UNIVERSIDADE DE SÃO PAULO
ESCOLA DE ARTES, CIÊNCIAS E HUMANIDADES
PROGRAMA DE PÓS-GRADUAÇÃO EM MODELAGEM DE SISTEMAS COMPLEXOS

LUCAS DA SILVA ALMEIDA

Dark Networks and Corruption: uncovering the offshore industry

São Paulo
2018

LUCAS DA SILVA ALMEIDA

Dark Networks and Corruption: uncovering the offshore industry

corrected version

Dissertation presented to the School of Humanities Arts and Sciences of the University of São Paulo for obtaining the title of Master of Sciences through the Post-graduate Program in Complex Systems Modelling

Concentration:

Applied Social and Ambiental Sciences

Advisor:

Prof. Dr.Andre Cavalcanti Rocha Martins

São Paulo

2018

CATALOGAÇÃO-NA-PUBLICAÇÃO
(Universidade de São Paulo. Escola de Artes, Ciências e Humanidades. Biblioteca)

Almeida, Lucas da Silva
Dark networks and corruption : uncovering the offshore industry / Lucas da Silva Almeida ; orientador, Andre Cavalcanti Rocha Martins. – 2018.
61 p. : il.

Dissertação (Mestrado em Ciências) - Programa de Pós-Graduação em Modelagem de Sistemas Complexos, Escola de Artes, Ciências e Humanidades, Universidade de São Paulo, em 2017.
Versão corrigida.

1. Redes sociais - Simulação; Modelagem. 2. Redes complexas. 3. Dark networks. 4. Corrupção. 5. Políticas públicas. 6. Lavagem de dinheiro. 7. Panama Papers. I. Martins, Andre Cavalcanti Rocha, orient. II. Título

CDD 22.ed.– 303.4833011

Nome:ALMEIDA, Lucas da Silva

Título: Dark Networks and Corruption: uncovering the offshore industry

Dissertation presented to the School of Humanities Arts and Sciences of the University of São Paulo for obtaining the title of Master of Sciences through the Post-graduate Program in Complex Systems Modelling

Concentration:

Applied Social and Ambiental Sciences

Approved in: 19 / 12 / 2017

Dissertation Comitee

Prof. Dr.	Flavia Mori Sarti	Institution:	USP-EACH
Judgement:	Approved	Signed:	_____
Prof. Dr.	Brooke F. Welles	Institution:	Northeastern U.
Judgement:	Approved	Signed:	_____
Prof. Dr.	Thais Gobet Uzun	Institution:	ITA
Judgement:	Approved	Signed:	_____

ABSTRACT

ALMEIDA, Lucas da Silva. **Dark Networks and Corruption:** uncovering the offshore industry . 2017. 50 p. Dissertation (Master of Sciences: Complex Systems Modelling) – School of Arts, Sciences and Humanities, University of São Paulo, São Paulo. Corrected Version.

Among the many social structures that cause inequality, one of the most jarring is on the use of loopholes to both launder money and evade taxation. Such resources fuel the "offshore finance" industry, a multi-billion dollar sector catering to many of those needs. These run under the logic of "Dark Networks" avoiding detection and oversight as much as possible. While there are legitimate uses for offshore services, such as protecting assets from unlawful seizures, they are also a well documented pipeline for money stemming from ilegal activities. These constructs display a high amount of adaptiveness and resilience and the few studies done had to use incomplete information, mostly from local sources of criminal proceedings. This work is to analyzes the network of offshore accounts leaked under the “Panama Papers” report by the International Consortium of Investigative Journalists. This registers the activities of the Mossack Fonseca law firm in Panama, one of the largest in the world on the Offshore field. It spans over 50 years and provide us with one of the most complete overview thus far of how these activities are connected, the topology of such network and what it displays in resilience against attempts to target this scheme

Keywords: Complexity and Public Policy, Complex Networks, Dark Networks, Network Resilience , Money Laundering

RESUMO

ALMEIDA, Lucas da Silva . **Redes Sombrias e Corrupção:** desvendando a industria offshore, 2017. 50 p. Dissertação (Mestrado em Ciências: Modelagem de Sistemas Complexos) – Escola de Artes, Ciências e Humanidades, Universidade de São Paulo, São Paulo, 2017. Versão corrigida.

Dentre as muitas estruturas sociais que causam desigualdades, uma das mais estarrecedoras é o uso de brechas para lavagem de dinheiro e evasão fiscal. Estes recursos sustentam a rede de finanças Offshore, uma industria multi-bilionária que oferece serviços para muitas dessas metas. Estas funcionam na lógicas das Redes Sombrias , evitando detecção e supervisão sempre que possível. Ainda que existam razões legitimas para o uso de serviços offshore, como a proteção de bens contra apropriação indébita, eles são um canal bem documentado para as receitas advindas de atividades ilegais . Este trabalho analisa a rede de contas offshore vazada sob a égide dos “Panama Papers” pelo Consorcio Internacional de Jornalistas Investigativos, que registrou a atividade da firma de advocacia Mossack Fonseca, sediada no Panama e uma das maiores do setor de Offshore. Com mais de 50 anos de registros, é ate o momento nosso panorama mais completo do padrão de conexão destas atividades, da topologia desta rede e do que ela demonstra de resiliência contra tentativas de desmontar esse esquema.

Palavras-chave: Complexidade e Políticas Publicas, Redes Complexas, Redes Sombrias, Resiliência de redes, Lavagem de Dinheiro

LIST OF FIGURES

LIST OF TABLES

SUMMARY

1. Introduction

In the literary series *Diskworld* created by Terry Pratchett, fantastical creatures, wizards and even humans live on a disk-shaped plane, balanced on top of four elephants, themselves standing atop a titanic turtle which traverses the cosmic space. At the plane is located the chaotic metropolis of Ankh-Morphok. The local government, headed by an *"elected despot"* has also a peculiar way of curbing crime: unionization. Both the guild of thieves and the guild of assassins work to make sure robberies and homicides stay below quota and follow the proper bureaucratic protocols, with the unsanctioned robbers being punished with death:

> *"...the modern, properly registered Thieves' Guild makes money mainly by having rich people pay an annual premium, and arrange for a convenient date to rob an acceptable amount from these rich clients in their own home. For the poorer (but not penniless) citizens who do not arrange for premiums and appointments, the Thieves quite politely rob them in the streets, in their business premises, or in their homes, not badly injuring them, and always leaving them a receipt which guarantees that these people will not be inconvenienced with another official robbery for the rest of the year."*
>
> *(Pratchett, 2000)*

This fictitious example, in its absurdity, manages to capture an interesting phenomena observed in reality: the porous boundary that exists between criminal activities and government. Its not unknown to have such arrangements in real life, with at least one being now confirmed by the Brazilian government: and agreement on which the state of São Paulo would guarantee the safety of the heads of the largest criminal organization in the country, the First Criminal Command (from the Portuguese : *Primeiro Comando do Crime - PCC*), which were at the time serving their sentences in state prisons, in exchange for the immediate cease in a wave of attacks. Another example, in the city of Rio de Janeiro, there

are strong ties between drug-trafficking gangs (known as *"the parallel power"* when compared to the state) and local politicians, brokered by churches engaged in social projects at the slums.

The exact scene of the book above has been emulated, literally the*"Red Command"* (Brazil's second largest gang) was prohibiting robberies and killings in their territory (BBC, 2016), as a measure of protection of local citizens. Across the globe, from Mexican cartels to Japanese yakuza, there is a promiscuous and complicated relationship between formal government and the *"dark networks"* that populate and challenge its territory. One of these, that remains woefully under explored by science, is the network of companies and individuals that engage in offshore financial activities. This work will explore what is most complete view of the offshore industry, given in the "*Panama Papers"* data leak.

It started in with the delivery of 2.6 Tb of files to the german newspaper *Suddeutsche Zeitung* (ICIJ, 2016) by an anonymous source. The 11 million files were on the archives of the Mossack Fonseca law firm, a little-known, yet very powerful law firm with branches in 35 countries, specialized in setting up shell companies for offshore banking purposes. There are companies and individuals from every country of the globe, with a time span of over 40 years. A year of investigations by the International Consortium of Investigative Journalists, the informations given were confirmed as true and released to the public.

The Offshore banking industry is a 32 trilllion-dollar business, according to the Tax Justice Network (Henry J. S, 2012), comprised of a true ecosystem of private banks, law firms, compliance consultants, far more complex than the proverbial tax haven :

> *"...private banking has long since become virtual. So the term "offshore" refers not so much to the actual physical location of private assets or liabilities, but to nominal, hyper-portable, multi-jurisdictional, often quite temporary locations of networks of legal and quasi-legal entities and arrangements that manage and control private wealth — always in the interests of those who manage it, supposedly in the interests of its beneficial owners, and often in indifference or outright defiance of the interests and laws of multiple nation states. (Ibid)*

Given their tremendous economic impact, it is surprising how little is known of the industry. Partially, this is due to the lack of data. Even the estimates of the Offshore world size and economic impact are wildly different across parties (Zucman, 2014), and there is essentially no consensus even on what practices (Ibid) configure tax avoidance and, which is legal and within the regular scope of such activities. This refers back to the traditional concept of embeddedness in social networks, since many accounts operate within large and established banks. In a few cases, it has been even used to bypass international sanctions regulations. For the purposes of this work I will adopt the understanding from Donovan, Wagner & Zeume (2017) that the majority of operations in the Panama Papers files represent illegal tax evasion instead of legal tax avoidance given the immense number of investigations and subsequent punishment of individuals and firms involved, implying that authorities had no awareness of these activities.

What this study aims for is a initial graph based analysis of the offshore industry. As far as the author is aware, there have been no preceding studies of this nature. The insights gained could be a baseline for further research or for policy decisions. More so, in order to understand the broad class of phenomena described as “Dark Networks” it is paramount to have the insights from these evasive collectives. It must be noted that given the tremendous volume of data, there will remain many aspects unexplored. I will briefly present the foundations of the the Complex Networks approach as it is used today, which has proven its value in analyzing social networks (Lazer et Al, 2009), as well as an overview of the findings from the subfield of social networks that investigates collectives which attempt to avoid detection, the so called dark networks, before presenting our analysis of the Panama Papers data.

1. Literature Review

1.1. Complex Networks Metrics and Models

The field of complex networks is widely known as one of the main components of complex systems. By treating different entities as graphs it is possible to analyze their characteristics with a common denominator (Amaral et Al, 2004). A brief review of the

fundamentals and techniques used in exploring the dataset will be presented, but it is by no means extensive.

A graph is a mathematical object that consist in nodes (N) and Edges (E), or interactions/connections between those objects (Barabasi, 2016). This simple schemata has been used to analyze successfully the spread of viral diseases (Vespignani, 2006), Email Contacts (Lazer, 2004), and it can result in remarkably complicated structures being described with simple rules, such as the famous models of the scale-free network (Barabasi, 2002) and the small world model (Watts & Strogatz, 2001). Networks can be directed, with the edges being asymmetrical in relation to the pair of nodes, but our treatment will be for the undirected case. One of its earliest applications was in the Erdos-Renyi model which generates graphs based on aleatory attachment of nodes and edges, (Erdos & Renyi, 1960) and could account for some elements in the growth process of networks, yet was very incomplete in describing the characteristics of real connected phenomena.

Much of the power of the network approach is that the topological properties are universal in their power to describe these entities. The first one that is the *degree* of a certain node (k) , which simply states how many links are connected to that node. It can represent the number of bridges connecting to a certain island, or the number of friends an individual has. By definition, the number of neighbours a node has can range from *0* to *N-1* if we do not allow multiple edges between the same two nodes. The total number of edges (E) in the network is the sum of node degrees, corrected for double counting by halving the result.

Equation 1 : Total Number of Edges

$$E = \frac{1}{2}\sum_{i=1}^{N} k_i$$

Its Density, or, how many links vs how many edges exist also gives important information about the object, given that most networks in nature are considerably sparse, for example, when compared to the theoretical upper bound, a complete graph in which every node has the maximum degree possible ($K_{max} = N - 1$) (Barabasi, 2016).

Equation 3: Graph Density

$$D = \frac{2E}{N(N-1)}$$

Normally the most important statistic for summarizing a graph is its degree distribution, of the probability that a randomly selected graph will have a certain degree k. The degree distribution is determinant about many important properties such as the average distance that one node is from another.

Equation 2: Degree Distribution

$$\sum_{k=1}^{\infty} p_k = 1$$

Distances in a network are considered in how many edges and nodes need to be traversed, and the distance between two nodes (without repeating any of them) is called a *path*, with its length being the amount of links hopped to reach its end. The path of least hops between two nodes is called the *shortest path* (or distance) In an undirected network, the shortest path is symmetrical for all pairs of nodes. The longest shortest path in a network is called its *diameter*. The average length of shortest path distances from node *i* to all other nodes on the network is called closeness centrality, first presented by Bavelas (1960). Nodes with high closeness allow "reaching" other nodes in less steps.

