DOI: 10.1478/AAPP.942A1

AAPP | Atti della Accademia Peloritana dei Pericolanti
Classe di Scienze Fisiche, Matematiche e Naturali
ISSN 1825-1242

Vol. 94, No. 2, A1 (2016)

RESILIENCE IN CRIMINAL NETWORKS

SALVATORE CATANESE,[ab] PASQUALE DE MEO,[c] AND GIACOMO FIUMARA [a*]
(communicated by Paolo V. Giaquinta)

ABSTRACT. Resilience identifies the ability of criminal networks to face pressures from law enforcement agencies and rapidly reorganize after perturbations or destabilizing attacks. Apart from environmental considerations, this concept is strongly tied to the topology of criminal networks which, unlike social networks, can be configured as hierarchical, cellular (or modular), flat or, even more frequently, as a combination of them. Resilience has implications in the techniques of investigation of law enforcement agencies especially during the phases of information gathering or planning of police actions. In this paper we review concepts and methods derived from Social Network Analysis and apply them to study the resilience of a criminal network. We also examine the evolution of a criminal network operating in Sicily (Italy), before and after the counter-actions of police agencies. We also show how the resilience of the network originated and the features that enable the dynamical reshaping of the criminal networks so as to continue illegal activities.

1. Introduction

Intelligence and law enforcement agency investigators adopt the term *criminal network* in reference to criminal organizations made up by some individuals interconnected and whose common goal is the execution of crimes aimed at obtaining an economic profit. In a broader sense, a criminal organization consists of various entities: individuals, locations and places, vehicles and weapons, societies and real estates, checking accounts and financial transactions, etc. An in-depth comprehension of the relations and interactions among these entities is of crucial importance in order to uncover and fight criminal activities.

Even if there is a strong difference between the locutions *criminal organization* and *criminal network*, in the following we shall use both as if they were interchangeable. Having in mind the analysis of networks, in fact, the criminal network obtained from investigations about a criminal organization is the only network representation of the organization we can work on and, as a matter of fact, *represents* the criminal organization.

Criminal organizations dynamically change as a consequence of several factors: pressure of competing groups, repressive actions of law enforcement agencies, new business opportunities (Sparrow 1991; Morselli 2008). To survive and prosper, criminal organizations must be sufficiently resilient and adapt to changes deriving from competing illicit activities, legislative interventions, controls of law enforcement agencies all of which may lead to the collapse, the stagnation or the adaptation of the network (Morselli 2008), to the expansion or contraction of criminal traffic (Ayling 2009).

Changes in a criminal network may also originate from internal conflicts: the organization may split up, merge with other groups or undergo a reorganization. The variable effects of the interruption of the network may therefore be understood only by studying its dynamics, such as adaptive complex systems (Sloot, Kampis, and Gulyas 2013).

Criminal networks differ from the social networks in the counterbalance between secrecy and efficiency (Toth *et al.* 2013). On the one hand, illegal activities have to remain concealed to governmental authorities and rival criminal organizations. As a consequence, communications among its members must be reduced to the minimum. On the other hand, to limit the risk of being uncovered during an illegal activity, it is necessary to ensure that communications among its members are highly efficient and trustworthy (Morselli, Giguere, and Petit 2007). Therefore, criminal organizations are constantly trying to keep an equilibrium between efficiency and secrecy with respect to their illegal interests (Baker and Faulkner 1993).

Network Analysis is an empirical tool that can be employed to identify, measure, visualize and analyze connections among people, groups and organizations (Scott 2000). It keeps track of relations among individuals or entities by representing them as nodes and showing the connections among them with lines (edges). Lines may be represented in different manners to show features such as the frequency or the type of relation. Nodes and edges form a network which describes relations among its members and the roles of the nodes: this is, for example, the case of gatekeepers (nodes which control the network), liaisons, core and peripheral members (Sparrow 1991). This way, hidden models of interaction are often discovered and the structure of the underlying connections can emerge (Cross, Borgatti, and Parker 2002). Graphical representations allow to explicitly analyze, although in an empirical way, the topology of the network, identify the weak nodes and suggest proper interventions. Link analysis is focused on methods of constructing criminal networks from database records or textual documents.

The mathematical roots of Network Analysis also provide network metrics able to formally capture dynamics and effective consistency and functioning of the networks. Through Social Network Analysis, the resiliency of a network can be examined by the identification of the central nodes, the availability of other nodes which could replace those central nodes in case of deletion, and those nodes which act as bridges in connecting remote sections of the network (South Bank Brisbane 2005). In this respect, measures such as density (the level of connectivity) and centrality (the level of concentration) also provide important insights about the structural properties of covert networks.

In this paper we describe the evolution of a criminal organization composed of about 500 members whose activity was focused in North Sicily (Italy). As we show in Section **7** our case study criminal network is resilient with respect to internal frictions (or even open internal fights) and law enforcement agencies repressive actions.

2. Related work

The resilience of a network which undergoes the deletion of nodes and/or edges has been studied in a number of scientific areas. The term resilience was first used in physics to illustrate the ability of certain materials to resume their original shape after external strain actions (Norris *et al.* 2008).

Albert, Jeong, and Barabási (2000) studied the effect of node deletion in two example networks: a 6,000-node network representing the topology of the Internet at the level of autonomous systems and a 326,000 - page subset of the World Wide Web. Both the Internet and the World Wide Web have been observed to have degree distributions that are approximately power-law in form (Albert, Jeong, and Barabási 1999; M. Faloutsos, P. Faloutsos, and C. Faloutsos 1999). The authors measured average node-node distance as a function of the number of nodes removed, both for random removal and for progressive removal of the nodes with the highest degrees. In the case of both networks, they found that distance was almost entirely unaffected by random node removal; that is, the networks were highly resilient to this type of removal. On the other hand, the removal of the highest degree nodes had a devastating effect. In this case, average node-node distance increases very sharply with the fraction of nodes removed, and typically only a few percent of nodes need to be removed before destroying almost all communication paths in the network. Albert, Jeong, and Barabási (2000) expressed their results in terms of the failure or sabotage of network nodes. The Internet (and the World Wide Web), they suggest, is highly resilient against the random failure of nodes in the network but highly vulnerable to a deliberate attack on its highest-degree nodes.

