Technology in Society 82 (2025) 102873

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

The organized activities of ransomware groups: A social network approach

Ekaterina Botchkovar [a,*], Kexin Cui [b], Olena Antonaccio [c], Robert Perkins [d], David Maimon [d]

[a] Northeastern University, USA
[b] Michigan State University, USA
[c] University of Miami, USA
[d] Georgia State University, USA

A B S T R A C T

Using Social Network Analysis (SNA), our study examines how cybercriminals organize and operate within Ransomware-as-a-Service (RaaS) networks by analyzing connections between 96 cybercriminals and 140 ransomware groups. We compared these online criminal networks to traditional organized crime groups to better understand their structure and operations. Initially, we expected to find RaaS networks operating similarly to traditional criminal organizations—with tight connections, central leadership, and close-knit teams. However, our analysis revealed that RaaS networks are more loosely organized and decentralized, with members being spread out rather than clustered in tight groups. However, similar to traditional organized crime groups, certain individuals play crucial roles as network "hubs" or "brokers" in RaaS networks. These key players maintain connections across different parts of the network and facilitate information sharing. Our statistical analyses, based on Ordinary Least Squares regression models with log-transformed outcomes, showed that individuals with more direct connections tend to be network "brokers", helping bridge different parts of the network. These findings suggest that while ransomware groups share some similarities with traditional organized crime, they operate in distinct ways. By identifying and targeting key network players who keep ransomware operations running, law enforcement may be more effective in disrupting these criminal networks.

1. Introduction

The integration of technology into modern life has been associated with an ever-increasing number of cybercrimes threatening individuals, organizations, and entire nation-states (Baranovska et al., 2024). Perhaps the most widely recognized cyberthreat today originates from ransomware, a type of malicious software that encrypts data stored on a device rendering them, and systems dependent on it, inaccessible. To retrieve at least some of their information, victims are compelled to pay significant ransom amounts (Cybersecurity and Infrastructure Security Agency, 2022). On average, the attackers offer a downtime of nineteen days to victims demanding payouts exceeding $230,000 (Lubin, 2022).

Creating and operating ransomware requires significant technological expertise, which used to serve as a barrier to entry for novice criminals. However, the cybercrime landscape underwent a significant transformation following the introduction of the Ransomware-as-a-Service (RaaS) business model in 2015 (Oz et al., 2022). RaaS has facilitated a rapid spike in the size and proliferation of cyber groups responsible for the majority of ransomware attacks. These processes have had a global impact, with schools, universities, governments, corporations, and even the healthcare industry all reporting victimization by ransomware groups (Teichmann et al., 2023). Despite the use of numerous strategies aimed at the early detection and prevention of ransomware attacks, their occurrence is escalating. In 2020, the frequency of these incidents surged to 20,000 to 30,000 per day in the U.S. alone, equating to a breach occurring roughly every 11 s. By 2022, the Internet Crime Complaint Center (IC3) documented 800,944 complaints, with projected total losses escalating from $6.9 billion in 2021 to over $10.2 billion in 2022 (Internet Crime Complaint Center, 2022). The arrests of ransomware group actors occur regularly (e.g. (Ryan, 2021),), but their effect is hard to ascertain with new threats mushrooming in cyberspace.

The looming threat of ransomware attacks on critical infrastructure underscores the urgent need for in-depth research on responsible online actors. The collective nature of RaaS indicates that ransomware, from its creation to the collection of ransom payments, is a group-driven phenomenon. Therefore, effective prevention strategies should prioritize disrupting the networks formed by these actors to stop attacks before they happen. However, scant attention has been paid to the organizational structure of ransomware teams, with existing inquiries often limited to the descriptive analyses of RaaS and its impacts (cf. (Ryan, 2021)– (Martin & Whelan, 2023)).

* Corresponding author. School of Criminology and Criminal Justice, 425 Churchill Hall, 360 Huntington Ave, Boston, MA 02115, USA.
E-mail address: e.botchkovar@northeastern.edu (E. Botchkovar).

https://doi.org/10.1016/j.techsoc.2025.102873
Received 12 October 2024; Received in revised form 5 February 2025; Accepted 8 March 2025
Available online 14 March 2025

Drawing on the insights from the growing research on the traditional forms of criminal networks such as criminal gangs and organized crime groups (e.g. (Morselli, 2009),- (Lopes et al., 2022)), our study seeks to understand the structure of networks created by online actors involved in RaaS activities and identify their strengths and vulnerabilities. To do so, we utilize unique data that map out the associations between individual actors and groups responsible for a large number of ransomware attacks around the world. We then assess the key characteristics of these connections along with the roles played by individual actors and groups in these networks. Our findings expand the horizons of the scholarship aimed at understanding the structure and dynamics of cybercrime groups, while also providing important clues about their vulnerabilities.

2. The growth of ransomware groups

With its promise of large profits, ransomware has experienced a significant increase in popularity over the last few years. Originating from the combination of two terms, “ransom” and “malware”, ransomware is typically associated with financial losses borne by individuals and organizations (Rehman et al., 2019). Three types of ransomware exist: locker, crypto, and scareware. Whereas scareware tricks the victim into believing they are required to download and pay for the fake “antivirus” software to remove a “virus” on their computer, the locker and crypto versions of ransomware lock the victim out of their computer or encrypt their files, making them inaccessible unless a “ransom” is paid. It is the crypto version of ransomware that has wreaked havoc on individual computers and computer systems—overcoming this type of malware is difficult, and the damage it causes is often irreversible (Beaman et al., 2021). While several modalities of extorting money from victims exist, ransomware groups commonly demand payment in cryptocurrency, which makes these operations difficult to trace (Nadir & Bakhshi, 2018).

The ease of committing these crimes, coupled with significant financial incentives, has driven the proliferation of the new Ransomware-as-a-Service (RaaS) model, enabling multiple parties to participate in extortion schemes. The RaaS model offers accessible and adaptable ransomware kits available for purchase on illicit platforms. Various payment arrangements exist, ranging from one-time licensing fees to monthly subscriptions for using the ransomware. Individual hackers often act as group “affiliates” launching the attacks, while core members focus on improving the malicious software. This development has led to the emergence of specialized cybercrime groups with diverse skill sets, making them effective in generating profits from victims. Today, ransomware groups typically consist of subgroups such as software "creators," extortion-focused "affiliates," coordinating "operators," information-providing "moles," victim “contact centers”, lenient "bulletproof" hosting providers, and "currency exchangers" facilitating cryptocurrency conversion (Smith & Plachkinova, 2022).