Equation 3: Closeness Centrality

$$C_i = \frac{N}{\sum_j D_{i,j}}$$

At the network level, its also relevant to calculate the the average between all pairs of shortest paths is called the average path length $\langle d \rangle$. This measure synthesizes the same information from closeness centrality, but for the entire collection of nodes.

Equation 4: Average Path Length

$$\langle d \rangle = \frac{1}{N(N-1)} \sum_{i,j=1,N;i\neq j} d_{i,j}$$

Another key metric, called betweenness centrality, relates how many of the networks shortest paths pass though a certain node. This is extremely useful to understand how to halt spreading processes or monitor information percolating the network. This measure was first formalized by Freeman (1977), as the sum of geodesic paths between all nodes that pass through node i :

Equation 5: Betweenness Centrality

$$B_i = \sum_{s,t} \frac{n_{s,t}^{i}}{n_{s,t}}$$

Regarding distances in networks, one of the most relevant findings came from the sociometric literature, known as the six degrees of separation phenomena, from the famous experiment by Stanley Milgram (Milgram, 1967) which found that individuals across the United States were approximately six social connections from one randomly selected person. Recently scientists from Facebook repeated the experiment and found that the distance measured had shrunk to an average of three and a half contacts (Backstrom, et al 2011). This brings the counter-intuitive fact that across the billions of individuals on the globe we're approximately three handshakes away from any other person. The small-word phenomena can be explained using graphs, given the presence of a small average path length when compared to total number of nodes (Watts & Strogatz, 2001). More specifically, if the average path length $\langle d \rangle$ which scales as the natural log of the number of nodes over the average degree.

Equation 6: Small world property in a graph

$$\langle d \rangle \approx \frac{\ln N}{\ln \langle k \rangle}$$

One the historical puzzles in network science was the presence of Small-World networks that had a higher clustering coefficient than what should be possible by the random Erdos-Renyi model. The clustering coefficient *(C_i),* is also known as triadic closure from the social sciences literature. This coefficient is a normalized metric of how many of a node's

neighbours connect to each other, as can be seen in Equation 6, with (L_i) being the total number of links between neighbours of (i) , divided the total possible number of links ($k_i(k_i - 1)$). It can represent for example, how many of node (i) friends are friends among themselves, or how many of firm (i) suppliers also are clients of each other.

Equation 7: Clustering Coefficient

$$C_i = \frac{2L_i}{k_i\left(k_i - 1\right)}$$

It is a particularly important factor in the small-world phenomena, since the Random Network model results in networks of low clustering and low average path length. The inadequacy in explaining high clustering in natural networks was one of the problems from the Erdos-Renyi model (Barabasi, 2016) that had a solution presented with with the Watts-Strogatz model. While there was success in explaining the variation in average path lengths and clustering, the degree distribution of real networks remained unaccounted in the models.

The Erdos-Renyi and Watts-Strogatz predicted Poisson degree distributions, yet the real datasets had more nodes of very large degree than what should have been possible, in fact, the statistical distribution that most closely resembled many examples of real data was the Power Law. In the Barabasi-Albert model (Barabasi & Albert, 2002) the preferential attachment follows the degree of a node, or, the more links a node has, the more likely it is to receive a link when a new node is added to the network.

This striking construct result in one of the most famous features of complex networks, the power-law degree distribution, present in a multitude of natural and real world examples (Barabasi, 2016). More so, the persistence of the power law degree distribution can be attributed to the mechanic of "preferential attachment", or pointing that nodes choose their connections instead of randomly making links. This resonates deeply with the literature of social connections in which individuals are known to have homophily, or the trend to connect with those who which there is a shared characteristic or interest.

In order to measure if this preference for connection translates into a changed topology of the network, the methods of community detection were developed. From the recognition that there are intra-networks aggregates, if those aggregates can be reflected in the topological structure through increased density of intra-aggregate links. (Louvain, 2009 ;

Girvan & Newman 2003; Barabasi , 2016). A more detailed example will be given in the data analysis section .

1.2.Dark Networks and Social Networks

The term "Network" has been used in the social sciences with the meaning of "distributed power" (Milward & Raab, 2003) and to denote less hierarchical organizational structures; predominantly horizontal, generally in a positive way, creating a connection to the logic collective action and social movements such as the fights for civil rights; focusing on ties between individuals rather than group-level properties. The founding paper in the field (*Dark Networks as Problems,* Ibid*)*, observes the existence of social network entities whose goal is to avoid detection and how they illustrated a flip side to the usual view of the horizontal social structures. Its also mentioned that those groups, despite their spread across many territorial areas, depend on a base of operations where they can act with the compliance of governmental entities, or at least capturing some agents of government. This observation is especially pertinent as the definition of "*illegal"* varies from country to country, and these organizations spread across borders.

The use of such decentralized organizational structures is always coupled with *"...a way to disseminate information quickly, foster innovation, make large hierarchical organizations more flexible and enhance competitiveness*" (Ibid). More so, the "dark" is defined as in opposition to "bright" networks that would *"...Advance the common good and doest not - at least intentionally - harm people. "* (Ibid). It should be noted in this axis that there is a level of moral judgment in order to classify a network as "dark" and there are conceivable examples of social resistance which are in opposition to authority, yet are done with the goal of social good. There are networks which fill the characteristic of illegal and covert, yet are done with a clear goal of advancing individual freedom, such as the groups that smuggle women outside of ISIS controlled territory, or the historical example of the Underground Railroad and the Suffragettes. While these networks also attempt to avoid detection by outsiders and government agents, and are by definition illegal, they are not the object of study. The dividing line this review uses is whether such groups resort to systematic violence in situations unsanctioned by local law. This definition, while imperfect, fits all of the "dark" networks analyzed here which have a physical counterpart.

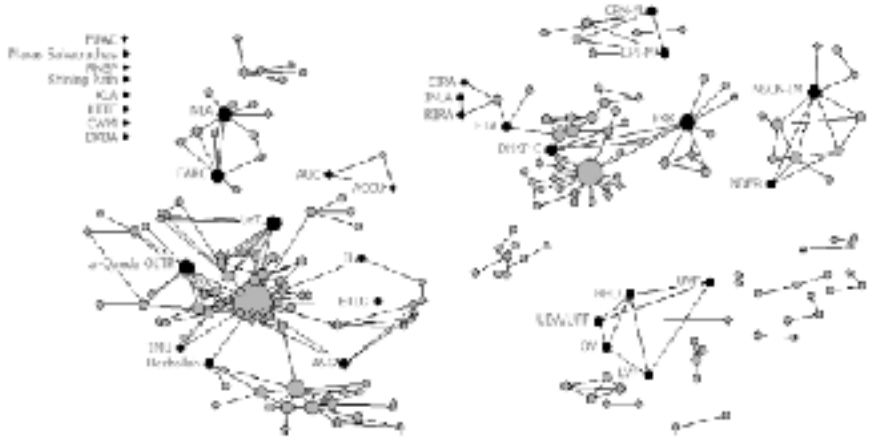
As with the Offshore entities leaked in the Panama Papers, these constructs seek to remain hidden from view both of law enforcement and the general population and can be reliably described and analyzed in terms of their topological structures in addition to their aggregated characteristics. Their goals being, on the surface to provide legal and compliant tax advice and structure operations, however, the multiple infractions and lack of action from the Mossack Fonseca firm clearly demonstrate their willingness to operate on the shadowy side of rules, towards their true purpose: evading accountability.

Same as with the Panamenian law company, the examples in Milward & Raab illustrate effectively that they have either economic goals, or political. The immediate example is drug trafficking. It is a global, sophisticated multibillion dollar market which is illegal, yet ubiquitous, in most nations. It defies states everywhere, and it helps fund other activities in which violence, more than a byproduct, is a goal:

> *"The nexus between organized crime and terrorism — in which illicit drug trafficking appears to play a role — poses a serious threat, as emphasized by recent Security Council resolutions calling for redoubled efforts to prevent terrorists from benefiting from transnational organized crime. "*
>
> *Source: UNDC (2015)*

This was pointed in the Milward & Raab paper, the "Dark Networks" also have connections to each other, reflecting a structure that is highly adaptive and able to customize its approach to different territories, indicating that these entities also network at a higher, organizational level. In fact, networks of networks are a powerful component of the international panorama of dark networks (Asal, Milward & Schoon, 2015). There is a substantial amount of interaction and cooperation between drug smugglers and and terrorist groups, which may result in these organizations learning from one another and adopting complementary strategies (Ibid), even if many organizations refuse to engage in this behaviour, *"as part of a tactical toolkit that is contingent on opportunity, access and need… we find no evidence that ideology directly hinders the formation of crime-terror nexus" (Ibid)* As can be seen in the graph below, these groups form a *"dark economy"*, which most likely is fully connected even if the links were not captured in the data.

Fig 1: Connections between terrorist groups that engage in drug trafficking.



Source: Asal, Milward & Schoon (2005)

Another example, the escalation of violence on Mexico which involved the transition from drug-trafficking to state defying terrorism (McCarthy-Jones & Baldino, 2016), indicating that not only organizations learn from each other, they can extensively deploy the tactics from their business "partners" (Espinal-Enriquez & Larralde, 2015). The actors in this case involved the "carteles" which have fixed memberships and defined roles and leadership, but can still be considered a dark network.

Some semantic confusion arises regarding the use of the term *network* due to it being employed in two different meanings in the literature, both with their own proper reasoning and tradition. The first considers networks as an arrangement of human structures as in opposition of the traditional view that humans organize in either markets or hierarchies (Powell, 1990), which is based on the Coasian view of economic exchange as being mediated either by price or hierarchy (Coase, 1937), and networks would be a third type of organization, qualitatively different from the two previously cited ones. According to Powell: *"Networks can be complex: They involve neither the explicit criteria of the market, nor the familiar paternalism of the hierarchy." (1990)*. The network would be based on a more *"trusting ethic"* (Page & Poldony, 1998).

The second perspective is of networks as a simple collection of individuals or organizations (nodes) and a certain number of ties between them (Scott, 2012). This ultimately treats the "network" part as a tool for understanding the object. While this may

appear as a loose definition, in fact it makes it a much more powerful intellectual construction. As stated by Campana:

> *"... by not assuming a structure a priori, it is possible to test hypotheses on the mechanisms that have brought about that very same structure. Network analysis can be combined with one or more substantive theories of network processes, such as preferential attachment, structural balance, social selection and social influence... There is no need to conflate the network approach with any prior assumption about the structure of a network, as the network model of organization would require"*
>
> *(Campana, 2016)*

I agree with the perspective that**, the essential characteristic of the dark networks is that their continued existence depends on secrecy, corruption of government agents or coercion** (Gerdes, 2014; Oliver et Al, 2014, Campana, 2016), since these are social structures to which the continued survival, even in strictly physical terms, depends on not being detected by law enforcement. This definition includes the remarkable variety of structures that appear in this field and share such characteristics. It also has the operational advantage of avoiding classification based on the "sample" from the entity. As even inside different organizations its possible to find local variations in the observed graph regarding density and arrangement, this is especially problematic for dark networks, which have relatively scarce information.

Interestingly, there is some preceding literature that touches on the need for criminal networks to coerce or copt state agents to survive, aptly encapsulated in Pablo Escobar famous quote: *" O plata, o plomo! - (either) silver or lead!"*, when referring to the choices policeman and politicians had. Cartier-Bresson's paper on the journal Political Studies (1997), which included implicitly many of the aspects to be formalized later in the field, including a valuable connection with social capital theory, pointing that corrupt networks rely on social capital activation for secrecy and growth of the criminal activities. While he does not make the direct link to network science (as the field was still to be established properly).

Its important to note that the conceptual evolution converged into two specific characteristics for identifying a network as dark, even by Milward and Raab. On their most

recent works, it has been narrowed as social construct that simultaneously attempts to be invisible for the casual observer and its illegal *(Bakker, Raab & Milward, 2011)*, in a sense extending the previous understanding in their that dark networks did not display hierarchical features. Some papers fail to make this distinction properly, which while not wrong by itself, may give an incomplete understanding of the phenomena or lead the reader to poor conclusions. By those concepts, we can safely situate most, if not all operations of Mossack Fonseca as being a dark network by itself embedded in the world of offshore finance.

1.2.1.Social Network Analysis

The role of social network analysis in understanding these groups is self evident. By considering them “problems” to be solved, when presented by the optics of a state actor, it follows that their properties happen at the network level instead of the individual level. As former prime minister David Cameron plead to the G8 leaders in 2013 : "*The way to sweep away the secrecy and get to the bottom of tax avoidance and tax evasion and cracking down on corruption is to have a register of beneficial ownerships so the tax authorities can see who owns beneficially every company*.” While that proposal did not gain any momentum, the statement accurately encapsulates the issue of mapping these connections, and finding the points of interest. However, this is not a trivial matter. In fact, the persistence of dark networks is one of their most remarkable characteristics.