Following these studies, many authors have investigated the question of resilience for other networks. In general, the results seem to be consistent with that seen in the Internet and the World Wide Web. Most networks are robust against random node removal but considerably less robust to targeted removal of the highest-degree nodes. Jeong *et al.* (2001) looked at metabolic networks; Dunne, R. J. Williams, and Martinez (2002a,b) investigated food webs; Newman, Forrest, and Balthrop (2002) explored email networks, and a variety of authors studied the resilience of model networks (Callaway *et al.* 2000; Cohen *et al.* 2000).

A particularly comprehensive study of the resilience of both real-world and artificially generated networks has been conducted by Holme *et al.* (2002), who investigated not only node removal but also edges removal. The authors also considered additional strategies for selecting edges and nodes. They compared the impact of node and edge removal on the size of the giant component for four removal strategies: initial degree, initial betweenness, recalculated degree, and recalculated betweenness. In the case of the two former strategies, nodes and edges were removed in order of decreasing initial degree and betweenness. In the case of the two latter strategies, nodes and edges were removed from the network in

decreasing order of degree and betweenness, where these two quantities were recalculated after each removal.

Bouchard (2007) used environmental studies of resilience to develop a 3-point list of characteristics which are useful in determining network resilience: *(i) vulnerability*, referred to the likelihood of damage from a specific type of attack; *(ii) elasticity*, the systems ability to return to its original state after taking damage; and, *(iii)* the *adaptive capacity*, the network's ability to change to reduce its vulnerability.

Brinton Milward and Raab (2006) identified three alternative criteria of resilience: *(i)* the members need to have characteristic traits that support the network; *(ii)* the members have to be able to trust each other; and, *(iii)* the network is more resilient if it has connectivity robustness —the ability to respond and recover from losses of critical nodes.

Ayling (2009) explored the possible sources of resilience of criminal organizations, with particular emphasis on institutionalized gangs. According to this study, the reduction of resistance increases the vulnerability. This can be achieved by shrinking the stability domain of the gang. For example, community support for a gang can be reduced by effectively improving financial and social conditions of the community.

Kenney (2007) presented a comparative study of Colombian drug-smuggling enterprises, terrorist networks, including al Qaeda, and the law enforcement agencies that seek to dismantle them. The analysis revealed that the resilience of the Colombian drug trade and Islamist extremism in wars on drugs and terrorism stems partly from the ability of illicit enterprises to change their activities in response to practical experience and technical information, store this knowledge in practices and procedures, select and retain routines that produce satisfactory results. Traffickers and terrorists learn, building skills, improving practices, and becoming increasingly difficult for state authorities to eliminate.

Recently, Duijn, Kashirin, and Sloot (2014) studied the resilience of criminal networks involved in organized cannabis cultivation.

In criminal networks, internal efficiency is somewhat hindered by secrecy. Therefore, even if a network becomes stronger after a targeted attack, the shortening of the chain of command causes a decrease of secrecy. Interventions of law enforcement agencies during the re-organization of a criminal network have a high chance to provoke a lasting disruption.

An interesting feature of fight against criminal and terrorist network consists in the identification of key players as introduced by Borgatti (2003). They are defined as those nodes whose removal *"would maximally disrupt communication among the remaining nodes"*. The problem of resilience of terrorist network has also been addressed by Spezzano, Subrahmanian, and Mannes (2014). The main idea is that the disruption of a network is efficient only if the key players are targeted and removed. To this purpose the authors developed STONE, a software platform which identifies the key players and suggests their removal. STONE is based on three algorithms which help in identifying: i) the successor of a terrorist, ii) the shape the new network will have after the removal of a group of terrorists, and iii) a set of new terrorists to remove from the new network.

Criminal and terrorist networks are known for their ability to regenerate after targeted attacks. Callahan *et al.* (2012) introduced a new approach: the resilience of a network is reduced by increasing its network-wide centrality (first introduced by Freeman (1979)), namely making it a more centralized organization. The authors introduce the term *shaping* to refer to the modifications that security or law-enforcement agencies have to induce in a network in order to increase its network-wide centrality and therefore make it more fragile to targeted attacks.

3. Resilience in criminal networks

Reducing the resilience of a network increases its vulnerability (Ayling 2009), since resilience is far more important than describing the vulnerability of central nodes or their features. As a matter of fact, the removal of key subjects, such as the most central nodes, does not necessarily imply the damaging or destruction of the network (Brinton Milward and Raab 2006). Resilient networks are flexible and adapt themselves for survival. The adaptation may acquire various forms among which we enumerate the substitution of lost nodes and the reshaping of the network.

Criminal networks develop the capacity of absorbing and tolerate inconveniences and adapt themselves to changes as a consequence of destabilizing or destroying attacks (Duijn, Kashirin, and Sloot 2014). According to various authors, resilience consists of two aspects: the capacity of absorbing and tolerating perturbations, and the ability of adapting, if necessary, to changes deriving from those interruptions (Bouchard 2007; Ayling 2009). The ability of absorbing perturbations depends on the level of redundancy of the criminal network, in the sense of the diversity of the relations among its actors. Redundancy allows network members to fulfill the tasks previously appointed to those members no more belonging to the criminal network as a consequence of action of the law enforcement agencies. Notwithstanding the fact that some relations were broken, the diversity of connections allows the network to keep operating.

Redundancy is also associated to strong ties among the members of the network able to pledge reliable alternative relations (Morselli 2008). Reliable substitutions can often be found within kinship connections, friendship or love affairs. This implies that substitutions often can be found at short distance from the cohesive nucleus. If actors with an essential expertise must be replaced, and if their role is uncommon within the network, it is necessary to find the substitutes outside the criminal network. In this case, non redundant connections become important for finding new associates who will be at greater distance from the reliable criminal nucleus. This principle, according to which non redundant ties within the network offer access to opportunities, resources and information to new members, is called the "strength of weak ties" (Granovetter 1983).

