Northeast Journal of Complex Systems (NEJCS)

Volume 3
Number 1 *Special Issue: NERCCS 2021 Papers*

Article 1

March 2021

Are Terrorist Networks Just Glorified Criminal Cells?

Elie Alhajjar
USMA, eliealhajjar@gmail.com

Ryan Fameli
College of William & Mary, rkfameli@email.wm.edu

Shane Warren
Missouri State University, shane.t.warren@gmail.com

Recommended Citation

Alhajjar, Elie; Fameli, Ryan; and Warren, Shane (2021) "Are Terrorist Networks Just Glorified Criminal Cells?," *Northeast Journal of Complex Systems (NEJCS)*: Vol. 3 : No. 1 , Article 1.
DOI: 10.22191/nejcs/vol3/iss1/1
Available at: https://orb.binghamton.edu/nejcs/vol3/iss1/1

Are Terrorist Networks Just Glorified Criminal Cells?

Elie Alhajjar, Ryan Fameli, Shane Warren
United States Military Academy (USMA)
Army Cyber Institute (ACI)
West Point, NY 10996

Abstract

The notions of organized crime and terrorism have an old and rich history around the globe. Researchers and practitioners have been studying events and phenomena related to these notions for a long time. There are pointers in the literature in which it is misleading to see the unfair comparison between terrorist and criminal networks with the argument that all actors involved in these networks are simply evil individuals. In this paper, we conduct a systematic study of the operational structure of such networks from a network science perspective. We highlight some of the major differences between them and support our hypothesis with analytical evidence. We hope our work will impact current and future endeavors in counter terrorism, especially within the cyber realm, inside the United States of America and across our allied nations.

1. Introduction

The Federal Bureau of Investigation (FBI) defines organized crime groups as self-perpetuating associations of individuals who operate, wholly or in part, by illegal means and irrespective of geography. They constantly seek to obtain power, influence, and monetary gains. There is no single structure under which these groups function; they vary from hierarchies to clans, networks, and cells, and may evolve into other structures. These groups are typically insular and protect their activities through corruption, violence, international commerce, complex communication mechanisms, and an organizational structure exploiting national boundaries (FBI, 2020).

With few exceptions, criminal groups have economic gain as primary goal, and they employ an array of lawful and illicit schemes to generate profit. Crimes such as drug trafficking, migrant smuggling, human trafficking, money laundering, firearms trafficking, illegal gambling, extortion, counterfeit goods, cultural property smuggling, and cybercrime are keystones within criminal enterprises. The vast sums of money involved can compromise legitimate economies and have a direct impact on governments through the corruption of public officials.

Criminal groups, often called transnational organized crime (TOC) groups, encompass both the Eastern and Western hemispheres and include persons with

ethnic or cultural ties to Europe, Africa, Asia, and the Middle East. These groups, however, are able to target victims and execute their schemes from anywhere in the world; thus, the extent of their presence within a particular area does not necessarily reflect the degree of the threat they pose.

With the increase of technology available around the world, TOC groups are more commonly incorporating cyber techniques into their illicit activities, either committing cybercrimes themselves or using cyber tools to facilitate other unlawful acts. Phishing, Internet auction fraud, and advanced fee fraud schemes allow criminals to target certain countries without being present in the country. Technology also enables TOC groups to engage in traditional criminal activity, such as illegal gambling, but with a greater reach through use of the Internet and offshore servers, thus expanding their global impact.

Criminal groups are engaged in significant criminal activities. According to Title 18 of the United States Code, Section 1961 (1), these activities include: bribery, counterfeiting, embezzlement of union funds, mail fraud, wire fraud, money laundering, obstruction of justice, murder for hire, drug trafficking, prostitution, sexual exploitation of children, alien smuggling, trafficking in counterfeit goods, theft and transportation of stolen property, etc.

There are a lot of transnational organized crime groups worldwide. Geographically, they are mainly classified as African TOC groups, Asian TOC groups, Balkan TOC groups, Eurasian TOC groups, Middle Eastern TOC groups, and Italian TOC groups. The latter ones are probably the most notorious due to their long history since the 1800s; there are four active groups: Cosa Nostra (Sicilian Mafia), Camorra, 'Ndrangheta, and Sacra Corona Unita. They are also known to collaborate with other international organized crime groups from all over the world to carry out their criminal activities.

