mathematics

MDPI

Article

Covert Network Construction, Disruption, and Resilience: A Survey

Annamaria Ficara [1,*], Francesco Curreri [1,2], Giacomo Fiumara [1], Pasquale De Meo [3] and Antonio Liotta [4]

[1] Department of Mathematical and Computer Science, Physical Sciences and Earth Sciences, University of Messina, 98166 Messina, Italy
[2] Department of Mathematics and Informatics, University of Palermo, 90123 Palermo, Italy
[3] Department of Ancient and Modern Civilizations, University of Messina, 98168 Messina, Italy
[4] Faculty of Computer Science, Free University of Bozen-Bolzano, 39100 Bolzano, Italy
* Correspondence: aficara@unime.it

Abstract: Covert networks refer to criminal organizations that operate outside the boundaries of the law; they can be mainly classified as terrorist networks and criminal networks. We consider how Social Network Analysis (SNA) is used to analyze such networks in order to attain a greater knowledge of criminal behavior. In fact, SNA allows examining the network structure and functioning by computing relevant metrics and parameters to identify roles, positions, features, and other network functioning that are not otherwise easily discovered at first glance. This is why Law Enforcement Agencies (LEAs) are showing growing interest in SNA, which is also used to identify weak spots and disrupt criminal groups. This paper provides a literature review and a classification of methods and real-case applications of disruption techniques. It considers covert network adaptability to such dismantling attempts, herein referred to as resilience. Critical problems of SNA in criminal studies are discussed, including data collection techniques and the inevitable incompleteness and biases of real-world datasets, with the aim of promoting a new research stream for both dismantling techniques and data collection issues.

Keywords: covert networks; dark networks; criminal networks; terrorist networks; network disruption; network resilience; human capital; social capital; graph theory; network centrality

MSC: 91D30

check for updates

Citation: Ficara, A.; Curreri, F.; Fiumara, G.; De Meo, P.; Liotta, A. Covert Network Construction, Disruption, and Resilience: A Survey. *Mathematics* **2022**, *10*, 2929. https://doi.org/10.3390/math10162929

Academic Editor: Shugang Li

Received: 12 July 2022
Accepted: 12 August 2022
Published: 14 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Organized crime is a category of groups operating covertly and illegally outside the boundaries of the law and could potentially have devastating effects on both the social and economic order [1,2]. Criminal relationships can be studied in terms of network theory as covert or dark networks. Such networks usually include terrorist and criminal networks, which can be mathematically represented by graphs [3]. Graphs come along with a theoretical framework that allows researchers to study the covert network structure and make statements about the behavior of criminal groups [3].

Terrorist organizations promote political and social changes through violence, operating within supportive and homogeneous communities that promulgate such a violent struggle [4,5]. Criminal organizations engage in illegal activities to provide goods and services in order to profit and gain achievements at the cost of other individuals, groups, or societies [6]. Different terms can be adopted to refer to organized crime, such as *syndicates* [7], *crews* [8], *gangs* [9], *firms* [7], or *mafia* [10]. Mafia is indeed defined by Gambetta as a "territorially based criminal organization that attempts to govern territories and markets" [11]; he in particular calls the criminal group located in Sicily the *original Mafia*.

Even though organized crime may be identifiable by different names, its main feature is being founded on relational traits. This is the reason why Social Network Analysis

(SNA) is adopted to analyze criminal phenomena [12]. In fact, the concept of conceiving of organized crime as a network, and not as a hierarchical and structured organization, has incrementally grown in criminologist literature over the last century.

The most popular approach to organized crime diffused in the last decades of the Nineteenth Century was the alien conspiracy theory. This suggested analyzing organized crime as a bureaucratic organization, arranged according to a formal hierarchy with specific functioning rules, blaming its origins on outsiders (hence the *alien* name). At the time, such an approach received considerable support from federal Law Enforcement Agencies (LEAs). Historically, it has however been suggested that the alien conspiracy theory was promulgated out of the popular hysteria caused by the media and supported by LEAs as well, to justify their inability to eliminate organized crime [13].

The alien theory was eventually abandoned in the early 1970s, and this led to new analytical methods. It was indeed suggested to analyze organized crime as a system of loosely structured relationships mainly based on patron–client relations [14]. In the same years, the concept of network analysis was firstly cited and described as "an anthropological tool used to chart social interactions" [15]. This was used to describe the structure and functioning of organized crime, but it still showed limited applications under an empirical point of view.

A few years later, LEAs started to develop interest in intelligence data analysis; by the early 1980s, they started to perform link analysis in organized crime investigations through visual representations of the structure of the criminal groups [16]. Academic scholars' research on organized crime inevitably merged with the LEAs' link analysis approach. For the first time, an application of network methods was applied to a fictional criminal organization as a demonstration, using some basic network concepts, such as density and centrality [16]. This study demonstrated how multiple methods could help to extract relevant information from police data.

From the 1990s to the first years of the 2000s, the adoption of SNA in the study of organized crime saw significant developments—the interest in the discipline grew significantly, contributing to opening new research trends [17,18].

Currently, SNA is a growing interdisciplinary science that focuses on discovering the patterns of individuals' interactions. It has found extensive application in studying organizational behavior, inter-organizational relations, criminal group analysis, the evaluation of breakouts, mental health, and the diffusion of information. As an interdisciplinary field, SNA spans different domains such as Anthropology, Sociology, Psychology, Economics, Mathematics, Medicine, and Computer Science [19]. Some of the challenges currently involving SNA deal with big data analytics, information fusion, scalability, statistical modeling for large networks, pattern modeling and extraction, or visualization.

In the field of criminal network analysis, SNA is exploited to systematically examine criminal networks in order to attain greater insights about criminal behavior [20–22]. SNA allows graphically visualizing complex social structures and examining them systematically by computing the relational patterns of nodes (which can represent the actors involved) and connections (which represent a kind of tie between them). Such computations provide significant metrics and parameters able to pinpoint features that are not easily discovered at first glance [23] and to assess network activity, roles, and positions, as well as other mechanisms based on social ties. Because of the ability to compute quantified network parameters, network characteristics are more prone to objective interpretations, reducing the risk of leaving out important information.

Most studies on SNA for criminal analysis focus on different approaches and methods for network measurements such as density and centralization, the analysis of clusters, and the measure of the centrality of individuals. In particular, centrality measures are relevant in criminal network analysis, being able to identify critical actors that are heavily involved in criminal activities and whose removal would maximize network *disruption* [24]. Such measurements are performed through network parameters such as degree, betweenness,

closeness, and the clustering coefficient. Besides identifying leaders within the criminal organization [25], they also allow constructing crime prevention systems [26].

SNA application to organized crime can be summarily categorized with either a *micro* or a *macro* approach. In the first case, the analysis is conducted within a limited criminal group or for a single organization having a somewhat small number of nodes. This type of approach provides an analysis of the structure and working mechanisms of a criminal organization. Examples are given by drug-trafficking organizations [27–29], mafia activity [30], or some other type of criminal groups [10]. The second approach is based on larger networks derived from more complex databases [31–34]. It focuses on regional, national, or international groups with the aim of analyzing the interplay between different networks. An example is also given by the analysis of the connection between terrorist groups, where the nodes in the network represent the individual terrorist organizations, whereas the edges represent the location of the attacks [35].

Even though network analysis can aid a researcher in reconstructing a criminal organization in terms of its structure and functioning, the applications have sometimes attracted limited interest from LEAs. Many of them have expressed skepticism towards the application of network analysis methods in actual cases, claiming that these did not provide critical advantages in their own everyday investigations [36,37]. Indeed, SNA hardly provides much additional knowledge to the more conventional long-lasting investigation. This happens because police usually have better insights on specific cases. Thus, the most important actors in a network (who are best suited for disruption) are typically well-known to the LEAs themselves.

Nevertheless, SNA can still play a significant role, for instance in combining the investigative data from different cases and providing an overall picture that would be too complex to compute otherwise. The hidden connections within an organization and in-between different ones can best be unveiled through SNA. Prominently, SNA studies have already shown how, by merging data from different cases, one can identify major changes in network structure, positioning, and functioning [10]. Moreover, SNA may allow estimating the evolution of criminal organizations as a reaction to LEAs' actions [24]. It can then represent a valuable way to assess the impact that police operations have on the organizations and how these react, re-arrange themselves, and evolve altogether [26,38–42].

Being a widely addressed topic in the literature, different books and handbooks have been written on the application of SNA to criminal networks in the last decade [36,43–46]. Works such as Everton [1], Bichler and Malm [47] describe how the disruption of covert networks may be exerted, whereas Duijn and Sloot [48] reviewed several criminal SNA methods. With such an abundant literature, the aim of our paper is to provide a literature review of the most significant and influential works, which, to the best of our knowledge, has not yet been performed.

This review shows the main two methods of human network dismantling: the *human capital* approach and the *social capital* approach. The first approach deals with techniques able to identify high human capital figures within the network. These figures are those having specific knowledge, skills, or competencies. The second approach identifies key actors based on the centrality measures derived from SNA, giving more importance to the communication flow within the network, rather than the importance of the actor's role. So far, the human capital approach and the social capital approach have been developed in a parallel fashion and exploit very different techniques. Only a few works try a unified approach, which seeks to identify nodes in the network that are simultaneously able to deteriorate both the human and the social capitals. However, a comprehensive approach that tries to jointly damage the human and social capital is still missing, and we hope, with this survey, to stimulate further research in this topic, which we regard as fundamental.

Another problem in the computational analysis of criminal networks is about *data quality*. In fact, in most cases, the practitioners adopt one of the few datasets already available, but a data collection protocol has as of yet not been defined. For instance, there are no papers that try to understand which and how many phone taps should be used

to construct a sufficiently detailed network and how such a selection affects the findings of SNA algorithms. This paper then tries to suggest the definition of a new universally accepted protocol that brings the construction of a graph of the criminal network starting from court records.

The review is then structured as follows. In Section 2, the data management issues are described, including the methods that may be used to collect and validate the data. We also introduce methods used to transform the original criminal information into graphs, which is crucial to unveil the roles and the importance of particular elements (i.e., centrality). In Section 3, network disruption methods are reviewed and classified into three main categories: the human capital approach, the social capital approach, and the mixed approach. Section 4 describes covert networks' reaction to disruption attempts, referred to as *resilience*, on the basis of three main network features: vulnerability, elasticity, and adaptive capacity. Tables that classify literature applications according to each method are provided in each section as well. In Section 5, we conclude the paper with a discussion of the most prominent issues, providing an outlook for the next steps.

Figure 1 presents a conceptual map of the survey.

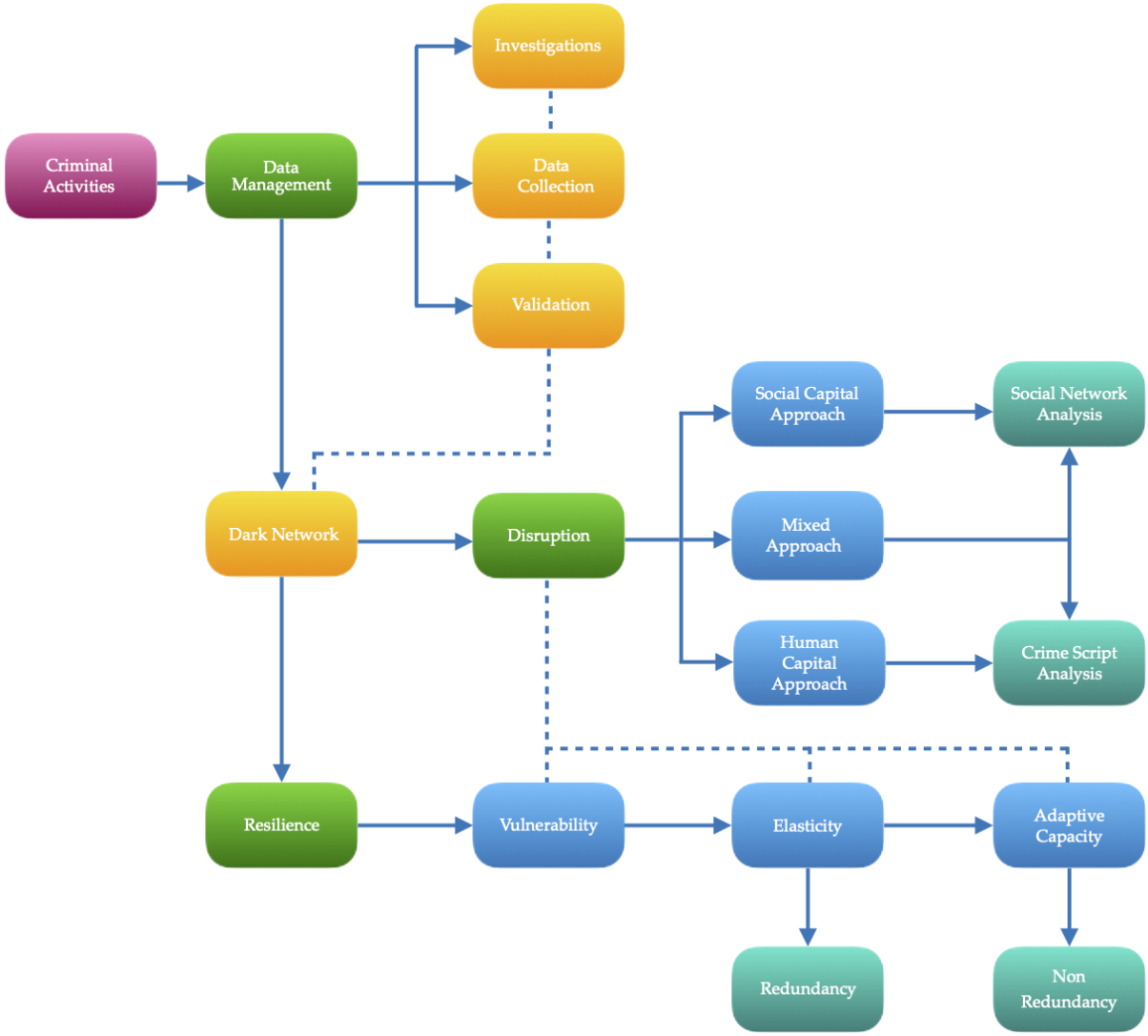


Figure 1. Conceptual map of the collected material for the survey.

2. Data Management

This section addresses the techniques adopted to gather criminal data, considering the crucial issues of data incompleteness and unreliability, and how such data may be

transformed into a graph for analysis. A basic introduction to the concepts in graph theory is given, for the benefit of the non-specialist reader.

Key references about data management are summarized in Table 1.

Table 1. Key references about data management in covert networks.

Approach	Network Type	Data Sources	Issues	References
Micro	Small size	Judicial documents Intelligence reports Investigation files	Misunderstanding or misjudgment of the specific node relevance Willing omission by the police	[10,28,36]
Macro	Larger and more complex	Intelligence databases collected by LEAs Databases created through archival analyses	Validity Reliability Database quality Missing data	[31,36,49]

2.1. Data Collection and Incompleteness

SNA is based on the adoption of real datasets as sources: this allows constructing the networks, which are then analytically studied [26,38,39,50–53]. The acquisition of complete network data that are able to describe the whole structure and all of the activities of a criminal group in its entirety is theoretically impossible [54].

During investigations, the subjects involved in LEAs' inquisitions will indeed always seek to conceal sensible information. That is why the investigators have to adopt alternative methods by exercising particular inquiring powers in order to collect evidence surreptitiously. Therefore, the information available for successive studies can be collected from sources such as phone taps and surveillance [27], archives [23,55], informants, interrogations of the people involved, such as witnesses and suspects [56,57], and even from infiltration operations by police.

Yet, in spite of providing significant advantages, the above sources come with an amount of drawbacks as well. For example, if the subjects under investigation become conscious of being phone-tapped, they are inclined to avoid speaking openly about what could turn into self-incriminating evidence [27]. Phone tap transcripts themselves are usually sampled and do not include all of the conversations that have occurred. The transcripts available to researchers come from different kinds of court records, which are the original wiretap records, police reports, arrest warrants, and finally, sentences [58]. In police reports, all relevant conversations are transcribed to be made available to the prosecutor and the judge. This means that anything deemed unrelated to criminal activities, such as conversations about personal or unrelated matters, is not included, which risks introducing misinterpretations by LEAs.

The arrest warrants typically include an even more sampled part of the whole transcripts, along with other relevant information that could come from other investigative sources. Finally, only a fraction of these data are reported in the final sentence, along with other evidence. This means that moving from the original records up to the final sentence, as shown in Figure 2, the amount of electronic surveillance data decreases, and it becomes more likely to lose relevant portions. For this reason, it is suggested to avoid using the sentence documentation as a data source for statistical analysis, since the data sampled at that stage are likely to be partial and biased, which may lead to unreliable results [58,59].

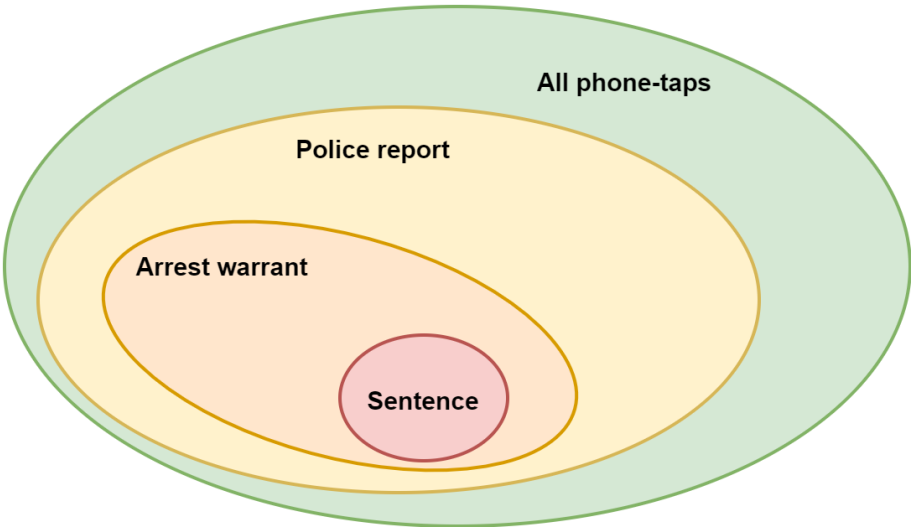


Figure 2. Sampled phone-tapped conversations between criminals in court records.

Another issue is represented by the fact that different phones and telephone lines are used in criminal communications, making it difficult for the police to phone tap all of them [60]. This can result in either missing links or missing nodes. In the latter case, we may end up missing some surveillance targets, who will not appear in the graphs, risking missing out on figures holding a central role in the organizations [10].

Longer-lasting investigations can minimize such problems, since these will reduce the amount of missing data. Interceptions and monitoring of a criminal group going on for months or years will lower the chances for some skilled criminal to avoid detection [10,28]. However, these prolonged investigations lead to datasets (and networks) that change over time, due to the dynamic nature of criminal roles and activities. Typically, actors come and go, social relations are built and dismantled, and criminal opportunities change alongside the social context [38,61].

It is worth noticing that a network analysis is based on a particular network composition, considered at a given point in time. Yet, since the network changes and evolves over time, different data collection methods may be required in order to cover more time spans [18]. While investigations are proceeding, the list of suspects tends to evolve as time goes by, not only because of the dynamic nature of such covert networks, but also as a function of strategic decisions by the police. In fact, LEAs normally start their investigations from some key subjects and, then, keep expanding their range by adding further subjects. This approach is close to snowball sampling [62], which is shown to be better suited for network analysis, as opposed to a random sampling approach. It is indeed shown that the latter holds very high chances of generating distorted inferences on network structures [63], and for this reason, it is not adopted.