The complex structures associated with ransomware production and distribution suggest the presence of extensive networks allowing the cybercriminals behind these operations to effectively communicate and function as a criminal syndicate (see also (Morselli, 2009)). Few studies, however, provide a glimpse of the internal connections within and across such cyber groups.

2.1. Crime-oriented social networks in cyberspace: research evidence

Recently, scholars have sought to investigate the nature of the networks formed by cyber criminals (e.g., (Holt & Bossler, 2013),(Holt et al., 2012)). Their research utilizes various data sources to explore the structure of cybercrime communities, such as online forums (e.g. (Grisham et al., 2017),- (Marin et al., 2018)), online drug markets (e.g., (Duxbury & Haynie, 2018a), (Duxbury & Haynie, 2018b)), and more amorphous groups whose membership was established through the analyses of social or news media sources (e.g. (Sarvari et al., 2014),). The accumulated evidence indicates the existence of network structures in the cyber world that not only enhance the effectiveness of criminal operations but also facilitate the transfer of knowledge and skills essential for committing crimes.

Although cybercrime groups tend to utilize multiple platforms for recruiting new members and conducting their criminal activities, dark net (or dark web) forums appear to be one of the primary mechanisms fostering these connections (Meland et al., 2020). Hosted on overlay networks and unindexed by regular search engines, dark web forums serve as unique ecosystems allowing cybercriminals to share crime-relevant skills and knowledge, buy and sell illegal goods, and form networks (Holt et al., 2012), (Grisham et al., 2017), (Holt, 2007), (Leukfeldt, Kleemans, & Stol, 2017a,b). Trust is a scarce commodity in crime-oriented groups (Lampe & Johansen, 2004),(Kleemans and Paoli, 2014), thus much of their communication occurs through private messages or on invite-only forum sections unavailable to other forum users. Forum-based studies confirm the existence of ties between key forum users. In one such study, Macdonald and Frank (Macdonald & Frank, 2016) analyzed 2458 users on a malware-focused forum, identifying tighter groups specializing in various malware-related activities (see also (Huang & Chen, 2016)). Similarly, Holt et al. (Holt et al., 2012) observed stronger central connections and looser peripheral ones in several malware-focused dark web forums.

A growing body of literature has specifically focused on hacker networks. Regardless of the type of hacking and data used, research confirms the existence of connections among hackers who tend to form small collectivities based on shared interests. For instance, Howell et al. (Howell et al., 2019) found that, among 396 hackers involved in website defacement, a small number of highly skilled actors were central in the network, while others were on the fringes. Similarly, Perkins et al. (Perkins et al., 2023) studied 786 hackers across 123 website defacement groups and discovered loosely structured networks that are relatively stable in time and centered around several influential groups. Finally, Décary-Hétu, Morselli, and Leman-Langlois (Decary-Hétu et al., 2012) researched warez groups, which they found to be fairly egalitarian, dispersed, short-lived, and not particularly productive.

To summarize, scarce research evidence shows that, regardless of specialization, offenders in cyberspace tend to form loose groups that tend to have core members as well as those peripheral to these networks. It is important to note that existing studies are often limited by their inability to verify the authenticity of connections between forum users, leaving uncertainty about whether the identified actors are directly involved in cybercrime. Furthermore, the narrow focus on specific cybercrimes (e.g., warez or website defacing) raises questions about whether these networks function similarly across other types of cybercriminal activities. Nonetheless, the growing body of evidence pointing to the existence of clandestine networks in cyberspace suggests that some formations may mirror those of traditional organized crime.

2.2. RaaS as a form of organized cybercrime

The growing complexity of networks formed by cybercriminals has prompted some scholars to liken them to the traditional forms of organized crime (e.g. (Grabosky, 2007),– (Jian et al., 2022)). For instance, Hutchings (Hutchings, 2014) notes that cybercriminals form connections that enable them to collaborate and learn from each other in crime commission, while McGuire’s (McGuire, 2012) report suggests that up to 80 percent of all online crimes are committed by organized crime groups. Yet other scholars emphasize the definitional challenges associated with organized crime, arguing that it cannot simply be considered a “crime that is organized” ([46; p. 289]; (McGuire, 2012), (Duijn et al., 2014)). Instead, they note, organized crime groups and cyber-based groups differ in the seriousness of the crimes they commit, their methods of recruitment and enforcement, and their goals (e.g., (Lavorgna, 2020),(Lusthaus, 2013)).

Discussing the challenges in defining traditional organized crime, Finckenauer (Finckenauer, 2005) outlines multiple criteria: ideology,

structure, continuity, use or threat of violence, restricted membership, illegal enterprises, penetration into legitimate businesses, and corruption. The analysis carried out by Finckenauer emphasizes the role of violence and corruption while downplaying the importance of ideology and hierarchy in organized crime groups. Contemporary organized crime, according to Finckenauer (Finckenauer, 2005), tends to be profit-oriented and loosely structured. Despite the loose structure, organized crime groups effectively engage in various illicit enterprises and remain closed to outsiders.

The absence of a universally accepted definition of traditional organized crime, often vaguely explained through the specific activities such groups may engage in (e.g., racketeering, loan sharking, or narcotrafficking) or their structure (Finckenauer, 2005), also makes it challenging to include cybercrime in the same category. Nonetheless, the growing evidence of existing connections between cybercriminals and their specialization points to the increasing organization within cybercrime teams (e.g. (Whelan et al., 2024),), thus suggesting that a new form of *organized cybercrime* is developing (DiMaggio, 2022), (Hutchings, 2014), (Jian et al., 2022).

To illustrate these points, Whelan and colleagues (Whelan et al., 2024) use the case of ransomware to argue that RaaS (Ransomware-as-a-Service) groups are an accurate representation of cyber forms of organized crime. Similar to traditional organized crimes, ransomware-based extortion requires forethought, careful planning, and activity specialization of the group members united by a pursuit of profits. The presence of core group members, responsible for ransomware production and effective functioning, and "affiliates," taking on less important roles, also suggests the presence of some form of hierarchy in these groups. Though not necessarily reminiscent of traditional crimes committed by La Cosa Nostra, the crimes committed by RaaS are predatory and often symbolically violent, particularly given the practice of sharing stolen information online to compel their victims to pay the ransom. At the same time, establishing control over territory, as is typical among traditional organized crime groups, is unnecessary in the largely unregulated digital world, which offers infinite opportunities for action.

