Covert networks: structures, processes and types

Kathryn Oliver

This paper describes the extant literature on covert networks, and provides an outline of the main substantive and methodological hypotheses suggested and/or tested in this field. We provide some preliminary analyses demonstrating the lack of consensus about these hypotheses, which will form the basis for a programme of work aiming to analyse covert network data.

1. Introduction

The application of network analysis to criminal, terrorist and other secret communities is intuitively appealing. They are not likely to leave around organizational charts of the kind favored by overt managements; nor are they likely to publicize membership lists. For parties interested in who these people are, what they do, and how they plan to do it, therefore, the data available on which to formulate these types of conclusion are primarily relational: communications, kinship ties, co-participation in events – and hence ideally suited to relational analysis.

Many applications of SNA to covert networks have focused on the disruption of criminal gangs – on enabling the construction of evidence about membership, actions and plans in order to prevent them. Thus, work has focused on concepts such as 'resilience' and 'disruption' of covert networks; on methodological difficulties such as link prediction (Rhodes and Jones 2009, 60:1373-1383) boundary definition and missing data; on how to maximise the eradication of such networks. This is entirely understandable given the motivation of the researchers and funders involved, who are primarily military and law enforcement organisations.

However, network analysts have gathered data on covert (or "dark" or "illegal") populations beyond criminals and terrorists. In many ways, the best definition is one of the earliest: "a secret society is a persisting pattern of relationship which links participants in secret activities " (Erickson 1981, 60:188-210). (Raab and Milward 2003, 13:413-439). Covert social movements such as Suffragettes may be reasonably included, as can political organisations such as Anonymous. A common factor to all covert networks is the need or wish to remain secret; although what is to be kept secret and from whom differs, and indeed is rarely specified (Crossley et al. 2010).

However, much of the literature on covert networks is an attempt to describe and resolve opposing tensions; the requirement to be secret and the ability to achieve network or individual aims. It is important to consider the severity of the consequences of network detection, 'infiltration' or 'exposure', which may range from embarrassment, to death (Bakker, Raab, and Milward 2012, 31:33-62). The danger to the individual will differ according to circumstance, as will the interest of the outside world in the network (e.g. drug dealing vs. swingers). The literature claims that covert networks are differently shaped by different types of risk (Erickson 1981, 60:188-210;Helfstein and Wright 2011, 55:785-813), but the concepts of secrecy and covertness are rarely developed in detail. Indeed, as Crossley and colleagues note, covertness is unlikely to be a discrete binary state, and secrecy is part of most human relationships (Goffman 1959;Simmel 1906, 11:441-498).

Nevertheless, perhaps driven by major security concerns, there are common assumptions regarding the nature of these networks; not least the assumption that structural properties will identify inherent vulnerabilities which allow these networks to be attacked. There is substantial controversy about the structure and nature of these networks. Most research in the area focuses on case studies or action sets (i.e. data gathered around a particular event such as 9/11), which may be untypical. There is significant disagreement about theoretical explanations and interpretations of covert network data, perhaps stemming from differences in approach, data used, methods, context or other exogenous factors. One of the difficulties in synthesizing knowledge on covert networks is the flexibility of terminology used. Often, colleagues come from disciplinary or practice backgrounds in which words have specific meanings. For example, in intelligence and security, a “strong tie” is one which has been ‘confirmed by a secondary source (Sparrow 1991, 13:251-274), whereas to a network analyst this indicates something different. Similarly a “weak tie” is an unconfirmed tie, but to Granovetter and colleagues a weak tie is a distal connection between alters (Granovetter 1973, 78).

In this paper, we aim to describe current debates, describe consensus and resolve controversy in the field, and produce appropriate and generalizable theory and methods for analysis of covert networks. This paper is structured as follows. We outline the state of the field in terms of theoretical and empirical literature on covert networks. We summarise what is known and unknown about the main theories, empirical findings and methodological questions and solutions proposed across the following themes: Network membership and ties, aims and activities, the characteristic structures of covert networks, formation, evolution and disruption covert networks. We discuss the nature of secrecy when applied to covert networks. Finally, we outline some methodological problems specific to covert networks and solutions proposed. On the basis of this review, we propose a research agenda.

2. Network membership and ties

As noted above, most work on covert networks has focused on criminal and terrorism, often focusing on military targets and problem solving. Milward and Raab argue that there is a distinction between overt and covert networks which is not the same as illegality (Milward and Raab 2006, 9:333-360) (see Figure 1. Lauchs (2012) adds to this definition, explaining that covert networks operate at the cost of other individuals and groups (Lauchs, Keast, and Yousefpour 2011, 21:110-127). What is sure is that there is a huge range of activities and organisations which can be designated ‘covert’ in some way. In fact, the defining characteristic of ‘covert’, ‘dark’, or ‘illicit’ networks is said to be their secrecy (Baker and Faulkner 1993:837-860;Raab and Milward 2003, 13:413-439). Secrecy operates at several levels. Identities, aims, activities, may all or some be secret, with different consequences and risks to the individual and the network as a whole.