This snowball-like sampling data collection technique is indeed mixed with purposive sampling [62], so that LEAs' decisions have a great impact at the point of being a valuable strategy. Sampling based on human insights is, however, also a possible source of biases. In practice, it may not be possible to monitor all the individuals that appear connected to the central ones. This may be due to a lack of resources, which makes it impossible to monitor all active criminals. The investigation is often focused on those individuals for whom it is easier to gather evidence. These constraints lead to partial data collection, with some groups operating under the police's sight, while others are left out.

Another source of error arises from the possibility that LEAs misunderstand or misjudge the relevance of specific nodes. There is also the case in which the police omit information, for instance when undercover agents have not yet been disclosed.

An important source of data is represented by other open sources such as public registries [23]. The records of cases prosecuted in the criminal courts are publicly available and may be used for research purposes, but only after the cases are closed. For instance,

American LEAs fill crime statistics using some defined standards, and these archives are available online. Nevertheless, as noted above for the case of sampled phone taps, the information coming from prosecutorial transcripts and criminal investigation files (in general from completed cases) may still present limitations in terms of data accuracy and completeness [59,60].

The files relating to concluded criminal investigations are kept by the police for long periods in order to allow for the examination of trends in policing, as well as in the criminal groups' behaviors and compositions [55,64]. These kinds of judicial documents, intelligence reports, or investigation files are the main data source in the case of micro studies, whereas in the case of macro studies, the main source is intelligence databases collected by LEAs [31,32,34] and databases created through archival analyses [65,66].

In light of the above considerations, it is now well accepted that criminal-related information (and networks) is typically incomplete or it is just limited to a specific time span. Therefore, it has to be taken for granted that it is not possible to attain complete network data [54]. The problem of missing information is particularly relevant in analyzing criminal networks, since it potentially affects the scope and structure of the network [10,20,31]. Such incompleteness translates into missing nodes and edges, which can create a domino effect, which alters the results of the measures, leading to incoherent inference problems [17,18]. However, some studies have showed that network measures may still be valid under some missing data scenarios [2,10,31,67].

2.2. Data Reliability and Validity

In addition to the missing data problem, criminal network data suffer also from incorrectness [54]. Data validity and reliability are indeed some of the main problems encountered in studies that apply SNA to organized crime. As stated above, during investigations, some of the consulted individuals to gain information might be reliable, as opposed to others, which might try to deceive the investigations in order to protect themselves or their associates or just to achieve some specific goal. This means that investigators deal with data of different qualities. Since there is not a typical method in SNA to deal with such different gauges of reliability, the subjective judgment of investigators becomes crucial in the analysis and interpretation of the available intelligence data.

The determination of relevant and irrelevant information is a task generally denoted as the problem of signal and noise. In such a context, relevant information and a considerable volume of irrelevant or unreliable information are merged. In fact, LEAs often face the issue of possessing very large amounts of data, some of which have hardly any importance. When they deal with great amounts of raw data gathered from several sources, the possibility for inconsistencies to occur becomes inevitably greater.

During collection, data can be evaluated according to the reliability of their source and the validity of the information [68]. In a criminal investigation setting, a source can be classified as:

(1) Reliable, when it is authentic, competent, and trustworthy;
(2) Usually reliable;
(3) Unreliable;
(4) Unknown, if there is no information about it.

On the other hand, information can be:

(1) Truthful, if it is shared by other sources as well, making it consistent;
(2) Probable;
(3) Doubtful;
(4) Unknown, if there are no other data it can be compared with.

Information that is doubtful or derives from sources of unknown reliability may include facts, partial truths, false information, or lies, and it consequentially has to be used carefully.

An example of reliability problems is given by data collected through surveys or interviews, which suffer from actors who are lying [69]. Information collected from interrogations are also affected by the risk that the interviewees downplay or amplify their real role and are not representative of the whole group.

In the case of data collected through phone taps, when the actors talk freely on the phone about some incriminating actions, the transcripts can be considered valid. Yet, a double-check is still needed in order to compare data collected from the taps and those collected from other official records relating to the case. Such a verification procedure is necessary, since communications among criminals are frequently packed with lies or codes in order to conceal the real intention of the conversation [70].

Besides the police seeking to verify the phone taps, the criminals themselves may also try to validate whether the information received by fellow criminals is accurate. Longer investigations and surveillance tend to eventually expose these kinds of lies. Yet, dynamics is another feature of criminal networks that affects data reliability since longer investigations lead to datasets changing over time. There is then the potential for a network analysis to become out of date in a short time [71]. Analytical techniques adopted by intelligence must be capable of handling large amounts of information and aiding in extracting the signal from the noise.

Because of the above reasons, we can say that data gathered during criminal investigations are affected by the following weaknesses:

- Incompleteness, which is inevitable given the covert nature of such types of networks;
- Incorrectness, which can be induced either by unintentional errors during data collection or criminals intentionally deceiving investigators;
- Inconsistency, which may occur when data regarding the same actors end up being collected multiple times, generating inconsistency inaccuracies. Such misleading information could, for instance, cause the same actor to appear as different individuals in a network.

Because of the described issues and since sources themselves reflect the perception of LEAs, the data used in the literature are all exposed to biases. This is the main reason why data mining and machine learning techniques are often unsuitable in criminal network analysis. These methods would be effective in discovering trends and patterns automatically from large volumes of data or for making predictions. On the other side, these methods require good-quality data, free of biases, errors, and missing data [72]. As it turns out, criminal network analysis mostly adopts a network science approach.

Scholars have indeed reported difficulties in managing such biases, analyzing the possible limitations they can bring [10,28,49,73]. Nevertheless, researchers have attempted to develop automated data mining techniques for LEAs, such as an automatic actors extractor from police reports and actors inconsistency detectors from networks [74].

2.3. Data to Graph Transformation

Another obstacle SNA has to deal with in the criminal field lies in how the data are transformed into actual graphs. There is no standard method for this task: the process goes through the subjective judgment of the analyst. For instance, it may be difficult for an analyst to decide whom to include or exclude from the network—the boundaries are often prone to ambiguity [18]. As stated by LEAs, the boundaries of the overall network do not necessarily correspond to the ones of the criminal group; so the analysts may identify by themselves the internal boundaries on the basis of personal experience and theoretical or practical considerations [10]. This problem is known as *fuzzy boundaries* and is a well-known challenge for practitioners [38,75–77]. Conversion of data turns out to be indeed a quite labor-intensive and time-consuming procedure.

A criminal network can be represented mathematically by a graph, which consists of nodes (i.e., individual actors) and edges (i.e., relationships between the individuals).

A graph $G = \langle V, E \rangle$ is defined as a structure consisting of two finite sets V and E [78]. The set $V = \{1, \ldots, N\}$ consists of the *nodes* (vertices or actors), where N is called the *size* of

the graph. The set $E \subseteq N \times N$ consists of the *edges* (links or ties) among the vertices. If two vertices are connected by an edge, they are said to be adjacent. A graph is called *complete* if each vertex is adjacent to every other one of the graph.

If all the edges of a graph are bidirectional, then the graph is *undirected*, whereas, in the opposite case, in which the edges are given by ordered pairs of vertices, then the graph is *directed*.

A positive numerical weight w_{ij} can be associated with an edge (i, j) with $i, j \in V$: in such a case, the edge is said to be *weighted*, as opposed to *unweighted* edges, whose associated weight can be conventionally considered as the default value $w_{ij} = 1$.

From a purely mathematical point of view, data contained in the sets V and E can be represented as a matrix, called the *adjacency matrix* [79] A. It is a matrix of dimension $N \times N$, and its generic element a_{ij} is defined as:

$$a_{ij} = \begin{cases} 1 & \text{if } v_i \to v_j \qquad i, j = 1, 2, ..., N \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

In the case of undirected graphs, the adjacency matrix A is symmetrical, since $a_{ij} = a_{ji}$ for all $i \neq j$.

In order to highlight particular characteristics of a network, some descriptive metrics can be defined. Firstly, the *degree* of a node $d(v_i)$ is the number of its neighbor vertices [79]:

$$d(v_i) = |\mathcal{N}(v_i)| = |\{v_j : \exists(v_i, v_j) \vee \exists(v_j, v_i), j \neq i\}|. \tag{2}$$

The minimum value of the degree is given when v_i is isolated, meaning that that node has no connections to other nodes, with a consequent value of 0; the maximum value is given when the node is connected to all the other ones in the network, showing a value of $N - 1$. The degree of a node v_i can be also calculated from the adjacency matrix A, by adding its columns (or rows) [79]:

$$d(v_i) = \sum_{j=1}^{N} a_{ij} = \sum_{i=1}^{N} a_{ij}. \tag{3}$$

In graphs, the distance between two vertices plays a central role. Such a distance is expressed as the *path length*, that is the number of edges contained in the path between two vertices. The *shortest path* between two vertices i and j, also called their distance d_{ij}, is the path with the fewest number of edges between them. In particular, in an undirected network, $d_{ij} = d_{ji}$.

Finally, the definition of *clique* is given. A clique C is a subset of vertices $C \subseteq V$ of an undirected graph $G = \langle V, E \rangle$, so that every two vertices of such a subset are adjacent, making C a complete subgraph.

2.3.1. Centrality Measures

Centrality is a core concept in SNA. Several centrality measures have been created to measure which actors in a network have the most influential or prestigious roles [80].

The *Degree* (*DG*) centrality [81] is used to evaluate the local importance of a node v_i counting the number of edges incident to v_i (i.e., the degree of v_i shown in Equation (2)). Values are normalized in order to adjust for network size by dividing by the maximum possible degree in a simple graph G (i.e., $N - 1$). It is defined as:

$$DG(v_i) = \frac{d(v_i)}{N - 1}. \tag{4}$$

The *Betweenness* (*BW*) centrality [82] is computed as the number of times that a node acts as a connection between other pairs of nodes [76,79,81]. It is defined as the sum of the fraction of all pairs' shortest paths that pass through v_i:

$$BW(v_i) = \sum_{v_j, v_k \in N} \frac{\sigma(v_j, v_k | v_i)}{\sigma(v_j, v_k)}. \tag{5}$$

Given a node v_i, the *Closeness* (*CN*) centrality [81,83] is the reciprocal of the sum of the length of the shortest paths between the node v_i and all the other nodes in G:

$$CN(v_i) = \frac{1}{\sum_{v_j} d(v_j, v_i)}. \tag{6}$$

Its normalized form refers to the average length of the shortest paths instead of their sum, and it is given by the previous multiplied by $N - 1$. In the case of larger graphs, the term 1 can be dropped so as to have:

$$CN(v_i) = \frac{N}{\sum_{v_j} d(v_j, v_i)}. \tag{7}$$

The *Eigenvector* centrality [84] is defined as follows. Given a graph G and its adjacency matrix $A = (a_{v,t})$, the relative centrality x of the node v is computed as:

$$x_v = \frac{1}{\lambda} \sum_{t \in M(v)} x_t = \frac{1}{\lambda} \sum_{t \in G} a_{v,t} x_t, \tag{8}$$

with $M(v)$ being the set of neighbors of the node v and λ a constant. It can be rewritten in eigenvector notation as:

$$Ax = \lambda x. \tag{9}$$

There will be different eigenvalue λ for which a non-zero eigenvector solution exists, and only the greatest one will result in the eigenvector centrality measure.

Two variants of such a measure are *Google's PageRank* (*PR*) [85] and the *Katz centrality* (C_{katz}) [86]. The first one is used by Google to assess the importance of a web page. It expresses the likelihood that a user randomly clicking on a hyperlink will arrive at that particular page. Given a directed graph and its adjacency matrix $A = (a_{i,j})$, the $PR(v_i)$ of node v_i is given by:

$$PR(v_i) = \alpha \sum_{v_j} \frac{a_{j,i}}{d(v_j)} PR(v_j) + \beta, \tag{10}$$

where α and β are constants and $d(v_j)$ is the out-degree of node v_j if such a degree is positive or $d(v_j) = 1$ if the out-degree of v_j is null.

The Katz centrality assesses the influence of a node by the number of its immediate neighbors and the number of all other nodes that connect to it through such immediate neighbors. For a node v_i, it is computed as:

$$C_{katz}(v_i) = \sum_{k=1}^{\infty} \sum_{j=1}^{n} \alpha^k (A^k)_{ji}, \tag{11}$$

where A is the adjacency matrix, k indicates the presence (or absence) of links between two nodes through intermediaries, and α is an attenuation factor.

The *Collective Influence* (*CI*) [87] of a node v_i is computed as:

$$CI_\ell(v_i) = (k_i - 1) \sum_{j \in \delta B(v_i, \ell)} (k_j - 1), \tag{12}$$

with k_i being the degree of node i; $B(v_i, \ell)$ the sphere of radius ℓ centered on the node v_i; $\delta B(v_i, \ell)$ the border of the sphere, which is the set of nodes at the exact distance ℓ from v_i. Given two nodes, their distance is intended as the number of links of the shortest path between them.

The *Network Capital* (*NC*) [88] is computed as:

$$NC = \frac{NS + CS}{N + [N(N-1)RSL]}, \tag{13}$$

where N is the total number of actors, while NS, CS, and RSL are, respectively, Node Score, Connection Score, and Resource Sharing Level, which are values computed starting from analyst-determined scores, according to the amount of resources an actor owns and is able to share. Further insights on such values are given in [88].

The *Attribute Gravity* (*AG*) centrality [89] measures the sum of the mutual cooperation of a node v_i with all the other nodes in the graph. Two nodes, whose masses are the attributes' weights, are in fact subject to mutual cooperation (i.e., sharing resources) proportional to their masses and inversely proportional to the square of the distance separating them. This measure is computed as:

$$AG_t(v_i) = \sum_{j \neq i} \frac{w_i w_j}{(d(v_i, v_j))^{\frac{1}{t}}}, \tag{14}$$

where w_i and w_j are the weight attributes of nodes v_i and v_j, respectively, $d(v_i, v_j)$ is the shortest distance between v_i and v_j, and t is a parameter that acts by changing the attractiveness of nodes and varies from zero to infinity.

The *Energy Disruptive* (*ED*) centrality [89] of node v_i is defined as the drop in the network energy caused by the removal of the node v_i from the initial graph G. It is computed as:

$$ED_t(G, v_i) = NE_t(G) - NE_t(G'), \tag{15}$$

where $NE_t(G)$ is the network energy of a graph G, which assesses the importance of an isolated node in G. When a node v_i is removed, the graph G is changed to a subgraph G'. The network energy is the sum of the nodes' attribute weights and the attribute gravity centralities. It is computed as:

$$NE_t(G) = \sum_{i=1}^{n} (w_i + AG_t(v_i)). \tag{16}$$

2.4. Summary

- Complete covert network data are impossible to obtain.
- Data are initially collected from phone taps, surveillance, archives, informants, infiltration operations, moving down to final sentence records, and a big amount of data is lost.
- Missing data can be overcome by longer investigations, but networks dynamically change over time.
- Investigations are based on snowball sampling and purposive sampling: being human-sensitivity based, this method is prone to biases.
- Investigation data suffer from inconsistent quality and reliability, and there is not a recognized method in SNA to deal with this problem.
- Because of the above, data inevitably suffer from incompleteness, incorrectness, and inconsistency.
- There is not a standard method in SNA to turn data into graphs.
- Centrality measures assess to what extent an actor in a network has the most influential or prestigious role.

- Centrality measures are based on graph properties such as degree, the number of nodes, shortest paths, and representation matrices.

3. Covert Network Disruption

Criminal intelligence has the aim of allowing the police to disrupt the working mechanisms and the structure of groups of individuals engaged in criminal activities.

According to Strang [90], there are two core questions that an intelligence professional should pose when applying SNA to disrupt organized crime:

(1) How does the organization operate?
(2) How could it be broken?

SNA allows discovering which individuals of the organization are most important and producing targeted recommendations for intelligence collection and operational disruption. Other tools such as attack preparations, value and production chains, and other criminal conspiracies have given practitioners insight into the core activities of criminal and terrorist organizations and have assisted in identifying their crucial requirements and potentials. To be successful in the disruption of organized crime, the aim is to disrupt its activities [90]. For instance, the Sicilian Mafia would stop being a problem if it maintained its structure, turning into a social club, rather than being an economic organization based on looting, coercion, and other illegal activities.

We can distinguish three indicators of destabilization for a criminal or terrorist organization [38]:

(1) A reduction of the quantity of the information that circulates in the organization;
(2) A reduction of the capacity to exercise its functions;
(3) A collapse or a significant decline of the decision-making process [91].

The three steps above can summarize the disruption of criminal and terrorist associations as the incapacity to diffuse information, goods, and knowledge in an efficient way [92].

Generally, disruption strategies can be categorized into two main techniques [38]: the human capital approach and the social capital approach [93]. The combination of the two gives rise to a third one: the mixed approach. These strategies can be applied to covert networks (i.e., criminal and terrorist), which are built from law enforcement data considering social relationships in terms of network theory. Key references in relation to this research field are summarized in Table 2.

Table 2. Key references about techniques in covert network disruption.

Approach	Key Concepts		References
Human capital	Substitutability		[18]
	Value chain		[94]
	Crime script analysis		[95,96]
	Crime and human capital accumulation		[97]
Social capital	Centrality measures from social network analysis	Degree centrality	[18]
		Betweenness centrality	[18]
		Closeness centrality	[83]
		Eigenvector centrality	[98]
		PageRank centrality	[99]
		Katz centrality	[39]
		Collective influence	[39]
		Network capital	[88]
		Attribute gravity centrality	[89]
		Energy disruptive centrality	[89]
	Order theory		[100]
	General network dismantling		[101,102]
Mixed	Combination of human and social capital techniques		[38,52,103]

3.1. The Human Capital Approach

Human capital was defined by the Organization for Economic Cooperation and Development (OECD) as "the knowledge, skills, competencies and attributes embodied in individuals that facilitate the creation of personal, social and economic well-being" [104].

The economic concept of human capital showed up in the earlier years of the 20th Century in the studies of the Scottish economist Adam Smith, but it was not really until the 1960s that economists systematically began to incorporate this idea into their work. In those years, some economists such as Theodore Schultz began to use the metaphor of "capital"—an economic concept of long-standing date—to explain how education and expertise contributed to prosperity and economic growth. They argued that people who invest in their education and training build a stock of skills and capabilities (capital) that will pay off in the long term. Such an investment can also be profitable for national economies and helps to fuel economic growth. Usually, human capital is defined in a broad sense as a mix of: (1) Skills and innate individual skills; (2) Competences and knowledge acquired at school and in courses of vocational training. Sometimes, health is also included in the definition of human capital. The world of industry, which adopted with enthusiasm this concept, tends to give it a more restrictive meaning, considering it mainly as a set of skills and talents of the workforce that contributes directly to the economic success of the company or one specific sector of industry.

The strength of a criminal organization, as for a company, depends on the human capital of their members, which includes their knowledge, skills, and expertise in a specific job. Criminal organizations are increasingly infiltrating very specialized areas of activity that require particularly important advisory services and competences. These may include pharmacological and chemical knowledge needed, for instance, in synthetic drug synthesis production or the skills of civil servants who are able, through technical suggestions, to facilitate the award of public contracts to companies close to criminal organizations. The removal of such important human capital could cause a weakening of the resilience of criminal organizations, as their elimination is not easily replaceable with other individuals [18,38,105].

Sparrow [18] suggested that a great opportunity to damage a criminal network is represented by the identification of subjects who own many resources, or present specialized skills, or can have access to scarce resources. He explained the concept of substitutability, which is an important criterion for network disruption. The removal of subjects with specific knowledge leads indeed to major consequences inside the criminal network, if compared to the removal of ones who are instead concerned with more general tasks and roles.