Overall, scholars argue for significant convergence between traditional and digital forms of organized crime, suggesting that the frameworks used to assess traditional crimes should be adapted to include emerging forms of organized crime in the digital realm (Irving, 2016). However, no research has yet investigated the complex networks formed by the rise and growing popularity of RaaS. With their extensive and complex nature as well as a distinct focus on profit, ransomware-based networks are likely to most closely resemble the traditional networks of organized crime groups operating in the physical world.

3. The current study

Our study focuses on the structure of RaaS (Ransomware-as-a-Service) groups to understand the similarities and differences between this form of cybercrime and those typically identified as traditional organized crime. The traditional forms of criminal networks have been investigated in the studies of gangs (Papachristos et al., 2012), (Papachristos et al., 2013), drug trafficking networks (Bichler et al., 2017), (Tenti & Morselli, 2014), organized crime groups (Campana & Varese, 2022), money laundering (Duijn et al., 2014), (da Cunha & Gonçalves, 2018), political corruption (Ribeiro et al., 2023), (Lopes et al., 2022), and others. This is the first study to systematically examine the connections between ransomware groups and affiliated individuals through the lens of organized crime, arguing that RaaS-based networks represent a form of organized cybercrime.

In particular, we will examine several propositions derived from previous research. First, Bouchard and Morselli (Irving, 2016) describe the formation of organized crime groups as a process of "resource pooling," a largely opportunistic activity where leadership is less crucial than the reliance on others for successful operations. In this perspective, illegal enterprises are seen as flexible, often short-lived formations, supported by easily replaceable members with varying levels of resources and expertise (Bouchard, 2020). While research on organized crime documents both highly centralized and decentralized as well as both dense and sparse organized crime networks (e.g. (Bichler et al., 2017),), Breuer and Varese (Breuer & Varese, 2023) suggest that strictly profit-oriented networks tend to be denser and more centralized, with shorter path length, to increase the efficiency of their operations, even at the cost of elevated vulnerability. Given these insights, we anticipate that individuals and groups within the RaaS network will be denser, more clustered and centralized, exhibiting shorter path lengths to increase the speed of the information flow across the network.

Second, scholars of organized crime emphasize the role of network "hubs," which control the flow of information, and "brokers," who connect otherwise unlinked network actors (e.g., (Calderoni et al., 2016); see also (Bichler et al., 2017)). Consequently, if the structure of organized cybercrime groups parallels that of traditional criminal networks, we should expect cyber networks to also include members who function as "hubs" and "brokers," facilitating the exchange of information within the group.

Finally, scholars (e.g. (Breuer & Varese, 2023),– (Savona et al., 2017)) note that organized crime groups may exchange members or collaborate to ensure their success and prolong their longevity. This suggests that groups, rather than individuals, could play a particularly crucial role in these networks, often mediating relationships between node pairs and supplying them with critical information. In our study, we expect ransomware groups to act as the primary "brokers" within the network.

3.1. Data

In this study, we utilized both open-source information (OSINF) and open-source intelligence tools (OSINT (Hwang et al., 2022);) to analyze publicly available yet dispersed data on 140 well-known groups and 96 individuals involved in RaaS activities over the past decade. The OSINT approach derives intelligence from raw data, such as exploring forums and social media platforms, while OSINF involves searching for open information from sources like articles, reports, blogs, and other publicly accessible materials. Our approach involved collecting social media posts, publicly available online conversations, reports, news coverage, and government releases related to RaaS group operations.

Our primary goal was to gather information on key ransomware groups, affiliated individuals, and the connections between them. Several important steps were followed during data collection for each group and individual. First, we identified relevant sources to gather information on RaaS operations. These included: a) cybersecurity reports published by independent researchers or cybersecurity firms tracking cybercriminal activities. These reports often link specific ransomware groups and individuals to particular ransomware strains; b) press releases from government agencies, such as the U.S. Department of Justice, typically announcing progress made in the investigation or prosecution of RaaS groups and individuals. These announcements often revealed connections between entities involved in RaaS activities; c) social media posts created by presumed RaaS members or their associates, which provided clues about connections and transactions between RaaS groups and individuals. Common platforms we examined included Twitter, as well as public posts and conversations extracted from dark web forums.

Our second step included cross-referencing information and attributing individuals to specific groups. Using these three key sources of information, we cross-referenced the data to establish connections between groups and individuals involved in RaaS activities. To attribute a particular individual identified by their online moniker(s) to a specific group, we used the process of triangulation. For instance, an internet moniker might be mentioned as a connection between two other monikers in cybersecurity reports. This connection could then be verified

using government press releases and various social media postings and forum conversations.

Finally, to ensure the accuracy of the connections drawn across RaaS-involved entities, we ascertained that the collected data were corroborated by multiple sources, including OSINT-based reports, government press releases, social media postings, and forum conversations. This data validation step is critical to maximizing the reliability of the gathered information and minimizing the chance of false positives.

Because we did not seek to reveal the real identities of RaaS group members, their real names were neither sought nor included in the final dataset. Instead, each entity within the network was assigned an anonymous numerical ID. As a result of the data collection process, we identified 437 connections between 236 internet monikers[1] involved in ransomware production and distribution. The collected information was then transformed into a dataset documenting the connections between these entities, indicating whether each entity was a person or a group. For privacy concerns, the final dataset has been redacted to remove the internet monikers used by the groups and individual actors included in the dataset.

3.2. Analytic strategy

First, we employed social network analysis (SNA (Scott, 2017);) to examine the structure of a social network of RaaS groups and individuals in order to compare it to traditional crime networks (DiMaggio, 2022), (Nadir & Bakhshi, 2018), (Meland et al., 2020), (Whelan et al., 2024). The data were initially analyzed using the *igraph, ggraph*, *tidyverse* and other packages used for social network analyses in the R software (Wickham et al., 2019) allowing us to gauge some network characteristics for each RaaS social network node (a group or an individual) as well as the social network as a whole.

