information

Article

Directed Criminal Networks: Temporal Analysis and Disruption

Efstathios Konstantinos Anastasiadis * and Ioannis Antoniou

Faculty of Sciences, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece; iantonio@math.auth.gr
* Correspondence: efanasta@physics.auth.gr

Abstract: We extend network analysis to directed criminal networks in the context of asymmetric links. We computed selected centralities, centralizations and the assortativity of a drug trafficking network with 110 nodes and 295 edges. We also monitored the centralizations of eleven temporal networks corresponding to successive stages of investigation during the period 1994–1996. All indices reach local extrema at the stage of highest activity, extending previous results to directed networks. The sharpest changes (90%) are observed for betweenness and in-degree centralization. A notable difference between entropies is observed: the in-degree entropy reaches a global minimum at month 12, while the out-degree entropy reaches a global maximum. This confirms that at the stage of highest activity, incoming instructions are precise and focused, while outgoing instructions are diversified. These findings are expected to be useful for alerting the authorities to increasing criminal activity. The disruption simulations on the time-averaged network extend previous results on undirected networks to directed networks.

Keywords: criminal networks; directed graphs; centrality; entropy; assortativity; disruption; strongly connected components

check for updates

Citation: Anastasiadis, E.K.; Antoniou, I. Directed Criminal Networks: Temporal Analysis and Disruption. *Information* **2024**, *15*, 84. https://doi.org/10.3390/info15020084

Academic Editor: Rami Puzis

Received: 10 January 2024
Revised: 31 January 2024
Accepted: 31 January 2024
Published: 4 February 2024

1. Introduction

The ever-increasing incidents of organized crime force the authorities to constantly monitor suspicious groups and individuals in order to intervene when needed. Such actions require meticulous prior planning, as law enforcement operations are time-consuming and expensive [1]. Social network analysis (*SNA*) can provide law enforcement agencies with useful tools for delving into the group dynamics and structure of Mafia syndicates [2,3], drug trafficking markets [4–7] and terrorist organizations [8–11].

Individuals or groups of individuals are modeled as nodes and linked according to confirmed affiliations. Depending on the nature of the relationship between two nodes, analysts may be able to construct criminal or terrorist networks based on trust, kinship, friendship [8] or financial and operational networks. Communication and proximity networks are also of great importance, although they are relatively hard to construct [12].

Ongoing research primarily focuses on identifying the most central actors within the aforementioned type of networks based on their links and positioning in the network. Several approaches for identifying such actors have been proposed, including the utilization of game theoretic measures [13], measures based on information theory [14,15] and elaborated constructed centralities that capture subtle features of the network's structure [16].

Due to the lack of complete and accurate data [1,8,17–19] some studies resort to machine learning and deep learning techniques to predict patterns and missing links that may unveil previously undisclosed relationships between members [20,21], potentially leading to more accurate network representations of the illicit organizations under investigation and consequently alleviating the development of misleading models [9].

The utilization of more accurate network models and datasets is pivotal for a further understanding of the structural mechanisms of illicit organizations and for bridging some conflicting opinions and findings. Although the consensus is that criminal and terrorist networks are configured to maintain a balance between efficiency and secrecy [8,12,18,22,23],

there is some contrasting evidence indicating that such networks may operate with small communication pathways [17,18].

The data gathered from the structural analysis can be used to design effective strategies aiming to fragment and/or disintegrate the network under investigation. Network fragmentation analysis can provide insight regarding the cost-benefit tradeoff the authorities need to address when crafting a policy strategy for tackling illicit organizations [24]. Researchers have primarily focused on simulating the effect of the removal of nodes with significant roles in the network [2,6,16]. The resilience of illicit networks under successive attacks has also been studied [6,17,25,26], and also combined with link prediction [11]. Many studies have confirmed that the elimination of individuals acting as mediators seems to be the strategy with the most significant impact on a network's cohesiveness [2,6,26].

1.1. Related Work in Criminal Network Analysis

The available criminal network datasets predominantly focus on drug distribution markets and Mafia syndicates, with less frequent attention given to gangs or human trafficking networks [27]. The scarcity of temporal datasets has resulted in a large portion of relevant research leaning toward static structural analysis and disruption simulations.

1.1.1. Disruption Analysis

Xu and Chen [17] studied the outcome of simultaneous or progressive isolations of nodes with a large number of links or nodes that acted as mediators. These strategies were applied to drug trafficking, gang and dark net networks. The simulations revealed that progressive attacks on either highly linked nodes or mediators were more devastating than the simultaneous removals of nodes.

Duijn et al. [25] examined the response of a cannabis cultivation network after implementing targeted or random removals of nodes and discovered that there existed a scenario where targeted attacks would render the network more resilient than before. Targeted and random node removals were also applied to a contact and an affiliation network of a Mafia syndicate. In this study, Agreste et al. [28] found that contact networks were more vulnerable to targeted attacks than affiliation networks.

Catanese et al. [29] investigated the resilience of a Mafia network under internal and external interventions. The external interventions were simulated as removals of the intermediaries. They discovered that Mafia networks were able to restore their functionality, confirming their high adaptability when facing possible threats.

Statistically significant degree disassortativity was observed by Wood [7] when examining the structure of a drug trafficking network, indicating that such networks are prone to removals of actors with a large number of direct links. The finding was also confirmed by the quick disintegration of the network when disconnecting a small number of highly-linked individuals.

Bright et al. [6] implemented different strategies of targeted attacks against a drug trafficking network, relying on both the positioning of each node in the network and on their human capital. The simulations were conducted with and without accounting for the network's adaptation, following each step of the disruption strategies. The removal of mediators was identified as the most effective attack strategy, closely followed by the removal of financially strong actors.

Duxbury and Haynie utilized agent-based modeling to model the response of criminal networks under different interventions. In the first study [26], they removed mediators or highly-linked nodes from a drug distribution and a stolen vehicle network. Single isolations of nodes resulted in the recovery of the networks. In contrast, simultaneous removals were more efficient for inflicting permanent damage on the networks. The authors also concluded that mediator-based attacks were more appropriate for the case of drug trafficking networks. Their second study [30] was focused on using the aforementioned attack strategies on an online drug market network, along with a third attack strategy focusing on the modification of the links' weights. Targeted attacks were deemed effective for large-scale attacks, whereas the remaining two strategies were more appropriate for local

attacks. The developed model also revealed that the nodes were acting more cautiously after the implementation of intentional attacks.

The resilience of another Mafia syndicate was examined by Cavallaro et al. [2]. The authors represented different law enforcement interventions with centrality-based attacks. The comparison between simultaneous and sequential node removals yielded no differences between them. The simulations also reconfirmed that the optimal intervention strategy for dismantling such networks was the elimination of intermediaries.

Finally, Diviak [31] explored the impact of different attack methods primarily based on centralities within a street gang network. The study also simulated the recovery of the network using three distinct mechanisms. Findings indicated that the removal of individuals with the highest centralities affected the network the most. Moreover, the study emphasized the significance of assessing the network's recovery, surpassing the disruption process's importance.