Figure 1 Covert/Overt and Legal/Illegal organisations, adapted from Milward (2006)

	Legal	Illegal
Overt	Sinn Fein	Charles Taylor’s Liberia
Covert	German Spies in Iraq	Al Qaeda, cocaine trafficking

A reasonable assumption would be that covert networks are so because membership or activities are kept secret. For example, members may wish to achieve ends which must be kept secret (e.g. purchasing sex or drugs); or activities which further those ends much be kept secret (such as individual acts of terrorism in a global Jihad). Work on the IRA and Suffragettes (Crossley et al. 2012, 34:634-644;Edwards 2014, 13:48-69;Edwards and Crossley 2009, 4;Stevenson and Crossley 2014, 13:70-91) shows however that secrecy of both identity and activities was managed on a case by case basis, in a subtle and nuanced manner. Secrecy operates at several levels. Identities, aims, activities, may all or some be secret, with different consequences and risks to the individual and the network as a whole. As noted above, the consequences of exposure will of course vary even with these simplistic parameters; being found having an affair will likely have drastically different results from being identified as a Mafia informer, for example.

A brief glance at the literature indicates that the terms 'covert network' and its synonyms have been used to describe individuals and groups including drug users, clubbers, men who have sex with men, swingers, terrorists, youth gangs, persecuted minorities and religious, political movements such as suffragettes and Critical Mass, Freemasons, and criminals of all types. Correspondingly, the ties which form these networks are diverse ranging from communication, transference (of money, disease, ideas, and so on), authority, and many others. Size is also disputed, with some claiming networks remain small to reduce risk (Bouchard 2007, 8:325-344) and others claiming large size as a methodological problem.

The requirements for different types of secrecy, for different lengths of time and from different audiences are surely likely to produce a range of network structures. Furthermore, the effects of these facets of secrecy are not well understood. Covert nodes may reasonably be assumed to have fewer ties than overt nodes (shown by Keegan et al 2010 using MMORPG data), but in a recent study of child exploitation websites, Westlake and colleague showed the reverse (Keegan et al. 2010:201-208). We find that the nature of secrecy is under-theorised.

Relatedly, we find that tie type is not considered in enough depth when theorising about covert networks (Crossley, Stevenson, Edwards, and Harries 2010). Communications ties are likely to form different types of structures from sexual partnerships, yet this diversity is not reflected in wider discussions. Often, studies conflate multiple types of ties into one network, or fail to specify the type of tie being used. This does not create a sense of trust in the reader. Furthermore, this leads to difficulty in boundary specification.

Pre-existing ties and segregation

One of the issues about boundary specification is that it is not always clear who is a member and who is not. For example, in a terrorist network, ties may include kinship or friendship (see e.g. PIRA work). However, this does not mean that all relatives of a terrorist are also terrorists, yet they would often be included in covert network graphs.

Theoretically speaking, following Erickson (Erickson 1981, 60:188-210) many people have theorised about the role of pre-existing ties in covert network formation and existence. Covert networks are said to be based on pre-existing ties, or rely on social proximity for formation (Harris-Hogan 2012, 5:137-154;Lauchs, Keast, and Yousefpour 2011, 21:110-127;Milward and Raab 2006, 9:333-360). Prior social interaction is said to increase resilience and reduce the vulnerability of covert networks by reliance on trustworthy individuals (Keegan, Ahmed, Williams, Srivastava, and Contractor 2010:201-208;Lauchs, Keast, and Yousefpour 2011, 21:110-127). Covert networks may be more or less embedded in overt social interactions (Carley, Lee, and Krackhardt 2002, 24:79-92;Cockbain, Brayley, and Laycock 2011, 5:144-157;Crossley, Edwards, Harries, and Stevenson 2012, 34:634-644).

Segregation (on a psychological level) may also facilitate recruitment (Raab and Milward 2003, 13:413-439). Since much of the data pertaining to segregation seems to come from military and conflict studies, such as factioning while at war (Caselli and Della Porta 1991;Crenshaw 2002;Della Porta 1992, 4:259-290), it is not surprising that many suggest that segregation is a natural consequence of forming covert networks. However, it seems likely that this would depend heavily on the types of activities, populations and wider social context of the network in question. Indeed, recent work exploring the networks of child trafficking offenders and victims identified segregation amongst ethnic lines – but noted that this segregation may part of the wider community, rather than specifically about sex offenders *per se* (Cockbain, Brayley, and Laycock 2011, 5:144-157).

External factors are also likely to affect the lifespan and boundary of the covert network. For example, the legal environment may change (legalising types of sexual behaviour or drug use). However, in the absence of empirical studies comparing segregation of covert network and over network members from wider communities, it is difficult to draw any conclusions.