Density is a network-level measure that evaluates the extent to which a social network is interconnected. It is calculated by dividing the sum of all existing ties in the network by the total number of possible ties between nodes. A density value of 1.0 means that all nodes are fully connected, whereas a value of 0 indicates no linked connectivity at all (Scott, 2017). In our study, a higher density value would reflect a greater cohesion among groups/individuals in the RaaS network, and a lower value would indicate sparse connections between them. *Transitivity*, also known as a clustering coefficient, is a network-level measure that estimates the likelihood that two nodes connected to a common node are themselves connected, forming a closed triad. It is computed a ratio of the number of closed triads (multiplied by 3) and the total number of connected triplets of nodes in the network. A transitivity value of 1.0 suggests that all nodes are part of closed triads, while a value of 0 indicates no three-way connections at all. In our study, this measure would indicate the extent to which the ransomware network groups and individuals form localized subgroups of RaaS groups/individuals. *Degree centrality* is a node-level network measure tapping into the number of direct connections a node has in a network(Scott, 2017). It quantifies how many links (edges) connect to a node, indicating its level of activity within the network. Nodes with a higher degree of centrality are more connected and can directly interact with more nodes, making them potentially more influential or central to the network's structure. Such nodes can act as "hubs" in organized crime networks. *Mean degree centrality* is a correspondent network-level measure indicating an average number of a single node's connections in the network. *Betweenness centrality* is a node-level measure that indicates the extent to which a node lies in on the shortest paths between other nodes in a network. It is computed as the sum of the fraction of the all-pair shortest paths that pass through each node. This measure reflects how often a node acts as a connecting link between other pairs of nodes.

In our study, higher betweenness centrality would point to more influential groups/individuals as "brokers" (Morselli, 2009),(Bichler et al., 2017) or intermediaries within the RaaS network. *Mean betweenness centrality* is a correspondent network-level measure averaging out the *betweenness centrality* values across all nodes in the network. It provides an overall measure of how, on average, the network's connectivity depends on its nodes acting as intermediaries. *Degree centralization* is a network-level measure that indicates how centrality is distributed among actors in the network. A high degree of centralization means that a few groups/individuals account for most connections in the network whereas a low degree of centralization indicates that connections are more evenly spread across the groups and individuals in the network. Finally, *mean distance* (also known as average path length) is a network-level measure that indicates the average number of steps along the shortest paths for all possible pairs of nodes in the network (Scott, 2017). It reflects how "close" or "far apart," on average, the nodes are from each other. In this study, a larger mean distance would imply that groups/individuals in the RaaS network are generally further apart, indicating a more dispersed network.

One more dataset was constructed for additional descriptive, bivariate, and multivariate analyses. In it, the original variable capturing group or individual status was combined with the computed network variables of each network node (degree of centrality and betweenness centrality). These data were then used to compute bivariate correlations and estimate the regression model predicting actors' betweenness centrality using the STATA software. Because of the skewed distribution of the outcome, a logged Ordinary Least Squares (OLS) regression model was estimated. Finally, using the group vs. individual status of all included entities, we utilized *t*-tests of group means to compare the RaaS networks of individuals and groups on the key parameters of the mean degree centralizations and betweenness centrality.

4. Results

Fig. 1 shows the connectivity between the nodes in the network, and the descriptive statistics detailing the key characteristics of the ransomware network are reported in Table 1. First, we seek to determine how dense or sparse the RaaS network is. A network density of .008 suggests that only .8 % of all possible connections between nodes are present. This indicates a very dispersed network, where most nodes are not directly connected. A mean degree centrality of 3.70 indicates that, on average, each node is connected to about 3.7 other nodes reflecting the network where nodes have relatively few direct connections and confirming a generally sparse network structure. The network degree centralization is relatively low (.12) indicating that few single nodes would be overwhelmingly more connected than others and that connections are rather evenly distributed across the network.

Our next step is to determine whether a certain degree of clustering is present in the network. A transitivity/clustering coefficient value of .202

Table 1
Key metrics describing RaaS network structure and dynamics.

Network Characteristics	
Nodes	236
Edges	437
Density	.008
Transitivity	.202
Mean Betweenness Centrality	182.55
Mean Degree Centrality	3.70
Degree Centralization	.12
Mean Distance	4.19

[1] While we distinguish between groups and individuals in the dataset, we recognize that anonymity online potentially allows multiple users to share individual and group accounts. We have attempted to minimize this possibility by only including the accounts that have been designated as groups or individuals by researchers. The distinction also remains important for our analysis, as group accounts may exhibit unique characteristics absent in the presumed individual accounts.

shows that about 20 % of the connections in the network tend to form closed triangles. Notably, network transitivity is about 25 times higher than its density indicating that, although the network is dispersed, there is some clustering in the network and some localized subgroups exist within it. A mean betweenness centrality of 182.55 is relatively high indicating that, on average, each node plays a relatively significant role in connecting others in the network by being part of many shorter paths. This also suggests that some nodes may act as bridges between otherwise disconnected parts of the network, even though the network does not have a high degree of centralization. The flow of information through the network is often dependent on those specific nodes, which can contribute to slightly longer mean distances because paths frequently converge on these key nodes. Finally, a mean path distance of 4.19 indicates that, on average, it takes about 4.6 steps to travel between any two nodes in the network. This shows that, in the RaaS network, nodes are not too far apart, and the network is not highly fragmented with the nodes in it fairly well connected. The nodes with high betweenness centrality could be key to maintaining these short paths, thus acting as "brokers" (Morselli, 2009),(Bichler et al., 2017).

We also seek to understand the variations in influence across the nodes included in the RaaS networks. The descriptive statistics of the node-level data shown in Table 2, Panel A, reveal that 59 % of the nodes in the network are groups and 41 % are individuals. The degree centrality ranging from 1 to 60 indicates that the maximum number of a node's edges in the network is 60. At the same time, the frequency distributions of the node-level degree centrality (available upon request) also show that less than 2 % of the nodes have 20 or more edges, acting as network "hubs." In particular, as illustrated in Fig. 1, these are the nodes with the IDs #2 (60 edges), #3 (53 edges), and #6 and #34 (20 edges each). When the sample of the nodes is split by the group status, the mean degree centrality is found to be somewhat higher for groups (3.71) than for individuals (3.69) but, according to the *t*-test, this difference is not significant. However, as demonstrated in Fig. 1, the most influential nodes with the highest values of degree centrality are still groups rather than individuals, thus reflecting a relatively normal distribution for the individual subsample (skewness of 1.6) and a much more skewed distribution for the group subsample (skewness of 5.5). Therefore, some groups in the network have extremely high degree centrality, whereas many others have relatively low values.