1.1.2. Temporal Analysis

Morselli and Petit [32] studied the evolution of a drug trafficking network under police investigation. The changes of two global network indices, specifically the degree and betweenness centralization (defined in Sections 2.7 and 2.8) were monitored to understand how the network responded to imminent law enforcement interventions. Additionally, the temporal positioning of the three most prominent members within the network was examined.

Bright and Delaney [33] also examined the growth of a drug trafficking network using local and global indicators from *SNA*. The authors demonstrated that the network under investigation maintained a relatively constant density (defined in Section 2.3) while slowly adopting a more decentralized structure. The calculated local indicators revealed that the members were constantly changing roles within the network.

In a forthcoming study, Bright et al. [34] used a stochastic model to simulate the evolutionary dynamics of a drug trafficking network. Their findings suggested that individuals preferred to maintain indirect connections as a strategy to limit their exposure to the authorities. The individuals were also observed to establish links with other individuals whose contribution to the network was different from their own.

The resilience of a network of thieves and a network of ex-inmates was examined by Ozgul and Erdem [35]. The authors proposed a resilience measure based on some global indicators of network analysis and simulated the networks' evolution under the influence of police prosecutions. The network of thieves demonstrated adaptability to exogenous interventions, sustaining its functionality. However, the ex-inmate network exhibited vulnerability, showing susceptibility to continuous police operations.

Berlusconi [36] studied the temporal change in the structure of another drug trafficking network by calculating network indicators and using selected graph models. The results indicated that the members of the network prioritized enhancing the overall security of the network after being targeted by the authorities. Despite the arrest of some key individuals, the network continued pursuing its objectives.

1.2. Contribution of the Manuscript

While the existing literature on criminal networks is varied and extensive, the analysis is restricted so far to undirected networks. The goal of this work is to extend network analysis to directed criminal networks, i.e., networks where we have to take into account the direction and the weight of the edges linking two nodes. In such networks the communication may be either one way only, or two way with both links between two nodes being present but with different weights. The weight matrix of directed networks is non-symmetric [37,38]. The directionality of the links in a criminal network reveals both the direction of the flow of information and the direction of the orders issued by the leaders in a criminal organization. The analysis of directed links provides additional options for disrupting criminal networks, as indicators such as centralities are no longer symmetric and are divided into in-and-out counterparts.

The rest of the manuscript is structured as follows. The selected local and global indicators for conducting structural analysis are presented in Section 2 and the results of the calculations are in Section 3. The dataset is described in Section 3.1. The disruption simulation is presented in Section 4 and our conclusions in Section 5.

2. Materials and Methods

We present the local and global indicators to be computed in Section 3.

Centralities are the most common local indicators. Centrality quantifies the importance and the role of each node resulting from the positioning in the network. High-centrality nodes are considered as more significant with respect to the property of interest [38,39]. Several centrality indices have been proposed for the analysis of criminal networks. However, the utility and the practical significance of centrality often depend on the specific criminal network examined [16]. For this study, we selected three centralities, specified in Sections 2.4–2.6.

Global indicators characterize the network as a whole. We selected the following global indicators to assess the criminal networks under investigation, namely: degree centralization, betweenness centralization, global efficiency, degree entropy, average clustering coefficient, assortativity, number of strongly connected components and the order of the largest strongly connected component.

The definitions and the meaning of the selected indicators are described below.

The three main indicators of a network are order, size and density:

2.1. Order

Order is the number of nodes present in the network, usually denoted by N.

2.2. Size

Size is the number of edges present in the network, usually denoted by E.

2.3. Density

Network density is the fraction of the size of the network over the theoretically maximum size (complete network):

$$\rho = \frac{E}{N(N-1)} \tag{1}$$

Networks with low density (close to 0) are called sparse networks, whereas highly dense networks (density close to 1) are almost complete networks.

The selected three centralities are:

2.4. Degree Centrality

Degree centrality [37–39] captures the role of each node i from the number of direct links. In the case of criminal networks, self-loops are excluded ($\alpha_{ii} = w_{ii} = 0$), α_{ij} are the elements of the adjacency matrix of the directed network and w_{ij} are the elements of the weight matrix of the directed network.

Thus, the in-degree and the out-degree centralities are:

$$DEG_i^{in} = \frac{1}{N-1} \sum_{\substack{j=1 \\ j \neq i}}^{N} \alpha_{ji} \tag{2}$$

$$DEG_i^{out} = \frac{1}{N-1} \sum_{\substack{j=1 \\ j \neq i}}^{N} \alpha_{ij}, \tag{3}$$

The weighted degree centrality, or strength centrality takes into account the weighted links:

$$DEG_i^{[w]in} = \frac{1}{N-1} \sum_{\substack{j=1 \\ j \neq i}}^{N} w_{ji} \tag{4}$$

$$DEG_i^{[w]out} = \frac{1}{N-1} \sum_{\substack{j=1 \\ j \neq i}}^{N} w_{ij}, \tag{5}$$

Nodes with high degree centrality (close to 1) are very popular, as they are linked with a large number of other nodes.

2.5. Betweenness Centrality

The amount of times a node i lies on shortest paths between pairs of other nodes is captured by betweenness centrality [37–39] and is defined as:

$$B_i = \frac{1}{(N-1)(N-2)} \sum_{\substack{j,k=1 \\ j \neq k \neq i}}^{N} \frac{\sigma_{j(i)k}}{\sigma_{jk}}, \tag{6}$$

where $\sigma_{j(i)k}$ is the number of directed paths from node j to node k that pass through node i and σ_{jk} is the number of directed paths from node j to node k. Nodes with high betweenness centrality act as mediators, brokers or liaison officers, maintaining high indirect connectivity [22] and ensuring control and protection [40].

2.6. Harmonic Closeness Centrality

Harmonic closeness centrality is a variation of closeness centrality [39,41] designed for application in disconnected networks. In the literature, harmonic centrality has been also referenced either as index power value [42], sum of reciprocal distances [43] or average reciprocal distance (ARD) [44]. We use the following definition of harmonic centrality:

$$HCL_i^{in} = \frac{1}{N-1} \sum_{\substack{j=1 \\ j \neq i}}^{N} \frac{1}{d_{ji}} \tag{7}$$

$$HCL_i^{out} = \frac{1}{N-1} \sum_{\substack{j=1 \\ j \neq i}}^{N} \frac{1}{d_{ij}}, \tag{8}$$

where d_{ji} is the asymmetric distance from node j to node i corresponding to the shortest directed path from node j to node i. Nodes with high out-harmonic closeness centrality are likely to act as influencers and also as spreaders. Nodes with high in-harmonic closeness centrality are highly accessible from other nodes.