3.1.1. Value Chains in Covert Networks

In the fight against organized crime, it can be useful to apply value configuration analysis to criminal organizations in order to better understand their structures and typical conduct [94]. The value chain is the best-known value configuration. In the chain, a value is created through the efficient production of goods based on the utilization of a variety of resources. Criminal organizations involve business procedures made of several stages of production and activity [10,64,106] and, therefore, are considered as a series or chain of activities. Just as in a typical chain structure, different kinds of information, goods, and human capital are exchanged at each step of the process and added to the next one. Based on the distinct features of the illegal activity, a distinct radius of both skills-based and knowledge-based human capital is necessary at each stage of the value chain [23,95,107].

Typical examples of value chains are the cocaine or heroin business [94].

Duijn et al. [38] offered an example of the value chain units in the case of organized cannabis cultivation (see Figure 3). Primary activities in this value chain are: (1) Finding a location; (2) Building; (3) Taking care of the cannabis; (4) Harvesting; (5) Storage and processing; (6) Distribution. Within this system, there are some roles such as the coordinator and the growshop owner, who administer the majority of the steps of the value chain. Since

they even gather the right roles at the right place and time, they function as criminal brokers, making their roles, under a human capital point of view, extremely vulnerable in terms of disruption. In the case of organized cannabis production, such a method allows indeed describing all the tasks, roles, information, and resources involved in the value chain for such a delicate business process. Therefore, value chains can be an important method to identify high human capital actors.

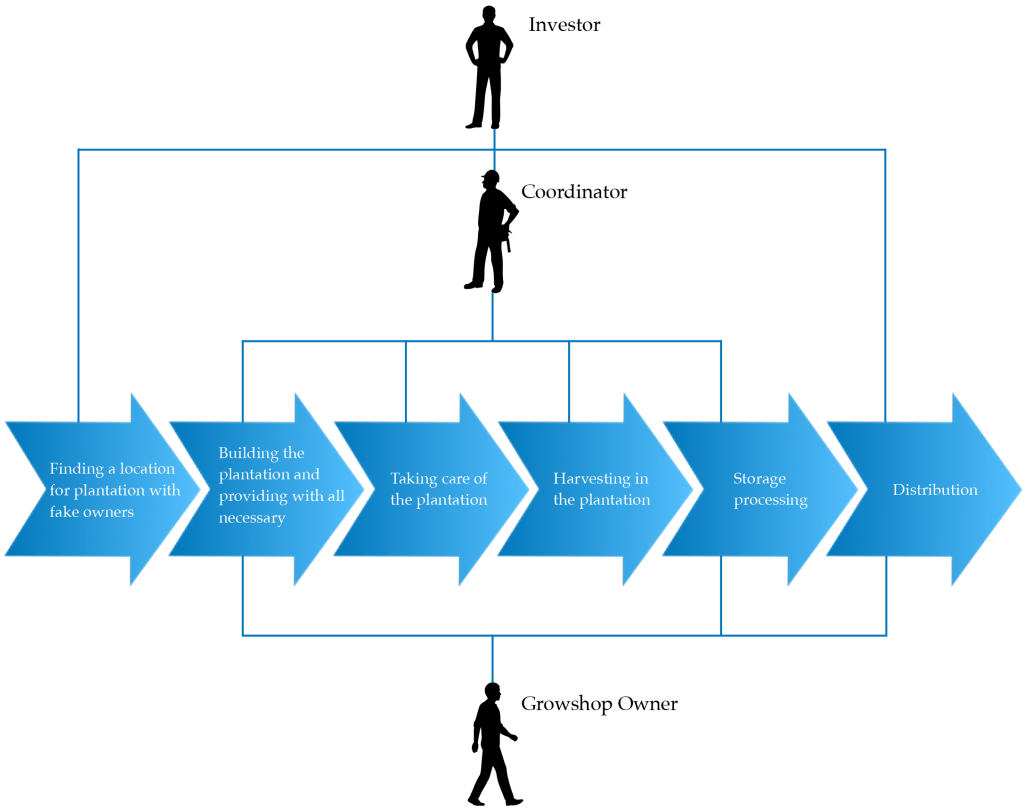


Figure 3. Crime script of cannabis cultivation.

3.1.2. The Crime Script

Cornish [95] introduced the notion of the script, which, if correctly identified, can prevent or disrupt the commission of a crime. Common routines or behavioral processes may be understood and represented through an event schema known as a script. The idea is that each crime requires the performance of certain actions, which must be repeated in a particular order, as in a comedy script. The scenes are sequential stages; the criminals are the actors; the tools they use are the props. Each crime, even the simplest one, requires the commission of a series of sequential decisions and actions. For example, a robbery script can be realized taking into account the crime setting, the entry to the setting, and awaiting or the establishment of conditions under which the robbery is committed. Information about preparations or aspects of the offense's aftermath are often missing and can be identified through the script. In this way, it is possible to find the motivation and purpose, which, together with the origins or development, are important to understand the crime act and its goals.

Following the notions by Cornish [95], Tremblay et al. [55] provided a case study on motor vehicles stolen for resale purposes, restricted to the period 1974–1992 and a Canadian province, and showed that script analysis provided a suitable strategy for detecting and understanding the selection and evolution of deviant solutions [108]. The deviant solution is a crime script. In fact, it deviates from routine crime commission pathways. At the same time, a substantial increase in offense levels occurs because of the successful diffusion of

the crime script itself. A combination of three pathways, which are the chopping, the body switching and the export scripts, conceptualized the structure of a criminal opportunity.

Bruinsma and Bernasco [107] merged such a script concept together with SNA, in order to pinpoint high human capital actors and substitutability within criminal networks. Their work showed the possibility to identify specialized roles in various criminal markets by analyzing crime scripts within the context of the criminal network. The authors particularly focused on the structure of networks that refer to the criminal activity of stolen car trading in the Netherlands. They studied, like Tremblay et al. [55] did, how these networks meet the demand of domestic and foreign public markets servicewise: it is the demand itself that causes an ordered chain-like structure and that combines the different criminal "clusters". Three clusters was identified: (1) A group of car thieves; (2) A group of car recyclers, who is also responsible for preparing the necessary documents; (3) A final group, who deals with the demand, organizing couriers responsible for bringing cars to their final destination. Since there is a lack of a central cluster, what is expected is that some subject contributes crucially at keeping the consecutive steps of the chain-like structure attached. Bruinsma and Bernasco suggested that the pivot of such a chain is represented by the brokers, who are the ones inside the second cluster that manage supplies and demand and that ensure financial arrangements, so as to guarantee the flow of the chain.

Levi and Maguire [109] explored the possibility to develop more efficient crime reduction strategies against organized crime by exploiting the crime script. They illustrated the difficulties in crime prevention when data quality and organization on the levels of crime are poor. They also analyzed some cases (e.g., financial crime) in which the effectiveness of crime prevention can be demonstrated thanks to the good quality of private sector data.

Chiu et al. [110] studied the crime commission process of clandestine drug laboratories. They also used crime scripts to identify significant points for intervention. They qualitatively analyzed the content of 25 court cases, realizing a crime script of seven stages.

Haas and Ferreira [111] hypothesized that rhino sustainability could be achieved through the combination of a disruption policy for horn trafficking syndicates and the problem of inequality rife in communities that live next to protected areas. The authors showed that the rhino slaughter crisis had two critical aspects: (1) People with no legal economic alternatives are attracted to the rhinos' slaughter; (2) This criminal operation is funded by efficient criminal networks. The authors also concentrated on some disruption strategies based on a supply chain that could be evaluated to avoid the extinction of the rhino.

Dehghanniri and Borrion [96] made a systematic review of over 100 crime scripts published between 1994 and 2018. Their results offered a comprehensive picture of crime scripting practice and highlighted new directions to develop effective situational crime prevention measures through the Internet of Things, as well as to use data from cyber systems.

3.1.3. Human Capital and Criminal Behavior

Human capital is not only important to recognize central actors in a criminal organization, but it also has a strong connection with crime. Lochner [112] developed a model of crime in which the expected costs associated with incarceration and the opportunity cost of crime from foregone work were increased by human capital. Fewer street crimes should be committed by older, more educated and intelligent adults. White collar crimes increase with age and education. The National Longitudinal Survey of Youth and the Uniform Crime Reports provide, respectively, self-reported data and arrest data, which offer broad empirical support to predict age–crime and education–crime relationships. Lochner also discussed how criminal behavior is affected by training, education, wage subsidies, and enforcement policies.

Huang et al. [113] studied the relation among criminal activities, unemployment, and the educational attainment levels in a given community. They proposed a dynamic general search-equilibrium framework to better understand and flesh out how the crime rate is affected by the opportunities available in the formal labor market and vice versa.

In their model, agents choose between crime-related activities (e.g., theft) and formal employment. Before choosing an occupation, agents raise their productivity by undertaking costly schooling. Crime reduces the value of any given level of schooling, acting as an indirect tax on human capital accumulation. As a consequence, companies are discouraged from entering a community that has increased unemployment because of low worker productivity. This generates more crime, and this is called the human capital effect. Multiple steady-state equilibria were exhibited by the model, and they were characterized by low levels of education, long periods of unemployment, poverty, and therefore, a high level of crime.

Mocan et al. [114] proposed a new model in which individuals possessed two different kinds of human capital: legal and criminal human capital. The former determines expected profits in the legal sector. The latter determines expected illegal profits. Both types of human capital can be improved through the participation in criminal and legal sectors. Investments can also increase the legal capital. Criminal behavior and its evolution were analyzed by the authors in several scenarios. For example, they studied how the acquisition of criminal and legal human capital was affected by the certainty and severity of punishment.

Coniglio et al. [115] analyzed the consequences of the presence of the Calabrian Ndrangheta on the long-term accumulation of human capital, which is inhibited both directly (i.e., reducing the incentive to invest in formal education) and indirectly (i.e., by increasing migration outflows).

Aizer and Doyle [116] studied the effects of juvenile incarceration in the United States, showing how this interrupted human capital formation, increasing the likelihood of later criminal behavior. Each year, over 130,000 juveniles are detained in the United States. Every day, 70,000 juveniles are detained. High school completion and the increment of adult incarceration are caused by detention. Even relatively short periods of incarceration can be very disruptive. In fact, after detention, a juvenile usually does not return to school. If he/she does, he/she is classified as disabled due to his/her social or behavioral disorder. This will likely reduce his/her probability of graduation, and it will possibly encourage future criminal behavior.

Brown and Velásquez [97] performed a similar study, estimating the effect of the unprecedented increase of drug-related violence in Mexico on human capital accumulation intended as the educational outcomes and employment behavior of young adults. These young adults are exposed to increased local violence and attained significantly fewer years of education. For this reason, they have less probability to complete compulsory schooling. Economic activities are restricted by local violence, reducing family resources. To provide additional income for the family, young male adults enter the labor market prematurely. According to the authors, there is a financial relationship between violence and human capital for young adults in Mexico.

3.2. The Social Capital Approach

Social capital may have first appeared in a book published in 1916 in the United States, which discussed how important community involvement was to the success of schools. In it, Lyda Hanifan referred to social capital as "those tangible assets that count for most in the daily lives of people: namely goodwill, fellowship, sympathy, and social intercourse among the individuals and families who make up a social unit" [104].

Society is made of understandings; shared values and links enable individuals and groups to trust each other and, so, work together. This is social capital, which can take various forms. We can divide this kind of capital into three main categories: linkages, bridges, and bonds [104]. Linkages are links to groups or individuals lower down or further up the social ladder. Bridges are links to individuals beyond a shared sense of identity such as associates, colleagues, or distant friends. Finally, bonds are links to individuals like us based on a sense of common identity such as people who share our ethnicity or culture, family, or close friends.

The creation of competitive advantages through social connections is the key for a criminal organization (just as it is for a company) to be successful in achieving goals that would not be feasible in its absence [117]. It is indeed clear that covert networks are heavily based on social ties, connections, and the capacity to retrieve resources to accomplish their tasks [20]. Such ties make it possible for actors in strategic positions to exchange and share resources with other individuals within the network [12,106,118–122].

Research in this field is commonly based on SNA, which considers social relationships in terms of network theory (see Section 2.3). SNA can be used to evaluate LEAs' interventions aimed at dismantling and disrupting criminal networks [38] because it allows identifying central actors, i.e., the ones involved with significant and powerful positions of social capital [123].

3.2.1. Centrality and Key Actors

Centrality is an intrinsically relational concept because an actor needs to have relations to be central [122]. An actor might be important because he/she is connected to other important actors or to a large number of different actors. An actor can also be important because, without his/her presence, the network would decompose into many isolated components. Centrality is also related to the power it might give to an actor. For example, an actor with a strategic position within a network will have high control over information flow [122].

Network centrality [3,80,124] can be measured in many ways through a set of centrality measures typical of SNA. A detailed description of these measures is given in Section 2.3.1. The removal of the most central actors according to the mentioned measures can significantly disrupt a covert network.

Degree centrality and betweenness centrality [18,106] are the most common centrality measures to find strategic positions within a network (see Equations (4) and (5), respectively). Actors having an increased connectivity with other actors in the network are called high-degree actors [79]. They possess higher social capital because they can exchange more information and resources than actors with fewer ties. High-degree actors are also called hubs since they are relevant in order for information and resources to flow through the network. As stated by Peterson [125], a high-degree centrality value can be a sign of vulnerability instead of strength. He argued that the most central actors in covert networks can be the most likely to be detected if they are the most visible. Figure 4 shows a simulation of the fragmentation of a Mafia network called Meetings analyzed in our previous works [26,39,53] and available on Zenodo [126]. At each step, the actor with maximal degree centrality is removed.

As opposed to high-degree actors, high betweenness actors occupy strategic positions within the network due to their ability to transfer and exchange resources [127–129]. They are called brokers and connect criminal networks linking criminal collectives within illegal markets [10,23,118,130]. Figure 5 shows another simulation of the fragmentation of the Meetings network. This time, at each step, the actor with maximal betweenness centrality is removed.

As also shown in Table 2, a number of other measures have been applied to criminal and terrorist networks [77]. For example, the eigenvector centrality measure (see Equation (8)) was applied to a large drug network in [98] and to a terrorist network, together with closeness centrality (see Equation (6)), in [1], PageRank (see Equation (10)) to a terrorist network in [99], and the Katz centrality (see Equation (11)) and the collective influence (see Equation (12)) to Mafia networks in [39]. de Andrade et al. [89] sought to more efficiently identify influential nodes and defined three new centrality measures based on the law of gravity. These measures are the attribute gravity centrality (see Equation (14)), the energy disruptive centrality (see Equation (15)), and the network energy (see Equation (16)).

In addition to the centrality measures, some authors used different methods to identify the key actors. For example, Bright et al. [103] tried to dismantle a drug trafficking network targeting social capital with a strategy based on the cut-set, i.e., a group of nodes or

edges whose removal can split a connected component of a network into two or more parts [105]. Farley [100] applied tools from order theory to a terrorist network modeling terrorist cells through ordered sets and defining in mathematical terms how to break them. Ren et al. [101] proposed a new method based on the combination between the spectral properties of a node-weighted Laplacian operator, a power-iteration method, and weighted node cover approximations.

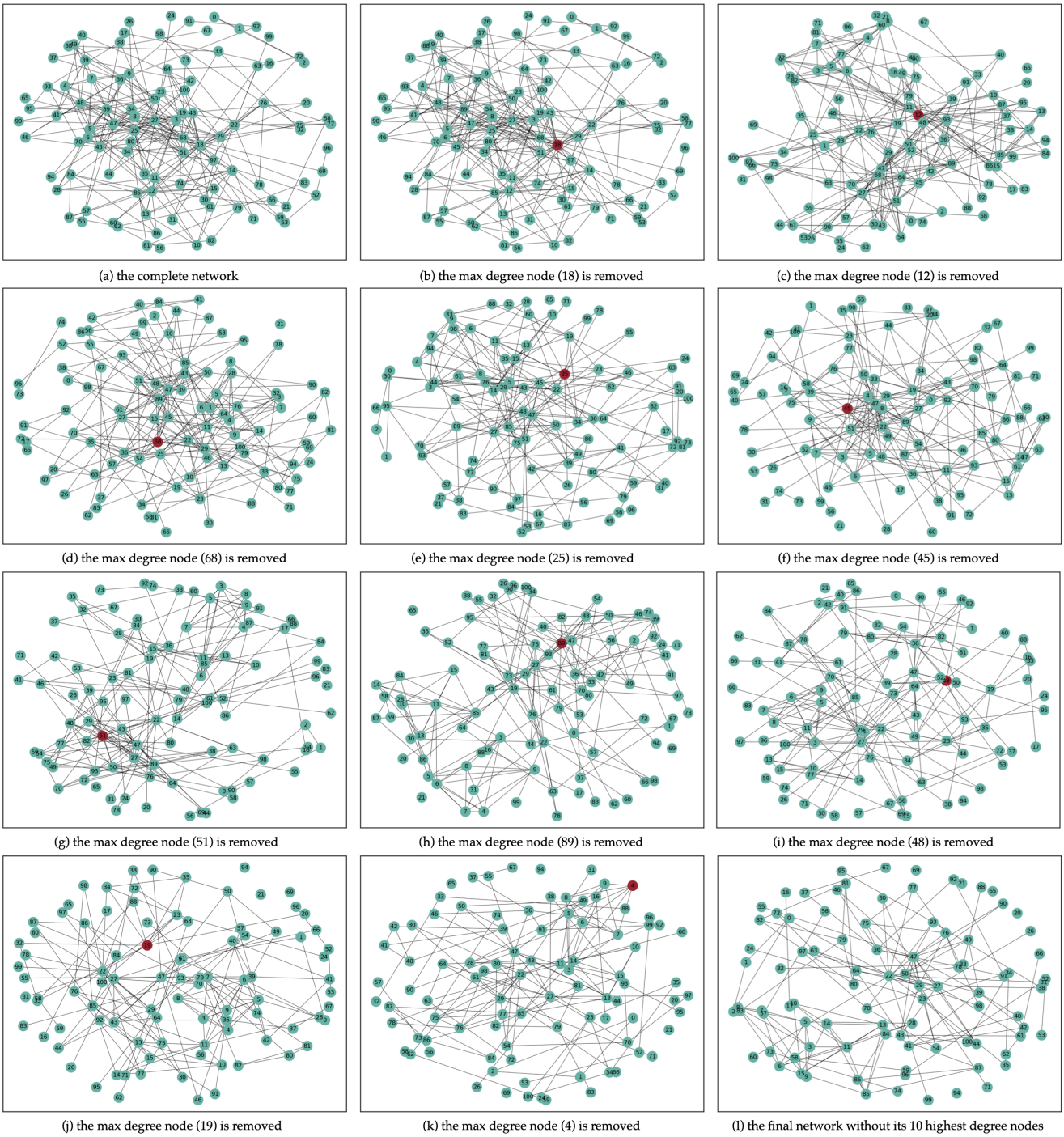
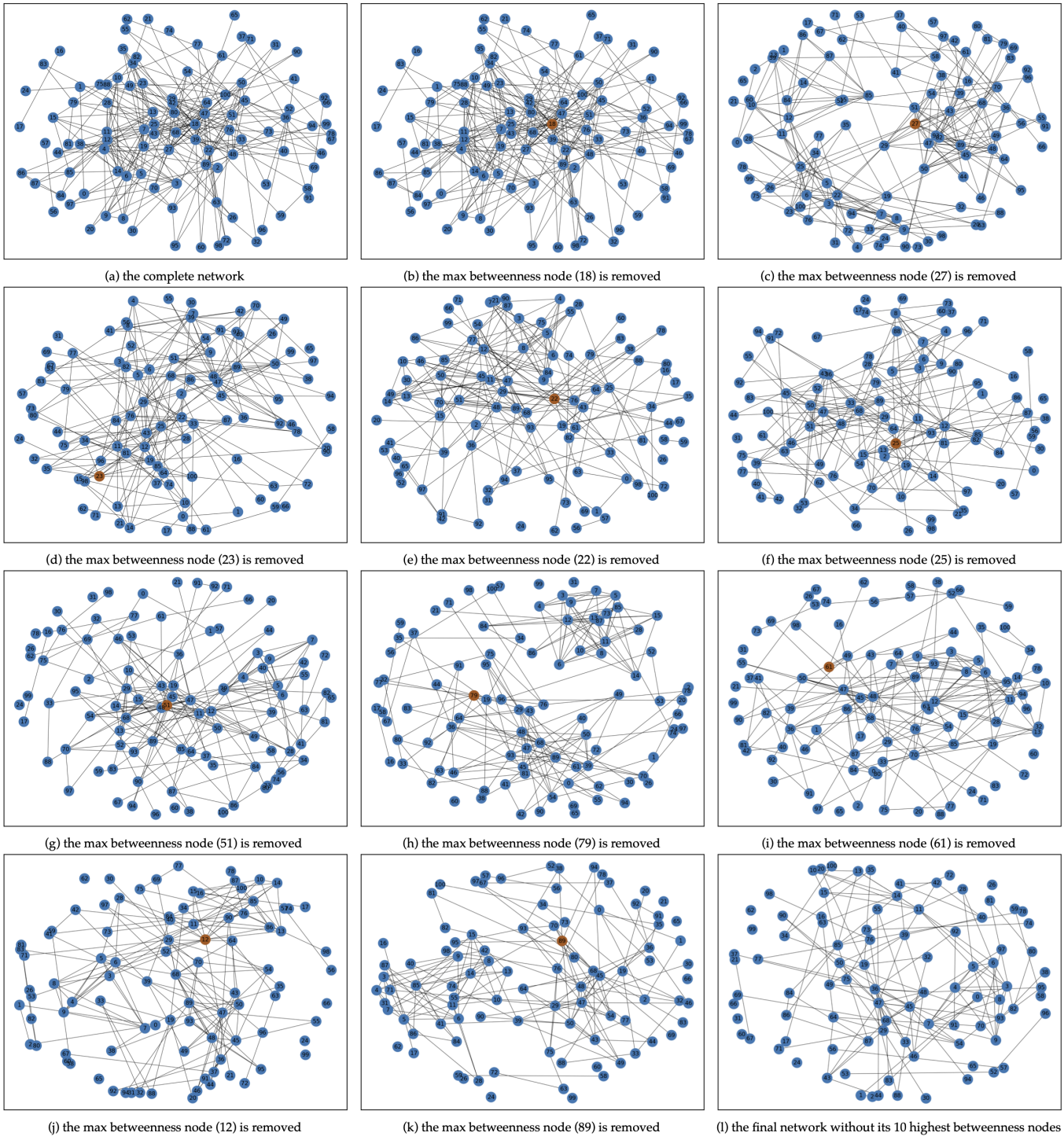