Even if weak ties could turn into new business opportunities, the quest for substitutes exploiting these connections implies serious risks in terms of network security. In fact, criminal networks searching for competent and reliable substitutes could need to cooperate with individuals whose reliability is uncertain. Moreover, this research requires smarter internal and external communication methods, whereas an increased volume of information

flow implies a certain exposure to security risks. In other words, the increase of information flow amplifies the risk of exposing the network as a whole, to contrast action of law enforcement agencies (Lindelauf, Borm, and Hamers 2009).

The capacity of adapting to new risks is the second important aspect of resilience. To adapt and protect the network from this kind of attacks, the flow of information is often managed by dividing the competencies into different subgroups. This means that important information is contained within various clans or organizational cells. This strategy prevents the exposure of the entire network in case a group is discovered and disrupted (P. Williams 2001).

These features make the resilience of criminal networks a paradoxical concept. On the one hand, it depends on redundancy, which is an essential ingredient to find reliable substitutes after the losses due to interruptions or external interventions. On the other hand, it depends on the non-redundancy, in the case of the partition of the flow of information in order to prevent further scans (Duijn, Kashirin, and Sloot 2014). The conclusion is that the resilience of a criminal network is a dynamic concept evolving along the trade-off between efficiency and security which consequently reshapes the structure of the network.

In Figure 1 is shown the possible dynamics of a criminal network as a consequence of both internal and external destabilizing attacks and the possibility of these organizations to resist and adjust to "environmental" changes. The evolution of the network exhibits a cyclic pattern since, after the splitting, an eventual merging of the group may occur, even if new members may adhere to the criminal organization or generational changes may happen.

4. Social Network Analysis tools

In recent years, the academic community working on applications of Social Network Analysis (SNA) to intelligence and study of criminal organizations has been constantly growing. One of the first contributions in this field is due to Sparrow (1991), who focused on the adoption of SNA to identify the vulnerabilities of different types of criminal organizations. He highlighted three key aspects of Criminal Network Analysis (CNA), namely: (i) the importance of SNA in order to analyze information; (ii) the potential of intelligence when applied to the analysis of the networks; and, (iii) the common results obtained from the collaboration of the two sectors. Sparrow also introduced the following definitions: (i) dimension —the Criminal Networks (CNs) may have up to few thousands elements; (ii) incompleteness — criminal or terroristic networks are inevitably incomplete due to the fragmentary or erroneous information available; (iii) undefined borders —it is difficult to determine all the relations of each member; and, (iv) dynamism —new connections necessarily imply an evolution of the structure of the network.

While analyzing criminal networks, detectives must focus on the features of the structure of the organization in order to answer the following questions (Sparrow 1991; McAndrew 1999): Who is central in the network? Which are the subgroups? Which are the models of interaction among subgroups? How does the overall structure of the network look like? The removal of which member(s) would perturb the network the most? How does

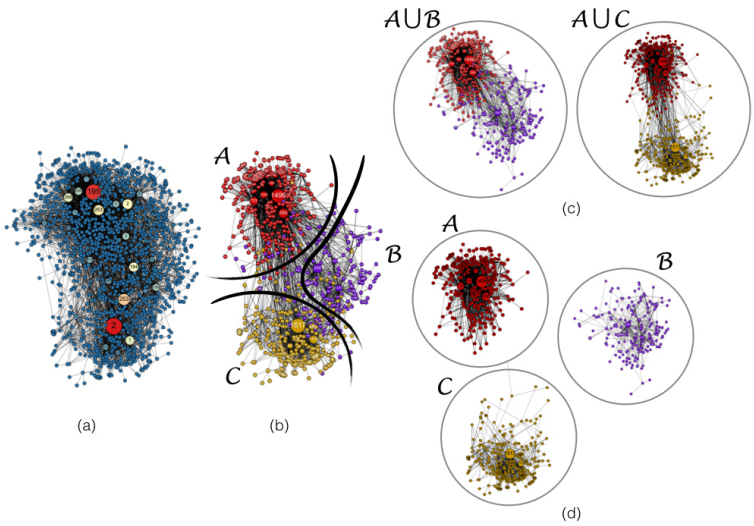

FIGURE 1. Resilience evolution of a criminal network. Figure (a): a criminal network constituted of a single gang; (b) the formation of clusters as a consequence of a destabilizing attack; (c) two possible reorganizations through the merging of distinct clans; and, (d) the splitting to face the attacks of law enforcement agencies.

information flow? The knowledge of these structural features may greatly help in detecting the vulnerabilities of criminal networks and has interesting implications in a criminal investigation.

The removal of central members may effectively dislocate the organization and interrupt the continuation of a criminal activity. Detectives should pay particular attention to subgroups or teams of criminal networks, since each of them may be responsible of specific tasks. Members of the group have to interact and cooperate to accomplish their illicit activities. Therefore, the detection of subgroups whose members are tightly inter-related may increase the comprehension of the CN organization. Groups may interact among them according to some given schemes. For example, members of a clan could frequently interact with those of another clan while seldom interact with the remaining members of the network. The detection of interaction dynamics and relations among subgroups often uncovers crucial information on the overall structure of the criminal network.

Reliable data and refined analysis techniques are crucial to fight criminal networks. Law enforcement and intelligence agencies often have to face the problem of handling large amounts of raw data gathered from various sources, including phone call logs, bank transactions, selling of cars and car registrations, etc. (Sparrow 1991; Canter and Alison 2000).

Mathematical models, along with network representations and metrics, make it possible to gain deeper insights into the actual texture and operation of these types of networks. Social Network Analysis can be used to examine the resilience of a network by analyzing its

vulnerability through the identification of central nodes, the availability of alternate nodes to take the place of lost central nodes, and less-central but bridging nodes tying together remote sections of the network (South Bank Brisbane 2005). Measures such as density (the level of connectivity) and centrality (the level of concentration) also provide important insights into the structural properties of dark networks.

Density is a measure, ranging from 0 to 1, of the number of actual connections compared to the total number of possible connections. The higher the density score, the higher the level of cohesion within a network. A clique network will have maximal density because all actors will be connected with the other actors.