Homophily

Several studies have described the role of homophily in creating covert networks. Covert networks are frequently described as being based on homophily (Gill and Freeman 2013, 1:68-94;Milward and Raab 2006, 9:333-360;Reed 2007;von Lampe 2009) of one kind or another. Shared aims, values and other personal reasons may motivate people to join and remain in covert networks (Harris-Hogan 2012, 5:137-154). Lauchs argues that the motivation of covert network members can be described in three ways: mercenaries, ideologues, captive participants (Lauchs, Keast, and Yousefpour 2011, 21:110-127). However, this does not account for the broader definition of covertness and covert networks discussed above.

show that ties in covert networks (criminal youth gangs) can be predicted by age, sex and type of crime) whereas Klerks (2001) using the Fijnaut Group dossier (1995-1998), which looked at organised crime, described covert network as becoming less ethnically homogenous over time (Carrington and van Mastrigt 2013, 14:123-140;Klerks 2001, 24:53-65;van Mastrigt and Carrington 2013:28). These findings – and questions – may simply reflect the type of data available to network analysts. Cockbain argues that covert networks may be ethnically homogenous, but this may reflect wider ethnic segregation rather than segregation based on covert activities (Cockbain, Brayley, and Laycock 2011, 5:144-157). However, Keegan et al (2010) have shown that both online and off-line covert networks display dissortative mixing, possibly as a means of reducing risk of identification (Keegan, Ahmed, Williams, Srivastava, and Contractor 2010:201-208).

Summary

Indeed, the field is characterised by a dearth of empirical data, and theories of which the generalizability is unclear. Covert networks can be described amongst many types of communities and groups. How, then, is it possible to theorise about such diverse groups in a way which retains the complexity of the literature and contexts within which these networks form, operate and dissolve?

3. Network aims and activities

Network aims and activities

As noted, covert networks come in many types. Yet the literature largely divides covert networks into groups with terrorist and/or criminal aims and activities (Harris-Hogan 2012, 5:137-154;Varese 2010). These aims and activities are likely to affect network structure. Morselli (2007) claims that network structure is affected by network aims, with terrorist networks being less centralised than criminal ones(Morselli, Giguire, and Petit 2007, 29:143-153). Krebs (2002) explicitly says that covert networks design their structure to maximise secrecy, efficiency and resilience through "judicious use of shortcuts" (Krebs 2002, 24:43-52). This point of view is widely suppor(Helfstein and Wright 2011, 55:785-813;Raab and Milward 2003, 13:413-439). There is a tendency to describe networks as though they are planned or designed for purpose; although in the absence of any evidence that network members can plan and modify network structures, or indeed achieve a birds-eye view of the overall structure, this should be interpreted with caution. However, the aim and activities of the networks likely affect the types of risks suffered by members and by the network overall (Morselli, Giguire, and Petit 2007, 29:143-153) and therefore identification of these and other exogenous factors on network properties, is worth considering.

Baker and Faulkner (1993) describe how network aims can be simple or complex using communications networks from conspiracies in electronics engineering (Baker and Faulkner 1993:837-860). They define complex network aims as those with high information requirements (for example, extremely technical knowledge) and simple aims as having low information requirements. They show relationships between these opposites and different network properties.

Of course, it should be noted that these examples are static, and do not account for the extremely likely possibility that covert network members adjust their activities according to risk and exposure. This dynamic aspect is discussed below in the section 'Network Evolution'.

Absorption

Another aspect of covert movements or organisations which bears re-examining is the amount of time invested in the covert activities in question; or, to put it another way, how absorbing the covert ties are. Although untested, the literature suggests that covert ties can take up a lot of members' time (Erickson 1981, 60:188-210;Raab and Milward 2003, 13:413-439). However, other metrics of 'absorption' may be of equal importance; for example attributed importance of the tie, or regularity of interaction.

Network effectiveness and capacity to act

Unsurprisingly, many studies focus on what covert networks *do*, rather than their nature *per se*. However, only a few studies report proxy measures for capacity or network effectiveness; number of casualties (Helfstein and Wright 2011, 55:785-813), ‘lethality’ (Asal and Rethemeyer 2008, 70:437-449;Horowitz and Potter 2013:0022002712468726), number of suicide attacks (Acosta and Childs 2013, 36:49-76) which is clearly not applicable to all contexts. Asal and Rethemeyer use NBREG models to test the effects or increased connectivity, state support, ideology and nationalism, and age and size on the lethality (capacity to act) of different terrorist networks (Asal and Rethemeyer 2008, 70:437-449). However, as with the concept of covertness itself, ‘capacity to act’ and ‘effectiveness’ are under-theorised. Both of these concepts operate at individual and organisational levels, for example.

A large proportion of studies focus on the resilience of covert networks. Largely this was interpreted as ‘retaining capacity to act; (Koschade 2006, 29:559-575;Krebs 2002, 24:43-52;Milward and Raab 2006, 9:333-360), although how this differs from ‘longevity’ is not always clear (Bouchard 2007, 8:325-344). Lauchs (2012) states that resilience is a measure of how difficult it is to disrupt networks; of the capacity to survive attack – although no proposed metrics to evaluate this are proposed (Lauchs, Keast, and Yousefpour 2011, 21:110-127). Bouchard develops this concept further, proposing three sub-concepts to resilience: vulnerability (likelihood of being damaged by external attack), elasticity (ability to return to prior state after shock) and adaptive capacity (ability to modify circumstances to protect components (Bouchard 2007, 8:325-344). Morselli (2007) and others prefer to consider ‘efficiency’ as a definition of capacity to act (Morselli, Giguire, and Petit 2007, 29:143-153); although this is largely meant as a synonym of ‘ease of communication’ (Lindelauf, Borm, and Hamers 2009, 31:126-137), and should therefore be interpreted with care.