Figure 4. Removal of the 10 most important nodes according to degree centrality in the Meetings network extracted from the Sicilian Mafia operation called Montagna [26]. The first picture (**a**) shows the complete network. Then, at each step (**b**–**k**), the node with the highest value of degree centrality is marked in red, then removed. The last picture (**l**) shows the network without its 10 most central nodes.



(a) the complete network (b) the max betweenness node (18) is removed (c) the max betweenness node (27) is removed

(d) the max betweenness node (23) is removed (e) the max betweenness node (22) is removed (f) the max betweenness node (25) is removed

(g) the max betweenness node (51) is removed (h) the max betweenness node (79) is removed (i) the max betweenness node (61) is removed

(j) the max betweenness node (12) is removed (k) the max betweenness node (89) is removed (l) the final network without its 10 highest betweenness nodes

Figure 5. Removal of the 10 most important nodes according to betweenness centrality in the Meetings network extracted from the Sicilian Mafia operation called Montagna [26]. The first picture (**a**) shows the complete network. Then, at each step (**b**–**k**), the node with the highest value of betweenness centrality is marked in brown, then removed. The last picture (**l**) shows the network without its 10 most central nodes.

The mentioned works together with other significant papers in which social capital strategies are used to dismantle criminal and terrorist networks are summarized in Sections 3.2.2 and 3.2.3, respectively.

3.2.2. Node Removal in Criminal Networks

Schwartz and Rouselle adopted Borgatti's approach [76] to identify key players in a criminal network, with [88] and without [131] incorporating the actor and link weights. Adding weights, the authors presented a more comprehensive SNA-based model targeting actors whose removal maximizes network disruption for intelligence or enforcement purposes. Their model is compatible with any numerical system used by LEAs.

Anggraini et al. [132] proposed a new criminal network disruption technique identifying at first the communities in the given network, removing the edges between them, then targeting nodes based on closeness centrality inside each community. This measure was chosen by the authors because it indicates the information speed from one node to the other reachable ones.

Bichler and Malm [47] edited an interesting volume, focusing on how SNA could be used to inform crime prevention strategies and, thus, reduce crime directly, rather than just for understanding social structures. In a chapter of this book, Bright [133] presented an application of SNA for LEAs to identify high-value targets in illicit drug production and distribution networks. Joffres and Bouchard [134] used SNA to compare the effectiveness of various disruption strategies against online child exploitation that vary in size and structure. Their study examined a particular type of online covert network that potentially contains child pornography. Décary-Hétu and Laferrière [135] focused their SNA on online criminal markets of personal and financial data, and specifically on the formation of trust and business ties in a carding forum. Their study demonstrated the usefulness of this methodological approach to properly plan crime prevention through the disruption of attacks (e.g., when multiple fake identities were used to provide positive reputation feedback for a malicious vendor in an online marketplace).

Berlusconi [136] discussed the network approach to study crime and the different fields of application of SNA in the criminologist context. She described how SNA can be considered not only a valuable science for research purposes, but it can also help LEAs in their investigations. However, there are some cases in which traditional methods of targeting leaders in criminal networks are not applicable (e.g., loose networks of collaborating criminals). In fact, leader removal does not automatically lead to the vulnerability of a criminal organization or its disruption, because the effects of LEAs' targeting can be reduced by the network flexibility [24,92,137]. Hence, the impact of LEAs' interventions is not always effective, for instance when it leads to better adaptation strategies by the targeted criminal group (rather than disrupting the network) [138].

We also performed a study [39] borrowing methods and tools from SNA to disrupt two real Sicilian Mafia networks. We tried to reduce the size of the Largest Connected Component (LCC), identifying the actors with a high level of social capital through four different centrality metrics: collective influence, degree, betweenness, and Katz centralities. Our goal was to remove the key actors within the criminal networks, increasing the LCC size drop.

Musciotto and Micciché [139] analyzed a collaboration network of affiliates participating in the same crimes inside the Sicilian Mafia and tried to disrupt it with random and targeted attacks based on ranked network centralities through a percolation-based toy model. According to the authors, the most efficient disruption strategy was the removal of nodes representing criminals from different mafia syndicates with a crucial role in the connection of the network in a unique component. This strategy led to similar results to the ones obtained using node removal according to their degree values. This could be a great advantage because it did not require complete knowledge of the criminal network.

Tostado et al. [102] built a real human trafficking network collecting data with the snowball sampling methodology from a border state in the southern part of Mexico. The authors used three different dismantling strategies to tackle the criminal organization, i.e., random node removal, hub removal based on the degree and betweenness centrality measures, and finally, the General Network Dismantling (GND) algorithm. According to the authors, GND is the optimum option for dismantling a network because it is able to

discover the isolating offenders with a low number of links. An ideal disruption strategy should be not based on the removal of peripheral or the most connected actors, but on the removal of the nodes moderately connected to people of their kind.

3.2.3. Node Removal in Terrorist Networks

Farley [100] used order theory to disrupt a terrorist cell quantifying the degree to which a terrorist network was still able to function. According to the author, his model could help LEAs allocate resources in the war against terrorism and have quantitative data to defend themselves from the public criticism concerning the resources needed to foil the attack.

Xu and Chen [2], Xu et al. [140], Xu and Chen [141] made several studies about the disruption of criminal and terrorist networks. They proposed the use of several descriptive measures from SNA research (i.e., centrality for individuals, stability for groups, density, and cohesion) to help detect and describe changes in criminal organizations [140]. Then, they highlighted how it could be useful to find the structural properties of a criminal network [142]: (1) The existence of subgroups; (2) The way these subgroups interact with each other; (3) Its overall structure; (4) The central and peripheral roles of the actors. Analysts may target central actors for surveillance or removal and identify network vulnerabilities to develop effective disruption strategies, through a clear understanding of the above structural properties. Finally, they tested the robustness of four covert networks, simulating two node removal attacks [2]: those targeting hubs (i.e., nodes with a high degree, which therefore have many links) and those targeting bridges (i.e., nodes with high betweenness). They used two attack strategies: (1) Simultaneous node removal based on degree or betweenness, without updating the measure after each removal; (2) Progressive node removal, updating the measure after each removal.

Hussain [143] introduced a novel approach to SNA for locating the important key players in the 11 September 2001 terrorist network [83]. His system predicted a path comprising selected nodes, which showed the vulnerability of the network and (when removed) would lead to a significant destabilization of the network. The paper also provided comparative results for a couple of random networks with a variety of nodes and connections.

Fellman [144] examined terrorist networks through SNA, agent-based simulation, and NK-Boolean fitness landscapes. The author studied the 11 September 2001 network [83], which embodies some of the emergent properties of terrorist networks such as centrality, distance, and hierarchy. According to the author, the efforts to disrupt the information transmission through these kinds of networks could produce fewer or more levels of fitness in the terrorist organizations.

Mac Ginty [145] employed a case study related to the government of Sri Lanka's SNA-assisted counterinsurgency campaign. Security agencies claimed they could render powerless militant movements using SNA application to target key nodes and edges in insurgent networks. The author made three arguments on the potentially counterproductive nature of SNA-assisted counterinsurgency campaigns. Firstly, SNA could prevent the negotiation of a peace accord. Secondly, SNA-assisted campaigns could fail to address the leading cause of the violent conflicts. Thirdly, by removing high social capital actors from the community, SNA, as a counterinsurgency tool, could condemn communities to underdevelopment and failed post-war reconstruction. In fact, the magic weapon of SNA could actually prolong the conflict rather than help to stop it. Mac Ginty concluded by considering if SNA could be put to more constructive uses, specifically in the rebuilding of communities after a violent conflict.

Petersen et al. [146] studied node removal techniques for criminal network disruption. They used the Crime Fighter Investigator tool, which supports a node removal approach with two perspectives: (1) Changes in the node importance observed through the standard centrality measures such as degree centrality; (2) New possible edges detected through an inference-based prediction. The authors tested a new node removal algorithm on the Greek

terrorist group November 17, which was built from open-source reports. They also created hypotheses based on path distance and degree centrality changes.

Everton [1] emphasized how SNA provides different metrics to study covert networks and, therefore, potentially different strategies to disrupt them. He focused on terrorist networks such as the one based on the 11 September 2001 event [83] or the one that carried out the 11 March 2004 Madrid train bombings [147]. They share similar dynamics, being characterized by weak ties [148], which allow the different cells to maintain their connections with the larger network while remaining relatively isolated from and unknown to one another. The presence of weak ties and the partial or total lack of knowledge of the networks' overall structure helped the networks remain relatively invisible to counterterrorism efforts. These networks also possessed a high degree of stability if and when group members were captured. The author noted that the strategic use of SNA to track and disrupt covert networks has so far focused on actions aimed at targeting key actors. According to the author, this approach may sometimes yield positive results, but there is no guarantee that it will. For instance, this is the case of decentralized organization such as the Animal Liberation Front (ALF), which has been relatively immune to targeted attacks by the FBI. Its efforts have only driven the ALF to be more decentralized and underground [149]. Targeting key players within a covert network may not always yield the results that many would expect. For this reason, it is necessary to also consider multiple strategies that take into account different approaches, different points of entry into the network, and its overall topography.

In the volume edited by Bichler and Malm [47], which is described in Section 3.2.2, Bush and Bichler [150] illustrated the potential of SNA for improving the understanding of how insurgent groups adapted to strategic attacks by evaluating how the communication chains among individuals and between operational roles changed during a period of targeted drone attacks against the Al Qaeda network. Their study showed how the network remained operational despite the loss of key actors and how emerging leaders became more central when the network was under attack.

Burcher and Whelan [77] applied SNA's most common measures (i.e., degree and betweenness centralities) to identify suitable targets for covert networks' disruption, considering the groups responsible for the 7 July 2005 London bombings and the 21 July 2005 attempted London bombings. They concluded that SNA is a valuable science for understanding crime and terrorist groups. Yet, their study had a main limitation, which concerned the problem of fuzzy boundaries. This issue refers to the identification of actors and links to include and/or exclude from an analysis. The same authors performed further research into whether and how LEAs could actually deal with the challenges caused by the application of various SNA techniques to criminal networks in an operational environment [71]. In addition, Bouchard [120] used Klerks' studies [106] as a guide to determine whether scientists used SNA or alternative methodologies. The author focused on the way analysts applied SNA (in general and during an investigation) and, more specifically, on the network vulnerabilities, the identification of key actors, avenues of enquiry, and node and edge weights.

Eiselt and Bhadury [151] performed a sensitivity analysis, which started with the current situation and assessed the changes after the addition or deletion of a node or edge. By doing so, they could identify the leader of the 11 September 2001 event group [83], following a meeting of confirmed and suspected terrorists. In another work, Eiselt [152] reviewed some of the usual measures of SNA to evaluate different positions in networks and described different methods to destabilize terrorist networks. Through sensitivity analyses, they could determine the potential of certain actions and the vulnerability of these networks.

Singh et al. [99] used the Grey Relational Analysis (GRA) method to find loopholes of criminal networks to destabilize them. They analyzed the data of the 26 November 2008 Mumbai (India) attacks. The GRA method was brought into effective actions to discern the

most noteworthy node in the terrorist network. To do so, they used betweenness, closeness, eigenvalue, and PageRank centralities.

de Andrade et al. [89] proposed two centrality measures, based on the law of gravity. In these measures, the strength of the relationships between two node attributes is combined with the strength of the attributes themselves. The authors tried to disrupt the terrorist network of the Al Qaeda 11 September 2001 attack [83] and a network of convicts, monitored electronically. They used an energy disruptive measure to target the most central nodes. It was the most efficient strategy, being able to damage the network more than the other centrality measures considered. The authors measured the network's robustness through the size of the LCC and two new measures proposed in their work, which are the attribute load and the toughness. The former measures the loss of node attributes. The latter considers the maximum sum of edge weights.

3.3. The Mixed Approach

The mixed approach consists of the use of disruption strategies that are characterized by a combination of social capital (i.e., SNA metrics) and human capital (i.e., special abilities or competences and the supposed substitutability within the value chain). Regarding human capital, nodes can also be targeted based on the highest value chain degree within the network [38], which is measured by the amount of edges defined within the social system of the value chain configuration (see Figure 3). This strategy refers to the LEAs' ability to identify actors who have a great reputation. These actors could commit to other and various value chains within the value chain network as well. This means that they could be the most visible within the network, and therefore, they could have a higher degree centrality. Robins [105] emphasized the interaction between the characteristics of the network topology and the factors at an individual level. Knowledge, skills, information, expertise, and all the other qualities of individual actors are essential to understand the complex dynamics of criminal networks.

Our study shows that there are very few approaches that attempt to view the problem of covert network disruption from both human and social capital perspectives. A real mixed approach, defined as an attempt to identify the candidate nodes for degrading simultaneously both the human and social capital of a criminal organization, is missing. A new line of research could develop along these lines.

Papers that used some sort of mixed approach are summarized in the remaining part of the subsection.

Krebs [83] looked at the difficulty in mapping covert networks. He examined a portion of the 11 September 2001 terrorist network, which was centered on 19 dead hijackers. The author showed how the network appeared to be easy to disrupt concentrating on both connectivity and unique skills in the same nodes. The project's mission and its goals could be maximally damaged by the removal of the necessary skills from the project itself. It was possible that actors with unique skills (i.e., unique human capital) would also have unique edges (i.e., unique social capital) within the network. In fact, because of their high levels of human and social capital, these actors were the best choice for removal from the network.

Tsvetovat and Carley [153] simulated terrorist networks through a computational methodology and evaluated some destabilization strategies. They proposed some network metrics to identify key actors to target for covert network destabilization. The destabilization strategies are based on random targeting centrality measures and, from a more dynamic network perspective, cognitive demand [91]. The centrality approach consisted of isolating actors in the network with the highest degree or betweenness centrality. The cognitive load approach described by Carley et al. [91] consisted of the identification of actors having the most people to talk to, the most and hardest tasks to do, the most information to process, the most people to negotiate with to get the job done, etc.

Morselli and Roy [23] analyzed two stolen vehicle exportation operations (i.e., Siren and Togo) within a framework that merged crime script analysis and SNA, to examine the impact of brokers on the crime commission processes. In fact, key players within a

criminal organization do not maintain authoritarian roles. They maintain instead brokerage positions that bring creativity, flexibility, and integration to the organization, and that benefit people occupying such positions [154].

Key players in criminal organizations, in fact, do not maintain authoritarian roles but instead maintain brokerage positions that bring flexibility, integration, and creativity to the ensemble of an organization and that benefit the individuals occupying such positions [154]. A broker occupies a position between disconnected nodes within a network. These disconnected nodes may be members of different criminal organizations working together for a given operation. They also may have a hierarchical role within the criminal organization. Brokers are at first identified through crime script analysis, which has as the main objective untangling how some participants (i.e., the brokers) in criminal activities contribute to varying degrees to keeping the inherent channels of a script in place. Then, they used two brokerage indicators from SNA: betweenness centrality [155] and brokerage leverage [156]. Their framework and results are particularly useful for research on disruption strategies in various criminal networks and for direct applications in law-enforcement settings.

Spapens [157] combined the social and human capital approaches, amplifying the effects of network disruption. He analyzed Dutch ecstasy production value chains, identifying brokerage roles having increased social capital within the criminal collectives, but also human capital. These brokers, in fact, owned the reputation and resources needed to handle an ecstasy production value chain.

Nguyen and Bouchard [158] explored a cannabis cultivation network of 154 adolescent offenders, analyzing the factors associated with different criminal achievement. They examined the role of drug use and social and human capital in providing either in-kind (e.g., cannabis) or monetary rewards from crime. Their results revealed that social and human capitals are related to performance, while drug use explains little of the variation in criminal performances. Criminal human capital is crucial to earn money, but it is insignificant to obtain larger payments in cannabis.

Duijn and Klerks [37] focused on a cannabis cultivation network called the Blackbird crime network, illustrating the potentiality of the combination of SNA and crime script analysis. The authors defined the topology of the Blackbird network and its substructures and exposed the key actors using a mix of qualitative and quantitative analysis. They showed how analysts and informant handlers could work together, developing a better understanding of the strategies to target key individuals and discover access points to criminal communities and markets. In another work, Duijn et al. [38] extracted a criminal network from unique data from the Dutch Police, discovering that targeted attacks could make criminal networks even stronger. Their results emphasized the importance of intervening on criminal networks at an early stage, before they have the chance to re-organize themselves, obtaining the maximum level of resilience. Disruption strategies such as the social and human capital approaches force criminal networks to have more exposure. This makes successful network disruption a long-term effort. Duijn and Sloot [48] also explained that LEAs are trying to find more dynamic targeting strategies to more efficiently disrupt these criminal network structures. To do this, LEAs have to better understand how criminal networks operate and adapt over time. Big data and big data analytics represent an often unexploited key element to develop this understanding. Furthermore, new perspectives on network resilience can be provided from the study of the network changes over time.