When it comes to the definition of terrorism, the FBI makes a subtle distinction between international and domestic fronts. On one hand, international terrorism is defined as violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations (state-sponsored). On the other hand, domestic terrorism is defined as violent, criminal acts committed by individuals and/or groups to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature.

Of particular interest to us is the notion of cyber-terrorism as defined by Denning in (Denning, 2000): "Cyber-terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks

that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact."

Terrorists' activities via cyberspace include creating websites/blogs, communication via email, discussion via chat rooms, e-transactions (e-commerce/ e-banking), using search engines to collect data and information, phishing/ hacking, viruses, malicious code, etc. As an example of such activities, we consider the website www.anshar.net created by Noordin Mohammed Top in Indonesia. Established for propaganda purposes, this website published successful terrorist attacks, recruited fellow prospective soldiers, and distributed training material for agents.

Both TOC and terrorist groups are involved in criminal work across the globe, the spectrum of which may vary from an instance to another. They are dubbed the name "networks" in the literature and the media alike. In (Campana, 2016), the author discusses two distinct perspectives on networks, namely a substantive approach that views networks as a distinct form of organization, and an instrumental one that interprets networks as a collection of nodes and attributes.

Given the ongoing relentless effort of the United States Government (USG) in analyzing, understanding, and responding to the terrorist threat, and given the general public's abuse of the term "networks" in daily life, it begs the following question: Are terrorist networks just glorified criminal cells?

This paper addresses the above question from a network science perspective. Network science is an academic field which studies complex networks such as telecommunication networks, computer networks, biological networks, cognitive networks, and social networks. We use publicly available data pertaining to 14 total networks: 8 terrorist networks and 6 criminal networks. All our data are retrieved from the John Jay & ARTIS Transnational Terrorism (JJATT) database (John Jay & ARTIS, 2009). We answer the main question in the negative: namely, we refute the idea that terrorist networks operate like criminal ones by highlighting the structural differences between the two types of organizations. We hope this will lead to a fundamental segregation when dealing with current and future cases.

The remainder of this paper is organized as follows. After this short introduction, we define the basics of graph theory and some tools for the statistical characterization and classification of large networks in the preliminaries section. In Section 3, we review the most relevant and up to date literature that deals with terrorist and criminal networks. Section 4 discusses the details of our methodology for analyzing criminal and terrorist networks separately. We record our findings in the results section and then contrast the main similarities and differences in the discussion section. We conclude the paper with a short summary and future recommendations.

2. Preliminaries

Networks are ubiquitous. The existence of society depends upon a variety of complex networks covering different domains. In the physical realm, they include highways, railroads, the air transportation network, the global shipping network, power grids, water distribution networks, supply networks, global financial networks, telephone systems, and the Internet. In the biological realm, they include genetic expression networks, metabolic networks, ant colonies, food webs, river basins, and the global ecological web of Earth itself. In the social realm, they include governments, businesses, universities, social clubs, churches, school systems, and military organizations. In this section we provide the basic notions and notations needed to describe networks. Needless to say, the expert reader can freely skip this section and use it later as a reference.

The terms *graphs* and *networks* are used indistinctly in the literature. The only nuance is that the term graph usually refers to the abstract mathematical concept of nodes and edges, while the term network refers to real-world objects in which nodes represent entities of some system and edges represent the relationships between them.

We adopt a natural framework for the rigorous mathematical description of networks, namely *graph theory*. Graph theory is a vast field of mathematics that can be traced back to the seminal work of Leonhard Euler in solving the Konigsberg bridges problem in 1736 (West, 1996) and (Agnarsson & Greenlaw, 2007). We will give some formal definitions below. In most of this section, we follow the terminology established in (Newman, 2010) and (Barabasi, 2016) and we encourage the reader to refer to these books for further details on the topic.

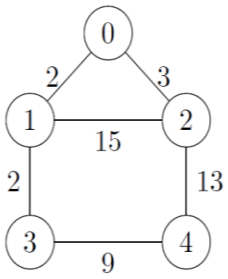
Let $V = \{v_1, v_2, \ldots, v_n\}$ be a finite set of elements and $V \times V$ the set of all ordered pairs $\{v_i,v_j\}$ of elements of V. A relation on the set V is any subset E of $V \times V$. A *simple graph* is a pair $G = (V, E)$, where V is a finite set of *nodes* (or *vertices*) and E is a relation on V such that $\{v_i,v_j\}$ is in E implies that $\{v_j,v_i\}$ is in E and $v_i \neq v_j$, that is G has no loops. The elements of E are called *edges* or *links*, we shall denote them as $E = \{e_1, e_2, \ldots, e_m\}$.