Resilience is said to be promoted by access to resources (territory, technology, finances, weapons and law), actors, and linkages (linkages such as pre-existing ties, kinship, friendship, shared ideology and values) (Krebs 2002, 24:43-52;Milward and Raab 2006, 9:333-360). Adaptable and flexible networks are said to be more resilient and are multiplex (Krebs 2002, 24:43-52;Raab and Milward 2003, 13:413-439). Structurally, decentralised networks with functionally or structurally equivalent central nodes are described as more resilient (Klerks 2001, 24:53-65;Koschade 2006, 29:559-575;Krebs 2002, 24:43-52) although this last is disputed (Koschade 2006, 29:559-575;Milward and Raab 2006, 9:333-360). Philips recently showed that covert organisations survived longer if they are themselves connected to high-degree organisations ((Phillips 2013:1-12) using BAAD database). Overt networks within which covert networks are embedded may increase resilience (Gimenez-Salinas Framis 2011).

Crenshaw (2010) provided a typology of consequences of changes to the external determinants of covert networks which works well as a definition of resilience: “[These] may be measured in terms of behaviour (level, frequency intensity of violence, strategic targeting, methods OR compromise with government), weakening or strengthening of the organization in term of size, resources, efficiency” (Crenshaw 2010). However, most, if not all of these statements remain hypothetical.

Summary

Network aims and activities may affect network structure, but again the relationship between individuals' ties and overall aims of social movements is not clear. Network capacity and resilience are described as a consequence of several network properties, although empirically these theories remain untested. Below, we examine some of the statements made about the characteristics of covert networks, in terms of overall network properties.

4. Characteristic network properties of covert networks

Covert networks are often described in terms of general network properties, or as lying along continuums**.** Although some suggest that covert networks are like overt networks (Asal and Rethemeyer 2008, 70:437-449;Crenshaw 2010), few comparative studies exist. Those that do tend to compare online and offline covert networks (Keegan, Ahmed, Williams, Srivastava, and Contractor 2010:201-208), which show apparently similar structures.

As the reviews above suggest, both endogenous and exogenous factors have been proposed which cause or are caused by covert networks. Implicitly or explicitly, researchers in the field of covert networks have described covert networks as exhibiting characteristic structures and microstructures.

Often these are presented as axes or opposing poles along which covert networks align. Lauchs and Morselli compare Terrorist and criminal enterprises as being more or less visible (Lauchs, Keast, and Yousefpour 2011, 21:110-127;Morselli, Giguire, and Petit 2007, 29:143-153). Everton presents two types of covert network; provincial and cosmopolitan. Provincial networks are described as dense, with high clustering and strong ties, whereas cosmopolitan networks are sparse, with low clustering and weak ties (Everton 2011, 32:12). Everton argues that both types of structure have pros and cons, and that effective covert networks balance between the two extremes. More generally, covert networks are described as loosely-organised (Natarajan 2000, 11:273-298), sparse (Krebs 2002, 24:43-52), centralised or decentralised (Erickson 1981, 60:188-210), hierarchical, flat or poly-centric (Harris-Hogan 2012, 5:137-154;Milward and Raab 2006, 9:333-360;Varese 2013, 29:899-909), show core-periphery structures (Demiroz and Kapucu 2012, 15:271-295) or exhibit other characteristic micro-structures (Gill and Freeman 2013, 1:68-94).

The evidence on these concepts are summarised briefly below.

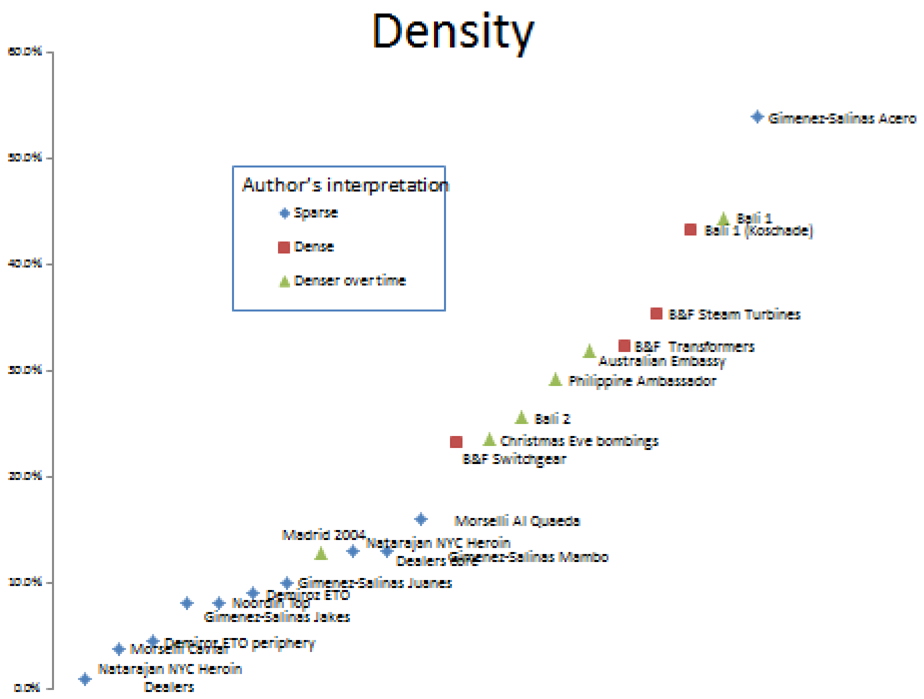
Density

Covert networks are said to be sparse or to have maximally low density (Demiroz and Kapucu 2012, 15:271-295;Gimenez-Salinas Framis 2011;Krebs 2002, 24:43-52;Milward and Raab 2006, 9:333-360;Natarajan 2000, 11:273-298;Toth et al. 2013, 222:1413-1439). Demiroz et al quantify this as having a density of 9%, with a core-periphery differential of 73.5% and 4.41% respectively. Naratajan