Bright et al. [103] explored the validity of five LEAs' interventions in dismantling and disrupting criminal networks. They tested three LEAs' strategies targeting social capital and two interventions targeting human capital in criminal networks. The authors identified the actor removal based on betweenness centrality as the most efficient strategy. This strategy led, in fact, to network disruption in a few steps, which was relatively consistent across all their experiments.

Villani et al. [52] studied the way to use a combination of disruption strategies based on human capital with those based on social capital to neutralize or, at least, reduce the resilience and the adaptive capacity of criminal organizations. The elements that influence

the resilience ability of a criminal network are various, such as the knowledge, skills, and technical abilities available in the network, which translate into the available human capital. Since their importance is often underestimated or ignored, the adoption of new and diversified repression policies based on both human and social capital could be profitable to develop a valid resilience index.

We also performed a study [159] applying a mixed approach on two Mafia networks, removing actors according to the maximal degree, betweenness, closeness, as well as according to special skills or knowledge. To this end, a labeled graph was built, where each node possessed a specific role according to the judicial documents of an anti-mafia operation called Montagna. Then, we tried to create a network model for criminal network disruption using scale-free networks (i.e., the network model that better reproduces a Mafia network according to our previous studies [21,22]) with the same number of nodes and edges of our Mafia networks. After identifying the key role in the hierarchy of a Mafia family [122] or in its criminal activities, it is possible to identify this role in scale-free models and apply a disruption strategy based on human capital to these models. Specifically, the human capital approach is simulated targeting nodes with the same rank of the caporegimes in our Mafia networks.

3.4. Summary

- A covert network can be disrupted using two different approaches: human capital and social capital.
- The human capital approach consists of the use of crime script analysis to identify people with specific skills and capabilities useful for criminal organizations who want to infiltrate specialized activities.
- The removal of high human capital individuals from a covert network can irremediably damage it because they are not easily replaceable with other individuals.
- The social capital approach consists of the use of the centrality measures from SNA to identify the most central individuals in a covert network.
- The removal of high social capital individuals can prevent the exchange of information and resources through the covert network.
- Social and human capital can be used together, creating a third approach, i.e., the mixed approach.
- Further development and wider use of the mixed approach could give a great contribution to the disruption of covert networks.
- Most of the works on covert network disruption refer to terrorist networks. There are very few manuscripts about Mafia network disruption, which might be worth investigating further.

4. Covert Network Resilience

Covert networks might be able to withstand or absorb disruption, adapting to changes when necessary—this is referred to as network resilience [38]. More precisely, these networks develop the above abilities as a consequence of being disrupted. Key references in relation to this research field are summarized in Table 3.

Table 3. Key references about covert network resilience.

Resilience	Description	References
Key concepts	Definition	[160]
	Characteristics	[138,161]
	Efficiency/security tradeoff	[162]
	Redundancy	[163]
	Non-redundancy	[38]

Table 3. *Cont.*

Resilience	Description	References
Case studies	Illegal drug markets	[161]
	Terrorism	[164]
	Street gangs	[138]
	People smuggling	[165]
	Police corruption	[166]
	Rhino horn trading	[167]
	Cannabis cultivation	[38]
	Mafia	[168,169]
	Financial crimes	[170]

The term resilience was first used in physics and mathematics to illustrate the ability of certain materials to return to their original shape after external strain actions [138,160,168,171]; it was actually Holling who introduced the concept of resilience in an ecological context [138,172]. This concept has since been applied to describe the adaptive capacities of individuals [173], human communities [174], and larger societies [175]. There are many ways to define resilience [160]. The most common definition is the adaptive capacity in disturbance, stress, or adversity situations.

Widely discussed is the difference between resistance and resilience in mathematics and technology. Given a system that has to return to equilibrium, resilience refers to the time required to achieve the purpose, while resistance refers to the force required to displace the system from equilibrium [176]. Across these definitions, all the scientists agree on two key points about the concept of resilience:

(1) It refers more to an ability or process than an outcome [177];
(2) It refers more to adaptability than stability [178].

The increasing awareness of a business's vulnerability to threats such as natural disasters, accidents and employee or management errors, neglect or recklessness, or terrorism or cybercrime has brought the attention on the concept of resilience also in the organizational literature and business circles [138]. An organization is resilient if it is able to change its operations and objectives to survive during a state of chaos [138,179].

Covert network resilience strongly depends to the difference between the structures of criminal and terrorist organizations. Morselli et al. [162] compared these structures explaining the connection between time-to-task (i.e., the interplay between time and action) and their vulnerability. Terrorist organizations are characterized by a limited time-to-task and a particularly efficient communication system at the core. In this way, actions take place as quickly as possible, and the probability of being detected is considerably reduced. A terrorist organization, in fact, might accomplish its intents by one single, but successful terrorist attack. Criminal organizations are characterized by a longer time-to-task and a less efficient communication system at the core. Actions may be delayed for an extended period, during which criminals can operate within secure settings. These organizations try to stand flexibly and agilely, adapting quickly to external shocks [180,181]. This flexibility is fundamental for criminal network resilience against dismantling attempts.

4.1. The Characteristics of a Resilient System

This subsection presents in chronological order the state-of-the-art publications that study the resilience of different criminal and terrorist organizations such as illegal drug markets, people smuggling, Al Qaeda, drug trafficking, street gangs, rhino horn trading, police corruption, the Sicilian Mafia, and cannabis cultivation. Each kind of covert organization has in fact specific characteristics that make the derived covert network more or less resilient against disruption.

4.1.1. Illegal Drug Markets

Bouchard [161] analyzed the concept of resilience to understand the impact of repressive policies on illegal drug markets. According to him, three main characteristics should be considered to determine if a system is resilient:

(1) Vulnerability;
(2) Elasticity;
(3) Adaptive capacity.

Vulnerability to attacks refers to the degree to which a network is likely to be damaged by an external shock [182]. It first depends on the network level of exposure to attacks (i.e., on its capacity to protect itself or hide from attacks). For example, an illegal drug market will suffer weaker external shocks if the police have to make a great effort to seize drugs or to arrest a dealer [161]. If the network cannot absorb an external shock without compromising its functioning, then it has to use its elastic properties to recover. Elasticity refers to the efficiency of the network to return to its original state after an external shock [183]. The network can go back to functioning properly using its elasticity and replacing what has been removed by the external shock. Illegal drug markets possess elasticity if they are able to replace specific drug dealers or drug quantities seized by LEAs [161]. A network may not necessarily use a recovery process to return to its original state, but it may adapt its structure. The adaptive capacity of the network consists of the possibility to make its components less vulnerable by modifying its circumstances [182]. Adaptation is considered as an option only when recovery is too difficult to achieve or it is not possible because it is more demanding than recovery. In illegal drug markets, adaptation can happen in a variety of ways: drug dealers can change the location of transactions or drug producers can make their sites less vulnerable to detection, changing their production methods.

Consequently, covert networks show resilience to attacks when they possess one of the mentioned features (i.e., vulnerability, efficiency, or adaptation) or a combination of them. The most resilient network will show a tendency towards all three characteristics [161].

4.1.2. People Smuggling

Munro [165] applied the three properties of a resilient network identified by Bouchard [161] to Indonesia-based people-smuggling networks. People smugglers have a specific task: they have to guarantee the delivery of people to Australian territorial waters without being intercepted and processed by the Australian authorities. There are many factors that can prevent a smuggler from achieving his/her goal and make him/her vulnerable: (1) The Indonesian Navy or Police can intercept vessels, forcing them to turn back to port; (2) Irregular migrants can be detained and deported by immigration and police; (3) Boats may turn back or sink due to poor sea conditions. The reputation of smugglers is essential. In fact, when news of failed ventures spreads, their operations are in danger and some other smuggler will be sourced. The people-smuggling networks show remarkable elasticity. The Indonesian crews of the smuggling vessels are expendable, as are their boats. These crew members are impoverished farmers, fishermen, and other people living in stressful economic conditions. They risk imprisonment and are poorly paid in Australia, but their prospects abroad are much more favorable than their situation back home. The adaptive capacity of people-smuggling networks is in their ability to use the geographic dynamics of Indonesia to hide their activities and capitalize on areas in which LEAs are vulnerable.

4.1.3. Terrorism versus Drug Trafficking

Milward and Raab [184] analyzed the evolution of the Al Qaeda terrorist network (already studied by Raab [181]) and of the cocaine trafficking network relating to the trade from Colombia to the United States. The authors wanted to understand the response of both networks to the massive efforts made by the governments to control and destroy them. According to them, the level of resilience of both covert networks depends on the quality of three elements: (1) The characteristics of the people in the network; (2) The

relationships among them; (3) The overall structure of the network. The first elements refer to the character traits of the networks actors such as their psychological state, their willingness to make sacrifices, their commitment to the social group or to the cause, and finally, their financial resources. The second element refers to the level of trust among the actors in times of extreme stress or crisis and to the channels of communication (i.e., the existence of fall-back options for the lack of a specific communication channel). The third element refers to the relationship between resilience and the structural characteristics of a covert network as a whole (i.e., the existence of critical nodes or edges that, if taken out, would disrupt the network in unconnected parts. This kind of resilience was also described by Dodds et al. [185] as the probability that a network continues to function even if individual elements fail, and therefore, it is called connectivity robustness.

4.1.4. Street Gangs

Ayling [138] explained the characteristics of resilient licit organizations, which include: (1) Approach based on capabilities; (2) Planning of strategic scenarios; (3) Good communication within the organization; (4) Good communication with key stakeholders; (5) Sharing of the same vision, sense of purpose, and set of values; (6) Distributed power; (7) Inbuilt redundancy; (8) Bricolage; (9) Inspirational, enthusiastic, and intellectually stimulating leaders; (10) Capacity for effective organizational learning. According to the author, these characteristics cannot simply be applied to illicit organizations because licit and illicit organizations have some differences, which have implications for their resilient characteristics. Criminal organizations, in fact, operate against the state [186] and constantly risk interference such as asset seizure or member arrest. For this reason, they must have an efficiency/security tradeoff, which is defined as "the interplay between the need to act collectively and the need to assure trust and secrecy within these risky collaborative settings" [162]. The resilience, which comes from transparent democratic processes, is undermined by the need for operational secrecy. At the same time, criminal organizations have a certain freedom, which can facilitate operational and structural changes because they do not have to report to stakeholders or explain their unethical behavior to institutions or the media. In particular, Ayling focused on street gangs, identifying three environmental sources of gang resilience: (1) High level of interpenetration between gangs and state authorities or other legitimate businesses; (2) Community support; (3) Thick crime habitats. A source of gang resilience to disturbance is provided by the associations between gangs, state authorities, and legitimate businesses. For example, gangs deal drugs in nightclubs, who, in turn, rely on them for security services. Some gangs have also extensive investments in legitimate businesses or actively support particular political factions. Sometimes, gangs are supported as institutions by the communities. This happens because gangs assist residents with bills and accommodation, protect them from exploitation and physical attacks, organize recreational activities, or keep local rents low. The community may also refuse to ostracize gang members because they are friends, children, or even, their own relatives. This kind of community support is clearly a source of resilience because it gives gang members places, materials, and psychological resources to reorganize and regroup after disruption. New criminal opportunities for the gangs are continually generated by thick crime habitats, which also make street gangs more resilient, providing, for example, a space to self-organize. In these spaces, gang members can find co-offenders, share information, or make plans; they can recover from setbacks, such as the injury or arrest of members. Large urban conglomerates, such as weak or failing states, are plentiful for thick crime habitats.

According to Ayling [138], the gang's structure, its operational methods, and all of its peculiar characteristics are part of the gang's resilience. The structure of a gang is quite simple. It is flat and minimally hierarchical. The decision-making power is equally distributed throughout the gang. Thanks to this kind of structure, gangs have the capacity of adaptation to changing conditions [187]. Gang members have a strong trust among them. This trust speeds the information flow through a gang and makes it possible to quickly adjust game plans and to facilitate longer-term adjustments through measured debates.

However, the vulnerability of a gang can also be increased by these close relationships in case of information leak. The security of information is a priority in a gang, and it can be achieved through compartmentalization (i.e., important information can be isolated within a specific organizational cell) [163,164]. Compartmentalization allows isolating the active parts (i.e., the cells that contain essential knowledge) of the gangs from the damaged ones and an adaptive and fast regeneration of gang operations after LEA attacks. The identity of leaders or other central roles is an example of information that can be compartmentalized by a gang. Gangs, in fact, cannot prosper without a leader who mentors younger members and provides continuity. The personal attributes of the leaders and the way they influence the leadership style and the decision-making may affect the gang's resilience. Skills of bricolage are required for gangs to creatively deal with hostile interventions and environmental changes. Bricolage consists of the ability to take available resources and make something new from them, even when these are seemingly unconnected.

4.1.5. Rhino Horn Trading

Ayling [167] also studied the degree of resilience of rhino horn trading networks, which depends on the structure of these networks. In the past, rhino horn and ivory traffickers and poachers were not organized criminal gangs, but, predominantly, single individuals or informal groups. In 2012, the trade became more organized, and consequently, these networks started to be more sophisticated, including: (1) Small-sized syndicates; (2) Actors with particular types of expertise (e.g., hunting, veterinary, book-keeping, logistics); (3) Highly specialized roles within the network; (4) Access to expensive equipment; (5) A willingness to cooperate across nationality/ethnicity lines; (6) Connections beyond the network itself that facilitate smuggling. These networks are quite small and, therefore, more flexible and able to avoid detection, reducing the need for intra-network transactions. If necessary, these networks are able to open up new avenues of trade, adapting their operational modes, if other avenues are closed down. Yet, small size can also suggest vulnerability rather than resilience. Smallness and high levels of participant specialization may in fact imply a certain level of redundancy in the network. Therefore, if one actor ceases to be operative for whatever reason (e.g., arrest, ill health, or desistance), the activities are blocked until a new actor with similar skills is located [138,163].

As in the case of street gangs (see Section 4.1.4), the resilience of these networks can be provided thanks to the communities that support the criminal activities or the environmental features. Another source of resilience is corruption. In fact, the participation of public and private sector individuals and businesses is required to effectively distribute and smuggle horn to overseas markets. This partnership is needed to provide appropriate documentation, holding facilities, and laundering transport or facilities.

4.1.6. Police Corruption

Lauchs et al. [166] studied a criminal network based on a group of corrupt police officers called The Joke. The Joke operated in Queensland (Australia) for a number of decades. The authors determined the resilient characteristics of The Joke network using SNA tools. According to them, police corruption can be easily described as a covert network for several reasons: (1) The corrupt officers rely on their guise and positions to obtain opportunities, power, and resources to exploit people outside the system (e.g., a corrupt officer can use his/her power and his/her agency's resources to have access to the criminal world and support his/her coercive and corrupt actions); (2) Police culture is characterized by rules of solidarity, silence, exclusivity, and cynicism; (3) A corrupt police network is based on clandestine and close relationships, as those existing in the police force.

The survival of this kind of covert network depends on the police culture of silence, in which loyalty comes before integrity. Taking into account the previous studies by Milward and Raab [184], Williams [163], Carley et al. [91], and Bouchard [161], the authors listed the resilience properties of The Joke. The network was slightly affected by the loss of one or a few individuals because The Joke was a large group of police officers willing to

supply bribes. The internal security of the police cultural wall of silence protected The Joke's members against inquiry. Moreover, the heuristic of protecting one's mates in the Force is also extended to non-The Joke officers. The corrupt officers could rely on different layers of protection. Bribers were protected by the Queensland Licensing Branch (QLB); the QLB was protected by the senior police; the senior police were protected by the union and politicians.

The Joke's network was redundant because key members were replaceable by multiple facilitators, commissioners, and bagmen. This was possible because The Joke's members continued to move between these positions. Only a few members were aware of the entire operation, and for this reason, The Joke can be defined as a decentralized network operating in a field with a low profile. The officers dealt with victimless (i.e., no one died) crimes such as prostitution and gambling. The network was also able to continually renew itself with new nodes.

4.1.7. The Sicilian Mafia

Catanese et al. [168] focused on the Sicilian Mafia, emphasizing its most peculiar features. After the capture of a boss (i.e., the leader of a Mafia family) and/or of his/her closer collaborators, this criminal organization shows high qualities in terms of the regeneration and rearrangement of top positions' equilibria. This ability allows it to reconstruct the specific skills of the various families active in the territory.

Mafia networks are able to resist even in situations of large pressure thanks to the large economic incomes that derive from the criminal activities and their networks during the regeneration process. Even after substantial node removals, the network efficiency seems not to be significantly affected.

On the contrary, this property increases over time when old paths are restored, new paths are built, and the overall dimension of the structure is reduced. Mafia associations have a powerful organizational structure, which is highly resistant, adaptive, and flexible, even after particularly incisive interruptions. Moreover, the Sicilian Mafia has a peculiar feature called apparent appeasement, which usually draws the attention of magistrates and LEAs. It consists of the ability to change its visibility strategy, maintaining the equilibrium, an internal peace status, and a low profile.

4.1.8. Cannabis Cultivation

Duijn et al. [38] studied the resilience of criminal networks involved in organized cannabis cultivation. They reminded about the studies of Bouchard [161] and Ayling [138], asserting that the notion of resilience involves two features: (1) The ability to undergo and resist disruption; (2) The ability to adapt to alterations caused by that disruption. Their work pointed out that cannabis cultivation is a delicate criminal process, which is highly resilient against disruption. This is due to its adaptive and flexible structure. The authors also showed how criminal network resilience is a paradoxical concept, which depends on: (1) Redundancy, which is essential to find trustworthy replacements when the network disruption causes the loss of key actors; (2) Non-redundancy, which is the compartmentalization of the information flow to prevent further detection, due to the increase of risks associated with the search replacement. The concepts of redundancy and non-redundancy are analyzed in detail in Section 4.2.

4.2. Redundancy and Non-Redundancy

The level of redundancy in a covert network structure affects its capacity to withstand and absorb disruption. According to Williams [163], certain forms of redundancy are often developed by criminal networks to facilitate their recovery, if part of the network is damaged or degraded.

Different from legitimate business in which redundancy is wasteful and inefficient, the more redundancy there is in a criminal organization, the more options there are in the case of attack and degradation by LEAs. If LEAs arrest, incarcerate, or kill specific

members of the criminal organization, their responsibilities and tasks are assumed by other members thanks to redundancy. In Sections 4.1.5, 4.1.6 and 4.1.8, more details about redundancy in rhino horn trading, corrupt police, and cannabis cultivation businesses are given. Morselli [10] also underlined that the adaptive properties of criminal organizations are in their flexibility, which is favorable to the uncertain and hostile environment typical of crime.

Therefore, a criminal network can function even if some connections are broken thanks to the diversity of different connections.