Centrality measures how concentrated a network is: a high concentration indicates that a small number of people control the flow of resources. The centralization score is expressed as a percentage and can vary from 0 (every member is connected to every other member) to 100 (all members are connected to only one member). A high centralization score indicates that some network actors have many more connections than others.

The two most common centrality measures that relate to strategic positions are degree centrality and betweenness centrality (Wasserman and Faust 1994).

The *degree centrality* of a node is defined as the number of edges adjacent to this node. For a directed graph $G = (V, E)$ with n nodes, we can define the in-degree and out-degree centrality measures as

$$C_D(v)_{in} = \frac{d_{in}(v)}{n-1}, \quad C_D(v)_{out} = \frac{d_{out}(v)}{n-1} \tag{1}$$

where $d_{in}(v)$ is the number of incoming edges adjacent to the node v, and $d_{out}(v)$ is the number of the outgoing ones.

Since a node can at most be adjacent to $n-1$ other nodes, $n-1$ is the normalization factor introduced to make the definition independent on the size of the network and to have $0 \leq C_D(v) \leq 1$.

In and out-degree centrality indicates how much activity is going on and the most active members. A node with a high degree can be seen as a hub, an active node and an important communication channel.

Hubs have great influence on the overall structure of the network, and the networks which mainly gravitate around some influential nodes are defined as scale-free networks. The main feature of these networks is the power-law distribution of the degree, which means that only a small fraction of nodes has a large number of connections (Albert, Jeong, and Barabási 2000). Scale-free networks are more resilient against random attacks because the majority of nodes is poorly connected (Watts and Strogatz 1998). For networks with central hubs the removal of peripheral nodes is less significant in terms of its survival. Viceversa, decentralized networks are more influenced by random attacks in which the loss of each member is more important for the rest of the network.

Under focused attacks, scale-free and random networks exhibit opposite resilience and vulnerability than in the case of random attacks: scale-free networks are very sensitive to

focused attacks (Albert, Jeong, and Barabási 2000), whereas random networks are less vulnerable. As central members are more likely to be attacked, centralized networks are more vulnerable to targeted attacks of decentralized ones. The knowledge of the structural features of a network is therefore of crucial importance to fully understand the effects of each intervention.

Betweenness centrality measures the extent to which a particular node lies between other nodes in a network. The core insight of betwenness centrality is that an actor is central if it lies along the shortest paths connecting other pairs of nodes. Highly central actors, like intermediaries, may yield strategic control and influence on other members of the network. An individual with a high betweenness may be a gatekeeper in the network. A gatekeeper criminal should often be targeted for removal because the removal may destabilize a criminal network or even cause it to fall apart (Carley 2006). The betweenness centrality of a node v can be defined as

$$B_C(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{2}$$

where σ_{st} is the number of shortest paths from s to t and $\sigma_{st}(v)$ is the number of shortest paths from s to t that pass through a node v.

Closeness centrality is the inverse of the sum of the shortest paths (geodesics) connecting a particular node to all other nodes in a network. The idea is that an actor is central if it can quickly interact with all the others, not only with its first neighbors (Newman 2005). The notion of closeness is based on the concept of shortest paths (geodesic) $d(u,v)$, the minimum number of edges traversed to get from u to v. The closeness centrality of the node v is defined as

$$C_C(v) = \frac{1}{\sum_{u \in V} d(u,v)}. \tag{3}$$

Such a measure is meaningful for connected graphs only, assuming that $d(u,v)$ may be equal to a finite value. In the context of criminal networks, this measure highlights entities with the minimum distance from the others, allowing them to send and receive information more quickly than anyone else in the organization. For this reason, the adoption of closeness centrality is crucial to highlight those individuals that are closer to others (in terms of communication paths). High values of closeness centrality in this type of communication networks are usually regarded as an indicator of the ability of the given actor to quickly spread information to all other actors of the network.

Eigenvector centrality is another way to assign the centrality to an actor of the network based of the idea that if a node has many central neighbors, it should be central as well. This measure establishes that the importance of a node is determined by the importance of its neighbors.

The eigenvector centrality of a given node v_i is

$$C_E(v_i) \propto \sum_{u \in N_i} A_{ij} C_E(u) \tag{4}$$

where N_i is the neighborhood of the given node v_i, and $x \propto Ax$ that implies $Ax = \lambda x$.

The centrality corresponds to the top eigenvector of the adjacency matrix A. High values of eigenvector centrality are achieved by actors who are connected with high-scoring neighbors, which in turn, inherited such an influence from their high-scoring neighbors, and so on. This measure well reflects an intuitive important feature of communication networks that is the influence diffusion.

Clustering coefficient (transitivity) of a graph measures its degree of connectedness. High clustering coefficients mean the presence of a high number of triangles in the network.

The local clustering coefficient C_i for a node v_i is the number of links among the nodes within its neighborhood divided by the number of links that could possibly exist among them

$$C_i = \frac{|\{e_{jk}\}|}{k_i(k_i-1)} : v_j, v_k \in N_i, e_{jk} \in E \tag{5}$$

where the neighborhood N of a node v_i is defined as

$$N_i = \{v_j : e_{ij} \in E \wedge e_{ji} \in E\}, \tag{6}$$

while $k_i(k_i-1)$ is the number of links that could exist among the nodes within the neighborhood.

It is known from the literature (Wasserman and Faust 1994) that communication networks show high values of clustering coefficient since they reflect the underlying social structure of contacts among friends and acquaintances. Moreover, high values of local clustering coefficient are considered a reliable indicator of nodes whose neighbors are very well connected and among which a substantial amount of information may flow.

Strategies of network disruption based on centrality considerations can be efficient to dismantle centralized or decentralized networks, but the application of this approach to criminal networks has some exceptions (Morselli 2008). In these type of networks, more central members could be at the same time more visible and therefore more detectable. As a consequence, central nodes are vulnerable (Peterson 1998). Furthermore, the most central node is not necessarily the member who holds the leadership. In criminal networks, leadership and centrality are usually detained by different actors; focusing on the central node does not necessarily imply a disruption of the network and the substitution of the leader with a more central member (Carley, Reminga, and Kammneva 1998; Carley 2006).