A weighted graph is a quadruple $G = (V, E, W, \varphi)$ where the sets V and E are as above, $W = \{w_1, w_2, \ldots, w_s\}$ is a set of weights (i.e., real numbers) and $\varphi: E \rightarrow W$ is a weight function, that is, a surjective mapping that assigns a weight to each edge. In our work, we assume the weights are natural numbers. This means that if the weight between two nodes is equal to k, then there are k edges joining the two nodes. When the weight of each edge is 1, we call G an *unweighted graph* or simply a graph.

If an edge e joins two nodes v_i and v_j, then we say that v_i and v_j are *adjacent* and they are *incident* to e. The simplest characteristic of a node is its *degree*, which is defined as the number of nodes adjacent to it. The *adjacency matrix* $A = (a_{ij})$ of

a weighted graph G is an n × n array (n being the number of vertices) defined as: $a_{ij} = \varphi(\{v_i,v_j\})$, if $\{v_i,v_j\}$ is in E; and 0 otherwise.

Note that for a simple undirected graph, the adjacency matrix is symmetric and the entries on the main diagonal are all equal to zero. Figure 1 shows an example of a simple graph with 5 vertices along with the corresponding adjacency matrix.



$$\begin{pmatrix} 0 & 2 & 3 & 0 & 0 \\ 2 & 0 & 15 & 2 & 0 \\ 3 & 15 & 0 & 0 & 13 \\ 0 & 2 & 0 & 0 & 9 \\ 0 & 0 & 13 & 9 & 0 \end{pmatrix}$$

Figure 1: A graph and its adjacency matrix

In a graph G = (V, E), a *path* from a node v_i to a node v_j is a collection of ordered vertices $\{v_i, v_{i+1}, \ldots, v_{j-1}, v_j\}$ in V and a collection of ordered edges $\{(v_i,v_{i+1}), (v_{i+1},v_{i+2}), \ldots, (v_{j-1},v_j)\}$ in E. The *length* of a path is the number of edges traversed along the path. A *shortest path*, or a *geodesic path*, from node a v_i to a node v_j is a path of shortest length. A *cycle* is a closed path, i.e., a path in which $v_i = v_j$.

We say that a graph is *connected* if there is a path between any pair of nodes in the graph. A *component* of a graph is a connected subgraph. A *tree* is a connected graph that has no cycles. One can easily derive that for a tree, there is a unique path between any two given nodes. Equivalently, the deletion of any edge breaks a tree into disconnected components. In the case there is a parent node, or *root*, from which the whole tree arises, then it is called a *rooted tree*. The nodes at the bottom that are connected to only one other node are called *leaves*.

The simplest characteristic of a node is its *degree*, which is defined as the number of nodes adjacent to it. For directed graphs, the distinction is made between the *in-degree* and the *out-degree* of a node. The former is the number of edges pointing in the direction of the node, while the latter is the number of edges going out of the node. The *average degree* of an undirected/directed graph is simply the arithmetic mean of the degrees of all nodes.

The *diameter* of a graph G = (V, E) is the maximum shortest path length in G. It simply measures the minimum number of edges needed to connect the two most distant nodes in G. The *average shortest path length* is the average value over all the possible pairs of vertices in the graph. The *density* of a graph is the ratio of the number of edges to the maximum such number, this maximum number being n*(n – 1)/2. We say that a graph is *sparse* if D <<< 1, and *dense* if D ~ 1 (real-world networks are sparse in general).

Let G = (V, E) be an undirected graph. The *degree distribution* p_k is the probability that a randomly chosen node has degree k. Such a distribution plays an important role in the characterization of a network since it provides information about the connectivity and the topology of the underlying graph.