The selected eight global indicators are:

2.7. Degree Centralization

Degree centralization indicates how central the node with maximum degree centrality is compared to the rest of the nodes with respect to degree centrality [39]. The in and out degree centralizations are:

$$DEG^{in} = \frac{1}{N-2} \sum_{j=1}^{N} \left(\max_{i \in N} \{DEG_i^{in}\} - DEG_j^{in} \right) \tag{9}$$

$$DEG^{out} = \frac{1}{N-2} \sum_{j=1}^{N} \left(\max_{i \in N} \{DEG_i^{out}\} - DEG_j^{out} \right) \tag{10}$$

The weighted degree/strength centralizations are:

$$DEG^{[w]in} = \frac{1}{N-2}\sum_{j=1}^{N}\left(\max_{i\in N}\{DEG_i^{[w]in}\} - DEG_j^{[w]in}\right) \quad (11)$$

$$DEG^{[w]out} = \frac{1}{N-2}\sum_{j=1}^{N}\left(\max_{i\in N}\{DEG_i^{[w]out}\} - DEG_j^{[w]out}\right) \quad (12)$$

Networks with high degree centralization (close to 1) are centralized on high degree nodes, while low degree centralization (close to 0) indicates a decentralized network with respect to degree.

2.8. Betweenness Centralization

Betweenness centralization indicates how central the node with maximum betweenness centrality is compared to the rest of the nodes with respect to betweenness centrality [39]:

$$B = \frac{1}{N-1}\sum_{j=1}^{N}\left(\max_{i\in N}\{B_i\} - B_j\right) \quad (13)$$

Networks with high betweenness centralization (close to 1) are centralized on nodes that are efficient mediators, while low betweenness centralization (close to 0) indicates that the network lacks mediators.

2.9. Global Efficiency

Global efficiency estimates the network's capability of exchanging information [45]. For a directed network, the in and out-global efficiencies are defined as:

$$E^{in}(G) = \frac{1}{N(N-1)}\sum_{i=1}^{N}\sum_{\substack{j=1\\ j\neq i}}^{N} d_{ji}^{-1} \quad (14)$$

$$E^{out}(G) = \frac{1}{N(N-1)}\sum_{i=1}^{N}\sum_{\substack{j=1\\ j\neq i}}^{N} d_{ij}^{-1}, \quad (15)$$

where d_{ij} is the asymmetric distance from node i to node j. The presence of the inverse distances in Equations (14) and (15) renders global efficiency applicable to networks with isolated nodes as well. Large values of global efficiency suggest instant communication between the nodes. To ensure that global efficiency is bounded between 0 and 1 in weighted networks, we multiply the above equations by the harmonic mean of the weights, $\frac{M}{\sum_{i\neq j}(\frac{1}{w_{ij}})}$ [46]. For trust or communication networks, the weights are reversed when calculating the global efficiency or other path-related measures.

2.10. Degree Entropy

Entropy is the diversification of the possible outcomes of a variable. We use Shannon's entropy [47] to assess the diversification of the in-degree and out-degree centrality distributions. The in and out-degree centrality entropies are defined as:

$$S^{in} = -\sum_{i=1}^{N-1} p_i^{in} log_2 p_i^{in} \quad (16)$$

$$S^{out} = -\sum_{i=1}^{N-1} p_i^{out} log_2 p_i^{out}, \quad (17)$$

where p_i^{in} and p_i^{out} are the probability distributions of the values of the in and out degree centralities. The values of the entropies, as calculated by Equations (16) and (17), are bits, taking values within the interval $[0, log_2(N-1)]$. Dividing by $log_2(N-1)$, we obtain

values normalized within the interval $[0, 1]$. Higher entropy indicates that the values of most degree centralities are equally probable. In contrast, low entropy indicates that most nodes have equal degree centrality, as in the case of regular networks.

2.11. Average Clustering Coefficient

The average clustering coefficient measures the average tendency of the nodes' neighbors to link to each other. There are several proposals for calculating the average clustering coefficient for networks with non-binary weights [48,49]. In this work, we shall use the definition by Fagiolo [50]:

$$clu_i^{[w]} = \frac{\left[W^{\frac{1}{3}} + \left(W^T\right)^{\frac{1}{3}}\right]^3_{ii}}{2\left[deg_i^{[w]}\left(deg_i^{[w]} - 1\right) - 2d_i^{\leftrightarrow}\right]}, \tag{18}$$

where W is the weight matrix, deg_i is the sum of the in and out degrees of node i and $d_i^{\leftrightarrow}$ is the number of neighbor nodes of node i for which both the links from node i to node j and from node j to node i exist. No self-loops are considered. The resulting average clustering coefficient is thus,

$$\overline{clu}^{[w]} = \frac{1}{N}\sum_{i=1}^{N} clu_i^{[w]}. \tag{19}$$

High values of the average clustering coefficient indicate better communication among the nodes of the network.

2.12. Assortativity

Degree assortativity quantifies the preference of nodes to link with other nodes with close degree values [38]. In this work, we examine the degree and weighted degree assortativity for both undirected and directed networks assuming linear relationships by using the Pearson correlation coefficient. In the case of directed networks, all possible combinations of directions are examined, namely: in-in, in-out, out-in and out-out.

Positive values of the degree assortativity coefficient imply that high degree nodes link together, while negative values suggest that high degree nodes link with low degree nodes. No specific mixing pattern exists when the assortativity equals zero.

2.13. Number of Strongly Connected Components

Real networks may not be strongly connected (for every two points i, j there is a directed path from i to j and also another directed path from j to i) [38]. The number of strongly connected components indicates the level of fragmentation of the network. Highly fragmented networks have poor functionality. In the case of fragmentation, we usually focus on the largest strongly connected component.

2.14. Order of the Largest Strongly Connected Component

The order (number of connected nodes) of the largest strongly connected component of a disconnected network is denoted by N_{LSCC}.

3. Network Diagnostics

3.1. Dataset and Software

The dataset used in this study (Project Caviar) stems from publicly released court data that were coded afterward by Morselli [51], resulting in the creation of eleven temporal networks. The nodes in each network are the individuals who participated in a drug-trafficking organization that was monitored by the authorities during the period 1994–1996. Each network corresponds to a successive 2-month period reflecting the stages of the authorities' investigation. A time-averaged network is also provided for the period 1994–1996 referring to the entire investigation interval.

All networks are directed and weighted. The direction of the links points from the caller to the receiver. The weights represent the number of exchanged phone calls between the members of the network. We normalized the weights by dividing them by the maximum number of calls registered in each of the twelve networks.

More specific information regarding the investigation and the interventions of the law enforcement agencies is presented in Table 1. The network operates without any exogenous interventions for the three initial stages of the investigation. After almost six months, the authorities begin confiscating trafficked drugs until the end of the 2-year operation [32].

Table 1. Number of police interventions during 1994–1996 for each stage of the investigation along with amount of confiscated drugs after each intervention. Interventions commence at least six months after the beginning of the operation.

Months	Number of Interventions	Seizures
2	-	-
4	-	-
6	-	-
8	1	Hashish: 300 kg
10	-	-
12	3	Cocaine: 15 kg, 15 kg, 2 kg
14	1	Hashish: 401 kg
16	1	Cocaine: 9 kg
18	2	Hashish: 500 kg, Cocaine: 2 kg
20	1	Hashish: 2200 kg
22	2	Cocaine: 12 kg, 15 kg

All calculations were performed with the 3.9.16 distribution of Python (Supplementary Materials). The network analysis was conducted with the NetworkX library (version 2.8.4). The libraries Matplotlib (version 3.7.1), Seaborn (version 0.12.2) and Pandas (version 1.5.3) were used for visualization purposes and the data analysis of the results. The used software is open-source.