The fact that many of these remained active for quite some time and had changes in leadership while maintaining their roles is probably the strongest evidence for their systemic level behavior. The use of disruption techniques has been twofold, while one part attempts to understand network-level dynamics. The other focuses on finding the centres of gravity in the network for targeting, or use the network to get information about particular nodes, generally with “kinetic” (force driven) methods. (Roberts & Everton, 2011 ; 2016). Two of the most famous examples of network-centric target acquisition were both Saddam Hussein and Osama Bin Laden. In 2004 the tracking of social relations through old family albums led to the pinpointing of the individual which was ultimately hiding Saddam. In the case of Bin Laden, the identification of a node (Abu Ahmed al-Kuwaiti) that was involved with

relaying information to an already monitored Al Qaeda member of high-level. That led ultimately to the conclusion that in the same complex where al-Kuwaiti lived, a third inhabitant was Bin Laden himself. (Knoke, 2010). However, attempts to use social network analysis to do organization-level disruption were mostly failures (Dugin Et Al, 2011; Knoke, 2010), that is most likely due to a misunderstanding in how to apply network concepts to their social counterpart, on the assumption that social ties could point to the best node for "removal. It has been reported for example that one node of high centrality in the Al Quaeda network was just an "errand boy", and his imprisonment was of no strategic value. (Knoke, 2010)

One interesting perspective on dark networks as being transaction based (rather than just link based) is given by Bienenstock & Salwen (In Gerdes, 2014), motivated by a very appropriate criticism on the naive approach to graph theory to analyze social networks which:

> *"... In many analyses, metrics created to analyze communication networks are applied to data on financial or terrorist affiliations networks because from a formal mathematical perspective, the same quantitative manipulations can be performed, but just because an algorithm is transferable does not imply that the metrics are similarly interpretable.*
>
> *Research on Social Exchange Networks, a specialized branch of SNA focused explicitly on exchange relation as distinct from networks of communication or friendship, challenges three implicit assumptions that presuppose much of the practice of applied network analysis today : (1)that social meaning can be "reverse engineered" from data and that dyadic relations are sufficient to reconstruct social context; (2) that the same metrics can be used to study any social structure regardless of the nature of the relationships ; and (3) that SNA metrics developed using small intimate data sets can scale and be applied to large or very large data sets."*
>
> *(Bienenstock & Salwen; In Gerdes, 2014)*

These methodological limitations are present on some measure on all studies of social networks. But given the stakes and nature of dark networks, they are especially prevalent. While the authors of this particular paper do not apply the Social Exchange Networks to any particular example, they make a compelling argument for exercising significant care on the importance of having the same kind of tie mapped, or to recognize that the different relationships (economic, kinship, friendship, operational relations) require a more specialized toolset for representation. In a certain measure, the extensions of network theory are able to address these concerns, multiplex (multiple types of links between nodes) , multi-layer (multiple networks with layer-crossing links) and temporal networks (in which the existence of a link or node is considered on a time continuum) all can be employed to give a more realistic picture. Even if in many cases, these still have open questions regarding basic metrics.

Dark networks must also be understood on the paradigm of a strategic challenge to regular combat forces. In the worlds of General McChrystal, one of the biggest supporters of the United States counterinsurgency doctrine (COIN), which had the uprooting of dark networks as its main goal.

> "*For the U.S. military that I spent my life in, this was not an easy insight to come by. It was only over the course of years, and with considerable frustrations, that I came to understand how the emerging networks of Islamist insurgents and terrorists are fundamentally different from any enemy the United States has previously known or faced."*
>
> *(McChrystal, 2011)*

The influence of this line of thought is prevalent especially at the early stages of DN's research. The problem which the US military and intelligence community faced demanded going deeper than wether combatant had the flags of country A or B. While its imaginable that DN's predate the twenty-first century (examples such as the anarchist groups in the last century, or the Green gang from the Chinese underground come to mind), their capacity to coordinate operations across long distances has been exponentially

increased by the advent of modern communication technologies In this sense, technology can be understood as allowing a substitution of some of the elements of structure and hierarchy that generally allow organizations to function (Milward & Raab, 2006).

The differences between traditional marxist insurgencies and islamist jihadi groups have been pointed out by Muckian (2006). He writes that *"the insurgent of today… draws support from criminal networks as opposed to popular mobilization"*. The traditional structuring of communist insurgencies, (of which arguably the most successful was the Maoist, but examples in Latin America are also valid) was to obtain massive popular support to supplant the state's structure: *"These military units were fully integrated with the political hierarchy, giving the Viet Cong tight organizational control" (Muckian, 2006).* There is however evidence of decentralized urban insurgency during the cold war. One of the most diffused illegal guides of leftist tactics, the *"Minimanual of the Urban Guerrilla"* by Carlos Marighella (1969), written in the context of the Brazilian dictatorships (both Vargas and Military) had this passage:

> *"Inside the firing squad there is supposed to be absolute confidence between comrades… When there are tasks assigned by the strategic command, these take preference. But there is no such thing as a firing squad without its own initiative. For that reason it is necessary to avoid any rigidity in the organization as a way to allow the largest possible capacity of initiative by the firing squad. The old type of hierarchy, the style of the traditional leftist does not exist in our organization…. This method of action eliminates the necessity of knowing who is realizing the actions… The organization is an indestructible net of firing squads…"*
>
> *(Marighella, 1969)*

Marighella was an important member of the marxist movements in South America. He had both contacts with the successful Cuban insurgency, as well as visited China to be educated on the finer points of Maoism. He was a strong proponent of terrorists attacks against civilians and non-combatants identified as either collaborators of capitalism or guilty

of simply being US citizens, while stressing the importance of preserving relations with common folk as a way to gather support. Another element that is present in his *"minimanual"* is the need to compartmentalize information as a measure of counterintelligence. This gives us a very useful historical perspective and its strong evidence that these decentralized insurgencies always existed but were limited in scale by communication technologies.

Nevertheless, indeed most of the insurgent groups the US faced across the globe were of the hierarchical variety. Opposite to that, insurgent groups in Iraq are fluid in allegiance and activity. As pointed in another paper:

> *"Unlike a "classical guerrilla-type campaign," the Iraq insurgency has no center of gravity. There appears to be no clear leader (or leadership), no attempt to seize and actually hold territory, and no single, defined, or unifying ideology. Most important, there is no identifiable organization… Rather, what is found in Iraq is the closest manifestation yet of netwar, the concept of warfare involving flatter, more linear networks rather than the pyramidal hierarchies and command and control systems (no matter how primitive) that have governed traditional insurgent organizations"*
>
> *(Hoffman, 2006)*.

Its interesting to see the term "*netwar"*, coined by Ronfeldt and Arquilla from RAND corporation (1999). Arguably, it became the basis for the doctrine of *"Network Centric Warfare"*. Despite the name, those two approaches to networks as a tool for war are diametrically opposed in their effects, the US Army one increasing synchronicity. implicating that Prof. Hoffman was adopting a liberal interpretation of the concept:

> *"Because of the increased access to information that a network-centric model provides to battlespace entities, those entities can have both better information and an improved ability to generate shared awareness than a platform-centric model, which restricts the flow of information. A*

network-centric model can also achieve higher levels of interoperability and collaboration"

(Alberts et Al, 2001

1.2.2.Specific Challenges of Dark Networks

Dark Networks provide a unique set of difficulties for performing analysis. By definition, its actors strive to stay hidden both from outsiders, and in some measure, from other nodes of the network as an internal measure of protection. (Gerdes, 2014). Their structure also means that internal differences both intra-networks and between networks cannot rely on the state as an arbiter for solving differences, they either use trust, or a peculiar form of internal arbiters based on hierarchy, or straight physical conflict. In fact some of the worst situations of organize violence rise from conflicts between different factions (Enriquez & Larralde, 2015).

The key question is "*why some networks are able to sustain shocks and attacks that would destroy others?"* (Bakker, Raab & Milward, 2012). Another underlying question, that rarely is asked in the examined literature, is whether use of different modes of network to achieve or security or economies of scale. (Farley, 2003). Wright and Helfstein present this correlation in a very compelling paper (2011) which identifies that the terrorist networks evolve over time and display increased density, while avoiding a power-law degree distribution. Their structure is more akin to the small-world model (Watts & Strogatz, 1998). It has been disputed however if there is indeed a general structure that can be applied to dark networks (Oliver, 2014). It is especially hard to study entities that have *"fuzzy boundaries" :*

"Fuzzy boundaries refers to the difficulty in determining which actors and relationships are to be included and or excluded in analysis. Analysts will generally put in place a boundary specification rule, a type of criteria for determining which actors and relationships are to be included in a study."

(Burcher & Whelan, 2015)

The boundary problem has two approaches: realist and nominalist, following the classification by Laumann. The first one has the actors themselves recognizing that they are a part of the network, in certain cases, there are concrete signals of this linkage, like gang tattoos, which allow for a precise definition at least for *"initiated"* individuals. The nominalist approach relies on the analyst himself drawing that line. For the second one, three elements can be used to make that decision. The first one is on individual markers on investigation, for example persons that receive pay from a determined entity and therefore is employed by it.

This approach suffers from ambiguity issues on most cases, with the exception of extremely well bounded entities, and even then, it usually has collaborators that sit on the grey zone. The second one is dyadic based, for example with a determined frequency of encounters, which involves in itself setting what is a "meaningful" boundary, since even most die hard criminals have regular social lives, and in certain cases, are extremely active in the "bright" local community. The third one relies on a certain definite event (or series of events) that tie the actors together. The most famous example is the Global Salafi Jihad Network by Sageman, which has groups that were involved in different attacks, such as in Bali, Mumbai and 9/11. Ideally, these strategies are combined to provide a multi-angled approach (Ibid). While it is known that the boundary decision changes the perception of the network, its appears to be impossible to predict in which way any of the different strategies go, however more studies are needed (Borgatti Et Al, 2006, Burcher & Whelan, 2015).

Given its immediate applications, this area has been empirically led, with many studies mapping covert networks based on whatever data was available. Curiously, this resulted in under-theorization (Oliver, 2014; Gerdes, 2014). There are a multitude of examples of dark networks analyzed, both structurally and theoretically. Two studies will be presented, one of the qualitative sociological analysis, the other using resources of graph theory. I believe those present an acceptable snapshot of the approaches employed and their limitations.

China provides one of the hallmark examples of Dark Networks. Their Triads have a long history in the limelight of society with its existence and influence being established public knowledge. Their modes of organization however are much more secretive While there are no studies that I am aware of in which their structure is charted. However, there is

an exceptional study done by Ming Xia from the City University of New York (2008) which presents a comparison of how structure in the organization of the *"dark forces"* is has been applied as a criteria for law enforcement in modern times in China and its effects.

Given the long history of criminal societies in that nations underground, Chinese laws themselves have a separate definition for criminal organizations: Criminal groups with mafia-style characteristics have tight and well-knit internal structure and a sizeable membership. They have internal strata and and role specification for the core group. According to the manual for law enforcement, the organized criminal groups were a *pagoda*:

> *Horizontally, a set of concentric circles is identifiable: the leaders or chieftains occupy the core of the criminal groups with mafia characteristics. Around the leadership are core members who are responsible for communication and coordination between the inner circle and the outer layer. The ordinary members are in the outer layer. Vertically, a power structure is formed as a pyramid: the leaders or chieftains sit atop the pyramid with enormous authority, and the subordinate members must worship them. In the middle are the core activists, who actively organize and participate in crimes, and also build their own authority and status on the basis of their superior capacity and rich experiences of committing crime. At the bottom are the ordinary participants.*
> *(Ming Xia, 2008)*

This depiction was used to check if individuals and entities were engaged in organized crime. However it is both inadequate and historically limited. The four Chinese secret societies (Green gang, Red gang, Triads - Also known as heaven and earth society-, and religious cults) had distinct modes of organization. They adapted to changes in Chinese society, acting to fill in the gaps when a government fell or had its power in a certain location diminished. In many cases, they became synonymous with regional power, and explored the burgeoning nascent capitalist society of east Asia. Even after a crackdown by Mao's regime, its cultural footprint did not disappear entirely, as usual, the secret societies are able to embed themselves among ties of kinship and form loyalty bonds, or to assume facets of regular entities, these last ones referred to as "hermit-crab" groups.

After the cultural revolution, there is a rebirth for many of these societies, inspired both by their old traditions as well as the influence of foreign films, especially *"The Godfather"*. They display richer structures than their previous counterparts, including ties to offshoots based in the Chinese diaspora, including Hong Kong, Taiwan, Singapore and even the US.

Some groups even display the characteristics of a network of different organizations:

> *"These five hooligan groups sometimes collaborated closely, sometimes were on their own. Sometimes they did business and made money together; sometimes they competed against each other for dominance and vanity resulting in the black eating black gang fights" (Ibid)*

In more recent years, the gangs have kept the "inner circle" with hierarchy, while having a more random and unstable outer layer of individuals, and rely on less formal means of structure as a deterrent of law enforcement, representing a particularly hard challenge.While the author does not make the connection to the field of Dark Networks, its direct similarities are evident.