Sparrow [188] identified the vulnerabilities of criminal networks in three concepts: (1) Centrality; (2) Role equivalence; (3) Weak ties. Centrality is an important ingredient in considering the identification of network vulnerabilities. As we already explained in Section 3.2.1, centrality metrics aid the identification of those actors who are pivotal, central, key, or vital and target them for surveillance or removal, which is the most common approach to incapacitate criminal organizations. However, the removal of one individual or a set of individuals may effectively disrupt a network when it depends on their uniqueness and not only on their centrality. In fact, these individuals are more difficult to replace, the more unique or unusual their role is. Therefore, the most central and difficult actors to replace are the most valuable targets. Network connections can be used to determine which individuals play similar roles. In SNA, this concept is called role equivalence, and it can assume different meanings. One of these meanings is that of substitutability, as explained in Section 3.1. The other one is role equivalence, which is a more intuitive and subtle idea of equivalence. If two individuals have the same role in different organizations, despite not having common acquaintances at all, they are considered equivalent. If two individuals possesses the same acquaintances or the same set of colleagues or friends, sharing the same immediate network neighborhood, they are considered substitutable or interchangeable. Weak ties are edges outside or between the denser cliques (definition given in Section 2.3), connecting otherwise distant parts of the network. These ties are called weak because they usually connect actors having no other obvious or direct connections. The completeness and the speed of network transmission can be greatly affected by the disabling of communication channels that are weak ties. The strength of weak ties consists of the use of brokers to find replacements [24]. Actors who possess essential knowledge and skills might have to be replaced, and non-redundant social connections are crucial to find them at a greater social distance from the trusted criminal core. Weak ties are non-redundant and offer access to new information, resources, and opportunities, which are not available within redundant networks [148,189]. Weak ties can cause great risks to network security. In fact, the search for trustworthy and capable replacements involves: (1) The cooperation with other criminals, whose reliability is difficult to assess [157,180]; (2) An increased transfer of information after disruption [190], which presents potential incriminating evidence and a risk of exposing the whole network by a single arrest [166,191].

The criminal network's capacity to adapt to the circumstances of increased risk refers to the resilience concept [38]. In order to facilitate this achievement, criminals use compartmentalization, as explained in Section 4.1. Baker and Faulkner [60] tried to disrupt illegal price-fixing networks finding a certain level of compartmentalization between the core and periphery within the networks. The chance of the leaders to become exposed after a single arrest decreased when the flow of information between members within the periphery and the visible core was deliberately separated. Therefore, covert networks such as illegal price-fixing networks, after disruption, tend to develop a form of non-redundancy within their internal flow of information to protect the most important members from being discovered [38].

Strong ties between network members are instead associated with the concept of redundancy. In uncertain and hostile criminal environments, the reciprocated trust offered by strong criminal ties is essential [10,38]. Replacements with a reliable reputation are often found at short social distances such as their social networks of affective ties, friendship,

or kinship [192,193]. Replacements are often found within the social connections directly embedding the actors involved within the criminal business process.

4.3. Covert Networks' Behavior after Disruption

Criminal organizations are resilient if they are able to respond quickly and effectively to disruption and to maintain illegal activities over time. Resilience can be measured according to network robustness to disruption and the recovery time after disruption [194]. In particular, network robustness depends on the structural characteristics that isolate the network from damage. Unfortunately, criminal network behavior and recovery after disruption are topics on which very little is known.

In the following subsections, we review relevant works for the cases of real terrorist and criminal networks, identifying prominent differences.

4.3.1. Terrorist Networks

Keller et al. [195] tried to dismantle terrorist networks using four strategies, which had different impacts on the capabilities and on the structure of these kinds of networks: (1) Leader-focused; (2) Grassroots; (3) Geographic; (4) Random. They tested the effects of each strategy on the resilience of terrorist networks in different scenarios in which these networks either had or did not have information about the impending attack. According to the authors, mature terrorist networks are more vulnerable in terms of total number of surviving leaders, average number of remaining connections per actor, and average resources remaining per actor. The evasion strategies did not influence the network vulnerability. The connectivity of a terrorist network is generally increased using evasion strategies in response to grassroots-focused attacks. If leader-focused strategies consist of the removal of actors involved in planning and leading activities, grassroots strategies concentrate on the removal of those actors who are responsible for conducting the activities. The latter strategies restrict the network capability to operate efficiently and perform its tasks.

Bakker et al. [196] studied three covert networks: (1) MK (i.e., the armed wing of the African National Congress in South Africa during apartheid); (2) FARC (i.e., the Marxist guerrilla movement in Colombia); (3) LTTE (i.e., the Liberation Tigers of Tamil Eelam in Sri Lanka). The authors defined the impact of shocks on the covert network' characteristics (i.e., legitimacy and resources), the network's capabilities (i.e., the replacement of actors and links, the balance between differentiation and integration), and in turn, how the covert network resilience is affected by them over time.

Everton and Cunningham [197] examined the resilience of the Noordin Top terrorist network over time to exogenous and endogenous shocks of violent extremists, who typically tried to balance operational security and capacity/efficiency. According to the authors, in terms of network resilience, potential advantages and disadvantages were offered by a network structure at either side of the cohesion and centralization continua. In their specific case study, the Noordin Top network needed to access different kinds of resources such as materials, weapons, or new recruits and, therefore, established external ties. However, this increase of external ties contributed to the network's disruption and exposure. Significant losses were faced by the network, which immediately rebuilt itself after each operation. In the end, this tendency to rebuild itself and the adoption of a centralized structure suggested that the Noordin network's disruption was due to the adoption of a suboptimal structure.

Diviák et al. [198] analyzed the structural changes in two Dutch Jihadi networks with 57 and 26 nodes, respectively, using descriptive measures of network cohesion, modularity, and a core-periphery model fit. In their experiments, the bigger network became less cohesive after disruption, while the smaller one became more cohesive, and this increased cohesion made it potentially more dangerous and efficient. The actor-level mechanisms were similar in both networks because the actors were inclined towards triadic closure and reliance on pre-existing edges. In particular, in the first network, more edges were created, but also more edges were dissolved for central actors.

4.3.2. Criminal Networks

Ozgul and Erdem [199] presented a resilience measure for criminal networks, which was tested on two real-world theft networks from Bursa (Turkey): the Cash network and the Ex-inmate network. They investigated the resilience properties of these networks in parallel with their growth, the thieves' activities, the recruitment policy, survival strategies, and secrecy after they were prosecuted. The Cash network recovered, keeping its tradeoff balance among secrecy, recruitment, and robustness. The Ex-inmate network appeared to not possess stability due to its recruitment policy. In fact, this network collapsed after several police raids and operations, showing its lack of secrecy and its vulnerability to unplanned recruitment.

Agreste et al. [169] described the evolution of a Mafia syndicate, building two networks from different judicial documents and digital trails in a period of ten years. The first network captured the phone contacts among suspected criminals. The second network included the relationships among individuals who were actively involved in several crimes. The authors investigated the network structure, highlighting that it was plastic against membership-targeting interventions and resilient after disruption attacks by the police. They also demonstrated that the phone call network was much more vulnerable to different kinds of attacks with respect to other types of criminal networks that are usually extremely resilient.

Leuprecht et al. [200] studied the transnational gun and drug trafficking of the Shower Posse, i.e., a violent international organized crime syndicate based in Jamaica, whose resilience proved particularly enigmatic. According to the authors, the Shower Posse case study showed the resilience of transnational criminal organizations when they could count on strong political connections. Measures to stop the political corruption that allows such gangs to flourish in their countries paid dividends by making criminal networks less resilient. The Shower Posse network also suggests that the network structure plays a key role to deter, detect, and disrupt them. Transnational networks span multiple jurisdictions, and for this reason, they represent a unique challenge. They are also able to adapt their structure because they straddle borders. Networks such as the Shower Posse can continue to operate after disruption attacks based on targeting street-level dealers because leaders, mules, distributors, and other dealers remain intact. The authors also showed that the removal of just one key actor from a criminal network cannot succeed in disrupting it. The way to bring it down is to make a highly coordinated effort targeting different structural roles at several levels of the network.

Duxbury and Haynie [201] performed a study on the disruption of a dark network concerning drug markets with 7295 nodes and 16,847 edges derived from population-level network data. Nodes were users of an active drug market. Edges were illicit drug exchanges between those users. An empirically grounded agent-based simulation was realized, and then, statistical methods were used to analyze the simulation. The authors considered three disruption strategies: (1) Targeted attacks (i.e., the removal of structurally integral nodes); (2) Weak link attacks (i.e., the removal of large numbers of weakly connected nodes); (3) Signal attacks (i.e., the saturation of the network with noisy signals). Targeted attacks appeared to be effective when conducted at a large scale. Weak link and signal attacks were able to identify more buyers and potential drug transactions when only a small portion of the network was attacked. Intentional attacks also affected the network behavior. When the network was attacked, actors created connections more cautiously, less frequently, and only with trustworthy other actors. According to the authors, the simultaneous use of weak link and signal attacks can compromise long-term network robustness and increase the network's vulnerability to future attacks.

Hardy and Bell [170] studied the key factors of resilience in a network derived from a sophisticated financial criminal enterprise applying SNA to the Madoff Investment Scheme. Four clusters of individuals were identified: core leadership, compliance, capital, and facilitator groups. These groups performed vital functions within the Madoff network, which used them to remain resilient against different kinds of shocks. The network was in fact highly resistant to exogenous shocks such as targeted investigations. It was able to

allay investigator suspects, fabricating professional legitimacy and convincing compliance paperwork thanks to the personal relationships with facilitators. The Madoff network was also resistant to endogenous shocks, such as investor withdrawals. In fact, it was able to borrow real and fraudulent investor capital, which was held in trading accounts or in banks. Its resilience was also due to the sticky money, which comprised intergenerational accounts containing funds. Therefore, according to the authors, sticky money and the ability to borrow investor capital were the key resilience factors of the Madoff network. These factors were removed from the network by the global financial crisis, which created a massive external pressure on the network and made it less resilient to endogenous shocks. The authors also used SNA to identify intergenerational accounts and loans against investor capital as the network resilience factors in fraud networks. The resilience of fraud networks can be provided by these factors, which also contribute to long-term financial crime.

Berlusconi [202] built a unique network from judicial court documents related to Operation Cicala, a two-year investigation of a criminal network trafficking drugs from Colombia and Morocco to Italy via Spain. The peculiar nature of the dataset allows comparing the network before and after disruption. In the middle of the police investigation, in fact, a key player was arrested, but police continued to monitor him for another year. The author showed how, after disruption, network actors favored security over efficiency, although criminal collaboration continued after the arrest of the key player.

4.3.3. Criminal versus Terrorist Networks

Gutfraind [203] studied the resilience to cascades in terrorist and guerrilla networks. Thanks to this kind of resilience, these covert networks can avoid a far-reaching domino effect caused by the failure of a single actor. Beyond a certain threshold, terrorist and guerrilla networks become more vulnerable. While maintaining high efficiency, these networks are uniquely cascade-resilient. An optimization method to construct networks characterized by a high passive cascade resilience was introduced by the author. It was based on cells with a star topology. The central node in a star network acts as a cascade blocker and keeps the average distance in the star short. For this reason, star-like designs are successful. Moreover, cells can provide covert network resilience, but also isolate actors in the network, reducing its efficiency.

Lindelauf et al. [204] analyzed the structure of two covert networks: a heroin distribution network in New York and Jemaah Islamiyah's Bali bombing. Despite normal social network topologies showing fast degradation under disruption and attack by counterterrorist agencies, which are often focused on the isolation and capture of highly connected individuals, terrorist networks are perfectly capable of outlasting targeted attacks, adopting secrecy and information-balanced networks. Transnational terrorist networks seem to be resilient because, as long as they are not completely dismantled by disruption strategies, they increase their capacity to remaining secret and do not lose the ability to operate at all.

Duxbury and Haynie [194] evaluated covert network resilience by examining network recovery from different disruption strategies on four covert networks: (1) The 11 September 2001 terrorist network [83]; (2) The Siren stolen vehicle exportation network [23]; (3) The Caviar network [162]; (4) The New York network Terrorist [118]. An agent-based model was used to evaluate the network recovery from disruption. Then, the most effective disruption strategies were identified. The effects of disruption and time to recovery observed on the covert networks were different. This depended on how the network was organized. Some networks in fact prioritized security; others privileged efficiency. According to the authors, efficiency-oriented networks tend to be less resilient than security-oriented networks in terms of both network recovery and robustness. Therefore, LEAs should develop disruption strategies considering network vulnerability in terms of both network recovery and robustness.

4.4. Summary

- Covert network resilience is the ability to withstand or absorb disruption, adapting to changes when necessary.
- The resilience of a covert network can be measured according to three different characteristics: vulnerability, elasticity, and adaptive capacity.
- Nevertheless, each kind of covert network (e.g., illegal drug markets, terrorism, street gangs, people smuggling, police corruption, rhino horn trading, cannabis cultivation, Mafia, and even, financial crimes) possesses specific characteristics that make it more or less resilient.
- Covert network resilience is affected by the level of redundancy. Here, redundancy consists of the presence of several individuals with the same skills who can substitute the others in case of police attacks.
- Non-redundancy can protect the most important individuals in a covert network from being discovered.
- Criminal networks are particularly resilient against disruption because of their flexibility, which allows them to quickly adapt to external shocks.
- Terrorist networks are less resilient than criminal networks, but they have a more efficient communication system and a limited interplay between time and action, which makes them hard to detect.

5. Concluding Remarks

This paper gave an overview of SNA techniques used for covert network disruption, describing how these networks react to such dismantling attempts. We provided the theoretical underpinning, as well as discussed the most significant real-case applications from the literature. The literature on the topic being rather abundant, the aim was to provide a systematic organization, which, to the best of the authors' knowledge, has not been executed before.

SNA allows understanding how a network functions and how it could be broken. Strategies and literature applications for covert network disruption are usually classified into two main approaches: human capital and social capital. The first approach consists of weakening a criminal organization by identifying and removing high human capital figures. This includes individuals that provide the organization with their specialized knowledge, skills, competences, and expertise. The second approach identifies key actors based on their centrality in terms of network theory. Being a network based on social ties by definition, central individuals are indeed evaluated purely based on their social connections within the network. The most effective centrality measures were given.

At the moment, these two approaches travel on almost parallel tracks and exploit very different techniques, which are crime script analysis and social network analysis. There are only a few studies that try to unify these two approaches considering the criminal organization in network terms and applying node removal procedures based on specific skills or centrality values. We named this technique the mixed approach. Nevertheless, through our literature review related to the destruction of social/human capital, we realized that there is a lack of a comprehensive approach that seeks to optimize the two parameters simultaneously; at present, there is little or nothing, and we have outlined the main findings in the two areas of social and human capital. This could stimulate a new line of research.

Our review also extends to covert networks' ability to withstand disruption and to adapt in the face of diverse dismantling attempts. This ability is called network resilience. Resilience is here classified by the different types of covert networks and in terms of network features such as vulnerability, elasticity, and adaptive capacity. Again, there are not many studies on network resilience. More accurate studies on the topic would indeed require access to information on how criminals rebuild their communication channels after arrest. In fact, most criminal networks are static, i.e., they lack data on network reconfiguration, as they are built from court data. Therefore, the analysis cannot fully capture the effects of disruption on the networks. In the case of dynamic graphs, i.e., snapshots of the graph

before and after police operations, one would indeed expect a significant re-tuning of the importance of nodes due to the internal reorganization of trusted affiliates used to spread messages within and outside the criminal network.

Another open issue in the application of SNA to covert network studies has to do with data collection. SNA techniques rely on real-world information, which is used to build the networks. However, data incompleteness and unreliability have been shown to be among the biggest issues in the field, since the collection of complete data is a virtually impossible task, with bias being inevitable as well. This is due to the nature of such kinds of networks: the examples provided in this paper show that covert networks should be seen as complex adaptive systems that show unpredictability and covertness in their structures, behaviors, and activities.

The risk of biases in the collection of data by LEAs appears to be a major issues in both micro and macro approaches. In the first case, a greater volume of data on an individual may suggest either a high level of activity by that actor or major attention by police. Such an issue is difficult to untangle, but shows the importance of interpreting findings in light of local operational experience and knowledge. The variable quality in intelligence data, known as the problem of signal and noise, can indeed create a false impression of the situation. Limitations suffered by each data source can be partially addressed by combining different data from different LEA sources. Yet, this method is complex, expensive, and time-consuming. In the same manner, in the case of macro studies, data are a reflection of LEAs' knowledge of markets and big criminal or terrorist groups. In this case, the reliability and bias problems are show to have a greater impact than micro studies.

Inevitably, however, any LEA's source is incomplete and will always suffer from missing data. This means that, in order to draw meaningful conclusions about the network structure, resilience, and dynamics, an understanding of both law enforcement and the criminal environment is necessary.

Moreover, novel information metrics need to be developed to better understand the effects of node manipulation in such networks. Most of the studies are based on static observations of criminal groups. The dynamics being one of the main features of such networks, more studies should focus on the disclosure of the mechanisms that involve the dynamics of these networks. This is indeed a non-trivial task, and only a profound integration of different scientific fields could bring the basis and the tools to uncover the complexity of their dynamics.

The works examined in this paper finally showed the scarcity of data availability in the case of micro studies of criminal groups, such as criminal gangs and mafia. Most of the studies in the literature focus indeed on macro studies of terrorist activity. Only future collaborations between academic practitioners and LEAs would eventually open the doors to a greater growth in the amount of available empirical data, which is needed to develop more studies and to fill more gaps.

Author Contributions: Conceptualization, A.F., G.F. and P.D.M.; methodology, A.F. and F.C.; software, A.F.; validation, A.F. and F.C.; formal analysis, A.F. and F.C.; investigation, A.F. and F.C.; resources, A.F. and F.C.; data curation, A.F. and F.C.; writing—original draft preparation, A.F. and F.C.; writing—review and editing, G.F., P.D.M. and A.L.; visualization, A.F. and F.C.; supervision, G.F., P.D.M. and A.L.; project administration, A.F.; funding acquisition, G.F., P.D.M. and A.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the INdAM—GNCS Project 2020 Algorithms, Methods and Software Tools for Knowledge Discovery in the Context of Precision Medicine.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

SNA	Social Network Analysis
LEAs	Law Enforcement Agencies
DG	Degree
BW	Betweenness
CN	Closeness
CI	Collective Influence
NC	Network Capital
NS	Node Scores
CS	Connection Scores
RSL	Resource Sharing Level
AG	Attribute Gravity
ED	Energy Disruptive
NE	Network Energy
OECD	Economic Cooperation and Development
LCC	Largest Connected Component
GND	General Network Dismantling
ALF	Animal Liberation Front
GRA	Grey Relational Analysis
QLB	Queensland Licensing Branch
MK	Umkhonto we Sizwe
FARC	Revolutionary Armed Forces of Colombia
LTTE	Liberation Tigers of Tamil Eelam

References

1. Everton, S.F. *Disrupting Dark Networks*; Structural Analysis in the Social Sciences; Cambridge University Press: Cambridge, UK, 2012. [CrossRef]
2. Xu, J.; Chen, H. The Topology of Dark Networks. *Commun. ACM* **2008**, *51*, 58–65. [CrossRef]
3. Ficara, A.; Saitta, R.; Fiumara, G.; De Meo, P.; Liotta, A. Game of Thieves and WERW-Kpath: Two Novel Measures of Node and Edge Centrality for Mafia Networks. In *Complex Networks XII*; Teixeira, A., Pacheco, D., Oliveira, M., Barbosa, H., Gonçalves, B., Menezes, R., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 12–23.
4. Laqueur, W. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*; Oxford University Press on Demand: Oxford, UK, 2000.
5. Perliger, A. Terrorist networks' productivity and durability: A comparative multi-level analysis. *Perspect. Terror.* **2014**, *8*, 36–52.
6. Finckenauer, J.O. Problems of definition: What is organized crime? *Trends Organ. Crime* **2005**, *8*, 63–83. [CrossRef]
7. Reuter, P. *Disorganized Crime: The Economics of the Visible Hand*; MIT Press Series on Organization Studies; MIT Press: Cambridge, MA, USA, 1983.
8. Adler, P.A. *Wheeling and Dealing: An Ethnography of an Upper-Level Drug Dealing and Smuggling Community*; Columbia University Press: New York, NY, USA, 1993.
9. Thrasher, F.M. *The Gang: A Study of 1313 Gangs in Chicago*; University of Chicago Press: Chicago, IL, USA, 2013.
10. Morselli, C. *Inside Criminal Networks*; Springer: New York, NY, USA, 2009; Volume 8.
11. Gambetta, D. *The Sicilian Mafia: The Business of Private Protection*; Harvard University Press: Cambridge, MA, USA, 1996.
12. Campana, P. Explaining criminal networks: Strategies and potential pitfalls. *Methodol. Innov.* **2016**, *9*, 2059799115622748. [CrossRef]
13. Lyman, M.D. *Organized Crime*, 7th ed.; Pearson: New York, NY, USA, 2019.
14. Albini, J.L. *The American Mafia: Genesis of a Legend*; Sociology Series; Appleton-Century-Crofts: New York, NY, USA, 1971.
15. Ianni, F.A.J. *Ethnic Succession in Organized Crime: Summary Report*; US Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice: Washington, DC, USA, 1973.
16. Lupsha, P.A. Networks versus Networking: Analysis of an Organized Crime Group. In *Career Criminals*; Waldo, G.P., Ed.; Sage Publications: Thousand Oaks, CA, USA, 1983; pp. 59–87.
17. Ianni, F.A.J.; Reuss-Ianni, E. Network Analysis. In *Criminal Intelligence Analysis*; Andrews, P.P., Jr., Peterson, M.B., Eds.; United States Department of Justice Office of Justice Programs: Washington, DC, USA, 1990; pp. 67–84.
18. Sparrow, M.K. The application of network analysis to criminal intelligence: An assessment of the prospects. *Soc. Netw.* **1991**, *13*, 251–274. [CrossRef]
19. Camacho, D.; Luzón, M.V.; Cambria, E. New research methods & algorithms in social network analysis. *Future Gener. Comput. Syst.* **2021**, *114*, 290–293.