Studies show that, even if the approach through the centrality measures is useful to identify the potentially critical actors to disrupt the criminal network, a qualitative evaluation at the individual level is essential to understand the effects of the disruption of the network.

5. Network visualization

For all these reasons, a number of visual representation methods has been introduced. The overwhelming majority of these metaphors are variations of sociograms, in which network components are shown as graphic elements and their relations as connection lines (Wasserman and Faust 1994). This representation allows an easy comprehension and provides detailed information about real relations emerging from data.

Graph drawing software platforms have evolved from academic applications to interactive applications. Among various tools designed for visual analysis we mention Prefuse, Pajek, JUNG, Tulip, Visone, shown by Freeman (2000), Klovdahl (1981), and Brandes *et al.* (1999). Some of these tools have been designed to analyze a generic graph. They often combine the node-link layout with standard statistical schemas, such as dispersion graphics and histograms. Although structural visualization are still used, technology succeeded in making graphic effects more and more refined and able to cover other dimensions beyond the structure of the network graph, such as the semantic and temporal dimension, necessary to comprehend social dynamics which allow user to assert hypotheses and validate theoretical and visual inferences (Correa and Ma 2011). In other words, analysis and visualization converge together with the interaction. The traditional analysis preceded by data processing and the visualization as a presentation instrument have been replaced by an interactive approach, in which visualization comprehends raw data and metrics derived from automatic analysis.

Force-directed layout, extensively used in the present work, assimilates the structure of the graph to a physical system, in which nodes are seen as material points subject to forces of various kinds; the coordinates of nodes (and therefore the layout) are calculated to obtain an equilibrium configuration of the modeled physical system (Brandes 2001). A force-directed strategy consists of two main phases: i) *modeling*: starting from the choice of the features to highlight in the layout, a physical model is studied, by assigning attractive/repulsive forces to all pairs of nodes and, eventually force fields independent from nodes; ii) *research of equilibrium configuration*: given the system of forces and starting from an initial configuration in which positions are approximately or randomly fixed, various iterations are needed in order to find a configuration which minimizes the total energy of the system.

6. Mafia

The term *mafia* is usually referred to a particular and specific type of criminal organization. The phenomenon has acquired various forms, albeit with similar structures and codes, different from region to region. In the case study we regard some properties of a criminal organization operating in Sicily and focus on the forms of resilience which allowed to resist every attack coming from institutions, reorganize and systematically strengthen in such a way to influence social, economic and political local life. Notwithstanding the incisiveness of fight conducted by law enforcement agencies, this organization still shows high qualities in terms of regeneration and rearrangement of top positions equilibria even after the capture of the boss and/or of his more close collaborators. This capacity allows *Cosa Nostra* (the Sicilian mafia) to rearrange the areas of competence among the various *families* active in the territory.

One of the most peculiar features of the resilience of *Cosa Nostra* is the so-called apparent appeasement. It is usually a cause of constant and very high attention by magistrates and law enforcement agencies because of the ability of *Cosa Nostra* to change its visibility strategy keeping a low profile and an internal peace status so to maintain the equilibria.

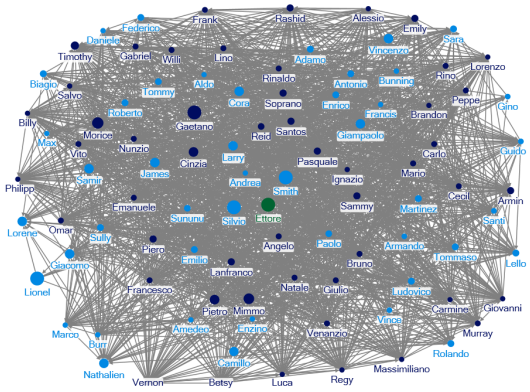

FIGURE 2. A criminal network in the initial phase of an internal fight. The color of nodes is proportional to the deployment of the members of the organization. The dimension of the nodes is proportional to their betweenness centrality. The green node has the highest betweeness centrality.

Network Metric	Value
Network type	undirected
Nodes	543
Edges	3745
Connected comp.	1
Self-Loop	0
Diameter	5
Avg. Geodesic Distance	1.308
Network Density	0.375
Modularity	0.445

TABLE 1. Structural properties of a criminal network

As a background strategy, *Cosa Nostra* pursues the consensus and the mediation as a privileged system to influence sectors of entrepreneurship, finance and public administration, specially in the context of public works and assignment of public services.

Therefore, prevails a policy of impenetrability which aims at protecting privacy and endurance of the mafioso association to preserve it from further defections, also thanks to the insertion of new type of leaderships having more competencies. This turns out to be one of the principal features of the evolution of the organization: some members have an appropriate cultural profile, some are brokers able to manage a criminal association more and more inclined to mediation and economic and financial infiltration.

In addition to traditional illicit sectors such as extortion and usury which can be regarded as instruments to control the territory, the infiltration in public contracts as well the management of the garbage disposal are important sources of enrichment. They are also functional to gain an approach with entrepreneurs formally unrelated to the criminal environment, since they allow to establish a reciprocity relationship. This way the criminal organization gains the appointment of undeserved advantages together with the possibility of infiltration and influence of various sectors of legal economy.

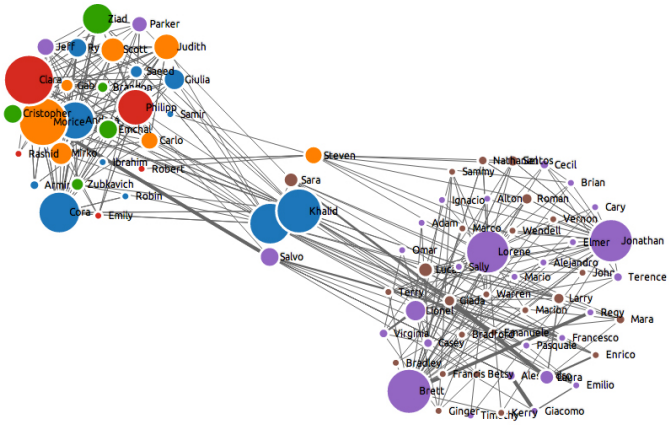

FIGURE 3. A criminal network during an internal struggle for a change at the top of the organization. The visualization layout applies diverging forces to nodes according to the group they belong to, thus resulting in the configuration depicted here. Dimension of nodes is proportional to their degree; color illustrates the criminal environment.