The *clustering coefficient* of a node measures the likelihood that the adjacent vertices to this node are connected to each other. There are two different definitions for the clustering coefficient in the literature, so the comparison of such coefficients among different graphs must use the same measure. The first definition, often referred to as the *local clustering coefficient*, is the ratio of the number of edges between the neighbors of the node and the maximum number of such possible edges. The second definition, often referred to as the *global clustering coefficient*, is the ratio of the number of triangles in the graph (cycles of length 3) to the number of connected triples (paths of length 2).

As a numerical illustration for the non-expert reader, we consider the graph in Figure 1. Recall that G is a graph with five nodes and six edges. The degree of node 1 is 3 since there are 3 edges attached to it. The path 0 – 1 – 3 – 4 is a path between nodes 0 and 4, but the shortest such path is 0 – 2 – 4. The diameter of the graph is 2 since it is possible to get from any node to any other node in 2 steps. The density of the graph is 6/10 = 0.6 since there are 6 edges and the maximum number of possible edges on a graph with 5 vertices is 10. The average degree of the graph is (2+3+3+2+2)/5=2.4 obtained by averaging the degrees of all nodes in the graph.

3. Related work

In the wake of the increase in the number of groups engaging in covert and illegal activities and the threat they pose across the world, social network analysis has emerged as a main tool to examine criminal and terrorist networks. In this section, we pinpoint some of the most recent literature pertaining to the topic at large.

In the paper (Morselli, Giguère, & Petit, 2007), the authors demonstrate that there exists a consistent trade-off facing participants in any criminal network between organizing for efficiency or security, i.e., participants collectively pursue an objective while keeping the action leading to that goal concealed. The distinction is most salient when comparing terrorist with criminal enterprise networks: terrorist networks are ideologically driven, while criminal enterprises pursue monetary ends. Using exploratory research on networks of terrorist cells and electronic surveillance transcripts of a drug importation network, their analyses show how these opposing trade-offs emerge in criminal group structures.

The article (White, Porter, & Mazerolle, 2013) explores patterns of terrorist activity over the period from 2000 through 2010 across three target countries: Indonesia, the Philippines and Thailand. Using self-exciting point process models, the authors create interpretable and replicable metrics for three key terrorism

concepts: risk, resilience and volatility. Analysis of the data shows significant and important differences in these concepts between the three countries. This makes such concepts into benchmark indicators for terrorist activity in a given country.

The authors in (Lantz & Hutchison, 2015) examine the characteristics of the most successful co-offender groups, the relationship between membership in these co-offender groups and individual criminal careers, and the impact of changing network structure, in the form of the arrest of co-offenders, on the criminal careers of connected co-offenders. They find that group participation rate reduces the effects of co-offender group size on group offending span, and that group ties are associated with individual offender persistence.

The research work in (Zech & Gabbay, 2016) emphasizes the importance of relational analysis and provides a variety of concepts, theories, and analytical tools to better understand questions related to militant group behavior and outcomes of terrorism and insurgent violence. The authors investigate how differences in network structure lead to divergent outcomes with respect to political processes such as militant group infighting, their strategic use of violence, or how politically salient variables affect the evolution of militant cooperative networks.

In studying the structural and functional changes in an Australian drug trafficking network across time to determine ways in which such networks form and evolve, the authors in (Bright, Koskinen, Holloway, Steglich, & Stadfeld, 2018) apply a stochastic actor-oriented model to explain the dynamics of the network across time. They find that actors do not seek to create an efficient network that is highly centralized at the expense of security. Rather, actors strive to optimize security through triadic closure, building trust, and protecting themselves and actors in close proximity through the use of brokers that offer access to the rest of the network.

Finally, a study (Ünal, 2019) on five narco-terror and five illicit drug networks in the Turkish context was able to identify and compare their approach to the security-efficiency tradeoff. Networks from both camps are structurally more efficiency driven; they are denser with more direct ties. Generally clustered into sub-groups attached to networks' cores and peripheries, they reflect coreness, where key players act in pivotal positions with high power, centrality, and brokerage to efficiently control and coordinate network activities.

4. Methodology

Centrality is arguably the most popular operational concept used by social network analysts. Node centrality measures tell us how the nodes within a network are positioned. This section is divided into two parts: first, we give an overview of the main centrality measures used in the literature, then we elaborate on the data sets we employ for our validation process.

By definition, centrality aims to capture the notion of "importance" of a node in a network. There are plenty of centrality measures in the literature and efficient algorithms to compute them for large networks. We will discuss below some of the most commonly used ones.