1.2.3. Topology of Dark Networks

One particularly interesting paper of Dark Networks topological analysis is by Xu and Chen (2008). It cross-comparisons a few compiled networks : 1 - The Global Salafi Jihad, 2- Meth World, a collective of drug traffickers investigated by the Tucson police department. and 3- A second group of gangs, created by co-ocurrence in police records. and 4- A list of connected terrorist websites, called the Dark Web:

Table 1: from Xu and Chen, displaying the basic statistics of the analyzed networks.

	GSJ	Meth World	Gang Network	Dark Web
Number of Nodes, n	366	1349	3917	104
Number of Links, m	1247	4784	9051	156
Size of Giant Component	356 (97.3%)	524 (38.5%)	2231 (57.0%)	80 (77.9%)
Average Degree, <k>	6.97	4.62	5.74	3.88
Maximum Degree	44 (12.4%)	37 (4.0%)	51 (2.3%)	33 (41.3%)
Link Density, d	0.02	0.01	0.003	0.05
Assortativity, r	0.41**	0.14**	0.17**	0.24*
Power-Law Distribution Exponent, γ	1.38	1.86	1.95	1.10
Goodness of Fit, R^2	0.74	0.89	0.81	0.82

Source: Xu and Chen (2009)

Their study point to these networks having a power-law degree distribution, as well as the small world property regarding high clustering and low average path length, supporting half the findings of Hefstein & Wright (2011), which indicate the small world model as being the best fit for these networks, but lacking a power law degree distribution.

Table 2: average path length, clustering coefficients and efficiency of the networks.

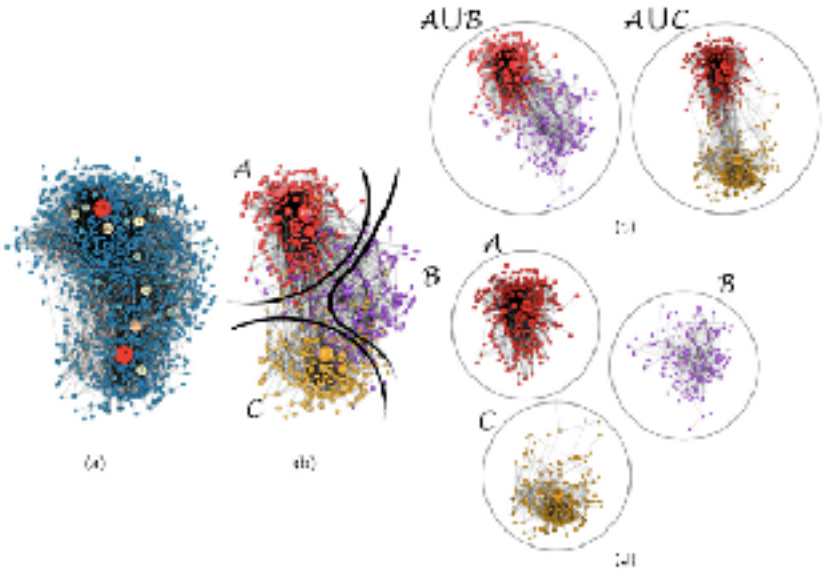
	GSJ		Meth World		Gang Network		Dark Web	
	Data	Random	Data	Random	Data	Random	Data	Random
Average Path Length, l	4.20	3.23 (0.040)	6.49	4.52 (0.056)	9.56	4.50 (0.034)	4.70	3.15 (0.100)
Average Clustering Coefficient, C	0.55	0.020 (0.0028)	0.60	0.005 (0.0014)	0.68	0.002 (0.0005)	0.47	0.049 (0.0155)
Global Efficiency, e	0.28	0.33 (0.004)	0.18	0.23 (0.003)	0.12	0.23 (0.001)	0.30	0.34 (0.019)

Source: Xu and Chen (2009)

It is still to be studied if these findings reflect biases in either network samplings, different methodologies for thresholding, or if indeed the findings are conflictive. Such contradictions are encountered very often in the literature and still demand more cross analysis (Oliver, 2014) . I believe that there is no topological signature for all dark networks, instead, each metric is altered in response to evolutionary pressures and on the cost of having a link formed and discovered.

Their findings broadly point out to highly efficient structures, with high clustering coefficient and the presence of certain nodes with very high betweenness centrality that act as “brokers” for flows inside the network, and apart from the dark web example, the hubs were not the brokers inside the network, indicating what could be an internal measure to increase resilience. They lack a more detailed discussion however of how each of the network thresholding methods can impact the findings for structure, and make the claims for resilience based essentially on the simple cascading failure model which simulates attacks by removing nodes without replacement based on different criteria. As we’ll see later, (Catanese, De Meo and Fiumara, 2016) the output in “illegal activity” from a network can be achieved also with non-connected components, so even cleaving key nodes of a criminal group might not result in better indicators.

Fig. 2: Interventions to split an Italian criminal network ended up creating three different groups capable of independent action, demonstrating resilience.



Source : Catanese, De Meo and Fiumara (2016)

There are many other studies mapping or analyzing perceived dark networks using the Social Network Analysis methods, but some examples are: MMO Illegal gold mining for Players(Keegan Et Al, 2010), Terrorist networks (Asal and Rethemeyer, 2008 ; Crenshaw, 2010, Morselli, 2009, Milward and Raab, 2006, Varese, 2013 ; Hefstein & Wright 2011; Sageman, 2006). Criminal networks are even more abundant, and a partial listing can be found in Morselli (2009). Particularly there is at least one application of network science without employing social network analysis, but studying the effects of the Mexican drug cartels (Enriquez & Larralde, 2015) on connected violence events using geo-tagged data.

1.2.4. Resilience of Dark Networks

Resilience as a general concept refers to the capacity of a certain system to withstand shocks and continue to function, generally by adjusting its behaviour (Barabasi, Barzel & Gao, 2016). In social networks, resilience can be correlated with its topology. Its is an especially pressing concern for dark networks, since one of the main goals is to understand how to counter that resilience. This field in itself is much older than networks and has been historically referred as counterinsurgency, and its classical ways of disrupting a movement were twofold, to decapitate (sometimes literally) its leaders and and win the people.

Probably the best historical example of crushing a revolt in the modern days is the Malayan communist uprising in 1948-1960:

> *"the British forcibly resettled a half-million peasants of predominantly Chinese ancestry into 450 guarded "New Villages". This strategy denied the guerrillas access to information and resources from a sympathetic population…Far less successful were two programs implemented by the United States during the 1955-1975 Vietnam war. The Strategic Hamlet Program, partially modelled on the British experience…the CIA's Phoenix Program in the late-1960 sought to "neutralize" -capture, convert or assassinate - suspected Viet Cong cadres… It tortured and killed tens of thousands of suspects…. "*
>
> *(Knoke, 2013)*

However, these are rather brutal, and ineffective operations. Their cost both in dollars and in human capacity and political capital far exceed their benefit. More so, they fail to properly capture the minds of people and create the conditions for support of "freedom fighters". For the 2003 invasion of Iraq and its occupation, early experiences reinforced that this strategy was especially poor for the fragmented local insurgency. The fear of a Vietnam style defeat (Ibid) created the demand for the COunter-INsurgency doctrine, also known as COIN, developed in 2006 with the input of many areas,*"ranging from veterans of Vietnam and El Salvador to human rights advocates"* (Ibid).

The new doctrine had the backing of high officials and was quickly implemented in classes at the Combined Arms Centre. It can be summed up to two principles: First, protecting the population its the key to success in counterinsurgency. That is realized through rapport building with the community, focusing on making them protected from violence. War turns into an effort of peace building, not only on security but providing essential services, medical care and trying to establish a normal life. The other principle is constant adaptation and learning. The forces on the ground should be as adaptive as the enemy and anticipate its movements. It proved relatively effective in Iraq (at least until the

collapse of Syria), but failed in Afghanistan due to differences in culture and resource constraints (Chandrasekaram, 2012).

The COIN doctrine is an excellent example of how complex it is to counter resilience in dark networks and that a simple attacking strategy is hopeless. This is not just applicable to terrorist or guerrilla groups, as it has been displayed in criminal entities too. According to Everton and Roberts (2011), the available strategies for countering dark networks are divided in Kinetic and Non-Kinetic. Kinetic ones being aggressive, offensive measures to eliminate or capture members of a network or their supporters. As mentioned above, the current understanding is that is is a limited approach regarding attacking a network, and while less tempting to many, the non-kinetic methods are the ones that have the most effectiveness: Institution-building, Psychological operations, Information operations, Rehabilitation and Tracking and monitoring. The "kinetic" part of those act as the old ideas of direct attack and have the preference of both the public opinion and many military experts; which use the measures of centrality as a way to pick targets, which they call the *"bias towards the center"*.

> *"Intelligence analysts, field operatives, and researchers using SNA to disrupt dark networks appear to be putting the cart before the horse. They tend to begin (and end) their analyses with centrality and/or brokerage metrics to identify a dark network's central players" (Everton and Roberts, 2011)*

Another extremely relevant study towards dark networks resilience is Baker, Raab and Milward (2012) focusing on the preliminary elements that can be characterized as network resilience in the the specific context of covert entities. Their six propositions are well grounded on the three cases presented as evidence (FARC in Colombia, MK anti-Apartheid network, LTTE in Sri Lanka). Their findings are that Resources and Legitimacy (both internal and external) are positively correlated with network resilience, as well as employing selective measures of integrating its members (Propositions 1, 2 and 4). Capacity to replace and maintain nodes and links in itself is positively correlated with operational capacity (Proposition 3; hardly a surprising finding, but does bear on the importance of network structure), while centrality is negatively correlated (Proposition 5). While there are structural differences in Grievance driven networks when compared to Greed driven ones;

the first being more sensitive to changes in legitimacy, while the second is more sensitive to changes in resources (Proposition 6). Their findings reinforce the need to think of dark networks as dynamic constructions, that not only require replacement, but require maintenance :

> *"The ability of leaders of dark networks to replace nodes with people who have equivalent skills and knowledge as those they replace is critical, as it replacing linkages that existed before the shock or attack. If not replace quickly, the linkages can quickly degrade and it may become much more difficult to find a safe house or new recruits may simply have fewer skills."*
>
> *(Baker, Raab & Milward, 2012)*

Interestingly, back in 1969, the terrorist Minimanual of Mr Marighella already made mentions of how comrades of *"firing squads"* should have critical capacities, without which the group would be unable to act on the revolution.

This insight is also shared by Toth et Al (2013), which create specific metrics for dark networks focused on understanding the dark network as an entity of a certain output, that therefore must have a differentiation structure inside that relates to value chains, and could be used to find the most interesting nodes to disrupt from this standpoint. These are: Alignment membership, or how many values chains is the node essential ; Distance of Replacements, or the distance in links that one node of a certain role has to another node of replaceable role, and the combination of two: Introduction distance, or how hard it would be for the nodes neighbours to find a replacement for a certain node. The further their search happens, the higher is this metric. In simulated networks, these metrics were found to be different enough from the usual metrics of degree, closeness and betweenness as to justify its use.

Three of the coauthors of the previous paper later published a simulation model to analyze how effective those metrics could be in disruption, including the use of node replacement by the network (Dujin, Sloot, & Kashrin, 2014). Surprisingly, in a network recovery scenario, even the updated metrics fail to properly cause significative disruption in activities or even network density. At best, the simulation points to a scenario of attrition,

where the dark network is forced to extend its reach for recruitment and thus becomes even more visible to the *"bright"* world, causing eventually it to become so visible it turns into an easier target. Even by the own authors, these findings are considered *"disturbing for government and law enforcement that fight to control criminal networks on a daily basis"* (Dujin, Sloot, & Kashrin, 2014).

Another study, this time analyzing *"mafioso"* networks in Italy (Catanese, De Meo, Fiumara, 2016), which also employs the targeting metrics and recovering networks found similar results:

> *"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 for 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. "*

One element that contributed to this resilience is the relentless internal and external pressure to which the individuals are exposed, both from competition from their peers and the possibility of law enforcement targeting. Also, the use of a betweenness node targeting strategy could result in the splitting of factions, that nevertheless were entirely capable of independently attacking and performing criminal activities, but which are harder to track than the larger, previous network (Ibid)

1.3.The Panama Papers

Partial data is publicly available on a dedicated website of the ICIJ , with the csv's that resulted from an extensive process of optical character recognition from the scanned documents. It has three lists of nodes and one of all the edges. The resulting data is rather confusing. The raw network has 1.2 million nodes and 3.5 million links, with more than 200 types of connections, four types of node (Company, Intermediate, Shareholder, Address),

with a tremendous amount of ambiguity (some names repeated over a hundred times) regarding the nodes, across multiple years of activity.