Also, shown in Table 2, the distribution of betweenness centrality of the nodes in the network is also very wide, ranging from 0 to 6593.48. Notably, the frequency distributions of the node-level betweenness centrality (available upon request) demonstrate that, whereas most nodes in this network have 0 betweenness centrality, about 10 % of them have betweenness centrality values higher than 300 and 5 % of them have betweenness centrality values higher than 1000. In addition, about 1 % have extremely high values of over 4000. As shown in Fig. 1, these are nodes with the IDs #2 (6593.48 betweenness centrality), #3 (4094.51 betweenness centrality), #6 (4185.33 betweenness centrality), which are also the nodes with the highest number of connections. Furthermore, when the sample of the nodes is split by the group status, the mean betweenness centrality is substantially higher for groups (234.68) than for individuals (105.82), and this difference is confirmed to be significant by the *t*-test. Thus, as expected, groups tend to be significantly more important than individual actors in fostering connections between nodes, and groups are thus more likely than individuals to serve as network "brokers."

We evaluate even more potential differences between groups and individuals included in the network. The bivariate correlations between several node-level characteristics are presented in Panel B, Table 2. These characteristics are the group vs. individual status, node's degree centrality, and node's betweenness centrality. Our results indicate that the correlation between the group status and the number of connections the node has is close to zero and nonsignificant. In contrast, the correlation between the group status and betweenness centrality is more substantial and positive, .094, yet still not significant due to the small sample size. On the other hand, the correlation between the node's degree centrality and its betweenness centrality is very strong (.811), positive, and significant ($p < .001$), indicating that highly connected nodes also tend to be more influential mediators in the network.

Finally, we seek to understand what determines the likelihood of being influential—having more direct connections or being a group rather than an individual. A logged OLS multivariate regression model was estimated to examine whether the node's group status and its degree centrality can predict the node's betweenness centrality, net of each other. The results from these analyses are presented in Panel C, Table 2. These figures show that the regression coefficient for the group status is positive and significant (.421, $p < .10$) indicating that, if the node is a group, its betweenness centrality is predicted to increase by approximately 52.3 % (exp (.421) ≈1.523), net of its degree centrality. Next, the regression coefficient for the node's degree centrality is positive, .262, and significant ($p < .001$) confirming that, net of its group status, for each one-unit increase in the node's degree centrality, its betweenness centrality is expected to increase by about 29.9 % (exp (.262) ≈1.299). The reported standardized regression coefficients demonstrate that the node's degree centrality is a much more powerful predictor of betweenness centrality as its standardized effect (B = .083) is about eight times larger than that of the group status (B = .673). Notably, the regression model explains a substantial portion (about 46 %) of the variation in betweenness centrality of the nodes in the network.

5. Discussion

The findings of this study offer valuable insights into cybercrime, providing mixed support for the assumption that cyber and traditional forms of organized crime closely resemble one another. Contrary to

Table 2
Descriptive statistics, bivariate correlations, and OLS regression results for social network metrics[a].

Variables	A. Descriptive Statistics											
	Mean or %	SD	Min	Max	Mean or %	SD	Min	Max	Mean or %	SD	Min	Max
	Total sample (n = 236)				Individuals (n = 96)				Groups (n = 140)			
Group	59 %	.49	0	1								
Degree	3.70	6.39	1	60	3.69	4.40	1	16	3.71	7.47	1	60
Betweenness Centrality	182.26	6.39	0	6593.48	105.82[a]	341.78	0	2137.76	234.68[a]	825.48	0	6593.48
B. Bivariate Correlations					**C. OLS Regression Predicting Logged Betweenness Centrality**							
	Degree		Betweenness Centrality						**b**	**SE**	**B**	
Group	.002		.094		Group				.421[a]	(.244)	.083	
Degree			.811***		Degree				.262***	(.019)	.673	
					Constant				.064	(.200)		
					Adj. R-squared				.46			

[a] Regression coefficients or differences in means significant at *$p < .10$, **$p < .05$, ***$p < .001$, two-tailed; the figures shown for OLS regression are unstandardized regression coefficients, standard errors (in brackets), and standardized regression coefficients.