Perhaps the most natural centrality measure for a node in a network is simply its degree or *degree centrality*, i.e., the number of nodes adjacent to it. Nodes with high degree centrality are those that attract a high concentration of direct connectivity within a network. It is a local indicator of a node's importance and does not take into consideration the global characteristics of the graph.

The *betweenness centrality* measures the extent to which a node lies on paths between other nodes. It introduces the concept that it is not the quantity but the quality of connections that matters more. Said differently, betweenness centrality measures the extent to which a node mediates relationships between other nodes by its position along paths within the network: the greater a node is located along the paths in the network, the higher its betweenness centrality is.

The *eigenvector centrality* measures the influence a node has in the network. It relies on the assumption that some nodes are central because they have a high degree of direct contacts and because these direct contacts are themselves in direct contact with high degree nodes in the same network. In other words, eigenvector centrality measures the extent to which a node is connected to other nodes that are high in degree centrality in the network.

In general, it is very hard to collect data sets pertaining to the criminal and terrorist realms. For our work, we resorted to publicly available data sets of 8 terrorist networks and 6 criminal networks (John Jay & ARTIS, 2009). Below we list these sets and provide some background on them. Note that the number of actors in these networks ranges between 20-50 each. The terrorist networks are:

- *17 November Greece Bombing* data set refers to the 17 November Revolutionary Organization, a Marxist urban guerrilla organization operating in Greece. The data refers to the specific temporal window which runs from 1975 to 2002. During these years, the group has been responsible for several violent acts such as assassinations, kidnappings, and symbolic attacks on government offices.
- *Australian Embassy Bombing, Indonesia, 2004* data set is a time series that treats specific attacks as endpoints and depicts the evolution of relations between individuals indirectly and directly associated with the Australian Embassy bombing.
- *Bali Bombing 2005* data set is a time series that treats specific attacks as endpoints and depicts the evolution of relations between individuals indirectly and directly associated with the 2005 Bali bombing by Jemaah Islamiyah.

- *Christmas Eve Bombings, Indonesia, 2000* data set is a time series that depicts the evolution of relations between individuals indirectly and directly associated with the 2000 Christmas Eve bombing.
- *Hamburg Cell 9/11, 2001* data set is a time series that relates individuals indirectly and directly associated with the sleeper Al Qaeda cell in Hamburg around the time of the 9/11 bombings.
- *Jakarta Bombing 2009* data set is a time series that describes the attack on the JW Marriott and the Ritz-Carlton Hotels in Setiabudi, South Jakarta in 2009.
- *Mali Terrorist Network* data set refers to a terrorist network operating in the Sahel-Sahara region and describes relationships between Islamists and Tuareg rebels during the Malian conflict. The data is extracted from a selection of newspaper articles published between 2010 and 2012.
- *Madrid Train Bombing 2004* data set reflects the simultaneous, coordinated bombings against the Cercanías commuter train system of Madrid, Spain, on the morning of 11 March 2004.

  On the other hand, the criminal networks we study are:
- *Project Caviar* data set is the result of a unique investigation that targeted a network of hashish and cocaine importers operating out of Montréal. The network was targeted between 1994 and 1996 by a tandem investigation uniting the Montréal Police, the Royal Canadian Mounted Police, and other national and regional law-enforcement agencies from various countries.
- *Project Ciel* data set is based on a small drug importation network that was importing liquid hashish from Jamaica to Montréal. This network was targeted by the Royal Canadian Mounted Police and the Montréal Police from May 1996 to June 1997.
- *Cocaine Dealing Natarajan* dataset comes from an investigation into to a large cocaine trafficking organization in New York City.
- *Cocaine Smuggling* data set refers to four groups involved in cocaine trafficking in Spain. Information comes from police wiretapping and meetings registered by police investigations of these criminal organizations between 2007 and 2009.
- *London Gang* data set is about a London-based inner-city street gang, 2005-2009, operating from a social housing estate. Data comes from anonymized police arrest and conviction for all confirmed members of the gang.
- *Montréal Street Gangs* data set was obtained from the Montréal Police's central intelligence base and was used to reconstruct the organization of drug-distribution operations in Montréal North. These operations were targeted during three separate investigations between 2004 and 2007 by the Montréal Police.