The variation in the number of participants and the links they formed within the criminal organization during the entire investigation is presented in Figure 1.

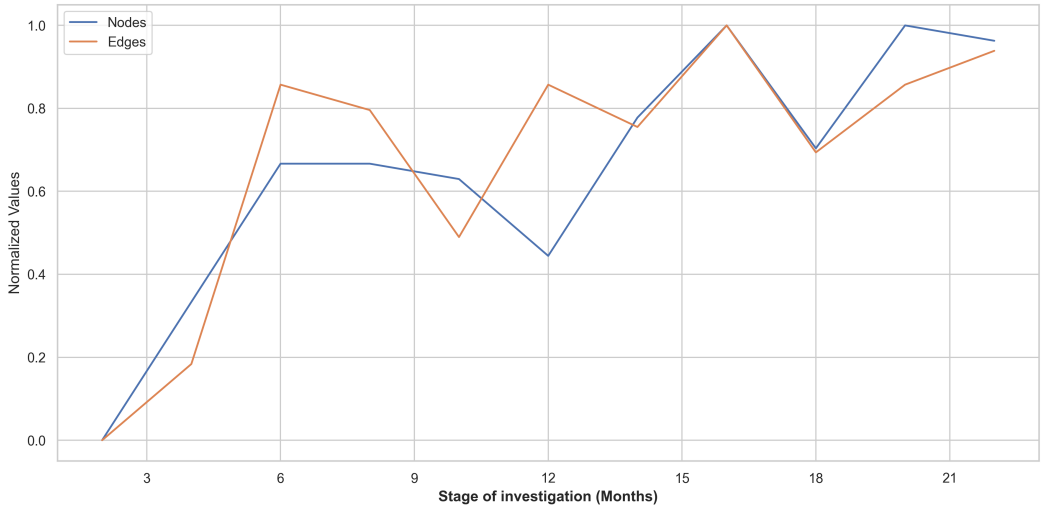

Figure 1. Normalized values of number of participants and number of formed links within the organization during 1994–1996. During the first six months of the investigation, the network grows significantly, while in the subsequent six months, a slight decrease in number of participants is observed. The number of edges exhibits more rapid changes compared to the number of nodes. In the final year of the 2-year period, the number of nodes increases again, reaching its peak at months 16 and 20. The number of edges follows a similar pattern, peaking at month 16.

3.2. Temporal Analysis

The changes in out-degree, in-degree (Section 2.7) and betweenness centralizations (Section 2.8) along with the changes in the global efficiency (Section 2.9), in and out-degree entropy (Section 2.10) and the average clustering coefficient (Section 2.11) for the directed and weighted temporal networks are presented in Figure 2.

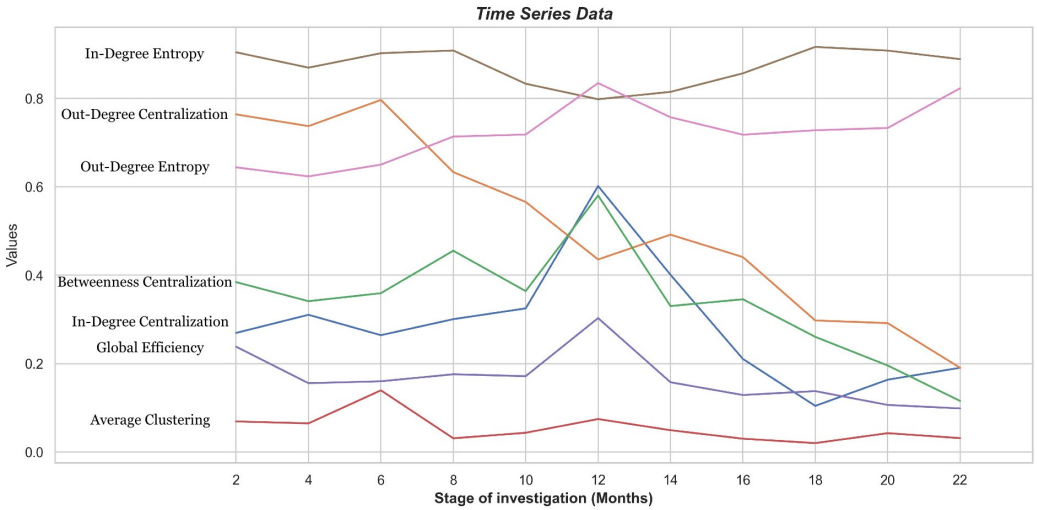

Figure 2. Changes in important global indicators across different stages of the investigation in months over the period 1994–1996. A notable difference is observed between the centralizations, namely: all centralizations achieve local maximum at month 12 except the out-degree centralization and the in-degree entropy which have a local minimum. The changes are significant (about 90%) in the case of in-degree and betweenness centralizations, small (less than 25%) in the case of the average clustering coefficient and the out-degree entropy and moderate (about 40%) in the case of the global efficiency. The changes of the in and out communication efficiencies are more or less identical. For this reason, the label global efficiency is used.

3.3. Analysis of the Time-Averaged Network

The values of global properties for the time-averaged network during 1994–1996 (Section 3.1) are presented in Table 2.

Table 2. Values of properties for the time-averaged network.

Indicator	Value
Order (Section 2.1)	110
Size (Section 2.2)	295
Density (Section 2.3)	0.025
In-Degree Centralization (Section 2.7)	0.3206
Out-Degree Centralization (Section 2.7)	0.4795
In-Strength Centralization (Section 2.7)	0.1456
Out-Strength Centralization (Section 2.7)	0.1775
Betweenness Centralization (Section 2.8)	0.5363
Global efficiency (Section 2.9)	0.1688
In-Degree Entropy (Section 2.10)	0.8509
Out-Degree Entropy (Section 2.10)	0.7746
Average clustering coefficient (Section 2.11)	0.03
Number of strongly connected components (Section 2.13)	45
N_{LSCC} (Section 2.14)	66

The assortativity (Section 2.12) for both the undirected and directed time-averaged networks is presented in Table 3.

Table 3. Degree assortativity of the time-averaged undirected and directed networks. The standard deviations of the computed values are estimated by the jackknife method [52,53] to assess the statistical significance of the results.

	Assortativity	**Standard Deviation**
Undirected	−0.36	0.03
Undirected Weighted	−0.37	0.05
in-in	−0.38	0
in-out	−0.34	0.04
out-in	−0.36	0.03
out-out	−0.36	0.61
weighted in-in	−0.33	0.07
weighted in-out	−0.33	0.24
weighted out-in	−0.32	0.35
weighted out-out	−0.34	0.14

Assortativity is restricted within the interval $[-0.32, -0.38]$. Statistically significant disassortative mixing patterns are observed at a 95% confidence level, except out-out, weighted in-out and weighted out-in.

3.4. Discussion of the Results

We observe that all centralizations achieve a local extremum at month 12 (Figure 2), corresponding to the most active stage of law enforcement interventions as shown in Table 1.