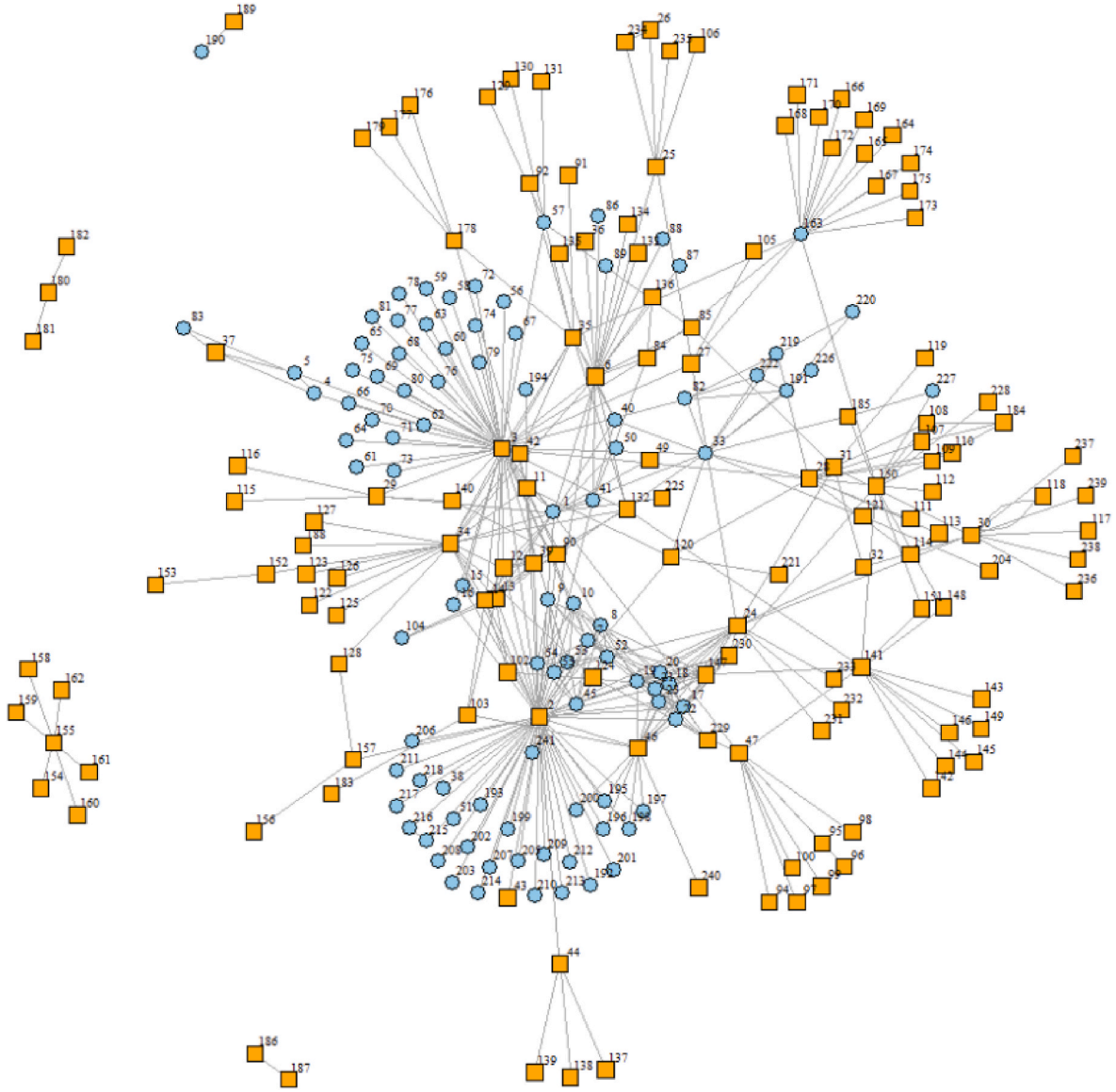

Fig. 1. Results of the social network analyses describing the relationships between fully Anonymized groups and individuals involved in ransomware operations *. *In this network visualization, nodes are colored to distinguish between two key actor types: individual actors (blue nodes) and ransomware groups (yellow nodes). The connections (edges) between these nodes demonstrate the relationships and interactions within the Ransomware-as-a-Service (RaaS) ecosystem, illustrating the decentralized and loosely connected nature of these criminal networks.

expectations drawn from the literature on organized crime, the examined RaaS network exhibits a sparse structure, with most members maintaining few direct connections. Additionally, the network demonstrates relatively low centralization, likely stemming from the nature of RaaS operations, which do not demand tight coordination among groups and individuals and allow actors to function more independently. While low density and centralization may hinder the efficiency of ransomware operations, these findings align with the research on cybercrime networks (e.g. (Decary-Hétu et al., 2012),). As highlighted in prior studies on organized crime, low-density, decentralized networks help reduce the risk of exposure (Ouellet et al., 2019),(Savona et al., 2017). This characteristic is likely crucial in the cyber realm, where trust among network members tends to be particularly limited (see also (Lampe & Johansen, 2004)).

However, consistent with expectations, the RaaS network was moderately clustered, and the pathways between nodes were short, indicating that, while the network exhibits some subgrouping, there is no significant lack of information flow or communication across the network. An important similarity between the traditional and cyber forms of organized crime is also the presence of "hubs" and "brokers"—actors who play important roles in the network. In both types of networks, “hubs” are essential for maintaining network cohesion by facilitating the flow of critical information (Morselli, 2009) across the nodes. Similarly, the functions of “brokers” in RaaS networks mirror the dynamics of traditional organized crime, where intermediaries enhance the flexibility and resilience of a network by linking otherwise isolated actors.

Notably, we anticipated that groups would play a more significant role as “brokers” and some of our findings support this conclusion. On one hand, we note the lack of a statistically significant correlation between group status and the likelihood of a node serving as a broker. On the other hand, the test of the means of betweenness centrality for groups vs individuals indicates a significant difference. Also, the results of OLS regression also reveal that group is a significant predictor of betweenness centrality. We hasten to note that this finding could be influenced by the sample size utilized in the study or the history of the

RaaS network.

Although our findings on the similarities between traditional and cyber forms of organized crime are mixed, it is important to note that cybercrime may follow different patterns and exhibit unique characteristics. Earlier research (e.g., (Holt et al., 2012),(Decary-Hétu et al., 2012)) underscores the decentralized and scattered nature of cybercriminal networks. Unlike members of traditional organized crime groups, cybercriminals may not identify as part of a larger entity and may not seek to increase their connections for that reason. Another possibility is that ransomware networks are a distinct form of crime network, with processes and characteristics that differ from other cybercrime groups. Finally, as previously mentioned, connections formed in cyberspace tend to be particularly fragile due to the pervasive lack of trust among participants. In environments where actors prefer to remain anonymous and have little trust in one another, the development of dense, centralized networks becomes more challenging.

The sparse and decentralized nature of ransomware networks may reduce their operational efficiency, but it also poses significant challenges for law enforcement. These networks are particularly fluid and amorphous, with peripheral members being quickly replaced and no clear central core. Additionally, their decentralized structure allows members to engage in transactions independently, provided they have access to the necessary tools, without requiring close collaboration. As a result, these networks can easily withstand the removal of peripheral members, maintaining overall stability over time. More effective law enforcement strategies should focus on targeting key nodes that serve as hubs and brokers, as these actors are critical to the network's longevity and functionality.

Our data are not without limitations. The relatively small sample size—140 groups and 96 individuals—and the narrow specialization of the network prevent us from drawing conclusions generalizable to other cybercrime networks. We note, however, that our sample size is in line with or larger than many others traditionally used in the studies of traditional organized crime and cybercrime that are often as small as 20 or 30 to 200–300 nodes (Bichler et al., 2017), (Breuer & Varese, 2023), (Calderoni et al., 2014)- (Tenti & Morselli, 2014). Additionally, our snapshot includes both group and individual nodes that were formed, and in some cases, discontinued their activities at different times. While this approach offers insight into the nature of connections between groups and individuals involved in ransomware operations over time, the nature of the sample may influence the results in ways unrelated to the theorized causes. Furthermore, despite our best efforts, the distinction between group and individual nodes may not always be accurate, as both types of accounts could be managed by multiple individuals. Nonetheless, our data provide a unique snapshot of ransomware networks over the past decade, offering valuable opportunities to compare and contrast cybercrime with traditional organized crime.