There are a handful of techniques in the literature to process intelligence data and make it useful for analysis. For example, in (Alhajjar & Morse, 2020) and (Alhajjar & Russell, 2019), the authors propose a new method for filtering intelligence data related to terrorist networks. The project is based on the idea of "collapsing" the different layered networks induced by several attributes of the agents in question. The resulting network becomes the main object of study and network centrality measures are performed therein.

An important challenge for social network analysts seeking to disrupt dark, covert, or criminal networks through the removal of central participants of various kinds is to address whether a fragment from a newly broken network still contains all the necessary and relevant information and the context is not lost through this operation (Everton, 2012).

Our aim in this paper is to use the repository of centrality measures to highlight the structural differences between the two types of networks: criminal versus terrorist networks. We use the data sets listed previously to showcase these differences in a systematic way. Results and findings are recorded in the next section.

5. Results

In this section, we apply centrality techniques and statistical measures to the 14 networks described in the previous section. The main goal here is two-fold; on one hand, we show the similarities between the different criminal networks even though they do not generally overlap in their operational activities. Likewise, we show the similarities between the different terrorist networks that span multiple geographical territories. On the other hand, we pinpoint the major differences between these two types of networks on a microscopic and macroscopic structural level.

For the sake of brevity, we choose the following measures to compute: the diameter, the average geodesic distance, the density, the average degree, the global clustering coefficient, the average eigenvector centrality, and the maximum betweenness centrality. Table 1 shows the values of these measures for the 8 terrorist networks, while Table 2 shows the corresponding values for the 6 criminal networks.

For a cumulative view, we average all our findings for terrorist and criminal networks separately. The results are shown in Table 3 below, where the reader can easily spot the gap in values between the two types of networks.

For the sake of visualization, Figure 2 depicts a sample of each of the two types of networks in question. Namely, we illustrate the topology of the 17 November Greece Bombing and the Cocaine Smuggling Spain data sets. Nodes represent actors in the network and links represent relationships between them

(kinship, friendship, cooperation, mentorship, etc.). The colors used are merely for visual distinction between the different communities formed therein.

Table 1: Centrality measures for terrorist networks

	Greece Bombing	Australian Embassy Bombing	Bali Bombing	Christmas Eve Bombings	Hamburg Cell 9/11	Jakarta Bombing	Mali Terrorist Network	Madrid Train Bombing
Diameter	4	7	7	7	8	12	7	8
Average Geodesic Distance	1.983	1.860	1.994	2.069	2.077	2.049	2.984	2.202
Density	0.286	0.319	0.256	0.235	0.159	0.101	0.106	0.128
Average Degree	6	8.296	6.667	10.356	5.235	2.714	3.72	6.778
Global Clustering Coefficient	0.529	0.565	0.547	0.545	0.566	0.363	0.394	0.451
Average Eigenvec. Centrality	0.469	0.469	0.409	0.348	0.323	0.236	0.319	0.252
Maximum Betweenness Centrality	0.348	0.276	0.301	0.188	0.176	0.171	0.581	0.169

Table 2: Centrality measures for criminal networks

	Project Caviar	Project Ciel	Cocaine Dealing Natarajan NYC	Cocaine Smuggling Spain	London Gang	Montreal Street gang
Diameter	7	4	11	7	6	4
Average Geodesic Distance	2.655	2.453	2.071	3.308	2.054	2.143
Density	0.034	0.117	0.106	0.073	0.220	0.131
Average Degree	3.727	2.8	2.857	3.647	11.667	4.457
Global Clustering Coefficient	0.123	0.172	0.124	0.274	0.519	0.336
Average Eigenvec. Centrality	0.044	0.176	0.164	0.201	0.405	0.311
Maximum Betweenness Centrality	0.637	0.641	0.887	0.495	0.109	0.211

Table 3: Comparison of average measures

	Terrorist Networks	Criminal Networks
Diameter	7.5	6.5
Average Geodesic Distance	2.152	2.447
Density	0.199	0.114
Average Degree	6.221	4.859
Global Clustering Coefficient	0.495	0.258
Average Eigenvec. Centrality	0.353	0.217
Maximum Betweenness Centrality	0.276	0.497