I performed a filtering procedure in four steps in order to get a representation that: **1- had equivalent link types, 2- disambiguated node identities, 3- Strictly entities that could receive or transfer capital trough the main network,** and **4- were active simultaneously at the most recent time period available.** The objective of this filtering is to allow the structure to be meaningful. For all the power of the Network Analysis approach, it can incur in validation mistakes if the links and nodes are not the same, or if being different, that is not taken in to account. More so, all links should be present simultaneously or the static network will create the illusion of connection where there was none. While the techniques of Temporal Networks could be performed, the lack of well grounded procedures for calculating metrics, simulations and the detection of communities (Barabasi, 2016) point towards a more conservative approach.

2. Analysis

2.1. Data

The Panama Papers files were delivered anonymously to a source at the german newspaper ***Suddeutsche Zeitung*** and posteriorly validated and investigated trough a combined effort of hundreds of journalists. The files themselves contained scanned pages from *Mossack Fonseca* corporate drawers across the globe. A partnership with the Neo4j relational database company allowed the use of both automated optical character recognition and encoding of the relations present in the data.

Partial data is publicly available on a dedicated website of the ICIJ , with the csv's that resulted from an extensive process of optical character recognition from the scanned documents. It has three lists of nodes and one of all the edges. The resulting data is rather confusing. The raw network has 1.2 million nodes and 3.5 million links, with more than 200 types of connections, four types of node (Company, Intermediate, Shareholder, Address), with a tremendous amount of ambiguity (some names repeated over a hundred times) regarding the nodes, across multiple years of activity.

I performed a filtering procedure in four steps in order to get a representation that: **1- had equivalent link types, 2- disambiguated node identities, 3- Strictly entities that could receive or transfer capital trough the main network,** and **4- were active simultaneously at the most recent time period available.** The objective of this filtering is to allow the structure to be meaningful. For all the power of the Network Analysis approach, it can incur in validation mistakes if the links and nodes are not the same, or if being different, that is not taken in to account. More so, all links should be present simultaneously or the static network will create the illusion of connection where there was none. While the techniques of Temporal Networks could be performed, the lack of well grounded procedures for calculating metrics, simulations and the detection of communities (Barabasi, 2016) point towards a more conservative approach.

The data was downloaded directly from the ICCJ website for the Panama Papers investigation. All of the CSV files containing the edges and nodes were combined in one full network, denominated Original. Approximately two thirds of the links in this stage were of the type “Same Name As” indicating that entities had been double counted in multiple documents and had the link as proof. Therefore the first step was to merge the nodes that had this type of linking, resulting in a non-redundant network. The second step filtered the nodes and edges that were active at the most recent period of the timestamps (2015). Given the long span of the data, which abridged over 40 years of activities, this allows us the best view of how these entities were structured. Coincidentally, this filtering step removed the edge types which were not of either “Ownership/Beneficiary/Intermediary“ (Functionally equivalent for our purposes since they allow transfer of funds) and “Registered Address” , which linked entities to whichever addresses were used in their registry, a useful signal since many shell companies tend to be registered in the same exact address. While this stage was much more tractable, it still suffers from the presence of two types of edge that have different structural meanings. The final filtering step removed the “Registered Address” edges and the isolated nodes. Since many metrics, like betweenness centrality can only be calculated for a single connected component it was particularly important to avoid isolates.

Table 3 - Comparison of the network in different filtering stages.

Filtering Stage	Nodes	Edges	Types of Edge
Original	~1.2 Million	~3.5 Million	Multiple
Disambiguated	~800.000	~1.2 Million	Multiple
Simultaneous	136,806	167,271	Ownership/Address
Capital-Flow	70,748	87,703	Ownership

Source: Lucas da Silva Almeida

2.2.Qualitative Aspects of the Network

As it has been presented before, the Nodes in the network consist of individuals or companies that engaged in business with the aid of *Mossack Fonseca* in for offshore financial activity. The company has offices in more than 30 countries and clients in almost all countries. According to an internal memorandum leaked in the Papers, (Garside et Al, 2016) , 95% of their work consisted in selling vehicles that would allow clients to pay less or no taxes.

The offshore services were varied, with the basic function being that Mossack Fonseca would create a shell company in the desired jurisdiction, generally tax havens such as the British Virgin Islands, Channel Islands, Bermuda, Panama, etc. Former British protectorates are particularly targeted since they have generous tax bilateral agreements with England, allowing access to the banking super-hub that is London. (Garside et Al, 2016). Its mechanisms of compliance were found to be at the best case, lacking, allowing individuals that had a criminal record in the US to acquire assets abroad, going against its own stated guidelines (Lipton, E. & Creswell , 2016).

One of the most common moves was to design a company to hold real estate as corporate property, when in fact it was a personal asset (subject to widely different taxation). Its clients had an entire facade ready to go, as stated by the firm partner Ramses Owens in one of the leaked emails when a customer inquired about how to send money to Panama without the knowledge of the US Government and to have profitable investments that would not be disclosed to the US Internal Revenue Service:

> *"We have right now a special offer by which we create a Private Foundation/ company combination for a flat fee of US$4,500.00," ... "It includes Charter Documents, Regulations, nominee officers and directors, bank account and management of funds, provision of authorized signatories, neutral phone and fax numbers and mail forwarding services for both the private foundation and its underlying company.With this legal structure in place ... any money placed in these accounts would essentially go into a black hole."*
>
> *(Lipton, E & Creswell, 2016)*

The nodes present in the network comprise the individual customers, their shell companies, and the intermediaries (Mossack Fonseca subsidiaries, lawyers, individuals with power of representation) who are allowed to move in funds and resources. It also crucially helps other offshore finance entities to establish connections in jurisdictions that allow secrecy. For example, by having a shell in Panama owning assets in the Bahamas and another offshore vehicle, in the Jersey Islands, owned by the real person, a British citizen, holding the Panamanian shell, its effectively impossible to trace the owner of the Hong Kong assets since the Panamanian company cannot be investigated by British tax inspectors. Those connections were usually employed in tandem with banks or other offshore finance providers, the latter of which also appear in the network.

Some of Mossack Fonseca customers are of the highest political standing. That includes members of the Qatari royal family, former Egyptian dictator Hosni Mubarak and his sons, and representatives of Robert Mugabe from Zimbabwe and the late Muammar Qaddafi, for a long time the ruler of Libya, plus other heads of state with varied levels of secrecy and involvement. In some cases, like of the former Icelandic premier Sigmundur Gunnlaugsson, his shell company was created to hide his investment in local banks, which would ordinarily have to be disclosed in his first run for parliament. These politically sensitive connections made Mossack Fonseca a very discrete entity, even by the standards of offshore finance.

The usual chain of ownership would create the connections from the source of the assets to the functional shell, with several intermediate steps, in many cases hopping jurisdictions. Those chains had few triangles, as we've seen before, its not in the interest of dark networks to maintain a large average clustering.

2.3.Network Topology

With the network already extracted, basic analysis of metrics was performed using both the functions of the Python package NetworkX and the software Gephi . Both resulted in the same numbers. Degree-preserved randomized networks using the configuration model were also generated for comparison purposes with the metrics below. While other types of generative models could be used for comparison, the simplicity of the parameters of the Preferential attachment (Barabasi-Albert) and the random links (Erdos-Renyi) allow the generation of the null model to be done with just the average degree and number of nodes. Other possibilities, like the Bianconi - Barabasi model or the Hierarchical Clustering model would require setting additional parameters, therefore insert several assumptions on the structure that interfere with its validity.

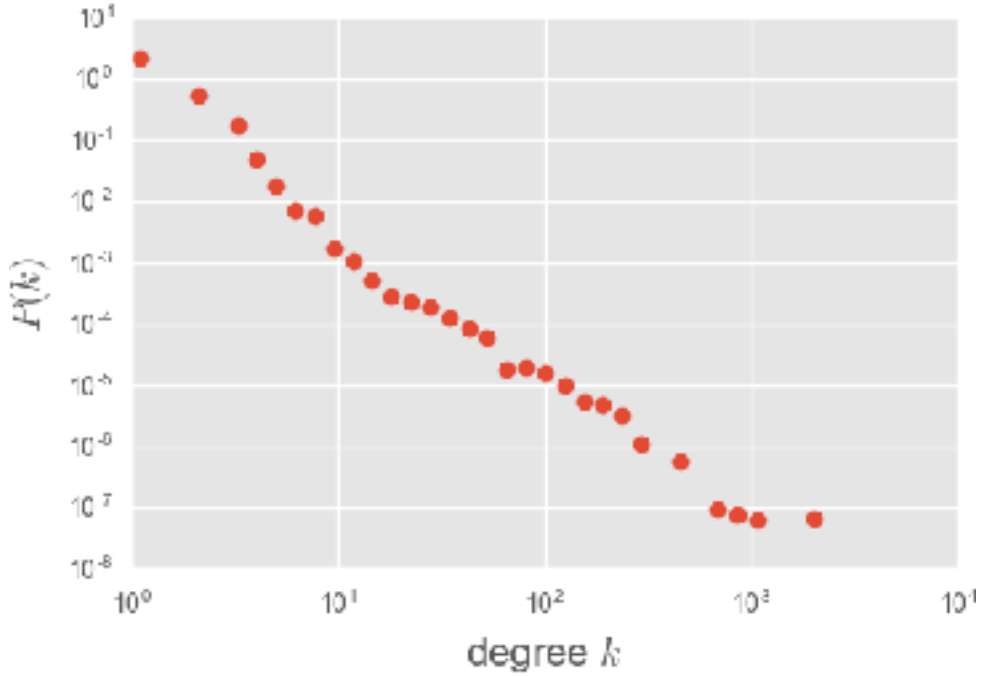
Table 4: Comparison of basic network statistics with degree-preserved null-models .

Statistic	Panama Papers	Erdos-Renyi	Barabasi-Albert
Average Degree	2,479	2,479	2,479
Average Path Length	23,44	~6	~3
Average Clustering	0,09500	~0.00035	~0.00176
Diameter	39	~12	~5

Source: Lucas da Silva Almeida

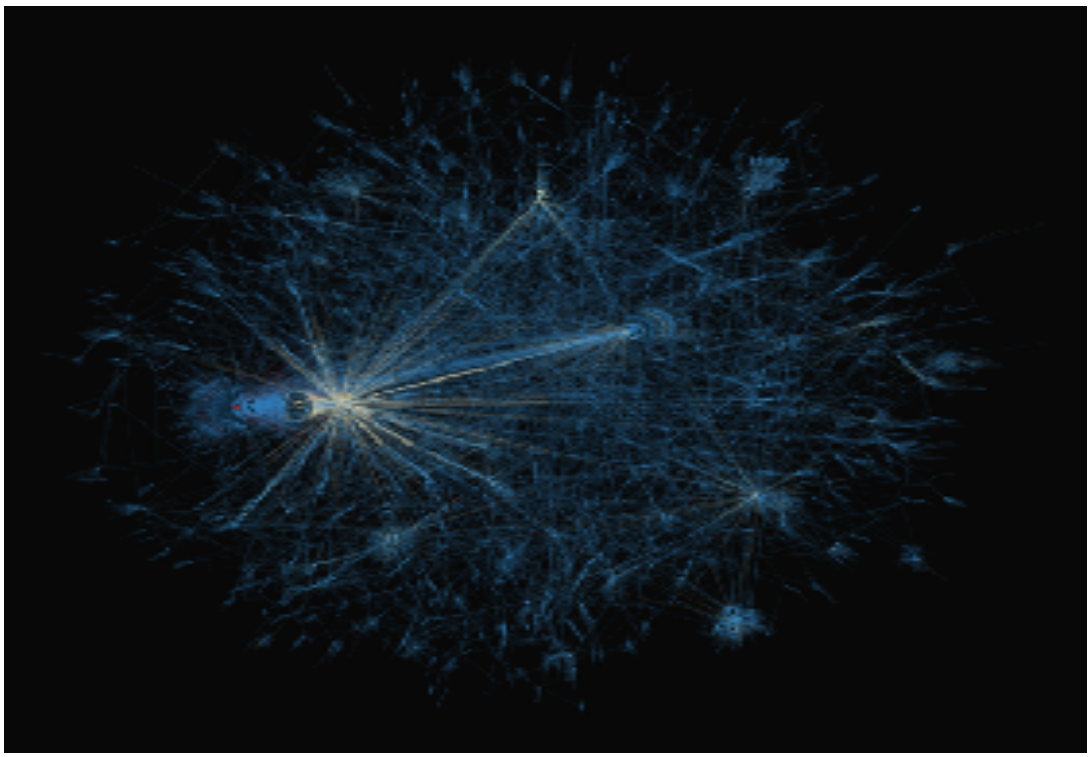
This preliminary snapshot against the null models indicates some interesting features. The network has a relatively large number of triangles (Average clustering), high average path length, and displays a degree distribution that assumes the form of a power law of degree exponent 2.1 as calculated with the Python package Powelaw . The high average path length and high diameter point out to a network that is not optimized for fast spreading or communications, while the high clustering indicates that at least some nodes have highly interconnected neighbours. As well see, those nodes correspond to “shells of shells”, nodes of low degree, in which the same shell company is appointed as shareholder/owner in different jurisdictions.