7. A case study

Datasets used in this Section have been built starting from publicly available judiciary documents relative to legal actions against a mafioso criminal organization active in Sicily. For privacy sake, in the following details about places and/or people will be omitted, since final sentences against some members of the organization have not yet been emitted. Information about interpersonal relationships have been integrated with data extracted from Facebook and a certain number of newspaper articles available on the Web.

The criminal organization under consideration, originally composed of more than 500 members, has a pyramidal scheme, the boss being on top. The boss takes advantage of the collaboration of a limited number of counselors, who in turn are in charge of specific tasks. Decisions are taken during secret meetings limited to the members of the directive council.

The initial configuration of the network representing is shown in Table 1 and in Figure 2.

A common feature of criminal organizations is represented by the attractiveness of apical positions, in particular of the boss position. This is particularly evident during interregna, when strong competing instances emerge before a member is appointed as the new boss. Usually, the need of turnover derives from an objective inadequacy of the boss and his action when situations change and may threaten economic incomes.

In the criminal organization whose network we studied, the internal power struggles were bloody but not devastating. Finally, clans recognized the supremacy of the winning part which, in turn, accepted new rules regarding the division of spheres of influence and the obedience to the boss of bosses.

In Figure 3 is shown the criminal network during the climax of the struggle for separation. The two groups show some significant structural differences. Although the group on the left is less numerous than the other, it is denser than the opposite group and it is composed of members more specialized in committing crimes of different types. On the other hand, the group on the right part of Figure 3 is characterized by a lesser number of interactions and it

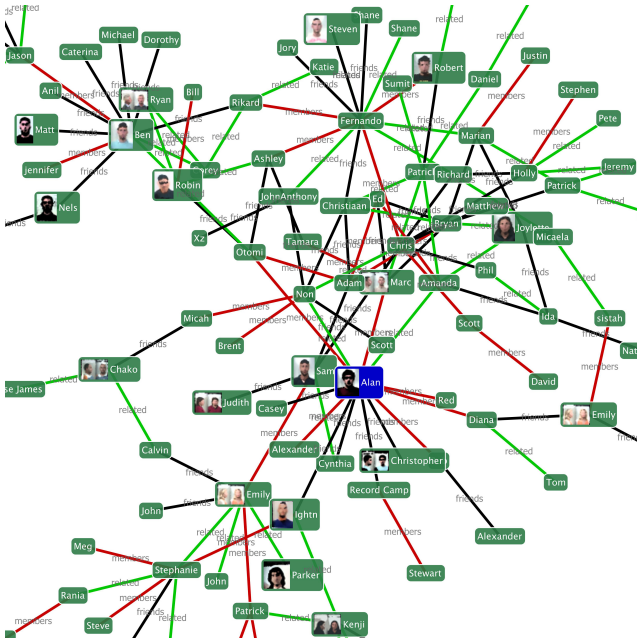

FIGURE 4. Criminal network visualization using a semantic layout. A detail of the central part (core) of the network.

shows less connection and amalgam. Moreover, members of this group are specialized in committing only two type of crimes. Key players shown in the middle of the graph will be subject to a destabilizing attack by the law enforcement agencies.

The intense internal struggle did not completely destroy the criminal network which maintained the control of illicit activities in the territory, even if a new structural configuration was implemented. The areas of competence and the coexistence relations have been strengthen.

The second phase of the study deals with the resilience of the organization to the strategies of attack conducted by the law enforcement agencies starting from the network structure shown in Figure 3.

The investigative phase focused on the so-called key players as they emerged from the transcripts of the court proceedings. Key players are the most important nodes: their rank has been attributed according to their position in the network rather than popularity. Nodes having the highest betweenness centrality have been focused. This strategy is associated to the potential control activity of key players that could be related to the promoters of the association or involve central and bridge actors.

The ability of a criminal network of restoring its structure after a disruptive strategy is based on the retrieval of those connections which were destroyed. It is necessary to find substitutes that may fill the gap left by the removed member (for example because he has been arrested) and that interrupted or destroyed the paths of the network he belonged to. The substitute must be endowed with the same competencies and knowledge of his predecessor. After the replacement of a member with another who is in charge of the same responsibilities, the essential connections are restored and the paths winding through the missing actor are active

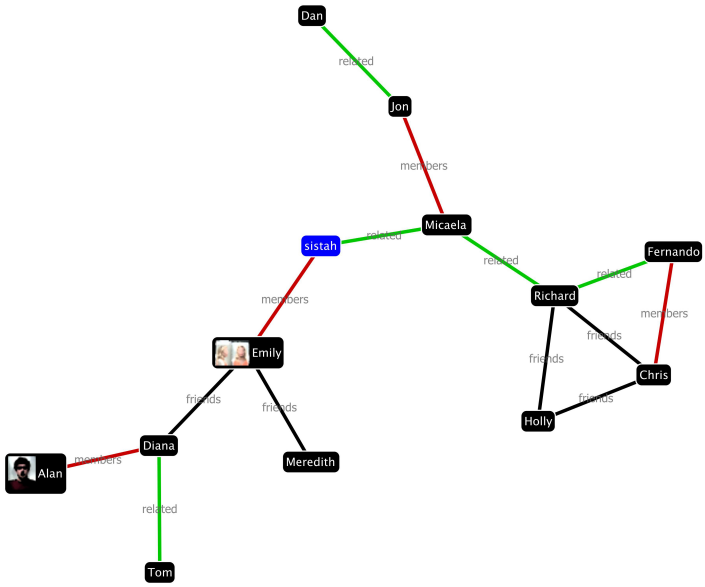

FIGURE 5. Filtered semantic layout

again. As already described in Section **3**, these substitutes are often redundant contacts of the network.