20. van der Hulst, R.C. Introduction to Social Network Analysis (SNA) as an investigative tool. *Trends Organ. Crime* **2009**, *12*, 101–121. [CrossRef]
21. Cavallaro, L.; Ficara, A.; Curreri, F.; Fiumara, G.; De Meo, P.; Bagdasar, O.; Liotta, A. Graph Comparison and Artificial Models for Simulating Real Criminal Networks. In Proceedings of the Complex Networks & Their Applications IX, Madrid, Spain, 1–3 December 2020; Benito, R., Cherifi, C., Cherifi, H., Moro, E., Rocha, L., Sales-Pardo, M., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 286–297. [CrossRef]
22. Ficara, A.; Curreri, F.; Cavallaro, L.; De Meo, P.; Fiumara, G.; Bagdasar, O.; Liotta, A. Social network analysis: The use of graph distances to compare artificial and criminal networks. *J. Smart Environ. Green Comput.* **2021**, *1*, 159–172. [CrossRef]
23. Morselli, C.; Roy, J. Brokerage Qualifications In Ringing Operations. *Criminology* **2008**, *46*, 71–98. [CrossRef]
24. Morselli, C.; Petit, K. Law-Enforcement Disruption of a Drug Importation Network. *Glob. Crime* **2007**, *8*, 109–130. [CrossRef]
25. Johnsen, J.W.; Franke, K. Identifying Central Individuals in Organised Criminal Groups and Underground Marketplaces. In Proceedings of the Computational Science—ICCS 2018, Wuxi, China, 11–13 June 2018; Shi, Y., Fu, H., Tian, Y., Krzhizhanovskaya, V.V., Lees, M.H., Dongarra, J., Sloot, P.M.A., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 379–386.
26. Calderoni, F.; Catanese, S.; De Meo, P.; Ficara, A.; Fiumara, G. Robust link prediction in criminal networks: A case study of the Sicilian Mafia. *Expert Syst. Appl.* **2020**, *161*, 113666. [CrossRef]
27. Natarajan, M. Understanding the structure of a drug trafficking organization: A conversational analysis. *Crime Prev. Stud.* **2000**, *11*, 273–298.
28. Calderoni, F. The structure of drug trafficking mafias: The 'Ndrangheta and cocaine. *Crime Law Soc. Chang.* **2012**, *58*, 321–349. [CrossRef]
29. Bright, D.; Hughes, C.; Chalmers, J. Illuminating dark networks: A social network analysis of an Australian drug trafficking syndicate. *Crime Law Soc. Chang.* **2011**, *57*, 151–176. [CrossRef]
30. Morselli, C. *Contacts, Opportunities, and Criminal Enterprise*; University of Toronto Press: Toronto, ON, Canada, 2005.
31. Malm, A.; Bichler, G.; Walle, S. Comparing the ties that bind criminal networks: Is blood thicker than water? *Secur. J.* **2010**, *23*, 52–74. [CrossRef]
32. Malm, A.; Bichler, G. Networks of Collaborating Criminals: Assessing the Structural Vulnerability of Drug Markets. *J. Res. Crime Delinq.* **2011**, *48*, 271–297. [CrossRef]
33. Malm, A.; Bichler, G.; Nash, R. Co-offending between criminal enterprise groups. *Glob. Crime* **2011**, *12*, 112–128. [CrossRef]
34. Heber, A. The networks of drug offenders. *Trends Organ. Crime* **2009**, *12*, 1–20. [CrossRef]
35. Asal, V.; Rethemeyer, K. The Nature of the Beast: Organizational Structures and the Lethality of Terrorist Attacks. *J. Politics* **2008**, *70*, 437–449. [CrossRef]
36. Calderoni, F. Social Network Analysis of Organized Criminal Groups. In *Encyclopedia of Criminology and Criminal Justice*; Bruinsma, G., Weisburd, D., Eds.; Springer: New York, NY, USA, 2014; pp. 4972–4981. [CrossRef]
37. Duijn, P.A.C.; Klerks, P. Social Network Analysis Applied to Criminal Networks: Recent Developments in Dutch Law Enforcement. In *Networks and Network Analysis for Defence and Security*; Springer International Publishing: Cham, Switzerland, 2014; pp. 121–159. [CrossRef]
38. Duijn, P.A.C.; Kashirin, V.; Sloot, P.M.A. The Relative Ineffectiveness of Criminal Network Disruption. *Sci. Rep.* **2014**, *4*, 4238. [CrossRef]
39. 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] [PubMed]
40. Fan, C.; Liu, Z.; Lu, X.; Xiu, B.; Chen, Q. An efficient link prediction index for complex military organization. *Phys. A Stat. Mech. Appl.* **2017**, *469*, 572–587. [CrossRef]
41. Lim, M.; Abdullah, A.; Zaman, N.; Supramaniam, M. Hidden Link Prediction in Criminal Networks Using the Deep Reinforcement Learning Technique. *Computers* **2019**, *8*, 8. [CrossRef]
42. Berlusconi, G.; Calderoni, F.; Parolini, N.; Verani, M.; Piccardi, C. Link Prediction in Criminal Networks: A Tool for Criminal Intelligence Analysis. *PLoS ONE* **2016**, *11*, e0154244. [CrossRef] [PubMed]
43. McGloin, J.M.; Kirk, D.S. Social Network Analysis. In *Handbook of Quantitative Criminology*; Piquero, A.R., Weisburd, D., Eds.; Springer: New York, NY, USA, 2010; pp. 209–224. [CrossRef]
44. Carrington, P.J. Crime and social network analysis. In *SAGE Handbook of Social Network Analysis*; Scott, J., Carrington, P.J., Eds.; SAGE Publications Ltd.: Thousand Oaks, CA, USA, 2011; pp. 236–255.
45. Haynie, D.L.; Soller, B. Network Analysis in Criminology. In *Encyclopedia of Criminology and Criminal Justice*; Bruinsma, G., Weisburd, D., Eds.; Springer: New York, NY, USA, 2014; pp. 3265–3275. [CrossRef]
46. Piquette, J.C.; Smith, C.M.; Papachristos, A.V. Social Network Analysis of Urban Street Gangs. In *Encyclopedia of Criminology and Criminal Justice*; Bruinsma, G., Weisburd, D., Eds.; Springer: New York, NY, USA, 2014; pp. 4981–4991. [CrossRef]
47. Bichler, G.; Malm, A. *Disrupting Criminal Networks: Network Analysis in Crime Prevention*; Crime Prevention Studies; FirstForum-Press, Incorporated: Boulder, CO, USA, 2015.
48. Duijn, P.A.C.; Sloot, P.M.A. From data to disruption. *Digit. Investig.* **2015**, *15*, 39–45. [CrossRef]
49. Bouchard, M.; Ouellet, F. Is small beautiful? The link between risks and size in illegal drug markets. *Glob. Crime* **2011**, *12*, 70–86. [CrossRef]

50. Rostami, A.; Mondani, H. The Complexity of Crime Network Data: A Case Study of Its Consequences for Crime Control and the Study of Networks. *PLoS ONE* **2015**, *10*, e0119309. [CrossRef]
51. Robinson, D.; Scogings, C. The detection of criminal groups in real-world fused data: Using the graph-mining algorithm "GraphExtract". *Secur. Inform.* **2018**, *7*, 2. [CrossRef]
52. Villani, S.; Mosca, M.; Castiello, M. A virtuous combination of structural and skill analysis to defeat organized crime. *Socio-Econ. Plan. Sci.* **2019**, *65*, 51–65. [CrossRef]
53. Ficara, A.; Cavallaro, L.; De Meo, P.; Fiumara, G.; Catanese, S.; Bagdasar, O.; Liotta, A. Social Network Analysis of Sicilian Mafia Interconnections. In *Complex Networks and Their Applications VIII*; Cherifi, H., Gaito, S., Mendes, J.F., Moro, E., Rocha, L.M., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 440–450. [CrossRef]
54. Rothenberg, R. From whole cloth: Making up the terrorist network. *Connections* **2002**, *24*, 36–42.
55. Tremblay, P.; Talon, B.; Hurley, D. Body Switching and Related Adaptations in the Resale of Stolen Vehicles. Script Elaborations and Aggregate Crime Learning Curves. *Br. J. Criminol.* **2001**, *41*, 561–579. [CrossRef]
56. Natarajan, M.; Belanger, M. Varieties of Drug Trafficking Organizations: A Typology of Cases Prosecuted in New York City. *J. Drug Issues* **1998**, *28*, 1005–1025. [CrossRef]
57. McGloin, J.M. Policy and Intervention Considerations of a Network Analysis of Street Gangs. *Criminol. Public Policy* **2005**, *4*, 607–635. [CrossRef]
58. Campana, P.; Varese, F. Listening to the wire: Criteria and techniques for the quantitative analysis of phone intercepts. *Trends Organ. Crime* **2012**, *15*, 13–30. [CrossRef]
59. Berlusconi, G. Do all the pieces matter? Assessing the reliability of law enforcement data sources for the network analysis of wire taps. *Glob. Crime* **2013**, *14*, 61–81. [CrossRef]
60. Baker, W.E.; Faulkner, R.R. The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry. *Am. Sociol. Rev.* **1993**, *58*, 837–860. [CrossRef]
61. Charette, Y.; Papachristos, A.V. The network dynamics of co-offending careers. *Soc. Netw.* **2017**, *51*, 3–13. [CrossRef]
62. Goodman, L.A. Snowball Sampling. *Ann. Math. Stat.* **1961**, *32*, 148–170. [CrossRef]
63. Robins, G. *Doing Social Network Research: Network-Based Research Design For Social Scientists*; Sage: Thousand Oaks, CA, USA, 2015.
64. Spapens, T. Interaction between criminal groups and law enforcement: The case of ecstasy in the Netherlands. *Glob. Crime* **2011**, *12*, 19–40. [CrossRef]
65. Mastrobuoni, G.; Patacchini, E. Understanding organized crime networks: Evidence based on federal bureau of narcotics secret files on american mafia. *Carlo Alberto Noteb.* **2010**, *152*, 1–58.
66. Papachristos, A.V.; Smith, C.M. The Small World of Al Capone: The Embedded and Multiplex Nature of Organized Crime. In *Crime and Networks*; Morselli, C., Ed.; Routledge: New York, NY, USA, 2013; pp. 97–115. [CrossRef]
67. Ficara, A.; Cavallaro, L.; Curreri, F.; Fiumara, G.; De Meo, P.; Bagdasar, O.; Song, W.; Liotta, A. Criminal networks analysis in missing data scenarios through graph distances. *PLoS ONE* **2021**, *16*, e0255067. [CrossRef] [PubMed]
68. McDowell, D. *Strategic Intelligence: A Handbook for Practitioners, Managers, And Users*; Scarecrow Press: Lanham, MD, USA, 2008; Volume 5.
69. Reuter, P.; Haaga, J. *The Organization of High-Level Drug Markets: An Exploratory Study*; Rand Santa Monica: Santa Monica, CA, USA, 1989.
70. Campana, P.; Varese, F. Cooperation in criminal organizations: Kinship and violence as credible commitments. *Ration. Soc.* **2013**, *25*, 263–289. [CrossRef]
71. Burcher, M.; Whelan, C. Social network analysis as a tool for criminal intelligence: understanding its potential from the perspectives of intelligence analysts. *Trends Organ. Crime* **2018**, *21*, 278–294. [CrossRef]
72. Murphy, K.P. *Machine Learning: A Probabilistic Perspective*; MIT Press: Cambridge, MA, USA, 2012; Volume 58.
73. Varese, F. The structure of a criminal network examined: The Russian Mafia in Rome. *Oxf. Leg. Stud. Res. Pap.* **2006**, *21*. Available online: https://ssrn.com/abstract=902406 (accessed on 11 July 2022).
74. Chen, H.c.; Chung, W.; Xu, J.J.; Wang, G.A.; Qin, Y.; Chau, M. Crime data mining: A general framework and some examples. *Computer* **2004**, *37*, 50–56. [CrossRef]
75. Athey, N.C.; Bouchard, M. The BALCO scandal: The social structure of a steroid distribution network. *Glob. Crime* **2013**, *14*, 216–237. [CrossRef]
76. Borgatti, S. Identifying Sets of Key Players in a Social Network. *Comput. Math. Organ. Theory* **2006**, *12*, 21–34. [CrossRef]
77. Burcher, M.; Whelan, C. Social network analysis and small group 'dark' networks: An analysis of the London bombers and the problem of 'fuzzy' boundaries. *Glob. Crime* **2015**, *16*, 104–122. [CrossRef]
78. Barabási, A.L.; Pósfai, M. *Network Science*; Cambridge University Press: Cambridge, UK, 2016.
79. Wasserman, S.; Faust, K. *Social Network Analysis: Methods and Applications*; Structural Analysis in the Social Sciences; Cambridge University Press: Cambridge, UK, 1994. [CrossRef]
80. Ficara, A.; Fiumara, G.; De Meo, P.; Liotta, A. Correlations Among Game of Thieves and Other Centrality Measures in Complex Networks. In *Data Science and Internet of Things: Research and Applications at the Intersection of DS and IoT*; Fortino, G., Liotta, A., Gravina, R., Longheu, A., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 43–62. [CrossRef]
81. Freeman, L.C. Centrality in social networks conceptual clarification. *Soc. Netw.* **1978**, *1*, 215–239. [CrossRef]

82. Brandes, U. On variants of shortest-path betweenness centrality and their generic computation. *Soc. Netw.* **2008**, *30*, 136–145. [CrossRef]
83. Krebs, V. Mapping Networks of Terrorist Cells. *Connections* **2002**, *24*, 43–52.
84. Bonacich, P. Power and Centrality: A Family of Measures. *Am. J. Sociol.* **1987**, *92*, 1170–1182. [CrossRef]
85. Page, L.; Brin, S.; Motwani, R.; Winograd, T. *The PageRank Citation Ranking: Bringing Order to the Web*; Technical Report 1999-66; Stanford InfoLab: Stanford, CA, USA, 1999.
86. Katz, L. A new status index derived from sociometric analysis. *Psychometrika* **1953**, *18*, 39–43. [CrossRef]
87. Morone, F.; Makse, H.A. Influence maximization in complex networks through optimal percolation. *Nature* **2015**, *524*, 65–68. [CrossRef]
88. Schwartz, D.; Rouselle, T. Using social network analysis to target criminal networks. *Trends Organ. Crime* **2009**, *12*, 188–207. [CrossRef]
89. de Andrade, R.L.; Rêgo, L.C.; Coelho da Silva, T.L.; de Macêdo, J.A.F.; Silva, W.C.P. Energy disruptive centrality with an application to criminal network. *Commun. Nonlinear Sci. Numer. Simul.* **2021**, *99*, 105834. [CrossRef]
90. Strang, S.J. Network Analysis in Criminal Intelligence. In *Networks and Network Analysis for Defence and Security*; Masys, A.J., Ed.; Springer International Publishing: Cham, Switzerland, 2014; pp. 1–26. [CrossRef]
91. Carley, K.M.; Lee, J.S.; Krackhardt, D. Destabilizing Networks. *Connections* **2001**, *24*, 79–92.
92. Carley, K.M.; Reminga, J.; Borgatti, S. Destabilizing dynamic networks under conditions of uncertainty. In Proceedings of the IEMC '03 Proceedings. Managing Technologically Driven Organizations: The Human Side of Innovation and Change, Cambridge, MA, USA, 30 September–4 October 2003; pp. 121–126.
93. McCarthy, B.; Hagan, J. When Crime Pays: Capital, Competence, and Criminal Success. *Soc. Forces* **2001**, *79*, 1035–1060. [CrossRef]
94. Gottschalk, P. Value configurations in organised crime. *Polic. Soc.* **2009**, *19*, 47–57. [CrossRef]
95. Cornish, D. The Procedural Analysis of Offending and its Relevance for Situational Prevention. In *Crime Prevention Studies*; Criminal Justice Press: New York, NY, USA, 1994; Volume 3, pp. 151–196.
96. Dehghanniri, H.; Borrion, H. Crime scripting: A systematic review. *Eur. J. Criminol.* **2019**, *18*, 504–525. [CrossRef]
97. Brown, R.; Velásquez, A. The effect of violent crime on the human capital accumulation of young adults. *J. Dev. Econ.* **2017**, *127*, 1–12. [CrossRef]
98. Hutchins, C.E.; Benham-Hutchins, M. Hiding in plain sight: Criminal network analysis. *Comput. Math. Organ. Theory* **2010**, *16*, 89–111. [CrossRef]
99. Singh, S.; Verma, S.K.; Tiwari, A. A novel method for destabilization of terrorist network. *Mod. Phys. Lett. B* **2020**, *34*, 2050298. [CrossRef]
100. Farley, J.D. Breaking Al Qaeda Cells: A Mathematical Analysis of Counterterrorism Operations (A Guide for Risk Assessment and Decision Making). *Stud. Confl. Terror.* **2003**, *26*, 399–411. [CrossRef]
101. Ren, X.L.; Gleinig, N.; Helbing, D.; Antulov-Fantulin, N. Generalized network dismantling. *Proc. Natl. Acad. Sci. USA* **2019**, *116*, 6554–6559. [CrossRef] [PubMed]
102. Tostado, S.d.l.M.; Núñez-López, M.; Hernández-Vargas, E.A. Human Trafficking in Mexico: Data sources, Network Analysis and the Limits of Dismantling Strategies. *arXiv* **2022**, arXiv:2206.02971.
103. Bright, D.; Greenhill, C.; Britz, T.; Ritter, A.; Morselli, C. Criminal network vulnerabilities and adaptations. *Glob. Crime* **2017**, *18*, 424–441. [CrossRef]
104. Keeley, B. *Human Capital*; OECD Publications and Information Centre: Paris, France, 2007; p. 150. [CrossRef]
105. Robins, G. Understanding individual behaviors within covert networks: The interplay of individual qualities, psychological predispositions, and network effects. *Trends Organ. Crime* **2009**, *12*, 166–187. [CrossRef]
106. Klerks, P. The Network Paradigm Applied to Criminal Organisations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands. *Connections* **2003**, *24*, 53–65.
107. Bruinsma, G.; Bernasco, W. Criminal groups and transnational illegal markets. *Crime Law Soc. Chang.* **2004**, *41*, 79–94. [CrossRef]
108. Cloward, R.A.; Ohlin, L.E. *Delinquency and Opportunity: A Theory of Delinquent Gangs*; Free Press Paperback; Free Press: New York, NY, USA, 1966.
109. Levi, M.; Maguire, M. Reducing and preventing organised crime: An evidence-based critique. *Crime Law Soc. Chang.* **2004**, *41*, 397–469. [CrossRef]
110. Chiu, Y.N.; Leclerc, B.; Townsley, M. Crime Script Analysis of Drug Manufacturing In Clandestine Laboratories: Implications for Prevention. *Br. J. Criminol.* **2011**, *51*, 355–374. [CrossRef]
111. Haas, T.C.; Ferreira, S.M. Combating Rhino Horn Trafficking: The Need to Disrupt Criminal Networks. *PLoS ONE* **2016**, *11*, e0167040. [CrossRef] [PubMed]
112. Lochner, L. Education, work, and crime: A human capital approach. *Int. Econ. Rev.* **2004**, *45*, 811–843. [CrossRef]
113. Huang, C.C.; Laing, D.; Wang, P. Crime and poverty: A search-theoretic approach. *Int. Econ. Rev.* **2004**, *45*, 909–938. [CrossRef]
114. Mocan, N.; Billups, S.C.; Overland, J. A Dynamic Model of Differential Human Capital and Criminal Activity. *Economica* **2005**, *72*, 655–681. [CrossRef]
115. Coniglio, N.D.; Celi, G.; Scagliusi, C. *Organized Crime, Migration and Human Capital Formation: Evidence from the South of Italy*; Technical Report; Dipartimento di Economia e Finanza—Università degli Studi di Bari "Aldo Moro": Bari, Italy, 2010.