The local minimum of the in-degree entropy and decreasing pattern of the out-degree centralization indicate a significant reduction in the diversification of the nodes providing instructions.

The reported low values of the average clustering coefficient during this two-year period reconfirm that covert networks do not favor high clustering [18]. The command and control strategy is usually adopted in criminal networks to mitigate the risk of exposure in case a member of the network is arrested.

Considering that the authorities' interventions follow to some extent the activity of criminal organizations, month 12 more or less coincides with the period of highest criminal activity. The betweenness and the in-degree centralization undergo a sharp increase at month 12. This indicates that the members of the criminal network communicate mainly through intermediaries at times of increased activity. Communication through intermediaries is a standard practice in criminal networks during periods of increased activity [54]. The global efficiency is also increasing at month 12, but not as sharply, given the precaution that communication is governed by intermediaries. In this sense, previous findings relating sharp changes in global network indicators with periods of intense activity of illicit organizations are confirmed [54,55]. A notable difference between the in and out degree entropies is also observed: the in-degree entropy reaches a global minimum at month 12, while the out-degree entropy reaches a global maximum. This confirms the previous remark that at the stage of highest activity incoming instructions are precise and focused, while outgoing instructions are diversified.

Linear regression analysis revealed that the increase in the order of the network may negatively affect the changes in in-degree and betweenness centralization and the changes in global efficiency. In contrast, when the size increases, the aforementioned indicators increase as well. The linear regression coefficients corresponding to the order and the size are opposite in sign and do not differ significantly in magnitude. The linear regression results for the rest of the global indicators examined in Figure 2 are not statistically significant.

The time-averaged network (Section 3.1) is sparse, with high betweenness centralization (0.5363, Table 2), low global efficiency (0.1688, Table 2), high in and out degree entropies (0.8509 and 0.7746, Table 2), low clustering (0.03, Table 2), a large number of strongly con-

nected components (45, Table 2) and a rather large strongly connected component with 66 members (Table 2).

The low efficiency and high betweenness centralization [56] indicate that to minimize the risk of exposure, communication is channeled through intermediaries and direct communication among members is not encouraged. This is also confirmed by the low clustering. As a result, diversification is emerging as indicated by the high values of the average degree entropies.

The large number of small strongly connected components (44) indicates that those strongly connected components participate in several "minor" criminal activities communicating with certain members of the large strongly connected component. This strategy also minimizes the risk of exposure.

The time-averaged network also displays a moderate degree of disassortativity (Table 3), higher than the values observed in similar drug trafficking networks [7,17]. The disassortativity is observed in both the undirected and directed networks, as well as in the corresponding weighted networks. Our findings indicate that members of a drug-trafficking network are more likely to establish disassortative connections, i.e., members of high degree are more likely to link with members of low degree, as observed before [7,17].

4. Attacking Criminal Networks

4.1. Methodology

The directed time-averaged network will be fragmented into multiple components by implementing node removals, a strategy commonly adopted in criminal and terrorist network analysis [2,5–7,11,17,25,57].

Both random and targeted sequential node removals are performed. In the targeted attacks, nodes are removed based on their centrality from highest to lowest. The strategy of centrality-based attacks can be justified by the centralized structure of the network as indicated by the calculated global indicators (Section 3.3, Table 2). We would not be able to attack the network effectively by targeting high centrality nodes if the network was decentralized [25,58,59]. The centralities used are described in Sections 2.4–2.6. The centralities of each node are recalculated after each removal.

The performance of each attack strategy after each removal is evaluated by the relative change in the N_{LSCC} (Section 2.14):

$$\frac{|N_{LSCC,0} - N_{LSCC,i}|}{N_{LSCC,0}},$$

where $N_{LSCC,0}$ and $N_{LSCC,i}$ refer to the order of the largest strongly connected component prior to any removal and after the removal of the i-th node, respectively.

The robustness of the network [16,60,61] aggregates the outcomes for each implemented attack strategy. We use the definition provided in [61]:

$$R = \frac{1}{T+1} \sum_{i=0}^{T} \frac{N_{LSCC}(i)}{N-i}, \tag{20}$$

where T is a threshold ($T < N$) above which the network is considered malfunctioned. We set the threshold as the number of nodes required to achieve the maximum number of strongly connected components (Section 2.13).

4.2. Results

The variations in the N_{LSCC} and the number of strongly connected components, respectively, as the attack strategies described in Section 4.1 are implemented, are presented in Figures 3 and 4. The horizontal axis of each plot demonstrates the time step of the simulation procedure, corresponding to the removal of a single node after each iteration.

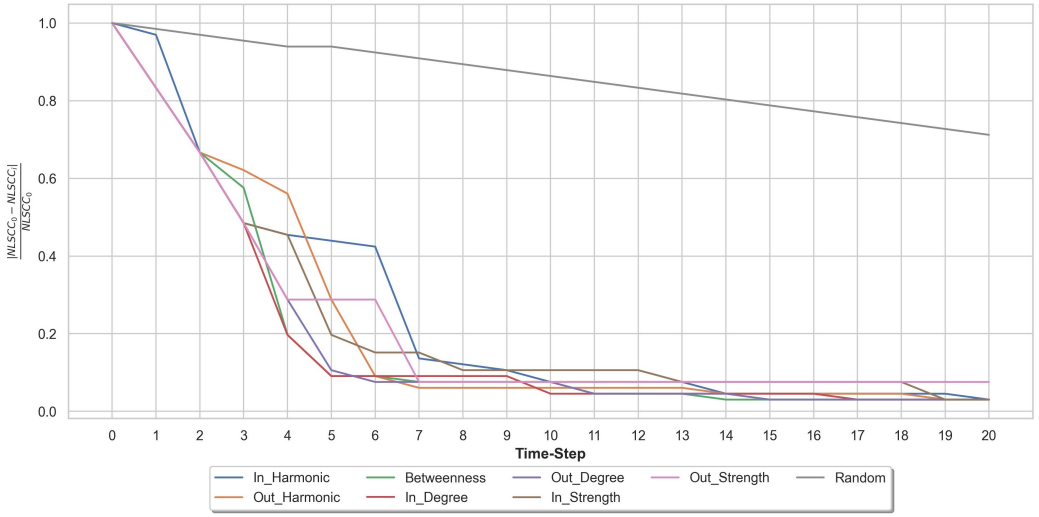

Figure 3. Reduction in Largest Strongly Connected Component order of the strongly connected directed and weighted time-averaged network after sequentially removing nodes with respect to their centrality scores. Nodes with highest centralities are disconnected first.