An example can clarify how this process takes place. The software tool we developed for the semantic visualization of the criminal network allows to analyze the relations among the members of the criminal network together with the relations of friendship and kinship every member maintains. In Figure 4 is shown the core of the criminal network. Edges of different colors have been used to represent different relations: i) black for friendship, ii) green for kinship and, iii) red for membership. The type of relation is also visible thanks to labels on the edges. This representation greatly helps in the analysis of the network when a path has been interrupted (for example, as a consequence of the removal of an element). The interaction and the filters allow to detect those links that are redundant or prone to their substitution, as shown in Figure 5.

If, for example, 'Sistha' were arrested, the structure of the organization could be significantly damaged as a consequence of the prestigious position she has. In this case, a possible and fast substitution could be represented by her kin 'Micaela' (who already belongs to the criminal organization). Although the two nodes were already connected through a relation of membership to the criminal network, the redundant links suggest more indications as to the dynamics of structural variations and therefore are very useful for the evaluation of the resilience and, from an investigative point of view, the weak members of the network on which an attack should be concentrated.

8. Conclusions

In this study we tried to unveil the dynamics of resistance of a mafioso-type criminal network as an effect of two different types of interruption. According to different strategies of resilience, it has emerged that notwithstanding strong perturbations, both internal and external, the criminal network succeeded in reconstructing its structure, by reorganizing and accomplishing the necessary substitutions of the missing members.

Large economic incomes, deriving from the criminal activities, sustain criminal networks during the transformation processes giving them the possibility to resist even in situations of large pressure.

Even after important removals, the efficiency of the network seems not to suffer significant effects. On the contrary, it increases over time thanks to strategies of restoring and/or building new paths and reducing the overall dimension of the structure. Results do confirm the powerful organizational structure of mafioso-like criminal associations which are flexible, adaptive, and highly resistant against the most incisive interruptions.

The ability of criminal networks of secretly reorganizing after an attack depends on its flexibility. It is necessary when trustable substitutions are needed within the network. Moreover, non-redundancy may be essential to find substitutions at larger distances, so to maintain secret both roles and information and avoiding to expose the overall organization to an arrest.

Thanks to these strategies of resilience, the network does not expose in the long term, thus avoiding significant perturbations.

Another conclusion that can be drawn from this study is the temporal evolution of a network and its consequences on the study of its resilience. A future study will focus on the resilience along a timeline rather than analyzing a few static snapshots of the network.

References

Albert, R., Jeong, H., and Barabási, A.-L. (1999). "Internet: Diameter of the world-wide web". *Nature* **401**(6749), 130–131. DOI: 10.1038/43601.

Albert, R., Jeong, H., and Barabási, A.-L. (2000). "Error and attack tolerance of complex networks". *Nature* **406**(6794), 378–382. DOI: 10.1038/35019019.

Ayling, J. (2009). "Criminal organizations and resilience". *International Journal of Law, Crime and Justice* **37**(4), 182–196. DOI: 10.1016/j.ijlcj.2009.10.003.

Baker, W. E. and Faulkner, R. R. (1993). "The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry". *American Sociological Review* **58**(6), 837–860. DOI: 10.2307/2095954.

Borgatti, S. P. (2003). "The Key Player Problem". In: *Dynamic social network modeling and analysis: Workshop summary and papers*. National Academies Press, p. 241. DOI: 10.17226/10735.

Bouchard, M. (2007). "On the resilience of illegal drug markets". *Global crime* **8**(4), 325–344. DOI: 10.1080/17440570701739702.

Brandes, U. (2001). "Drawing on Physical Analogies". In: *Drawing Graphs*. Ed. by M. Kaufmann and D. Wagner. Vol. 2025. Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 71–86. DOI: 10.1007/3-540-44969-8_4.

Brandes, U., Kenis, P., Raab, J., Schneider, V., and Wagner, D. (1999). "Explorations into the Visualization of Policy Networks". *Journal of Theoretical Politics* **11**(1), 75–106. DOI: 10.1177/0951692899011001004.

Brinton Milward, H. and Raab, J. (2006). "Dark Networks as Organizational Problems: Elements of a Theory 1". *International Public Management Journal* **9**(3), 333–360. DOI: 10.1080/10967490600899747.

Callahan, D., Shakarian, P., Nielsen, J., and Johnson, A. N. (2012). "Shaping operations to attack robust terror networks". In: *Social Informatics (SocialInformatics), 2012 International Conference on*. IEEE, pp. 13–18. DOI: 10.1109/SocialInformatics.2012.22.

Callaway, D. S., Newman, M. E. J., Strogatz, S. H., and Watts, D. J. (2000). "Network Robustness and Fragility: Percolation on Random Graphs". *Phys. Rev. Lett.* **85**(25), 5468–5471. DOI: 10.1103/PhysRevLett.85.5468.

Canter, D. V. and Alison, L. J. (2000). *The Social Psychology of Crime: Groups, Teams, and Networks*. Offender Profiling Series, Vol. 111. Ashgate.

Carley, K. M., Reminga, J., and Kammneva, N. (1998). "Destabilizing Terrorist Networks". *Institute for Software Research* **45**.

Carley, K. M. (2006). "Destabilization of Covert Networks". *Comput. Math. Organ. Theory* **12**(1), 51–66. DOI: 10.1007/s10588-006-7083-y.

Cohen, R., Erez, K., ben-Avraham, D., and Havlin, S. (2000). "Resilience of the Internet to Random Breakdowns". *Phys. Rev. Lett.* **85** (21), 4626–4628. DOI: 10.1103/PhysRevLett.85.4626.

Correa, C. and Ma, K.-L. (2011). "Visualizing Social Networks". In: *Social Network Data Analytics*. Ed. by C. C. Aggarwal. Springer US, pp. 307–326. DOI: 10.1007/978-1-4419-8462-3.

Cross, R., Borgatti, S. P., and Parker, A. (2002). "Making invisible work visible: Using social network analysis to support strategic collaboration". *California Management Review* **44**(2), 25–46. DOI: 10.2307/41166121.

Duijn, P. A. C., Kashirin, V., and Sloot, P. M. A. (2014). "The Relative Ineffectiveness of Criminal Network Disruption". *Sci. Rep.* **4**, 4238. DOI: 10.1038/srep04238.