5.1. Conclusion

In conclusion, while the RaaS network shares some characteristics with traditional organized crime networks—particularly the reliance on hubs and brokers for cohesion and information flow—it also displays a notable level of decentralization and sparsity. This decentralized yet interconnected structure, characterized by smooth information flow and short paths between members, is essential for the longevity of cybercriminal enterprises. Much like traditional organized crime groups, this adaptability and resilience enable ransomware networks to withstand external disruptions and persist over time.

CRediT authorship contribution statement

Ekaterina Botchkovar: Writing – review & editing, Writing – original draft, Supervision, Resources, Project administration, Methodology, Investigation, Data curation, Conceptualization. **Kexin Cui:** Writing – review & editing, Data curation. **Olena Antonaccio:** Methodology, Formal analysis. **Robert Perkins:** Formal analysis. **David Maimon:** Writing – review & editing, Validation, Funding acquisition.

Acknowledgments

This study was supported by award #E205949B from CINA/DHS

Data availability

The authors do not have permission to share data.

References

Baranovska, T., et al. (2024). The impact of cybercrime on state and institutional security: Analysis of threats and potential protection measures. *Economic Affairs, 69* (Special Issue), 33–42. https://doi.org/10.46852/0424-2513.1.2024.5

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security, 111*, Article 102490. https://doi.org/10.1016/j.cose.2021.102490

Bichler, G., Malm, A., & Cooper, T. (2017). Drug supply networks: A systematic review of the organizational structure of illicit drug trade. *Crime Science, 6*. https://doi.org/10.1186/s40163-017-0063-3

Bouchard, M. (2020). Collaboration and boundaries in organized crime: A network perspective. *Crime and Justice, 49*, 425–469. https://doi.org/10.1086/708435

Breuer, N., & Varese, F. (2023). The structure of trade-type and governance-type organized crime groups: A network study. *British Journal of Criminology, 63*, 867–888. https://doi.org/10.1093/bjc/azac065

Calderoni, F. (2016). Predicting organized crime leaders. In G. Bichler, & A. Malm (Eds.), *Disrupting criminal networks: Network analysis in crime prevention* (pp. 89–110). Lynne Rienner Publishers. https://doi.org/10.1515/9781626372573-007.

Calderoni, F., Skillicorn, D. B., & Zheng, Q. (2014). Inductive discovery of criminal group structure using spectral embedding. *Information Security, 31*, 49–66. https://doi.org/10.11610/isij.3102

Campana, P., & Varese, F. (2022). Studying organized crime networks: Data sources, boundaries and the limits of structural measures. *Social Networks, 69*, 149–159. https://doi.org/10.1016/j.socnet.2022.04.003

Cybersecurity and Infrastructure Security Agency. (2022). Ransomware guide. https://www.cisa.gov/stopransomware/ransomware-guide.

da Cunha, B. R., & Gonçalves, S. (2018). Topology, robustness, and structural controllability of the Brazilian Federal Police criminal intelligence network. *Applied Network Science, 3*, 36. https://doi.org/10.1007/s41109-018-0092-1

Decary-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*, 359–382. https://doi.org/10.1177/0022427811420876

DiMaggio, J. (2022). *The art of cyberwarfare: An investigator's guide to espionage, ransomware, and organized cybercrime*. No Starch Press.

Duijn, P. A., Kashirin, V., & Sloot, P. M. (2014). The relative ineffectiveness of criminal network disruption. *Scientific Reports, 4*, 4238. https://doi.org/10.1038/srep04238

Duxbury, S. W., & Haynie, D. L. (2018a). Building them up, breaking them down: Topology, vendor selection patterns, and a digital drug market's robustness to disruption. *Social Networks, 52*, 238–250. https://doi.org/10.1016/j.socnet.2017.09.003

Duxbury, S. W., & Haynie, D. L. (2018b). The network structure of opioid distribution on a darknet cryptomarket. *Journal of Quantitative Criminology, 34*, 921–941. https://doi.org/10.1007/s10940-017-9359-4

Finckenauer, J. O. (2005). Problems of definition: What is organized crime? *Trends in Organized Crime, 8*, 63–83. https://doi.org/10.1007/s12117-005-1038-4

Grabosky, P. (2007). The internet, technology, and organized crime. *Asian Criminology, 2*, 145–161. https://doi.org/10.1007/s11417-007-9034-z

Grisham, J., Samtani, S., Patton, M., & Chen, H. (2017). Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence. In *2017 IEEE international conference on intelligence and security informatics (ISI)* (pp. 13–18). IEEE. https://doi.org/10.1109/ISI.2017.8004867.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28*, 171–198. https://doi.org/10.1080/01639620701233218

Holt, T. J., & Bossler, A. M. (2013). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Holt, T. J., Strumsky, D., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology, 6*(2), 891–903.

Howell, C., Burruss, G., 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*, 1–15. https://doi.org/10.1080/0735648X.2019.1691859

Huang, S.-Y., & Chen, H. (2016). Exploring the online underground marketplaces through topic-based social network and clustering. In *2016 IEEE conference on intelligence and security informatics (ISI)* (pp. 145–150). IEEE, 10.1109/ISI.2016.7745458.

Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change, 62*, 1–20. https://doi.org/10.1007/s10611-014-9520-z

Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., & Kim, D. (2022). Current status and security trend of OSINT. *Wireless Communications and Mobile Computing, 1290*. https://doi.org/10.1155/2022/1290129

Internet Crime Complaint Center. (2022). 2022 internet crime report. *Federal Bureau of investigation*. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

Irving, D. (2016). *The digital underworld: What you need to know*. RAND Review. Retrieved from https://www.rand.org/pubs/articles/2016/the-digital-underworld.html.

Jian, J., Chen, S., Luo, X., Lee, T., & Yu, X. (2022). Organized cyber-racketeering: Exploring the role of internet technology in organized cybercrime syndicates using a grounded theory approach. *IEEE Transactions on Engineering Management, 69*, 3726–3738. https://doi.org/10.1109/TEM.2020.3002784

Kleemans, E. R. (2014). Theoretical perspectives on organized crime. In L. Paoli (Ed.), *Oxford handbook of organized crime* (pp. 32–52). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199730445.013.005.