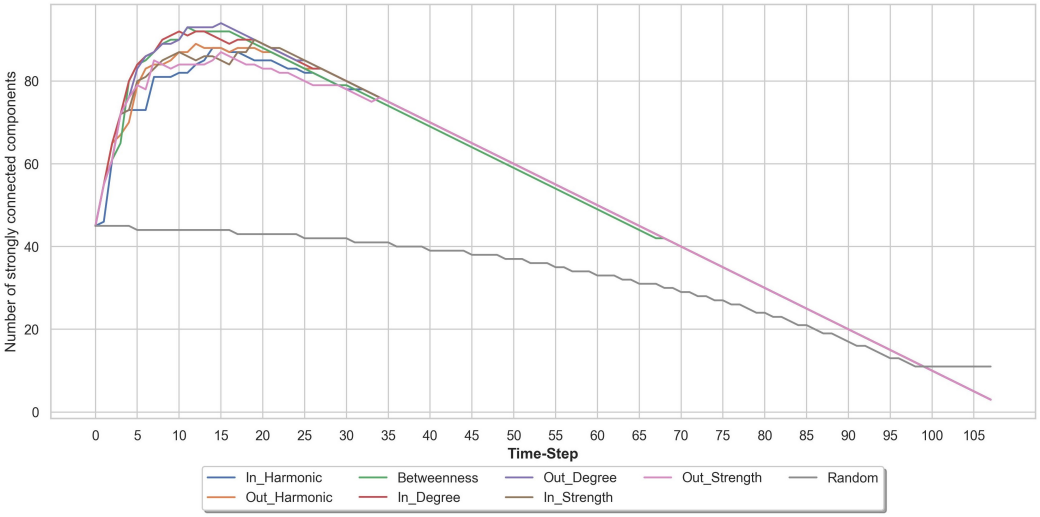

Figure 4. Change in the number of strongly connected components for the strongly connected directed and weighted time-averaged network after sequentially removing nodes with respect to their centrality scores. Nodes with highest centralities are disconnected first.

The robustness of the time-averaged network until the threshold is hit and the selected threshold for every targeted attack strategy is presented in Table 4.

Table 4. Calculated robustness for every centrality measure along with the threshold that corresponds to the required number of nodes whose removal results in the highest disintegration of the time-averaged network into multiple components.

Centrality	R	Threshold
In-Harmonic	0.2127	14
Out-Harmonic	0.2082	12
Betweenness	0.1936	11
In-Degree	0.2042	10
Out-Degree	0.1530	15
In-Strength	0.1554	19
Out-Strength	0.1739	15

4.3. Discussion of the Results

Random attacks emerge as the least efficient method for disrupting the network, requiring a substantial number of removals to significantly damage the network, as indicated by the slow decrease in the N_{LSCC} (Figure 3). The number of strongly connected components when implementing random removals also follows a consistently decreasing pattern, compared to the non-monotonous curves produced by targeted attacks, as illustrated in Figure 4.

In contrast, targeted attacks induce immediate damage to the network. Notably, the removal of just two nodes reduces the N_{LSCC} by more than 30%.

The superiority of targeted over random attacks is anticipated, as the time-averaged network is highly centralized (Sections 3.3 and 3.4, Table 2) and disassortative (Sections 3.3 and 3.4, Table 3) [7].

In terms of individual centrality performance, the isolation of a single node reveals that attacks based on in-harmonic centrality are significantly less effective in reducing N_{LSCC}, compared to the other centralities. Betweenness and in-degree-based attack strategies induce an 80% reduction in N_{LSCC}, requiring only the removal of four nodes, signifying the importance of mediators for the network's cohesiveness.

When aiming for the complete minimization of N_{LSCC}, in-strength centrality emerges as the most effective strategy, requiring the fewest nodes to be removed (22), closely followed by out-degree centrality (25 nodes required).

Attacks based on out-degree centrality disconnect the network into the largest number of multiple components, requiring 15 nodes to achieve such an outcome (Figure 4). Although other centralities require fewer nodes to achieve the maximal disintegration of the network into multiple parts, they do not produce as many components as out-degree centrality.

The effectiveness of attacks focusing on targeting individuals with increased out-degree centralities is further highlighted by the lowest robustness score compared to the other centralities, as shown in Table 4. In general, all robustness scores are relatively small, reaffirming that the network is vulnerable to targeted attacks, as previously stated.

The selection of the optimal centrality-based attack is not particularly straightforward and depends on the intentions of the attacker. When opting for the entire disintegration of the network we showed that in-strength centrality minimizes the N_{LSCC} the fastest, compared to the other centralities. Out-degree centrality, in contrast, appears as the most effective for producing the largest number of components. Betweenness centrality, on the other hand, induces immediate damage, since the removal of the intermediaries can disrupt the communication between distant parts of the network and emerges as a useful strategy when law enforcement agencies operate with restricted resources.

5. Concluding Remarks

5.1. Contribution

Monitoring the temporal evolution of the selected network indices in time may provide law enforcement authorities with data-oriented intelligence that can complement empirical evidence and expert opinion.

This is demonstrated by the observed sharp increase in certain network indices during the monitoring period (Section 3.2), a finding that can be proved useful for alerting the authorities to increasing criminal activity [54,55].

The incorporation of the direction of the links also provides further insight into the direction of information flow throughout the network, as highlighted by the notable difference between the entropies: the in-degree entropy reaches a global minimum at month 12, while the out-degree entropy reaches a global maximum. This confirms the remark that at the stage of highest activity, incoming instructions are precise and focused, while outgoing instructions are diversified.

The directed criminal network analysis also allows the analyst to design attack strategies based on directed centralities (Section 4.1). We did not find any prior work focusing on directed criminal network analysis, except for a recommendation on using directed networks to craft relevant disruption strategies [3].

When attempting to dismantle the criminal network, the inferiority of random node removals (Section 4.3) highlighted the need to design well-crafted targeted attacks due to its highly centralized structure. The use of aggregating measures, like robustness (Section 4.1), is convenient for assessing the overall attack outcomes.

Finally, we can render the attack simulations more useful when setting a threshold above which the network becomes non-operational, as stated in Section 4.1, to account for the large financial costs and resources law enforcement operations require in practice. Operations can effectively stop when the selected threshold is reached, without achieving the complete disintegration of the criminal network. In this work, we selected the threshold solely based on the behavior of the number of strongly connected components curve (Figure 4); however, in a real-life scenario, the threshold should be decided in collaboration with law enforcement experts.

5.2. Future Work

Further insight could be gained if we modeled the response of the network after implementing attacks of any kind towards it. This endeavor usually requires dynamic network analysis [6,25] and agent-based models [26,30], which goes beyond the scope of this work.

Additional attack strategies could also be implemented and tested, mainly based on community identification analysis to extend the disruption analysis beyond the use of centralities [62]. Depending on the data available, attacks based on human capital (i.e., the specific skills each individual offers in the network) can also be implemented [6,25,63]. The combination of centrality-based attacks with attacks targeting human capital can be useful for designing more sophisticated disruption strategies. Intervention strategies that do not exclusively resort to the elimination of nodes may also be studied [64].

Monitoring additional variables, besides the number of strongly connected components (Section 2.13) and N_{LSCC} (Section 2.14), may also offer a better assessment of the outcomes of each strategy on the functionality of the network. The change in global efficiency, for instance, is a meaningful indicator for evaluating the capacity of the network to continue disseminating information among its members [25].

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/info15020084/s1, Supplementary Material S1: Targeted removal; Supplementary Material S2: Centralities for each investigation stage for the temporal networks; Figure S1: Time-Averaged Network; Supplementary Material S3: Linear Regression Results.