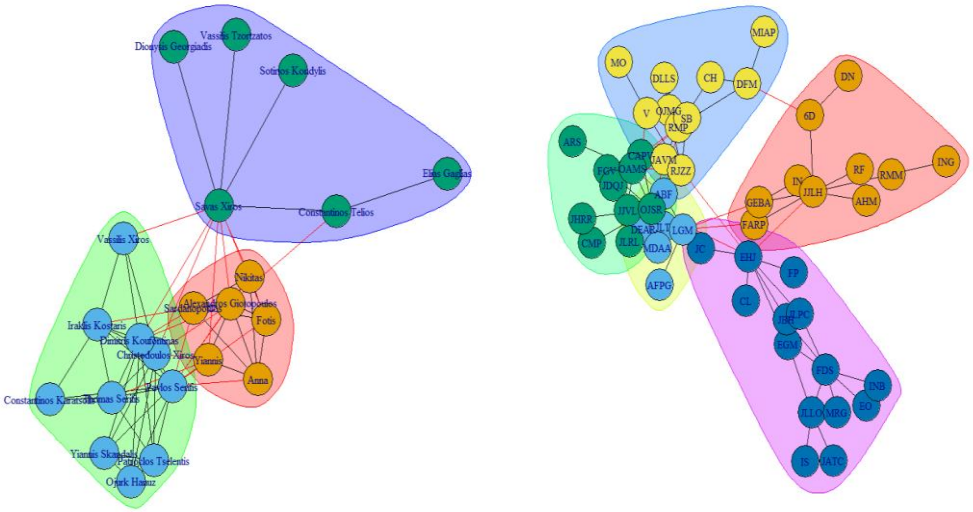


Figure 2: Visualization of the Greece bombing and Spain smuggling networks

6. Discussion

The results highlighted in the previous section hint at a multitude of similarities between networks of the same type, yet a handful of structural differences between terrorist and criminal networks. We aim at identifying these similarities/differences in this section and give a plausible interpretation for their occurrence.

Considered separately, we remark that both terrorist and criminal networks have a more-or-less similar average geodesic distance ranging between 2 and 3.

Also, the density of the networks falls within a small range of values. Recall that the density measures the proportion of edges present in a graph (see the Preliminaries section). Likewise, the global clustering coefficient, the average eigenvector centrality, and the maximum betweenness centrality are comparable within the same type of networks (see Table 1 and Table 2). It is worth mentioning however that the diameter of the networks fluctuates in values between 4 and 12, which is dependent, among other things, on the presence or the absence of low degree nodes (irrelevant actors) in the corresponding networks.

When contrasted with each other on average, the analytical measures on terrorist and criminal networks reveal surprising differences. Among these measures, some are higher in value in terrorist networks and lower in criminal networks, while the remaining ones are the other way around. Table 4 summarizes the comparison between the corresponding values. We provide some fundamental justification regarding this discrepancy:

- Terrorist networks reveal a low average geodesic distance, a high average degree, and a high average eigenvector centrality. This supports the idea that a typical member in terrorist networks maintains a high communication level with other members of the same network, a factor considered crucial in the success of coordinated attacks. The opposite is true for criminal networks, i.e., a low communication level is maintained within a given network which points to a hierarchical structure (tree-like) in the network.
- The density and the global clustering coefficient are higher in terrorist networks than in criminal networks, which indicates that the relationships between actors are tighter in terrorist networks. Moreover, this observation implies that terrorists have a higher tendency to form cliques within their networks.
- The maximum betweenness centrality is remarkably higher in criminal networks. This suggests the presence of one or more focal actors who control the information flow throughout the network, whereas information is spread more evenly within terrorist networks.

7. Conclusion

In this paper, a systematic study between criminal and terrorist networks was carried out from a network science perspective. We employed 14 different data sets from publicly available sources to study structural characteristics of these networks. Based on centrality and statistical analysis, we were able to infer that the two types of networks are indeed not similar in the way they operate and as such, they should not be treated alike in counter efforts.

In summary, each actor in a terrorist network is important and well connected with the rest of the network. Therefore, the actors operate in a tightly

Table 4: Summary of differences between networks

	Terrorist Networks	Criminal Networks
Diameter	High	Low
Average Geodesic Distance	Low	High
Density	High	Low
Average Degree	High	Low
Global Clustering Coefficient	High	Low
Average Eigenvec. Centrality	High	Low
Maximum Betweenness Centrality	Low	High

knit team structure, i.e., in small groups of connected individuals. This fact explains the increasing success rate of highly coordinated attacks by maintaining secrecy and trust between clusters of actors from within the whole network.