(2000) uses percent-density scores to describe cocaine trafficking networks in NYC, finding that the communications network for this organisation was sparse (Natarajan 2000, 11:273-298).

However, Baker and Faulkner (1993) tested this hypothesis on three communications networks and found densities of 23.3%, 32.4% and 35.5% respectively, and claimed this disproved the 'sparse' theory (Baker and Faulkner 1993:837-860). Koschade 2002 defined 'high density" as 43% (Koschade 2006, 29:559-575), and Milward and Raab draw a connection between shared aims and values and high density (Milward and Raab 2006, 9:333-360). Clearly there has been no common frame of reference as to what 'sparse' and 'dense' mean in networks (see Figure 2).

Figure 2 Reported density in covert networks



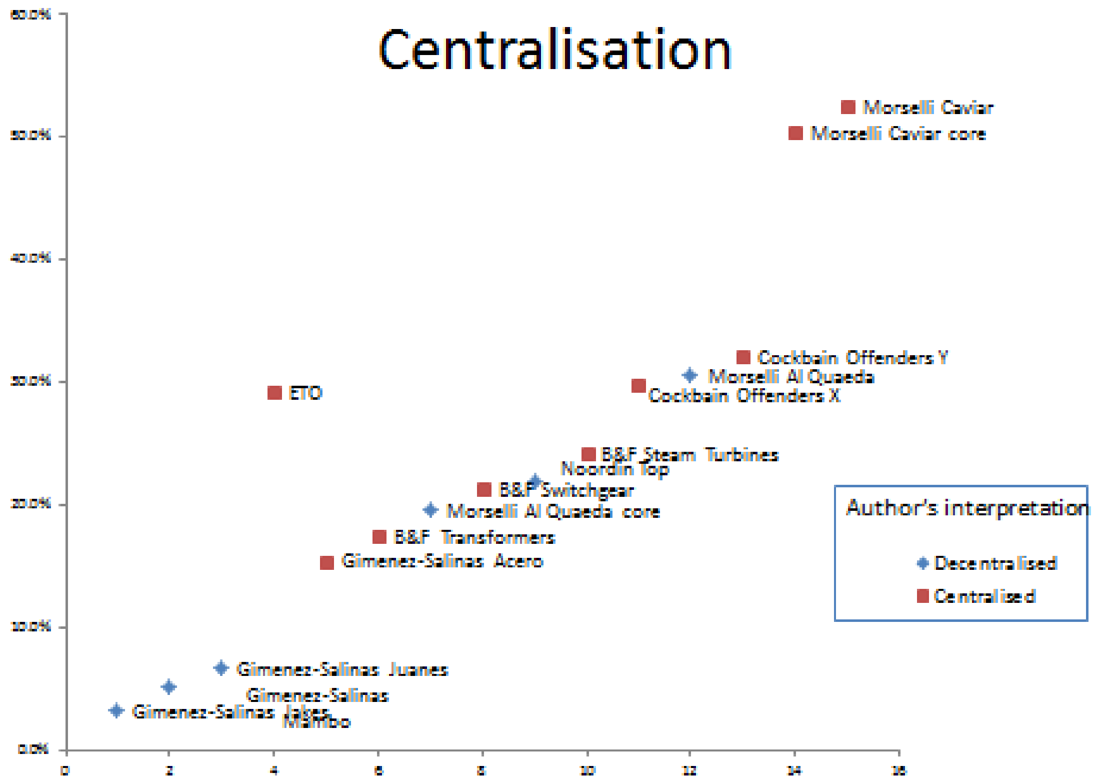
Morselli argues that density is related to the type of covert activity, with terrorists requiring more secrecy than criminals, and hence exhibiting denser networks (Morselli, Giguire, and Petit 2007, 29:143-153). Density of covert networks was shown by Helfstein and Wright (2011) to increase over time, analysing six terrorist attack networks (Helfstein and Wright 2011, 55:785-813). Others suggested that density of networks was increased in the presence of pre-existing ties, but this remains untested (Krebs 2002, 24:43-52;Raab and Milward 2003, 13:413-439). Specific attributes may explain variation in density. More skilled covert network members (proxy: better educated) tended to adopt less dense structures in attack networks, for example (Helfstein and Wright 2011, 55:785-813).

However, most social networks are sparse, so the relative sparseness of covert networks compared with overt is debateable, even without the clearly contentious theoretical perspectives. Moreover, the effects and causes of density and changes to density are not clear.