116. Aizer, A.; Doyle, J.J.J. Juvenile Incarceration, Human Capital, and Future Crime: Evidence from Randomly Assigned Judges. *Q. J. Econ.* **2015**, *130*, 759–803. [CrossRef]
117. Coleman, J.S. *Foundations of Social Theory*; Belknap Press, Harvard University: Cambridge, MA, USA, 1990.
118. Natarajan, M. Understanding the Structure of a Large Heroin Distribution Network: A Quantitative Analysis of Qualitative Data. *J. Quant. Criminol.* **2006**, *22*, 171–192. [CrossRef]
119. Bouchard, M.; Malm, A. *Social Network Analysis and Its Contribution to Research on Crime and Criminal Justice*; Oxford Handbooks Online: Oxford, UK, 2016. [CrossRef]
120. Bouchard, M. Collaboration and Boundaries in Organized Crime: A Network Perspective. *Crime Justice* **2020**, *49*, 425–469. [CrossRef]
121. Burcher, M. Social Network Analysis and Crime Intelligence. In *Social Network Analysis and Law Enforcement: Applications for Intelligence Analysis*; Springer International Publishing: Cham, Switzerland, 2020; pp. 65–93. [CrossRef]
122. Ficara, A.; Fiumara, G.; De Meo, P.; Catanese, S. Multilayer Network Analysis: The Identification of Key Actors in a Sicilian Mafia Operation. In *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*; Perakovic, D., Knapcikova, L., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 1–15. [CrossRef]
123. Lin, N.; Cook, K.; Burt, R.S. *Social Capital: Theory and Research*; Sociology and Economics: Controversy and Integration: An Aldine de Gruyter Series of Texts and Monographs; Transaction Publishers: Piscataway, NJ, USA, 2001.
124. Ficara, A.; Fiumara, G.; De Meo, P.; Liotta, A. Correlation analysis of node and edge centrality measures in artificial complex networks. In *Sixth International Congress on Information and Communication Technology*; Yang, X.S., Sherratt, S., Dey, N., Joshi, A., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 901–908. [CrossRef]
125. Peterson, M.B. *Applications in Criminal Analysis: A Sourcebook*; Greenwood Press: Westport, CT, USA, 1994.
126. Cavallaro, L.; Ficara, A.; De Meo, P.; Fiumara, G.; Catanese, S.; Bagdasar, O.; Song, W.; Liotta, A. *Criminal Network: The Sicilian Mafia. "Montagna Operation"*; Zenodo: Meyrin, Switzerland, 2020. [CrossRef]
127. Burt, R.S.; Jannotta, J.E.; Mahoney, J.T. Personality correlates of structural holes. *Soc. Netw.* **1998**, *20*, 63–87. [CrossRef]
128. Burt, R.S. *Brokerage and Closure: An Introduction to Social Capital*; Clarendon Lectures in Management Studies; Oxford University Press: Oxford, UK, 2007.
129. Morselli, C. Assessing Vulnerable and Strategic Positions in a Criminal Network. *J. Contemp. Crim. Justice* **2010**, *26*, 382–392. [CrossRef]
130. Morselli, C. Structuring Mr. Nice: Entrepreneurial opportunities and brokerage positioning in the cannabis trade. *Crime Law Soc. Chang.* **2001**, *35*, 203–244. [CrossRef]
131. Schwartz, D.; Rouselle, T. Targeting Criminal Networks: Using Social Network Analysis To Develop Enforcement and Intelligence Priorities. *IALEIA J.* **2008**, *18*, 18–43.
132. Anggraini, D.; Madenda, S.; Wibowo, E.P.; Boumedjout, L. Network Disintegration in Criminal Network. In Proceedings of the 2015 11th International Conference on Signal-Image Technology Internet-Based Systems (SITIS), Bangkok, Thailand, 23–27 November 2015; pp. 192–199. [CrossRef]
133. Bright, D. Identifying Key Actors in Drug Trafficking Networks. *Disrupting Crim. Netw. Netw. Anal. Crime Prev.* **2015**, *28*, 67–88.
134. Joffres, K.; Bouchard, M. Vulnerabilities in online child exploitation networks. *Disrupting Crim. Netw. Netw. Anal. Crime Prev.* **2015**, *28*, 153–175.
135. Décary-Hétu, D.; Laferrière, D. Discrediting vendors in online criminal markets. *Disrupting Crim. Netw. Netw. Anal. Crime Prev.* **2015**, *28*, 129–152.
136. Berlusconi, G. Social Network Analysis and Crime Prevention. In *Crime Prevention in the 21st Century: Insightful Approaches for Crime Prevention Initiatives*; LeClerc, B., Savona, E.U., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 129–141. [CrossRef]
137. Bright, D.; Greenhill, C.; Levenkova, N. Dismantling Criminal Networks: Can Node Attributes Play a Role? In *Crime and Networks*; Morselli, C., Ed.; Routledge: London, UK, 2013, pp. 148–162. [CrossRef]
138. Ayling, J. Criminal organizations and resilience. *Int. J. Law Crime Justice* **2009**, *37*, 182–196. [CrossRef]
139. Musciotto, F.; Miccichè, S. Effective strategies for targeted attacks to the network of Cosa Nostra affiliates. *EPJ Data Sci.* **2022**, *11*, 11. [CrossRef]
140. Xu, J.; Marshall, B.; Kaza, S.; Chen, H. Analyzing and Visualizing Criminal Network Dynamics: A Case Study. In *Intelligence and Security Informatics*; Chen, H., Moore, R., Zeng, D.D., Leavitt, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 359–377.
141. Xu, J.; Chen, H. Criminal Network Analysis and Visualization. *Commun. ACM* **2005**, *48*, 100–107. [CrossRef]
142. McAndrew, D. The structural analysis of criminal networks. In *Social Psychology of Crime: Groups, Teams, and Networks*; Ashgate Publishing: Aldershot, UK, 1999; pp. 53–94.
143. Hussain, D.M.A. Destabilization of terrorist networks through argument driven hypothesis model. *J. Softw.* **2007**, *2*, 22–29. [CrossRef]
144. Fellman, P.V. The Complexity of Terrorist Networks. In Proceedings of the 2008 12th International Conference Information Visualisation, London, UK, 9–11 July 2008; pp. 338–340. [CrossRef]
145. Mac Ginty, R. Social network analysis and counterinsurgency: A counterproductive strategy? *Crit. Stud. Terror.* **2010**, *3*, 209–226. [CrossRef]

146. Petersen, R.R.; Rhodes, C.J.; Wiil, U.K. Node Removal in Criminal Networks. In Proceedings of the 2011 European Intelligence and Security Informatics Conference, Athens, Greece, 12–14 September 2011; pp. 360–365. [CrossRef]
147. Rodríguez, J.A. *The March 11th Terrorist Network: In Its Weakness Lies Its Strength*; Departament de Sociologia i Anàlisi de les Organitzacions, Universitat de Barcelona: Barcelona, Spain, 2005.
148. Granovetter, M. The Strength of Weak Ties: A Network Theory Revisited. *Sociol. Theory* **1983**, *1*, 201–233. [CrossRef]
149. Brafman, O.; Beckstrom, R.A. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*; Penguin: New York, NY, USA, 2006.
150. Bush, S.; Bichler, G. Measuring Disruption in Terrorist Communications. In *Disrupting Criminal Networks: Network Analysis in Crime Prevention*; Lynne Rienner Publishers: Boulder, CO, USA, 2015; pp. 177–207.
151. Eiselt, H.A.; Bhadury, J. The use of structures in communication networks to track membership in terrorist groups. *J. Terror. Res.* **2015**, *6*, 1–18. [CrossRef]
152. Eiselt, H.A. Destabilization of terrorist networks. *Chaos Solitons Fractals* **2018**, *108*, 111–118. [CrossRef]
153. Tsvetovat, M.; Carley, K.M. Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence. *JoSS Artic.* **2005**, *6*. [CrossRef]
154. Burt, R.S. *Structural Holes: The Social Structure of Competition*; Harvard University Press: Cambridge, MA, USA, 1992.
155. Freeman, L.C. A Set of Measures of Centrality Based on Betweenness. *Sociometry* **1977**, *40*, 35–41. [CrossRef]
156. Gould, R.V.; Fernandez, R.M. Structures of Mediation: A Formal Approach to Brokerage in Transaction Networks. *Sociol. Methodol.* **1989**, *19*, 89–126. [CrossRef]
157. Spapens, T. Macro Networks, Collectives, and Business Processes: An Integrated Approach to Organized Crime. *Eur. J. Crime, Crim. Law Crim. Justice* **2010**, *18*, 185–215. [CrossRef]
158. Nguyen, H.; Bouchard, M. Need, Connections, or Competence? Criminal Achievement among Adolescent Offenders. *Justice Q.* **2013**, *30*, 44–83. [CrossRef]
159. Ficara, A.; Curreri, F.; Fiumara, G.; De Meo, P. Human and social capital strategies for Mafia network disruption. *IEEE Trans. Inform. Forensics Secur.* 2022, *under review*.
160. Norris, F.H.; Stevens, S.P.; Pfefferbaum, B.; Wyche, K.F.; Pfefferbaum, R.L. Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness. *Am. J. Community Psychol.* **2008**, *41*, 127–150. [CrossRef] [PubMed]
161. Bouchard, M. On the Resilience of Illegal Drug Markets. *Glob. Crime* **2007**, *8*, 325–344. [CrossRef]
162. Morselli, C.; Giguère, C.; Petit, K. The efficiency/security tradeoff in criminal networks. *Soc. Netw.* **2007**, *29*, 143–153. [CrossRef]
163. Williams, P. Transnational criminal networks. *Netw. Netw. Future Terror. Crime Militancy* **2001**, *1382*, 61.
164. Kenney, M. *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation*; Penn State University Press: University Park, PA, USA, 2007.
165. Munro, P. People smuggling and the resilience of criminal networks in Indonesia. *J. Polic. Intell. Count. Terror.* **2011**, *6*, 40–50. [CrossRef]
166. Lauchs, M.; Keast, R.; Chamberlain, D. Resilience of a corrupt police network: The first and second jokes in Queensland. *Crime Law Soc. Chang.* **2012**, *57*, 195–207. [CrossRef]
167. Ayling, J. What Sustains Wildlife Crime? Rhino Horn Trading and the Resilience of Criminal Networks. *J. Int. Wildl. Law Policy* **2013**, *16*, 57–80. [CrossRef]
168. Catanese, S.; De Meo, P.; Fiumara, G. Resilience in criminal networks. *Atti Accad. Peloritana Pericolanti- Sci. Fis. Mat. Nat.* **2016**, *94*, 1. [CrossRef]
169. 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]
170. Hardy, J.; Bell, P. Resilience in sophisticated financial crime networks: A social network analysis of the Madoff Investment Scheme. *Crime Prev. Community Saf.* **2020**, *22*, 223–247. [CrossRef]
171. Oliver, K.; Crossley, N.; Edwards, G.; Koskinen, J.; Everett, M.; Broccatelli, C. *Covert Networks: Structures, Processes and Types*; University of Manchester: Hong Kong, China, 2014; Unpublished manuscript.
172. Holling, C.S. Principles of insect predation. *Annu. Rev. Entomol.* **1961**, *6*, 163–182. [CrossRef]
173. Bonanno, G. Loss, Trauma, and Human Resilience: Have We Underestimated the Human Capacity to Thrive After Extremely Aversive Events? *Am. Psychol.* **2004**, *59*, 20–28. [CrossRef]
174. Kulig, J.C.; Edge, D.S.; Townshend, I.; Lightfoot, N.; Reimer, W. Community Resiliency: Emerging Theoretical Insights. *J. Community Psychol.* **2013**, *41*, 758–775. [CrossRef]
175. Adger, N. Social and ecological resilience: Are they related? *Prog. Hum. Geogr.* **2000**, *24*, 347–364. [CrossRef]
176. Bodin, P.; Wiman, B. Resilience and Other Stability Concepts in Ecology: Notes on their Origin, Validity, and Usefulness. *ESS Bull.* **2004**, *2*, 33–43.
177. Pfefferbaum, B.J.; Reissman, D.B.; Pfefferbaum, R.L.; Klomp, R.W.; Gurwitch, R.H. Building Resilience to Mass Trauma Events. In *Handbook of Injury and Violence Prevention*; Doll, L.S., Bonzo, S.E., Sleet, D.A., Mercy, J.A., Eds.; Springer: Boston, MA, USA, 2007; pp. 347–358. [CrossRef]
178. Handmer, J.W.; Dovers, S.R. A Typology of Resilience: Rethinking Institutions for Sustainable Development. *Ind. Environ. Crisis Q.* **1996**, *9*, 482–511. [CrossRef]

179. Lengnick-Hall, C.A.; Beck, T.E. Adaptive Fit Versus Robust Transformation: How Organizations Respond to Environmental Change. *J. Manag.* **2005**, *31*, 738–757. [CrossRef]
180. Kleemans, E.; van de Bunt, H. The social embeddedness of organized crime. *Transnatl. Organ. Crime* **1999**, *1999*, 19–36.
181. Raab, J. Dark Networks as Problems. *J. Public Adm. Res. Theory* **2003**, *13*, 413–439. [CrossRef]
182. Luers, A.L.; Lobell, D.B.; Sklar, L.S.; Addams, C.L.; Matson, P.A. A method for quantifying vulnerability, applied to the agricultural system of the Yaqui Valley, Mexico. *Glob. Environ. Chang.* **2003**, *13*, 255–267. [CrossRef]
183. Gunderson, L.H.; Holling, C.S. *Panarchy: Understanding Transformations in Human and Natural Systems*; Island Press: Washington, DC, USA, 2001.
184. Milward, H.B.; Raab, J. Dark Networks as Organizational Problems: Elements of a Theory. *Int. Public Manag. J.* **2006**, *9*, 333–360. [CrossRef]
185. Dodds, P.S.; Watts, D.J.; Sabel, C.F. Information exchange and the robustness of organizational networks. *Proc. Natl. Acad. Sci. USA* **2003**, *100*, 12516–12521. [CrossRef]
186. Paoli, L. The paradoxes of organized crime. *Crime Law Soc. Chang.* **2002**, *37*, 51–97. [CrossRef]
187. Cunha, M.; Vieira da Cunha, J. Toward a complexity theory of strategy. *Manag. Decis.* **2006**, *44*, 839–850. [CrossRef]
188. Sparrow, M.K. Network vulnerabilities and strategic intelligence in law enforcement. *Int. J. Intell. Count. Intell.* **1991**, *5*, 255–274. [CrossRef]
189. McCarthy, B.; Hagan, J. Getting into Street Crime: The Structure and Process of Criminal Embeddedness. *Soc. Sci. Res.* **1995**, *24*, 63–95. [CrossRef]
190. Czaplicka, A.; Holyst, J.A.; Sloot, P.M.A. Noise enhances information transfer in hierarchical networks. *Sci. Rep.* **2013**, *3*, 1223. [CrossRef]
191. Lindelauf, R.; Borm, P.; Hamers, H. The influence of secrecy on the communication structure of covert networks. *Soc. Netw.* **2009**, *31*, 126–137. [CrossRef]
192. McCarthy, B.; Hagan, J.; Cohen, L.E. Uncertainty, Cooperation, and Crime: Understanding the Decision to Co-offend. *Soc. Forces* **1998**, *77*, 155–184. [CrossRef]
193. Kleemans, E.R.; de Poot, C.J. Criminal Careers in Organized Crime and Social Opportunity Structure. *Eur. J. Criminol.* **2008**, *5*, 69–98. [CrossRef]
194. Duxbury, S.W.; Haynie, D.L. Criminal network security: An agent-based approach to evaluating network resilience. *Criminology* **2019**, *57*, 314–342. [CrossRef]
195. Keller, J.P.; Desouza, K.C.; Lin, Y. Dismantling terrorist networks: Evaluating strategic options using agent-based modeling. *Technol. Forecast. Soc. Chang.* **2010**, *77*, 1014–1036. [CrossRef]
196. Bakker, R.M.; Raab, J.; Milward, H.B. A preliminary theory of dark network resilience. *J. Policy Anal. Manag.* **2012**, *31*, 33–62. [CrossRef]
197. Everton, S.F.; Cunningham, D. Dark network resilience in a hostile environment: Optimizing centralization and density. *Criminol. Crim. Justice Law Soc.* **2015**, *16*, 1.
198. Diviák, T.; van Nassau, C.S.; Dijkstra, J.K.; Snijders, T.A. Dynamics and disruption: Structural and individual changes in two Dutch Jihadi networks after police interventions. *Soc. Netw.* **2022**, *70*, 364–374. [CrossRef]
199. 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, Paris, France, 25–28 August 2015; ASONAM '15; Association for Computing Machinery: New York, NY, USA, 2015; pp. 1368–1372. [CrossRef]
200. Leuprecht, C.; Aulthouse, A.; Walther, O. The puzzling resilience of transnational organized criminal networks. *Police Pract. Res.* **2016**, *17*, 376–387. [CrossRef]
201. Duxbury, S.W.; Haynie, D.L. The responsiveness of criminal networks to intentional attacks: Disrupting darknet drug trade. *PLoS ONE* **2020**, *15*, e0238019. [CrossRef]
202. 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]
203. Gutfraind, A. Optimizing Topological Cascade Resilience Based on the Structure of Terrorist Networks. *PLoS ONE* **2010**, *5*, e0013448. [CrossRef]
204. Lindelauf, R.; Borm, P.; Hamers, H. Understanding Terrorist Network Topologies and Their Resilience Against Disruption. In *Counterterrorism and Open Source Intelligence*; Wiil, U.K., Ed.; Springer: Vienna, Austria, 2011; pp. 61–72. [CrossRef]