Dunne, J. A., Williams, R. J., and Martinez, N. D. (2002a). "Food-web structure and network theory: The role of connectance and size". *Proceedings of the National Academy of Sciences* **99**(20), 12917–12922. DOI: 10.1073/pnas.192407699.

Dunne, J. A., Williams, R. J., and Martinez, N. D. (2002b). "Network structure and biodiversity loss in food webs: robustness increases with connectance". *Ecology Letters* **5**(4), 558–567. DOI: 10.1046/j.1461-0248.2002.00354.x.

Faloutsos, M., Faloutsos, P., and Faloutsos, C. (1999). "On Power-law Relationships of the Internet Topology". *SIGCOMM Comput. Commun. Rev.* **29**(4), 251–262. DOI: 10.1145/316194.316229.

Freeman, L. C. (1979). "Centrality in social networks: conceptual clarification". *Social networks* **1**(3), 215–239. DOI: 10.1016/0378-8733(78)90021-7.

Freeman, L. C. (2000). "Visualizing Social Networks." *Journal of Social Structure* **1**.

Granovetter, M. (1983). "The Strength of Weak Ties: A Network Theory Revisited". *Sociological Theory* **1**(1983), 201–233. DOI: 10.2307/202051.

Holme, P., Kim, B. J., Yoon, C. N., and Han, S. K. (2002). "Attack vulnerability of complex networks". *Phys. Rev. E* **65** (5), 056109. DOI: 10.1103/PhysRevE.65.056109.

Jeong, H., Mason, S. P., Barabási, A.-L., and Oltvai, Z. N. (2001). "Lethality and centrality in protein networks". *Nature* **411**(6833), 41–42. DOI: 10.1038/35075138.

Kenney, M. (2007). *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation*. Pennsylvania State University Press. DOI: 10.1017/S1537592709990156.

Klovdahl, A. S. (1981). "A note on images of networks". *Social Networks* **3**(3), 197–214. DOI: 10.1016/0378-8733(81)90016-2.

Lindelauf, R., Borm, P., and Hamers, H. (2009). "The influence of secrecy on the communication structure of covert networks". *Social Networks* **31**(2), 126–137. DOI: 10.2139/ssrn.1096057.

McAndrew, D. (1999). "The structural analysis of criminal networks". *The Social Psychology of Crime: Groups, Teams, and Networks*, 53–94.

Morselli, C. (2008). *Inside Criminal Networks*. Studies of Organized Crime. Springer. DOI: 10.1007/978-0-387-09526-4.

Morselli, C., Giguere, C., and Petit, K. (2007). "The efficiency/security trade-off in criminal networks". *Social Networks* **29**(1), 143–153. DOI: 10.1016/j.socnet.2006.05.001.

Newman, M. E. J. (2005). "A measure of betweenness centrality based on random walks". *Social Networks* **27**(1), 39–54. DOI: 10.1016/j.socnet.2004.11.009.

Newman, M. E. J., Forrest, S., and Balthrop, J. (2002). "Email networks and the spread of computer viruses". *Phys. Rev. E* **66** (3), 035101. DOI: 10.1103/PhysRevE.66.035101.

Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., and Pfefferbaum, R. L. (2008). "Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness". *Americhe Journal of Community Psychology* **41**(1-2), 127–150. DOI: 10.1007/s10464-007-9156-6.

Peterson, M. B. (1998). *Applications in Criminal Analysis: A Sourcebook*. Praeger.

Scott, J. (2000). *Social Network Analysis: A Handbook*. 2nd ed. Thousand Oaks, CA, US: Sage Publications.

Sloot, P. M. A., Kampis, G., and Gulyas, L. (2013). "Advances in dynamic temporal networks: Understanding the temporal dynamics of complex adaptive networks". *The European Physical Journal Special Topics* **222**(6), 1287–1293. DOI: 10.1140/epjst/e2013-01926-8.

South Bank Brisbane (2005). *The network approach to evaluation: uncovering patterns, possibilities and pitfalls.*

Sparrow, M. K. (1991). "The application of network analysis to criminal intelligence: An assessment of the prospects". *Social Networks* **13**(3), 251–274. DOI: 10.1016/0378-8733(91)90008-H.

Spezzano, F., Subrahmanian, V. S., and Mannes, A. (2014). "Reshaping terrorist networks". *Communications of the ACM* **57**(8), 60–69. DOI: 10.1145/2632661.2632664.

Toth, N., Gulyas, L., Legendi, R. O., Duijn, P., and Sloot, P. M. A. (2013). "The importance of centralities in dark network value chains". *The European Physical Journal Special Topics* **222**(6), 1413–1439. DOI: 10.1140/epjst/e2013-01935-7.

Wasserman, S. and Faust, K. (1994). *Social Network Analysis: Methods and Applications*. Structural Analysis in the Social Sciences. Cambridge University Press. DOI: 10.1017/CBO9780511815478.

Watts, D. J. and Strogatz, S. H. (1998). "Collective dynamics of 'small-world' networks". *Nature* **393**, 440–442. DOI: 10.1038/30918.

Williams, P. (2001). "Transnational Criminal Networks". In: *Networks and Netwars: The Future of Terror, Crime, and Militancy*. RAND Corporation. Chap. 3, pp. 61–98. DOI: 10.1080/00396338.2002.9688556.

[a] Università degli Studi di Messina
Dipartimento di Scienze Matematiche e Informatiche, Scienze Fisiche e Scienze della Terra
Viale F. Stagno D'Alcontres 31, I-98166 Messina, Italy

[b] Università degli Studi di Catania
Dipartimento di Matematica e Informatica
Viale Andrea Doria 6, I-95125 Catania, Italy

[a] Università degli Studi di Messina
Dipartimento di Civiltà Antiche e Moderne
Viale Annunziata - Polo Universitario, I-98168 Messina, Italy

[*] To whom correspondence should be addressed | Email: gfiumara@unime.it

Communicated 5 June 2014; manuscript received 21 October 2014; published online 13 May 2016