Author Contributions: Conceptualization, E.K.A. and I.A.; methodology, E.K.A. and I.A.; software, E.K.A.; data curation E.K.A.; writing-original draft preparation, E.K.A. and I.A.; writing-review and editing, E.K.A. and I.A.; supervision, I.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data used in this work are published freely for research use at https://sites.google.com/site/ucinetsoftware/datasets/covert-networks/caviar (accessed on 29 September 2023). The name of each individual corresponding to a node in the networks is undisclosed for privacy reasons.

Acknowledgments: The remarks of the reviewers contributed to the improvement of the manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Sparrow, M.K. The application of network analysis to criminal intelligence: An assessment of the prospects. *Soc. Netw.* **1991**, *13*, 251–274. [CrossRef]
2. Cavallaro, L.; Ficara, A.; De Meo, P.; Fiumara, G.; Catanese, S.; Bagdasar, O.; Song, W.; Liotta, A. Disrupting resilient criminal networks through data analysis: The case of Sicilian Mafia. *PLoS ONE* **2020**, *15*, e0236476. [CrossRef]
3. Musciotto, F.; Miccichè, S. Effective strategies for targeted attacks to the network of Cosa Nostra affiliates. *EPJ Data Sci.* **2022**, *11*, 11. [CrossRef]

4. Bouchard, M. On the Resilience of Illegal Drug Markets. *Glob. Crime* **2007**, *8*, 325–344. [CrossRef]
5. Bright, D.A. Disrupting and Dismantling Dark Networks: Lessons from Social Network Analysis and Law Enforcement Simulations. In *Illuminating Dark Networks*, 1 ed.; Gerdes, L.M., Ed.; Cambridge University Press: Cambridge, UK, 2015; pp. 39–51. [CrossRef]
6. Bright, D.; Greenhill, C.; Britz, T.; Ritter, A.; Morselli, C. Criminal network vulnerabilities and adaptations. *Glob. Crime* **2017**, *18*, 424–441. [CrossRef]
7. Wood, G. The structure and vulnerability of a drug trafficking collaboration network. *Soc. Netw.* **2017**, *48*, 1–9. . [CrossRef]
8. Krebs, V. Uncloaking Terrorist Networks. *First Monday* **2002**, *7*, 941. [CrossRef]
9. Carley, K.M. Estimating vulnerabilities in large covert networks. In Proceedings of the 2004 International Symposium on Command and Control Research and Technology, Evidence Based Research, Vienna, VA, USA, 14–16 September 2004.
10. Cunningham, D.; Everton, S.F. Dark Network Resilience in a Hostile Environment: Optimizing Centralization and Density. *Criminol. Crim. Justice Law Soc.* **2015**, *16*, 1–20.
11. Su, Z.; Ren, K.; Zhang, R.; Tan, S.Y. Disrupting Terrorist Networks Based on Link Prediction: A Case Study of the 9–11 Hijackers Network. *IEEE Access* **2019**, *7*, 61689–61696. [CrossRef]
12. Eiselt, H. Destabilization of terrorist networks. *Chaos Solitons Fractals* **2018**, *108*, 111–118. [CrossRef]
13. Lindelauf, R.; Hamers, H.; Husslage, B. Cooperative game theoretic centrality analysis of terrorist networks: The cases of Jemaah Islamiyah and Al Qaeda. *Eur. J. Oper. Res.* **2013**, *229*, 230–238. [CrossRef]
14. Nie, T.; Guo, Z.; Zhao, K.; Lu, Z.M. Using mapping entropy to identify node centrality in complex networks. *Phys. A Stat. Mech. Its Appl.* **2016**, *453*, 290–297. [CrossRef]
15. Ai, X. Node Importance Ranking of Complex Networks with Entropy Variation. *Entropy* **2017**, *19*, 303. [CrossRef]
16. De Andrade, R.L.; Rêgo, L.C.; Coelho Da Silva, T.L.; De Macêdo, J.A.F.; Silva, W.C. Energy disruptive centrality with an application to criminal network. *Commun. Nonlinear Sci. Numer. Simul.* **2021**, *99*, 105834. [CrossRef]
17. Xu, J.; Chen, H. The topology of dark networks. *Commun. ACM* **2008**, *51*, 58–65. [CrossRef]
18. Lindelauf, R.; Borm, P.; Hamers, H. *Understanding Terrorist Network Topologies and Their Resilience against Disruption*; Operations Research; Springer: Vienna, Austria, 2009; pp. 61–72.
19. De Seranno, S. Using Social Network Analysis to Unravel Illicit Drug Supply Networks: A Systematic Literature Review. *Maklu* **2023**, *7*, 129–152.
20. Ahmadi, Z.; Nguyen, H.H.; Zhang, Z.; Bozhkov, D.; Kudenko, D.; Jofre, M.; Calderoni, F.; Cohen, N.; Solewicz, Y. Inductive and transductive link prediction for criminal network analysis. *J. Comput. Sci.* **2023**, *72*, 102063. [CrossRef]
21. Ribeiro, H.V.; Lopes, D.D.; Pessa, A.A.; Martins, A.F.; Da Cunha, B.R.; Gonçalves, S.; Lenzi, E.K.; Hanley, Q.S.; Perc, M. Deep learning criminal networks. *Chaos Solitons Fractals* **2023**, *172*, 113579. [CrossRef]
22. Morselli, C.; Giguère, C.; Petit, K. The efficiency/security trade-off in criminal networks. *Soc. Netw.* **2007**, *29*, 143–153. [CrossRef]
23. Freeman, M.E. Pushing the Envelope of Pedagogical Gaming: Dark Networks. *Political Sci. Politics* **2017**, *50*, 1083–1088. [CrossRef]
24. Dempsey, D. Social Network Analytics in Policing and Security: Efficacy and Ethical Considerations. 2021. Available online: https://www.westmidlands-pcc.gov.uk/wp-content/uploads/2021/10/2021-07-21-EC-Agenda-Item-2-Social-Network-Analysis-Primer.pdf?x95272 (accessed on 9 January 2024).
25. Duijn, P.A.C.; Kashirin, V.; Sloot, P.M.A. The Relative Ineffectiveness of Criminal Network Disruption. *Sci. Rep.* **2014**, *4*, 4238. [CrossRef]
26. Duxbury, S.W.; Haynie, D.L. Criminal network security: An agent-based approach to evaluating network resilience*. *Criminology* **2019**, *57*, 314–342. [CrossRef]
27. Ficara, A.; Curreri, F.; Fiumara, G.; De Meo, P.; Liotta, A. Covert Network Construction, Disruption, and Resilience: A Survey. *Mathematics* **2022**, *10*, 2929. [CrossRef]
28. Agreste, S.; Catanese, S.; De Meo, P.; Ferrara, E.; Fiumara, G. Network structure and resilience of Mafia syndicates. *Inf. Sci.* **2016**, *351*, 30–47. [CrossRef]
29. Catanese, S.; Meo, P.D.; Fiumara, G. Resilience in criminal networks. *AAPP Cl. Sci. Fis. Mat. Nat.* **2016**, *94*, A1. [CrossRef]
30. Duxbury, S.; Haynie, D.L. The responsiveness of criminal networks to intentional attacks: Disrupting darknet drug trade. *PLoS ONE* **2020**, *15*, e0238019. [CrossRef] [PubMed]
31. Diviak, T. Structural resilience and recovery of a criminal network after disruption: a simulation study. *J. Exp. Criminol.* **2023**. [CrossRef]
32. Morselli, C.; Petit, K. Law-Enforcement Disruption of a Drug Importation Network. *Glob. Crime* **2007**, *8*, 109–130. [CrossRef]
33. Bright, D.A.; Delaney, J.J. Evolution of a drug trafficking network: Mapping changes in network structure and function across time. *Glob. Crime* **2013**, *14*, 238–260. [CrossRef]
34. Bright, D.; Koskinen, J.; Malm, A. Illicit Network Dynamics: The Formation and Evolution of a Drug Trafficking Network. *J. Quant. Criminol.* **2019**, *35*, 237–258. [CrossRef]
35. Ozgul, F.; Erdem, Z. Deciding Resilient Criminal Networks. In Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015 (ASONAM '15), New York, NY, USA, 25–28 August 2015; pp. 1368–1372. [CrossRef]
36. Berlusconi, G. Come at the king, you best not miss: criminal network adaptation after law enforcement targeting of key players. *Glob. Crime* **2022**, *23*, 44–64. [CrossRef]

