are primarily monetary. Furthermore, it is possible that other hacker groups may not be interested in promoting or sponsoring the activities and sale of datasets from their competitors. Thus, it is suggested that research regarding monetisation-oriented hacker groups should take place through different approaches other than social network analysis. In conclusion, this study demonstrates the capacities of social network analysis methodology to extract significant insights from the hacker groups' digital ecosystem on Telegram. The findings of this research demonstrate that the complex ecosystem

of hacker groups can be successfully examined to draw valuable information by analysing the structure and content.

In consideration of this, it is suggested that further research could explore deeper network mapping, including access to closed channels and groups, while taking appropriate measures to ensure security and privacy. Additionally, other network analyses and measures could be performed to verify the obtained results. Regarding the content analysis, future research could examine the sentiment of the content disseminated through the network, considering a larger number of key nodes and considering weighting for each identified cluster. Furthermore, analysing mentions in addition to forwards could provide additional insight into the nature of the content shared within the network. These approaches could enhance the understanding of the hacker groups' digital ecosystem on Telegram structure and content dissemination, leading to more nuanced and comprehensive insights.

References

Abbasi, A., Li, W., Benjamin, V., Hu, S., & Chen, H. (2014). Descriptive Analytics: Examining Expert Hackers in Web Forums. *2014 IEEE Joint Intelligence and Security Informatics Conference*, 56–63. https://doi.org/10.1109/JISIC.2014.18

Aleksejeva, N., & Mammadova, S. (2023, March 1). Networks of pro-Kremlin Telegram channels spread disinformation at a global scale. *Digital Forensic Research Lab (DFRLab)*. https://medium.com/dfrlab/networks-of-pro-kremlin-telegram-channels-spread-disinformation-at-a-global-scale-af4e319bd51e

Aslan, C. B., Li, S., Celebi, F. V., & Tian, H. (2020). The World of Defacers: Looking Through the Lens of Their Activities on Twitter. *IEEE Access*, *8*, 204132–204143. https://doi.org/10.1109/ACCESS.2020.3037015

Atkinson, R., & Flint, J. (2001). Accessing hidden and hard-to-reach populations: Snowball research strategies. *Social Research Update*, *33*(1), 1–4.

Bastian, M., Heymann, S., & Jacomy, M. (2009). Gephi: An Open Source Software for Exploring and Manipulating Networks. *Proceedings of the International AAAI Conference on Web and Social Media*, *3*(1), 361–362. https://doi.org/10.1609/icwsm.v3i1.13937

Blondel, V. D., Guillaume, J.-L., Lambiotte, R., & Lefebvre, E. (2008). Fast unfolding of communities in large networks. *Journal of Statistical Mechanics: Theory and Experiment*, *2008*(10), P10008.

Bucher, T., & Helmond, A. (2018). The Affordances of Social Media Platforms. In *The SAGE Handbook of Social Media* (pp. 233–253). SAGE Publications Ltd. https://doi.org/10.4135/9781473984066.n14

Cohen, N., & Arieli, T. (2011). Field research in conflict environments: Methodological challenges and snowball sampling. *Journal of Peace Research*, *48*(4), 423–435. https://doi.org/10.1177/0022343311405698

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160–175. https://doi.org/10.1080/17440572.2012.702523

Décary-Hétu, D., Morselli, C., & Leman-Langlois, S. (2012). Welcome to the Scene: A Study of Social Organization and Recognition among Warez Hackers. *Journal of Research in Crime and Delinquency*, *49*(3), 359–382. https://doi.org/10.1177/0022427811420876

Dupont, B., Côté, A.-M., Boutin, J.-I., & Fernandez, J. (2017). Darkode: Recruitment Patterns and Transactional Features of "the Most Dangerous Cybercrime Forum in the World". *American Behavioral Scientist*, *61*(11), 1219–1243. https://doi.org/10.1177/0002764217734263

Dupont, B., Côté, A.-M., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime*, *17*(2), 129–151. https://doi.org/10.1080/17440572.2016.1157480

Fisher, A., & Prucha, N. (2022). 'Working and Waiting': The Salafi-Jihadi movement on Telegram in 2021. *Sicurezza, Terrorismo e Società*, *1*(2022), 149–178.

Grabosky, P. (2016). The evolution of cybercrime, 2006-2016. In T. Holt (Ed.), *Cybercrime Through an Interdisciplinary Lens* (1st ed., pp. 29–50). Routledge. https://doi.org/10.4324/9781315618456

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171–198. https://doi.org/10.1080/01639620601131065

Holt, T. J. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime*, *14*(2–3), 155–174. https://doi.org/10.1080/17440572.2013.787925

Holt, T. J., & Kilger, M. (2008). Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers. *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing*, 67–78. https://doi.org/10.1109/WISTDCS.2008.9

Howell, C. J., Burruss, G. W., Maimon, D., & Sahani, S. (2019). Website defacement and routine activities: Considering the importance of hackers' valuations of potential targets. *Journal of Crime and Justice*, *42*(5), 536–550. https://doi.org/10.1080/0735648X.2019.1691859

Jordan, T., & Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review*, *46*(4), 757–780. https://doi.org/10.1111/1467-954X.00139

Krona, M. (2020). Collaborative Media Practices and Interconnected Digital Strategies of Islamic State (IS) and Pro-IS Supporter Networks on Telegram. *International Journal of Communication*, *14*, 1888–1910. Scopus.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks. *British Journal of Criminology*, *57*(3), 704–722. https://doi.org/10.1093/bjc/azw009

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017b). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis.