Fig 3: Degree Distribution



Source: Lucas da Silva Almeida

Fig 4 . Network with nodes coloured by degree range, hotter hues being a higher value



Source: Lucas da Silva Almeida

Some of those features are puzzling to the known models of network growth. From the Small-World model I should expect a network with high average clustering to feature a low average path length. More so, the average clustering is more than fifty times the one from the Barabasi-Albert model, indicating a relative abundance of triadic closure. Yet the average path length is much higher that what the preferential attachment model would expect. It is possible to notice that there is a substantial element of preferential attachment in the dynamics of evolving the network.

This aberrant behaviour can be explained by the property of Betweenness centrality of the network, which correlates with nodes that have the role of brokers inside the network. It is even steeper than the degree distribution. While the vast majority of nodes in the network are not pathways, there is a very small number of entities with extremely high betweenness centrality. Those entities match the service providers for the offshore industry .

Fig 5 . Distribution of the Betweenness Centrality

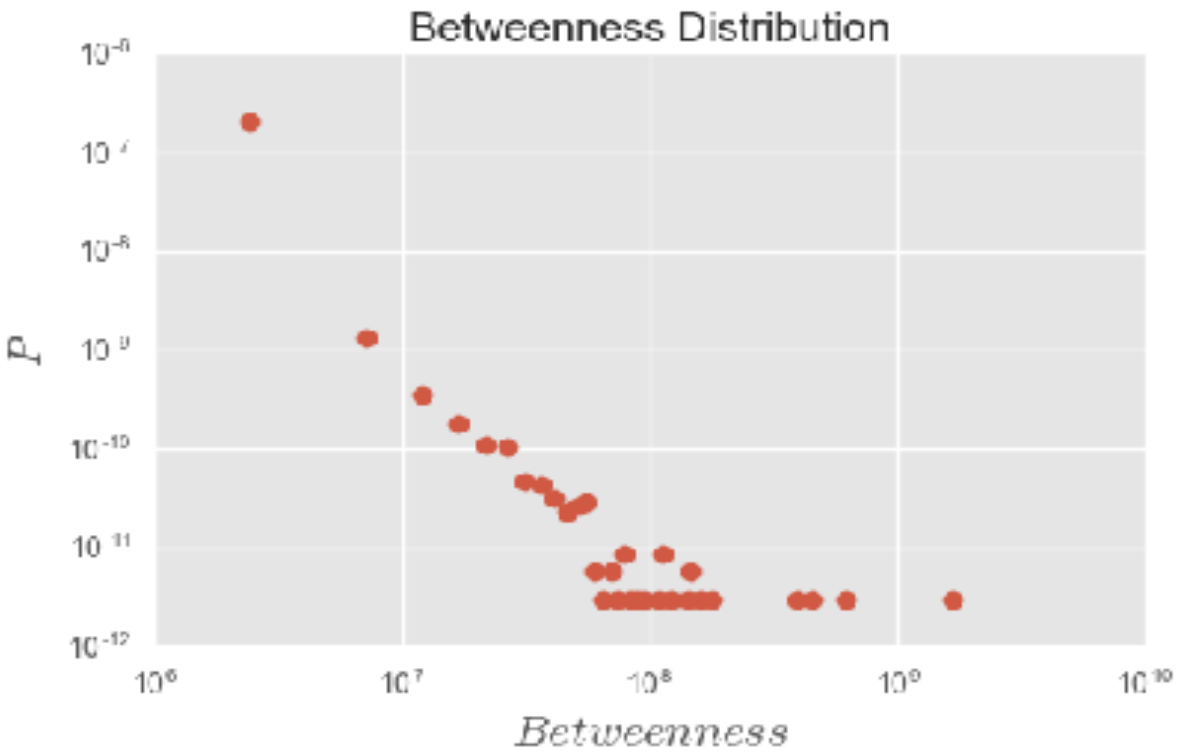
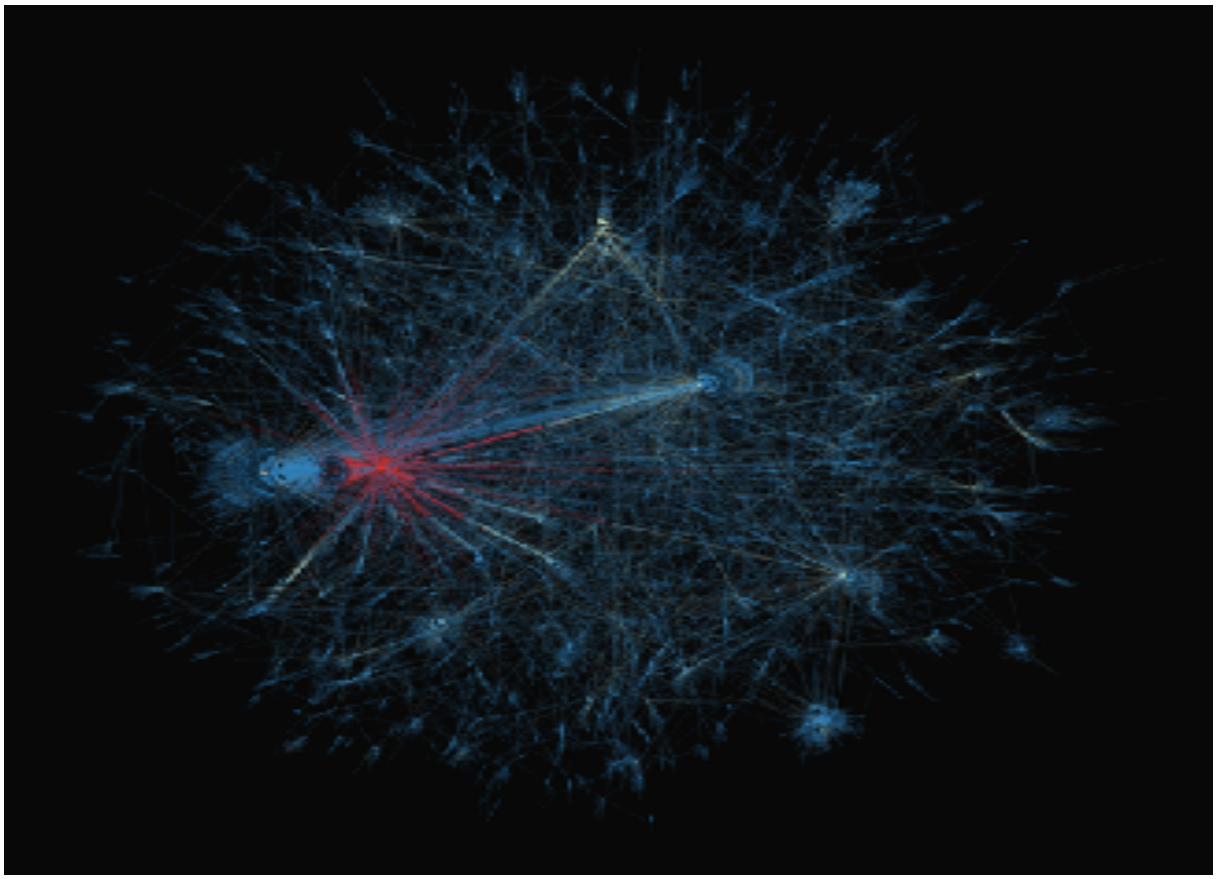


Fig 6. Network with nodes coloured by Betweenness centrality range, hotter hues being a higher value

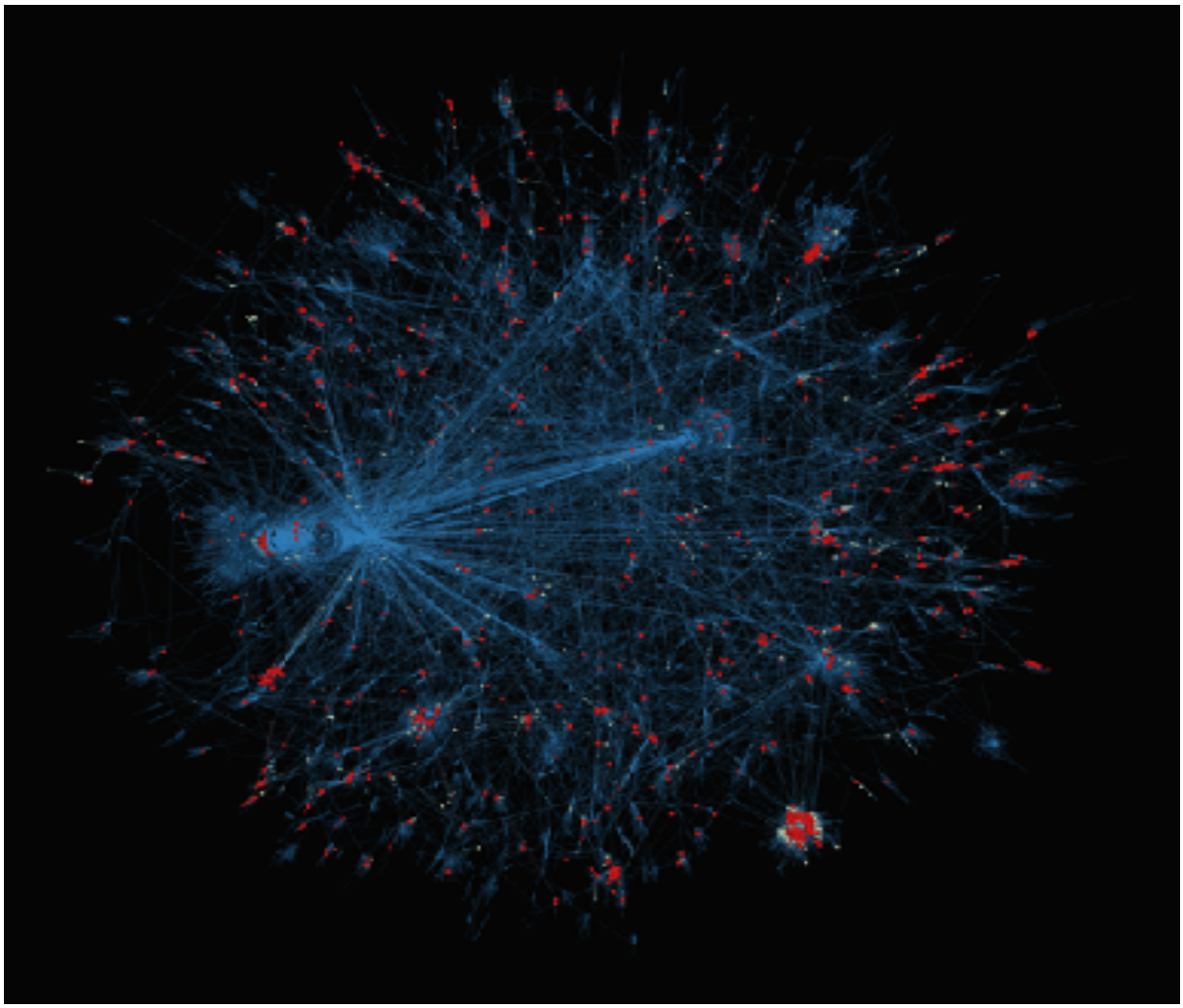


Source:Author

As can be seen in the figure above, one of the nodes, corresponding to *Mossfon. Subscribers* in West Samoa has almost ten times the betweenness centrality of the second on the list (Orion House Services, the largest hub in the network). This abrupt scaling points to the backbone of the network being comprised of this "highway" of service providers on critical jurisdictions. The most intense interactions are seen between Mossfon Subscribers and Orion House, respectively West Samoa and Hong Kong based. Both are offshore service providers, but their roles are clear from the metrics, Orion House creates more links while Mossfon serves as a pathway to capital, which matches the role of each country in the international offshore environment.

The clustering of the network, as pointed out is also abnormally high, even if the absolute majority of nodes has it in the vicinity of zero. The ones with clustering close to one are highlighted below. All of them are in the 3-4 degree range, and their triangles are mostly due to the use of the same offshore provider company being used as a shareholder to shells that are also shareholders of each other, closing the triangle.

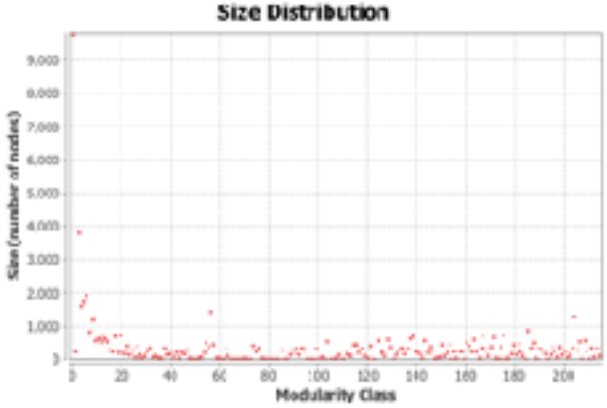
Fig 8. Network map with coloured nodes by range of Clustering Coefficients Red nodes have their CC equal to 1 and were enlarged to be visible.