37. Wasserman, S.; Faust, K. *Social Network Analysis: Methods and Applications*, 1st ed.; Cambridge University Press: Cambridge, UK, 1994. [CrossRef]
38. Newman, M.E.J. *Networks*, 2nd ed.; Oxford University Press: Oxford, UK; New York, NY, USA, 2018.
39. Freeman, L.C. Centrality in social networks conceptual clarification. *Soc. Netw.* **1978**, *1*, 215–239. [CrossRef]
40. Grassi, R.; Calderoni, F.; Bianchi, M.; Torriero, A. Betweenness to assess leaders in criminal networks: New evidence using the dual projection approach. *Soc. Netw.* **2019**, *56*, 23–32. [CrossRef]
41. Rochat, Y. *Closeness Centrality Extended to Unconnected Graphs: The Harmonic Centrality Index*; ASNA: Zurich, Switzerland, 2009.
42. Gil, J.; Schmidt, S. The origin of the Mexican network of power. In Proceedings of the International Social Network Conference, Evanston, IL, USA, 25–27 July 1996; pp. 22–25.
43. Borgatti, S.P. Identifying sets of key players in a social network. *Comput. Math. Organ. Theory* **2006**, *12*, 21–34. [CrossRef]
44. Borgatti, S.P.; Everett, M.G.; Freeman, L.C. *Ucinet for Windows: Software for Social Network Analysis*; Analytic Technologies: Harvard, MA, USA, 2002; Volume 6, pp. 12–15.
45. Latora, V.; Marchiori, M. Efficient Behavior of Small-World Networks. *Phys. Rev. Lett.* **2001**, *87*, 198701. [CrossRef]
46. Gutfraind, A. Optimizing Topological Cascade Resilience Based on the Structure of Terrorist Networks. *PLoS ONE* **2010**, *5*, e13448. [CrossRef]
47. Shannon, C.E. A Mathematical Theory of Communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
48. Saramäki, J.; Kivelä, M.; Onnela, J.P.; Kaski, K.; Kertész, J. Generalizations of the clustering coefficient to weighted complex networks. *Phys. Rev. E* **2007**, *75*, 027105. [CrossRef]
49. Antoniou, I.E.; Tsompa, E.T. Statistical Analysis of Weighted Networks. *Discret. Dyn. Nat. Soc.* **2008**, *2008*, 375452. [CrossRef]
50. Fagiolo, G. Clustering in complex directed networks. *Phys. Rev. E* **2007**, *76*, 026107. [CrossRef]
51. Morselli, C. *Inside Criminal Networks*; Studies of Organized Crime; Springer: New York, NY, USA, 2009; Volume 8. [CrossRef]
52. Newman, M.E.J. Mixing patterns in networks. *Phys. Rev. E* **2003**, *67*, 026126. [CrossRef]
53. Pigorsch, U.; Sabek, M. Assortative mixing in weighted directed networks. *Phys. A Stat. Mech. Its Appl.* **2022**, *604*, 127850. [CrossRef]
54. Spyropoulos, A.Z.; Bratsas, C.; Makris, G.C.; Ioannidis, E.; Tsiantos, V.; Antoniou, I. Investigation of Terrorist Organizations Using Intelligent Tools: A Dynamic Network Analysis with Weighted Links. *Mathematics* **2022**, *10*, 1092. [CrossRef]
55. Spyropoulos, A.Z.; Bratsas, C.; Makris, G.C.; Ioannidis, E.; Tsiantos, V.; Antoniou, I. Entropy and Network Centralities as Intelligent Tools for the Investigation of Terrorist Organizations. *Entropy* **2021**, *23*, 1334. [CrossRef]
56. Oliver, K.; Crossley, N.; Edwards, G.; Koskinen, J.; Everett, M.; Broccatelli, C. *Covert Networks: Structures, Processes and Types*; Unpublished Manuscript; University of Manchester: Manchester, UK, 2014; pp. 4–13.
57. Sageman, M. *Understanding Terror Networks*; University of Pennsylvania Press: Philadelphia, PA, USA, 2004. [CrossRef]
58. Arquilla, J.; Ronfeldt, D. *The Advent of Netwar*; RAND Corporation: Santa Monica, CA, USA, 1996. [CrossRef]
59. Arquilla, J.; David Ronfeldt, E. *Networks and Netwars: The Future of Terror, Crime, and Militancy*; RAND Corporation: Santa Monica, CA, USA, 2001. [CrossRef]
60. Schneider, C.M.; Moreira, A.A.; Andrade, J.S.; Havlin, S.; Herrmann, H.J. Mitigation of malicious attacks on networks. *Proc. Natl. Acad. Sci. USA* **2011**, *108*, 3838–3841. [CrossRef]
61. Lou, Y.; Wang, L.; Chen, G. Structural Robustness of Complex Networks: A Survey of *A Posteriori* Measures [Feature]. *IEEE Circuits Syst. Mag.* **2023**, *23*, 12–35. [CrossRef]
62. Roberts, N.; Everton, S., Monitoring and Disrupting Dark Networks: A Bias Toward the Center and What It Costs Us. In *Eradicating Terrorism from the Middle East: Policy and Administrative Approaches*; Dawoody, A.R., Ed.; Springer International Publishing: Cham, Switzerland, 2016; pp. 29–42. [CrossRef]
63. Ficara, A.; Curreri, F.; Fiumara, G.; De Meo, P. Human and Social Capital Strategies for Mafia Network Disruption. *Trans. Info. For. Sec.* **2023**, *18*, 1926–1936. [CrossRef]
64. Roberts, N.; Everton, S.F. Strategies for Combating Dark Networks. *J. Soc. Struct.* **2011**, *12*, 1–32. [CrossRef]