Lampe, K., & Johansen, P. O. (2004). Organized crime and trust: On the conceptualization and empirical relevance of trust in the context of criminal networks. *Global Crime, 6*, 159–184. https://doi.org/10.1080/17440570500096734

Lavorgna, A. (2020). *Organised crime and cybercrime*. Palgrave Macmillan.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change, 67*, 21–37. https://doi.org/10.1007/s10611-016-9662-2

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017b). Organised cybercrime or cybercrime that is organised? An assessment of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research, 23*(3), 287–300. https://doi.org/10.1007/s10610-016-9332-z

Lopes, D. D., Cunha, B. R.d., Martins, A. F., et al. (2022). Machine learning partners in criminal networks. *Scientific Reports, 12*, Article 15746. https://doi.org/10.1038/s41598-022-20025-w

Lubin, A. (2022). The law and politics of ransomware. *Vanderbilt Journal of Transnational Law, 55*(5), 1177–1216.

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime, 14*, 52–60. https://doi.org/10.1080/17440572.2012.759508

Macdonald, M., & Frank, R. (2016). The network structure of malware development, deployment and distribution. *Global Crime, 18*, 49–69. https://doi.org/10.1080/17440572.2016.1227707

Marin, E., Shakarian, J., & Shakarian, P. (2018). Mining key-hackers on darkweb forums. In *2018 1st international conference on data intelligence and security (ICDIS)* (pp. 73–80). https://doi.org/10.1109/ICDIS.2018.000181

Martin, J., & Whelan, C. (2023). Ransomware through the lens of state crime: Conceptualizing ransomware groups as cyber proxies, pirates, and privateers. *State Crime, 12*(1), 1–25. https://doi.org/10.13169/statecrime.12.1.0001

McGuire, M. (2012). *Organised crime in the digital age*. John Grieve Centre for Policing and Security and BAE Systems Detica.

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security, 92*, Article 101762. https://doi.org/10.1016/j.cose.2020.101762

Morselli, C. (2009). *Inside criminal networks*. Springer Publishing. https://doi.org/10.1007/978-0-387-09526-4

Nadir, I., & Bakhshi, T. (2018). Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques. In *2018 international conference on computing, mathematics and engineering technologies (iCoMET)* (pp. 1–7). https://doi.org/10.1109/ICOMET.2018.8346368

Ouellet, M., Hashimi, S., Gravel, J., & Papachristos, A. V. (2019). Network exposure and excessive use of force: Investigating the social transmission of police misconduct. *Criminology & Public Policy, 18*, 675–704. https://doi.org/10.1111/1745-9133.12459

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys, 54*. https://doi.org/10.1145/3464226

Papachristos, A. V., Braga, A. A., & Hureau, D. M. (2012). Social networks and the risk of gunshot injury. *Journal of Urban Health: Bulletin of the New York Academy of Medicine, 89*(6), 992–1003. https://doi.org/10.1007/s11524-012-9703-9

Papachristos, A. V., Hureau, D. M., & Braga, A. A. (2013). The corner and the crew: The influence of geography and social networks on gang violence. *American Sociological Review, 78*(3), 417–447. https://doi.org/10.1177/0003122413486800

Perkins, R. C., Ouellet, M., Howell, C. J., & Maimon, D. (2023). The illicit ecosystem of hacking: A longitudinal network analysis of website defacement groups. *Social Science Computer Review, 41*, 390–409. https://doi.org/10.1177/08944393221097881

Rehman, H. U., Yafi, E., Nazir, M., & Mustafa, K. (2019). Security assurance against cybercrime ransomware. In P. Vasant, I. Zelinka, & G. W. Weber (Eds.), *Intelligent computing & optimization: ICO 2018* (Vol. 866, pp. 33–43). Springer. https://doi.org/10.1007/978-3-030-00979-3_3.

Ribeiro, H. V., Lopes, D. D., Pessa, A. A., Martins, A. F., Cunha, B. R., Gonçalves, S., Lenzi, E. K., Hanley, Q. S., & Perc, M. (2023). Deep learning criminal networks. *arXiv, 2304.08457*. https://arxiv.org/abs/2304.08457.

Ryan, M. (2021). *Ransomware revolution: The rise of a prodigious cyber threat*. Springer International Publishing. https://doi.org/10.1007/978-3-030-66583-8

Sarvari, H., Abozinadah, E., Mbaziira, A., & McCoy, D. (2014). Constructing and analyzing criminal networks. In *2014 IEEE security and privacy workshops* (pp. 84–91). IEEE. https://doi.org/10.1109/SPW.2014.22.

Savona, E., Calderoni, F., Superchi, E., Comunale, T., Campedelli, G. M., Marchesi, M., & Kamprad, A. (2017). Systematic review of the social, psychological, and economic factors relating to criminalisation and recruitment to organized crime. Retrieved from https://www.projectproton.eu/wp-content/uploads/2018/01/D1.1_Report-on-factors-relating-to-OC_rev.pdf.

Scott, J. (2017). *Social network analysis*. Thousand Oaks, CA: Sage Publications. https://doi.org/10.4135/9781529716597

Smith, T., & Plachkinova, M. (2022). Towards a taxonomy for classifying knowledge on Ransomware as a Service (RaaS) specializations. In *Proceedings of DESRIST*. https://www.usf.edu/business/documents/desrist/paper_40.pdf.

Teichmann, F., Boticiu, S. R., & Sergi, B. S. (2023). The evolution of ransomware attacks in light of recent cyber threats: How can geopolitical conflicts influence the cyber climate? *Int. Cybersecur. Law Rev., 4*, 259–280. https://doi.org/10.1365/s43439-023-00095-w

Tenti, V., & Morselli, C. (2014). Group co-offending networks in Italy's illegal drug trade. *Crime, Law and Social Change, 62*(1), 21–44. https://doi.org/10.1007/s10611-014-9518-6

Whelan, C., Bright, D., & Martin, J. (2024). Reconceptualising organised (cyber)crime: The case of ransomware. *Journal of Criminology, 57*, 45–61. https://doi.org/10.1177/26338076231199793

Wickham, H., François, R., Henry, L., & Müller, K. (2019). Welcome to the tidyverse. *Journal of Open Source Software, 4*, 1686. https://doi.org/10.21105/joss.01686