Source: Lucas da Silva Almeida

2.4.Panama Papers Community Structure

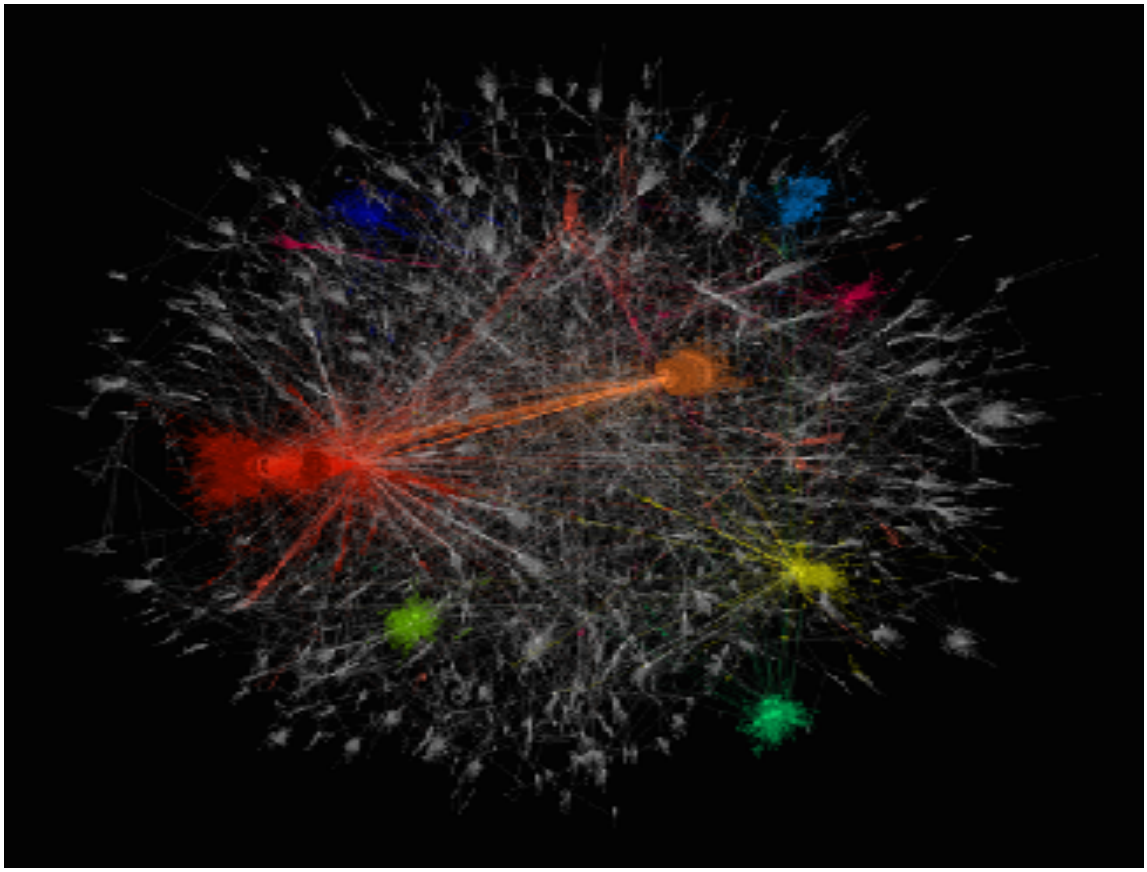
Fig 10. Size distribution of the communities in the Panama Papers network



Source: Lucas da Silva Almeida.

The Panama Papers network is very tractable with the use of community detection methods. For speed and reliability, the Louvain method was utilized, with the resulting modularity of 0.946, a very good metric pointing that the community structures extracted are far from what would be the random expectation. The most interesting component is that the interaction between the two largest nodes Mossack Fonseca and Orion House is so intense they were merged into one super community (which has approximately ten thousand nodes), by far the largest one in the graph. Most groups detected barely reach one thousand nodes. This is consistent with the previous topological observations, yet also with the ground truth from the original documents in which these entities are listed, validating the results. There are some communities such as Cannon Asset Management(Yellow on Fig.9) and Consulco International (Green on bottom right on Fig.9) have a strong national component, respectively Hong Kong and United Arab Emirates.

Fig 9. Network map with coloured nodes by Modularity class , from the ten largest communities, hotter colours point to larger groups.



Source: Lucas da Silva Almeida

2.5.Panama Papers Resilience Simulations

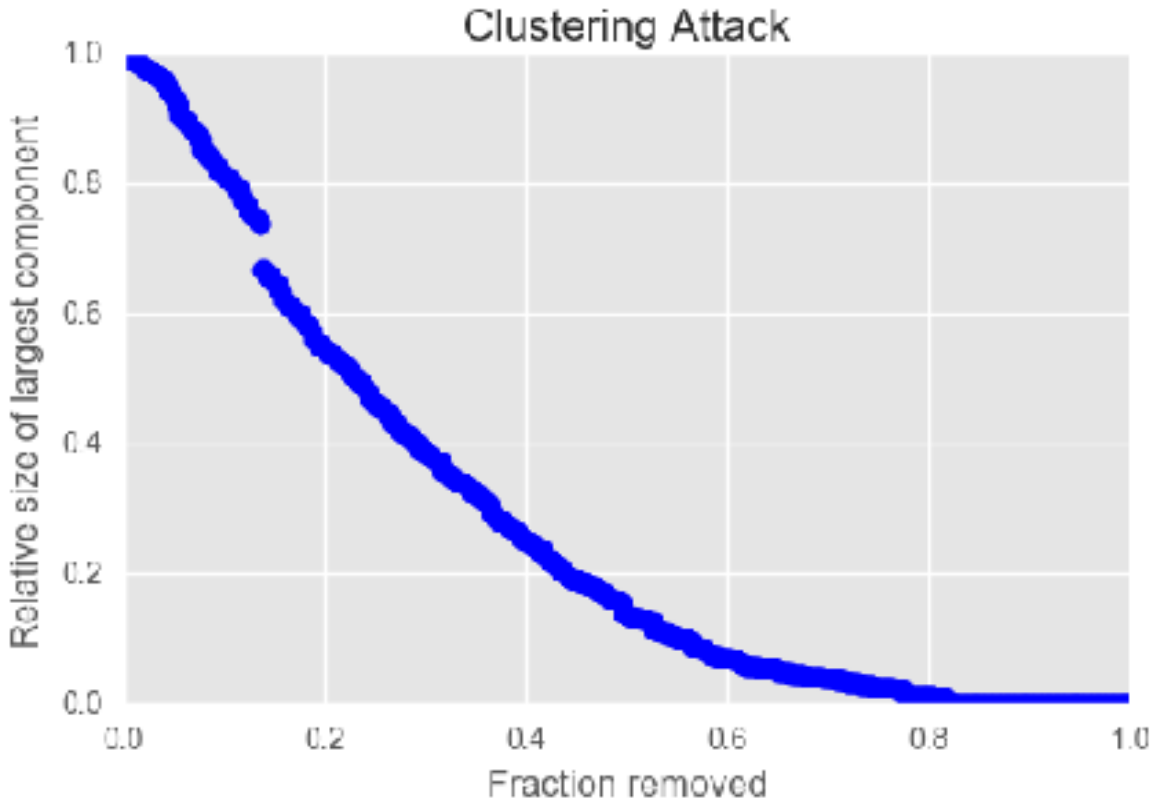
Some of the complex phenomena which are particularly tractable with networks are distributed failures. Famously, the occurrence of energy blackouts can be modelled as a series of node removals, the first event triggering a cascading failure which percolates throughout the graph and causes the breakdown of general connectivity. (Crucciti et al, 2004, Barabasi , 2016 ; Watts, 2004).

The procedure used for these simulations was to remove nodes based on two different strategies, a clustering targeted removal and a degree targeted removal. Given the goal of Dark Networks to optimize resilience against scrutiny, investigations and other legal probings, its already well established that their topology reflects the goal of operational security (Hefstein and Wright , 2011), as well as from Xu & Chen (2008). Operational security being defined as resilience specifically against attacks which focus on dismantling the network.

Simulations were done using the NetworkX python package on top of the extracted graph. At every step, one node was removed based on being the one with the highest centrality (either degree or clustering) as well as all its links. After the removal, the size of the largest component of the network is registered, and the next node is removed. Its expected that a critical transition will happen once the hubs of the network are targeted, given their crucial nature in keeping the connectivity of the graph.

It must be noted that this is a highly simplified scenario. In the real world, networks evolve, adapt and replace nodes and the Dark ones are especially adept at it. As the research done by De Meo and Fiumara (2016), as well as Dugin & Sloot (2015) state, not using replacement puts a burden on the exact validity of this modelling. Nevertheless, the attempts at making these simulations closer to reality (De Meo and Fiumara, 2016) still lack a firmer ground, and have not been validated with real data. The use of automated replacements in a model can overestimate the capacity to recover from removal critical nodes, and the use of dark networks-specific centrality measures (Dugin and Sloot, 2015) lacks the robust comparison literature from the more widely used approaches.

Fig 11. Results of the Clustering attack simulation.



Source: Lucas da Silva Almeida

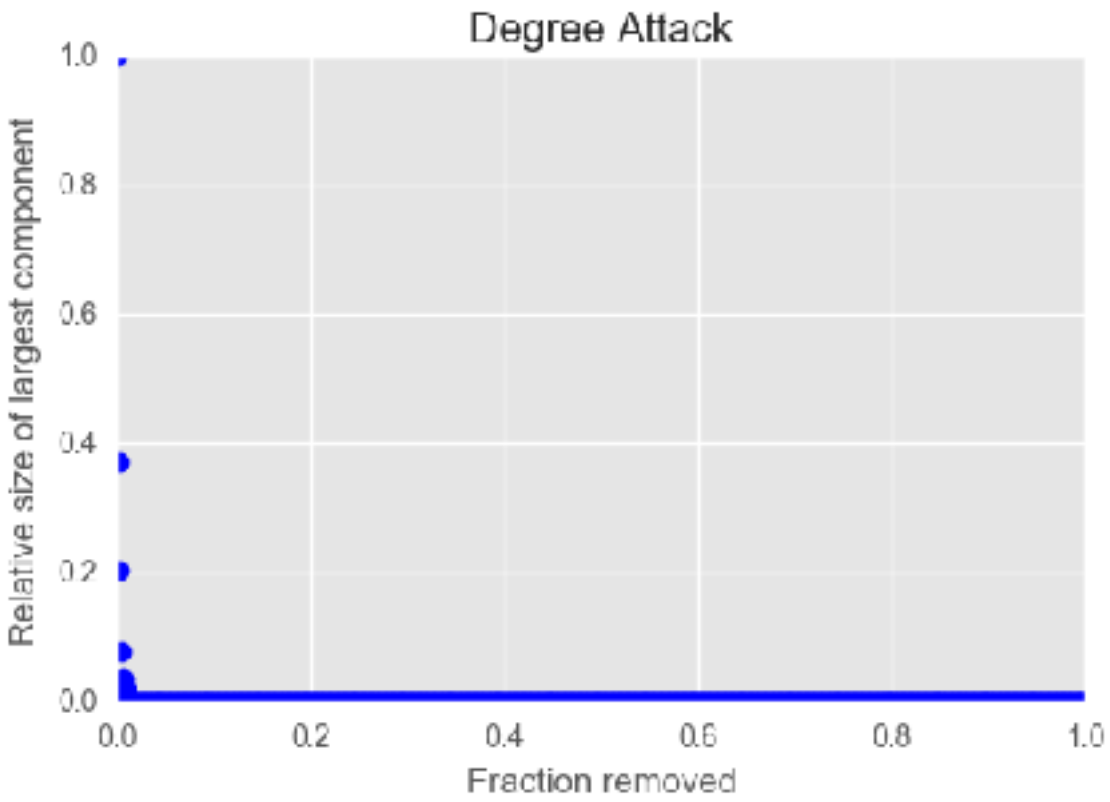
The first attack simulation was done using the Clustering Coefficient as the target marker. It is a measure that represents local density of a node's ego network. If there is a correlation between hubs being the ones with highest clustering I should expect a large transition somewhere early in the model. Networks with topological hierarchy (Strong correlation between node degree and clustering) are known to be particularly resistant against clustering attacks, more than BA or Random networks.

On the graph above I can see that apart from a small discontinuity, the breakage of the giant component is smooth. The curve points to a total breakdown of the component at approximately 80% removal, which is almost the same effectiveness of a random target approach on a power law network.