Crime, Law and Social Change, *67*(1), 39–53. https://doi.org/10.1007/s10611-016-9663-1

Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social network analysis of a criminal hacker community. *Journal of Computer Information Systems*, *51*(2), 31–41.

Macdonald, M., & Frank, R. (2017). The network structure of malware development, deployment and distribution. *Global Crime*, *18*(1), 49–69. https://doi.org/10.1080/17440572.2016.1227707

McGloin, J. M., & Nguyen, H. (2013). The importance of studying co-offending networks for criminological theory and policy. In *Crime and networks* (pp. 13–27). Routledge.

Morselli, C., Giguère, C., & Petit, K. (2007). The efficiency/security trade-off in criminal networks. *Social Networks*, *29*(1), 143–153. https://doi.org/10.1016/j.socnet.2006.05.001

Newman, M. E. J., & Girvan, M. (2004). Finding and evaluating community structure in networks. *Physical Review E*, *69*(2), 026113. https://doi.org/10.1103/PhysRevE.69.026113

Oliver, D., & Randolph, Adriane. B. (2022). Hacker Definitions in Information Systems Research. *Journal of Computer Information Systems*, *62*(2), 397–409. https://doi.org/10.1080/08874417.2020.1833379

Paracha, A. A., Arshad, J., & Khan, M. M. (2023). S.U.S. You're SUS!—Identifying influencer hackers on dark web social networks. *Computers and Electrical Engineering*, *107*, 108627. https://doi.org/10.1016/j.compeleceng.2023.108627

Perkins, R. C., Ouellet, M., Howell, C. J., & Maimon, D. (2022). The Illicit Ecosystem of Hacking: A Longitudinal Network Analysis of Website Defacement Groups. *Social Science Computer Review*, 089443932210978. https://doi.org/10.1177/08944393221097881

Pete, I., Hughes, J., Chua, Y. T., & Bada, M. (2020). A Social Network Analysis and Comparison of Six Dark Web Forums. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 484–493. https://doi.org/10.1109/EuroSPW51379.2020.00071

Peter, V., Kühn, R., Mitrović, J., Granitzer, M., & Schmid-Petri, H. (2022). Network Analysis of German COVID-19 Related Discussions on Telegram. In P. Rosso, V. Basile, R. Martínez, E. Métais, & F. Meziane (Eds.), *Natural Language Processing and Information Systems* (Vol. 13286, pp. 25–32). Springer International Publishing. https://doi.org/10.1007/978-3-031-08473-7_3

Porrino, G., & Borgonovo, F. (2023, February 13). PMC Wagner Propaganda Ecosystem. *ITSTIME*. https://www.itstime.it/w/pmc-wagner-propaganda-ecosystem-by-giulia-porrino-federico-borgonovo/

Rogers, R. (2020). Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media. *European Journal of Communication*, *35*(3), 213–229. https://doi.org/10.1177/0267323120922066

Shapiro, J. N. (2013). *The Terrorist's Dilemma: Managing Violent Covert Organizations*. Princeton University Press. https://doi.org/10.1515/9781400848645

Simon, M., Welbers, K., C. Kroon, A., & Trilling, D. (2022). Linked in the dark: A network approach to understanding information flows within the Dutch Telegramsphere. *Information, Communication & Society*, 1–25. https://doi.org/10.1080/1369118X.2022.2133549

Steinmetz, K. F. (2015). Craft(y)ness: An Ethnographic Study of Hacking. *British Journal of Criminology*, 55(1), 125–145. https://doi.org/10.1093/bjc/azu061

Telegram FAQ. (n.d.). Telegram. Retrieved 21 March 2023, from https://www.telegram.org/faq?setln=en#q-there-39s-illegal-content-on-telegram-how-do-i-take-it-down

Tremblay, R. E., Welsh, B. C., & Sayre-McCord, G. (2019). Crime and the Life-Course, Prevention, Experiments, and Truth Seeking: Joan McCord's Pioneering Contributions to Criminology. *Annual Review of Criminology*, 2(1), 1–20. https://doi.org/10.1146/annurev-criminol-011518-024712

Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review*, 23(1), 8–23.

Urman, A., & Katz, S. (2022). What they do in the shadows: Examining the far-right networks on Telegram. *Information, Communication & Society*, 25(7), 904–923. https://doi.org/10.1080/1369118X.2020.1803946

Zehring, M., & Domahidi, E. (2023). German Corona Protest Mobilizers on Telegram and Their Relations to the Far Right: A Network and Topic Analysis. *Social Media + Society*, 9(1), 205630512311551. https://doi.org/10.1177/20563051231155106

Questo volume è stato stampato
nel mese di giugno 2023
su materiali e con tecnologie ecocompatibili
presso la LITOGRAFIA SOLARI
Peschiera Borromeo (MI)

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 979-12-5535-127-6