Centralisation

Covert networks have been described generally as decentralised structures (Clutterbuck 2008;Keegan et al. 2011:24), which is attributed to the need to protect leaders, to maintain secrecy, to remain efficient (Enders and Su 2007, 51:33-57). This is contested, however (Sageman 2004). Baker and Faulkner tested degree centralisation on three conspiracy networks (1983), and showed these covert networks exhibited centralised structures. This has been supported by later empirical work (Cockbain, Brayley, and Laycock 2011, 5:144-157;Demiroz and Kapucu 2012, 15:271-295;Varese 2013, 29:899-909). Helfstein and Wright (2011) show that covet networks are not scale free, in their paper applying ERGMS to the JJATT database of attack networks over multiple time periods (Helfstein and Wright 2011, 55:785-813). This supports the suggestion that decentralisation is the norm. Overall covert networks have been described with both centralised and decentralised structures (Crenshaw 2010;Gimenez-Salinas Framis 2011) (see figure 3).

Figure 3 Distribution of centralisation scores across available covert network data



To some extent, centralisation has been conflated – theoretically speaking – with hierarchy. Klerks (2001) studies organised crime in the Netherlands, suggesting that hierarchical models (meaning highly centralised models) are becoming a rarity as these businesses move away from tradition, authoritative setups (Klerks 2001, 24:53-65). Similarly, Natarajan uses low centralisation of NYC heroin dealers to argue that covert networks are non-hierarchical (Natarajan 2006, 22:171-192).

Degree centralisation is a continuous outcome, and it is clear from this figure that there is no agreement on defined thresholds for the binary outcomes of 'centralised' or 'decentralised'. However, theories supporting and explaining both outcomes have been proposed, some tested, which may explain the breadth.

As this summary shows however, there are theories and empirical data on both sides, and little agreement on the definitions of centralised networks. These exogenous and endogenous factors require systematic testing to identify relationships between them and degree centralisation.

Core-periphery/poly-centric structures

Varese's study of the Russian Mafia proposed an alternative theory. In opposition to most literature on Mafia networks which are claimed to be flat, Varese found a polycentric structure around a few central actors (Varese 2013, 29:899-909). To some extent, this is supported by studies which identify core-periphery structures in covert networks. Demiroz and Kapucu's study of Turkey's Ergenkon Terrorist Organisation network, developed from indictment documents showed a network with core periphery statistics of 73.5% and 4.41% density respectively (Demiroz and Kapucu 2012, 15:271-295). It is argued that cores which specialised skills (e.g. finance, strategy, planning) benefit terrorist networks (Raab and Milward 2003, 13:413-439), possibly to increase security for central members. However, not all networks show this property (Lauchs, Keast, and Yousefpour 2011, 21:110-127). Gimenez-Salinas compared 4 criminal networks in Spain which all exhibited core-periphery structures (Gimenez-Salinas Framis 2011). However, Morselli argues that terrorist networks do not show core-periphery structures, whereas criminal networks do (Morselli 2007) although he uses only one case study of each to support this claim (Morselli, Giguire, and Petit 2007, 29:143-153).

Microstructures

Perhaps following the idea of small cells as an organising principle in covert networks, both clusters (Memon et al. 2008:339-344) and cliques (Gill and Freeman 2013, 1:68-94) have been proposed as common micro-structures, often based on homophily around ethnicity and occupation, role/skill specialisation, or pre-existing ties (Demiroz and Kapucu 2012, 15:271-295;Harris-Hogan 2012, 5:137-154;Milward and Raab 2006, 9:333-360;Raab and Milward 2003, 13:413-439).

Memon (2008) showed that many terrorist networks exhibit small world characteristics, i.e. high clustering coefficients and low path length (Memon, Hicks, Harkiolakis, and Rajput 2008:339-344). However, modelling using idealised networks structures did not show clustering (Toth, Guly+ís, Legendi, Duijn, Sloot, and Kampis 2013, 222:1413-1439) and Helfstein and Wright used attack networks to show that covert networks which maximise secrecy do not show clustering (Helfstein and Wright 2011, 55:785-813).

Kirby (2007) re-analyses Sagemen's data (2004) to describe the formation of cliques (Kirby 2007, 30:415-428;Sageman 2004). He argues that cliques can be self-starters, and progress towards fragmentation and isolation, and that they can generate collective identities for members, although these are not tested.

Keegan et al (2011) used online covert networks to test a series of hypotheses about microstructures including reciprocal ties, cyclical structures, and transitivity (Keegan, Ahmed, Williams, Srivastava, and Contractor 2011:24). Using ERGMs, they show that covert networks avoid cyclical structures and are highly reciprocal. They also show that covert networks tend to have few brokerage positions. They argue this increases security, reduces risk of infiltration and protects network members. Helfstein and Wright on the other hand argue that covert networks are more likely to form triads over time (Helfstein and Wright 2011, 55:785-813).

A range of exogenous and endogenous factors affecting or causing these network properties have been proposed. The bidirectional relationships between network properties and these factors are examined below.

Summary

Covert networks are said to display characteristic structures at a whole-network and micro-level. However, the evidence is conflicting and shown to vary with context.

5. The effects of secrecy and risk, and other contextual factors on network properties

All the network properties shown above are, while sometimes assuming diagnostic properties, also said to vary with contextual factors. A complete list of hypotheses summarising these is available from the author, and briefly summarised below.