With all of the caveats that this simple approach has, I can conclude that this network displays substantial robustness to a density-based attack. For law enforcement and intelligence agencies, this illustrates how difficult it is to use connections from actors that are not strictly in the high degrees of the network. The high betweenness centrality

distribution makes it hard to disrupt the connections without necessarily reaching the central nodes. It also points to the challenge of an investigation to map these structures effectively.

Fig 12. Results of the Degree attack simulation.



Source: Lucas da Silva Almeida

The Degree attack simulation as can be seen above is brutally efficient. With approximately the ten largest nodes being removed the giant component breaks down to zero, an absurdly small fraction. This extreme vulnerability was not to be expected, given that the benchmark for power-law networks is around the 25% (Barabasi, 2016). This network is therefore more vulnerable than the null model once the “spine” is found and attacked.

The caveat being that total degree is a property that can only be assessed once the network is fully mapped, as well as the clustering coefficient. This luxury is not present in the real world, where dark networks are always hidden in their extension. Nevertheless, the results of the simulation point to the existence of fragilities in this dark network.

3. Conclusion and Discussion

Comparing it with other dark networks (Meth World, Global Salafi Jihad, Tucson Gang Network, Dark Web pages) (Xu & Chen, 2008), it indeed seems that the Panama Papers offshore network displays different characteristics in terms of statistics:

Table 5. Comparison of the Panama Papers with other dark networks

Statistic	Panama Papers	Meth World	Gang Net	Dark Web	Global S. Jihad
Average Degree	2,479	4,62	5,74	3,88	6,97
Average Path Length	23,44	6,49	9,56	4,70	4,20
Average Clustering	0,095	0,60	0,68	0,47	0,55

Source: Lucas da Silva Almeida

These comparisons should be tempered with the knowledge that these are different phenomena being analyzed. It is much easier to create a webpage than it is to establish an offshore company. Also, both the meth world and the gang network are strictly local, so the comparison with massive global enterprises even if using averages demands some consideration. Yet, the lack of similar constructs in the literature forces us to use the best available solution. Further studies could estimate the statistical relevance of these metrics using the Exponential Random Graph methodology, however given the size of the network it is prohibitive to execute as of now.

While there is still much to delve from the data, our analysis allows us to understand the convoluted nature of this structure. It is much less clustered than other dark networks, avoiding triangles as a way of increasing is resilience to outside probing. More so, the use of the betweenness centrality “spine” reinforces its comparative efficiency in remaining globally active, yet safe. The predictions of Hefstein & Wright (2011) of a Small-World in the dark networks were not successful in this case, both due to the average path length and the existence of a power law distribution. Similarly, Xu & Chen (2008) were more accurate in their characterization, correctly predicting the high-betweenness structure and some of the resilience characteristics, but mistakenly identified that the brokers were not the hubs. This could point to a larger plasticity of dark networks than it was previously noted.

In broader strokes, the Offshore industry is a particularly powerful example of how globalization changed the rules of markets and governments. What was a niche sector of banking became a de facto pipeline for tax avoidance and evasion, and more so, a conduit for laundering money into safer jurisdictions. The ease into which it is possible now to create an offshore representation, transferred the hubs of such activities to Asia, with the Orion House Hong Kong - Mossack Fonseca Panama being the most prolific connection. For interventions, the Betweenness centrality property of nodes should be particularly effective for monitoring these activities.

References

- Alkemade, R. Outsiders Amongst Outsiders: A Cultural Criminological Perspective on the Sub-Subcultural World of Women in the Yakuza Underworld. (Wolf Legal Publishers, 2014).
- Amaral, L. A. N. & Ottino, J. M. Complex networks. The European Physical Journal B - Condensed Matter 38, 147–162 (2004).
- Arquilla, J. & Ronfeldt, D. The Advent of Netwar: Analytic Background. Stud. Conflict Terrorism 22, 193–206 (1999).
- Asal, V. & Rethemeyer, R. K. The Nature of the Beast: Organizational Structures and the Lethality of Terrorist Attacks. J. Polit. 70, 437–449 (2008).
- Asal, V., Milward, H. B. & Schoon, E. W. When Terrorists Go Bad: Analyzing Terrorist Organizations' Involvement in Drug Smuggling. Int. Stud. Q. 59, 112–123 (2015).
- Ayling, J. What Sustains Wildlife Crime? Rhino Horn Trading and the Resilience of Criminal Networks. J. Int. Wildl. Law Policy 16, 57–80 (2013).
- Backstrom, L., Boldi, P., Rosa, M., Ugander, J. & Vigna, S. Four Degrees of Separation. arXiv [cs.SI] (2011).
- Bakker, R. M., Raab, J. & Milward, H. B. A preliminary theory of dark network resilience. J. Policy Anal. Manage. 31, 33–62 (2012).
- Barabási, A.-L. Network Science. (Cambridge University Press, 2016).
- Bavelas, A. Communication Patterns in Task‐Oriented Groups. J. Acoust. Soc. Am. 22, 725–730 (1950).
- Bienenstock, E. J. & Salwen, M. in Illuminating Dark Networks (eds. Gerdes, L. M. & Gerdes, L. M.) 8–18 (Cambridge University Press, 2015).
- Bodine-Baron, E., Helmus, T. C., Magnuson, M. & Winkelman, Z. Examining ISIS Support and Opposition Networks on Twitter. RAND Corporation 29–30 (2016).
- Borgatti, S. P., Carley, K. M. & Krackhardt, D. On the robustness of centrality measures under conditions of imperfect data. Soc. Networks 28, 124–136 (2006/5).
- Bouchard, M. & Amirault, J. Advances in research on illicit networks. Global Crime 14, 119–122 (2013).
- Bouchard, M. Advances in Research on Illicit Networks. (Routledge, 2016).
- Bouchard, M. Social Networks, Terrorism and Counter-terrorism: Radical and Connected. (Routledge, 2015).

- Broadhurst, R. in Routledge Handbook of Transnational Organized Crime (Routledge, 2012).
- Burcher, M. & Whelan, C. Social network analysis and small group ‘dark’networks: an analysis of the London bombers and the problem of ‘fuzzy’boundaries. Global Crime 16, 104–122 (2015).
- Calderoni, F., Brunetto, D. & Piccardi, C. Communities in criminal networks: A case study. Soc. Networks 48, 116–125 (2017/1).
- Cartier-Bresson, J. Corruption Networks, Transaction Security and Illegal Social Exchange. Polit. Stud. 45, 463–476 (1997).
- Catanese, S., De Meo, P. & Fiumara, G. Resilience in criminal networks. Atti della Accademia Peloritana dei Pericolanti - Classe di Scienze Fisiche, Matematiche e Naturali 94, 1 (2016).
- Chandrasekaran, R. Little America: The War Within the War for Afghanistan. (A&C Black, 2013).
- Crenshaw, M. Mapping terrorist organizations. Unpublished working paper (2010).
- Crucitti, P., Latora, V. & Marchiori, M. Model for cascading failures in complex networks. Phys. Rev. E Stat. Nonlin. Soft Matter Phys. 69, 045104 (2004).
- Duijn, P. A. C. & Sloot, P. M. A. From data to disruption. Digital Investigation 15, 39–45 (2015).
- Duijn, P. A. C., Kashirin, V. & Sloot, P. M. A. The relative ineffectiveness of criminal network disruption. Sci. Rep. 4, 4238 (2014).
- Erdos, P. & Rényi, A. On the evolution of random graphs. Publ. Math. Inst. Hung. Acad. Sci (1960).
- Eric Thomas Messersmith, U. of M. & Authors. Political corruption in Japan: A study of the theory, causes and effects with particular reference to the Yakuza factor in banking scandals and prolonged recession. (University of Miami, 2003).
- Espinal-Enríquez, J. & Larralde, H. Analysis of México’s Narco-War Network (2007--2011). PLoS One 10, e0126503 (2015).
- Espinal-Enríquez, J. & Larralde, H. Analysis of México’s Narco-War Network (2007-2011). PLoS One 10, e0126503 (2015).
- Flanigan, S. T. Terrorists Next Door? A Comparison of Mexican Drug Cartels and Middle Eastern Terrorist Organizations. Terrorism and Political Violence 24, 279–294 (2012).
- Freeman, L. C. A Set of Measures of Centrality Based on Betweenness. Sociometry 40, 35–41 (1977).

- Garside, J., Watt, H. & Pegg, D. The Panama Papers: how the world's rich and famous hide their money offshore. The Guardian (2016).
- Gerdes, L. M. in Illuminating Dark Networks (eds. Gerdes, L. M. & Gerdes, L. M.) 19–38 (Cambridge University Press, 2015).
- Hamilton, D. S. Dark Networks in the Atlantic Basin: Emerging Trends and Implications for Human Security. (Center for Transatlantic Relations, 2015).
- Helfstein, S. & Wright, D. Covert or Convenient? Evolution of Terror Attack Networks. J. Conflict Resolut. 55, 785–813 (2011).
- Hoffman, B. Insurgency and Counterinsurgency in Iraq. Stud. Conflict Terrorism 29, 103–121 (2006).
- Kenney, M. The Architecture of Drug Trafficking: Network Forms of Organisation in the Colombian Cocaine Trade. Global Crime 8, 233–259 (2007).
- Knoke, D. 'It Takes a Network': The Rise and Fall of Social Network Analysis in US Army Counterinsurgency Doctrine. Official Journal of the International Network for Social Network Analysts (2013).
- Lazer, D. et al. Life in the network: the coming age of computational social science. Science 323, 721 (2009).
- Lazer, D. et al. Life in the network: the coming age of computational social science. Science 323, 721 (2009).
- Leuprecht, C., Aulthouse, A. & Walther, O. The puzzling resilience of transnational organized criminal networks. Police Pract. Res. 17, 376–387 (2016).
- Lipton, E. & Creswell, J. Panama Papers Show How Rich United States Clients Hid Millions Abroad. The New York Times (2016).
- Marighella, C. Minimanual of the urban guerrilla. Survival 13, 95–100 (1971).
- Masys, A. J. Networks and Network Analysis for Defence and Security. (Springer Science & Business Media, 2014).
- McCarthy-Jones, A., D Baldino, U. of N. D. A. & Authors. Mexican drug cartels and their Australian connections: tracking and disrupting dark networks. The Journal of the Australian Institute of Professional Intelligence Officers 24, (2016).
- McChrystal,S. A. It Takes a Network. Foreign Policy (2011). Available at: http://foreignpolicy.com/2011/02/21/it-takes-a-network/. (Accessed: 21st April 2017)
- Messersmith, Eric Thomas, Political corruption in Japan: A study of the theory, causes and effects with particular reference to the Yakuza factor in banking scandals and prolonged recession. (University of Miami, 2003).

- Morselli, C. Inside Criminal Networks: (Springer New York, 2009).
- Muckian, M. J. Structural vulnerabilities of networked insurgencies: Adapting to the new adversary. Parameters 36, 14 (2006).
- Munro, P. People smuggling and the resilience of criminal networks in Indonesia. Journal of Policing, Intelligence and Counter Terrorism 6, 40–50 (2011).
- Owens, P. Economy of Force: Counterinsurgency and the Historical Rise of the Social. (Cambridge University Press, 2015).
- Raab, J. & Milward, H. B. Dark Networks as Problems. Journal of Public Administration Research and Theory: J-PART 13, 413–439 (2003).
- Rak, J. in Resilient Routing in Communication Networks 11–43 (Springer International Publishing, 2015).
- Roberts, N. & Everton, S. in Eradicating Terrorism from the Middle East (ed. Dawoody, A. R.) 29–42 (Springer International Publishing, 2016).
- Scott, J. Social Network Analysis. (SAGE Publications, 2012).
- Shawn T. Flanigan, S. D. S. U. Motivations and Implications of Community Service Provision by La Familia Michoacána / Knights Templar and other Mexican Drug Cartels. Journal of Strategic Security 7, 5 (2014).
- Simser, J. Plata o plomo: penetration, the purchase of power and the Mexican drug cartels. Journal of Money Laundering Control 14, 266–278 (2011).
- Siniawer, E. M. Ruffians, Yakuza, Nationalists. (Cornell University Press, 2017).
- Souza, F. ‘Quem for pego roubando será punido severamente’: o cartaz anticrime atribuído ao Comando Vermelho - BBC Brasil. BBC Brasil (2016). Available at: http://www.bbc.com/portuguese/brasil-36980813. (Accessed: 5th April 2017), authors translation
- Toth, N. et al. The importance of centralities in dark network value chains. Eur. Phys. J. Spec. Top. 222, 1413–1439 (2013). World Drug Report, 2015. (UN, 2015).
- Xu, J. & Chen, H. Criminal Network Analysis and Visualization. Commun. ACM 48, 100–107 (2005). in Drugs on the Dark Net (ed. Martin, J.) (Palgrave Macmillan, 2014).