On the contrary, low-level actors in a criminal network have little to no influence within the network and rely heavily on their chain of command. Thus, criminal networks exhibit a hierarchical structure in which powerful individuals control the rhythm/flow of the operations and transfer information through multiple layers of less influential actors.

Practitioners dealing with organized crime and terrorist networks have developed views around the activities and causes leading individuals to join such networks. There is a misconception in general that the two types of networks resemble each other, the argument behind this statement being "bad guys are bad regardless of what they do".

Looking back at the original title of our work: *Are Terrorist Networks Just Glorified Criminal Cells?* we hope that we conveyed enough analytical evidence to answer this question in the negative. Namely, our results show that terrorist networks have indeed many structural differences that set them apart from criminal networks. Based on our thorough study, we recommend that counter terrorism efforts take this matter into consideration and treat terrorist cells as "spread out" clusters of actors. We strongly believe that going after the new version of Bin Laden or the new version of Al Baghdadi (whoever they might be) is not the guaranteed effective way to dismantle emerging terrorist groups, since such groups are switching their operations into a decentralized fashion.

Moving forward, covert networks should be viewed as highly clustered networks more so than tree-like structures. Hence, the mindset of the policy makers and the security agencies involved in counter terrorism initiatives should veer from targeting the main actor in a given network and more towards dismantling the set of clusters, whether simultaneously or one cluster at a time.

References

Agnarsson, G., & Greenlaw, R. (2007). *Graph Theory: Modeling, Applications, and Algorithms.* Upper Saddle River, NJ: Pearson Prentice Hall.

Alhajjar, E., & Morse, S. (2020). A Layered Network Collapse Method in Cyber-Terrorism. *Proceedings of the 15th International Conference on Cyber Warfare and Security.* Norfolk, VA.

Alhajjar, E., & Russell, T. (2019). A Case Study of the Noordin Network. *Proceedings of the International Conference on Social Computing, Behavioral-Cultural Modeling, & Prediction and Behavior Representation in Modeling and Simulation.* Washington, DC: Springer.

Barabasi, A. L. (2016). *Network Science.* Cambridge University Press.

Bright, D., Koskinen, J., Holloway, J., Steglich, C., & Stadfeld, C. (2018). Change we can believe in: comparing longitudinal network models on consistency, interpretability and predictive power. *Soc Netw 52*, 180-191.

Campana, P. (2016). Explaining criminal networks: Strategies and potential pitfalls. *Methodological Innovations Volume 9*, 1-10.

Denning, D. (2000). *Cyber-terrorism. Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services.* Washington, DC: US House of Representatives.

Everton, S. (2012). *Disrupting Dark Networks.* New York: Cambridge University Press.

FBI. (2020). *Federal Bureau of Investigation*. Retrieved from FBI: http://www.fbi.gov

John Jay & ARTIS. (2009). Retrieved from John Jay & ARTIS Transnational Terrorism: http://doitapps.jjay.cuny.edu/jjatt/data.php

Lantz, B., & Hutchison, R. (2015). Co-offender ties and the criminal career: the relationship between co-offender group structure and the individual offender. *J Res Crime Delinq 52(5)*, 658-690.

Morselli, C., Giguère, C., & Petit, K. (2007). The efficiency/security trade-off in criminal networks. *Soc Netw 29*, 143-153.

Newman, M. E. (2010). *Networks: An Introduction.* Oxford: Oxford University Press.

Ünal, M. (2019). Do terrorists make a difference in criminal networks? An empirical analysis on illicit drug and narco-terror networks in the prioritization between security and efficiency. *Soc Netw 57,* 1-17.

West, D. B. (1996). *Introduction to Graph Theory.* Upper Saddle River, NJ: Prentice Hall.

White, G., Porter, M., & Mazerolle, L. (2013). Terrorism risk, resilience and volatility: a comparison of terrorism patterns in three southeast Asian countries. *J Quant Criminol 29(2)*, 295-320.

Zech, S., & Gabbay, M. (2016). ocial network analysis in the study of terrorism and insurgency: from organization to politics. *Int Stud Rev 18*, 214-243.