The factors which promote successful longevity of covert networks, such as those described by Crenshaw (2010) described above, also function as a useful framework to think about contextual factors affecting network structure (Crenshaw 2010). All covert networks – and indeed overt networks – are shaped by external factors. A useful typology of these factors was developed by Crenshaw (2010) using her work on Palestinian groups. The external determinants of covert network evolution include: "government actions (either coercion *or* conciliation), changes in social and/or financial-logistical support, and technological change (especially communications and weaponry). The organization's internal capacity to adapt to the environment and maintain organizational cohesion is also a critical factor". State sponsorship or foster-hood of covert networks (in the form of terrorists) has been described (Raab and Milward 2003, 13:413-439) and shown to facilitate covert network formation and existence (Barnett et al. 2013, 3:721-747;Phillips 2013:1-12).

Thus, a large proportion of the work has been around identifying the relationship between these contextual factors and network properties, and many areas have been touched on already in this paper. Table 1 is a preliminary summary of the overall findings regarding on the characteristics of covert networks and factors said to influence them.

Table 1 Characteristics of covert networks and factors said to be related to them

Contextual factor	Network property (reference)

	Shows increases……………….	Shows decreases
Increasing risk and need for secrecy	Increased density Coleman 1988, 1990)	Decreased density (crossley and Edwards, supported for co-arrest and imprisonment network ties) (Enders and Su 2007)
	Increased centralisation (Demiroz and Kapucu (2012) citing Epstein and wright) Morselli 2009, Morselli et.al 2007)	Descreased centralisation (crossley and Edwards, supported for co-arrest and imprisonment network ties)
	Core periphery structures found (Lauchs)	Core periphery structures not found (Lauchs)
	Role specialisation and leadership concentrated in the core (Morselli 2007)	
	High reciprocity Keegan et al. (2011) High triads Helfstein and Wright (2011), Raab and Milward 2003 Transitive hierarchies formed Keegan et al. (2011)	Reduced brokerage positions Keegan et al. (2011) Reduced cyclical structures Keegan et al. (2011)
Increased vulnerability to node removal or network attack	Increased centralisation	Decreased centralisation (Demiroz and Kapucu)
Stable environments		Decreased centralisastion (Enders and Su 2007)
High individual effort	Increased centralisation (Enders and Jindapon 2010)	
Increased time	Increased density Formation of cliques and triads (Helfstein and Wright)	Decreased density Decreased centralisation (Described using Sageman’s Al Qaeda data (Xu and Qin 2004) and Colombian cocaine trafficking (Milward and Raab 2006), Jamaah Islamiyah (Helfstein and Wright 2011), drug trafficking (Jackson, Herbrink, Jansen 1996 /Klerks 2001/Layne et. al. 2001/ Brezezinski 2002/ Griffith 199, Raab and Milward 2003
Complex aims/information requirements	Increased centralisation Baker and Faulkner 1993)	Reduced density (Morselli 2007, Helfstein and Wright 2011)
Simple aims and information requirements	Increased density (Morselli 2007)	
Criminal rather than terrorist activities	Increased centralisation Krebs and Caviar data (Morselli 2007) Core-preiphery structrues present	
Centralised control of resources	Increased centralisation Auschwitz underground, Luppollo crime family, English marijuana network, norwegian underground (Erickson 1981) Increased central recruitment (Erickson 1981)	Fissioning of network (Crossley 2010)
State support	Network formation (Philips 2014, Barnett 2013)	

However, network properties are themselves also theorised to influence the processes and outcomes associated with covert networks. Overall, these are summarised in **Table 2**.

Table 2 Effects of network properties on covert networks

	Supported	Not supported
High Centralisation	Increased vulnerability to attack or node removal (Jackson, Herbrink, Jansen 1996 /Klerks 2001/Layne et. al. 2001/ Brezezinski 2002/ Griffith 1997Raab and Milward 2003 Carley, Lee, Krackhardt (2002) Milward and Raab (2006) Cockbain (2011) citing McAlister)	Enders and jindapon 2010, Enders and Su 2007 Bouchard 2007
Low centralisation	More resilient network (Milward and Raab 2006)	
High density	High efficiency Koschade (2006), Morselli 2007 High security/secrecy Koschade (2006) Morselli 2007	
Low density	Low efficiency Morselli 2007 Low security Morselli 2007	
CLiques	Memon 2009	Toth 2013 Helfstein and Wright 2011

One of the biggest discussions in this field is around the tension between secrecy and 'efficiency' – or the need to be able to communicate (Crossley, Edwards, Harries, and Stevenson 2012, 34:634-644;Lindelauf, Borm, and Hamers 2009, 31:126-137;Morselli, Giguire, and Petit 2007, 29:143-153). However, as this table shows, this binary relationship is likely to be far more complex.

Summary

The context within which covert networks form and operate is likely to affect the types of structures which form and are able to survive.

Thus, in the absence of good empirical evidence supporting these theories, I now summarise the evidence about the processes which covert networks are said to undergo; network formation, control, and dissolution.

6. Network formation

Formation of ties within covert networks is naturally enough a topic of interest. Methodological questions about node addition and tie formation translate into substantive questions about how people become recruited to covert organisations.

Recruitment

Locating recruitment within a network would be informative about mechanisms of network formation. Using an Islamist attack network, Helfstein and Wright show that scale-free covert networks do not use high-degree actors to recruit new members (Helfstein and Wright 2011, 55:785-813). However, this theory may not allow for the role of context. Erickson (1981) compared networks with centralised (e.g. Auschwitz support networks) and decentralised (e.g. marijuana users in Cheltenham) control of recruitment, noting that they produced corresponding centralised and decentralised structures (Erickson 1981, 60:188-210).

The mechanism of recruitment is still unclear. Cockbain (2011) suggests victim recruiters to networks of child sex trafficking can be identified through high betweenness scores (Cockbain, Brayley, and Laycock 2011, 5:144-157). Recruitment to offender networks on the other hand can be based on pre-existing ties to offenders or victims, or can be recruited directly by other offenders. Duering (2014) explores initiation of ties amongst support networks for Jews during the Holocaust, showing that several mechanisms (self-initiated, pre-existing ties, referral) described the formation of ties in these networks (Düring 2014).

This discussion illuminates a fundamental tension between the need for secrecy and the need for survival (Baker and Faulkner 1993:837-860). Covert networks may recruit trustworthy individuals in order to protect themselves. Alternatively, networks which are easy to join, such as drug dealing networks may be protected in that networks remain elastic and leaders may be easily replaced (Bouchard 2007, 8:325-344).

Pre-existing ties

As described earlier, pre-existing ties are said to underpin and help to maintain covert networks. This is part around formation of networks, where pre-existing ties are said to be important (Crossley, Edwards, Harries, and Stevenson 2012, 34:634-644;Edwards and Crossley 2009, 4;Erickson 1981, 60:188-210;Sageman 2004). Conversely, new ties may be generated through covert activities (Diani 1997, 2:129-147;Feld 1981:1015-1035;Feld 1982:797-801) which suggest recruitment occurs through individuals attempting to join, rather than being sought out. As Coleman says (1990) networks are often the unintended consequences of other activities, so it is important to bear this in mind so that the network analyses are not over-analysed (Coleman 1990:91-112). However, the literature seems to suggest that networks tend to form around shared spaces, events and activities. Pre-existing ties may or may not play a role in bringing people to those shared arenas, and suggest that covert networks are multiplex in nature (Klerks 2001, 24:53-65;Reed 2007).

Factioning

The other main theory about the formation of covert networks states that factioning and fragmentation lead to the formation of covert groups as ‘spin-offs’ of earlier groups (Crenshaw 2010;Della Porta 1995;Rapoport 2002, 8:42-43;Sedgwick 2007, 30:97-112)Crenshaw also develops the idea that generational ‘waves of action’ contribute to this process.

Summary:

- Covert networks form through fragmentation or factioning

- Recruitment to covert networks may rely on pre-existing ties, self- or alter-referral, or other mechanisms
- The location of recruitment within a network may be related to centrality or the overall network structure

None of these theories have been empirically tested.

7. Network control and leadership

Leadership

Attention has often focused on who controls and leads covert networks. For example, some claim that the most central actors in covert networks are the most vulnerable (Baker and Faulkner 1993:837-860;Krebs 2002, 24:43-52), and are therefore unlikely to be the leaders (Lauchs, Keast, and Yousefpour 2011, 21:110-127) Carley, Lee and Krackhardt 2001; (Crenshaw 2002;Crenshaw 2010;Jackson, Herbrink, and Jansen 1996, 2:83-105;Westlake, Bouchard, and Frank 2011, 3:1-32)Westlake 2011). Conversely, others claim that centrality measures are good predictors of the most important people or leaders of covert networks (Koschade 2006, 29:559-575;Lindelauf, Borm, and Hamers 2009, 31:126-137;van der Hulst 2009, 12:101-121;Varese 2013, 29:899-909) especially in centralised networks (Carley, Lee, and Krackhardt 2002, 24:79-92) – even if they are the most vulnerable (Koschade 2006, 29:559-575;Raab and Milward 2003, 13:413-439). Complicating the matter further, Demiroz and Kapucu show that membership of elite sections of society can protect high-centrality actors from prosecution even when they are active members of covert networks (Demiroz and Kapucu 2012, 15:271-295). Here, the social context was such that even though centrality accurately predicted the leaders of terrorist organisations, they were individual held in such high social standing that they were not vulnerable to attack.

Most studies use degree centrality or betweenness centrality (e.g. (Gimenez-Salinas Framis 2011;Sparrow 1991, 13:251-274;Varese 2013, 29:899-909) to identify leaders. Others have developed specific measures, discussed below under methodological questions. Klerks suggests that brokerage and 'bridging' identifies important actors (Klerks 2001, 24:53-65). Natarajan (2000) uses content analysis-correlation between status (use of 'Sir' in phone conversations) with expressing satisfaction and providing information with requesting information and clarifying orders (Natarajan 2000, 11:273-298). This innovative approach showed how covert network members have differential power statuses. However, these studies outline a fundamental tension between the need for access to network members (in order to enact leadership or control) and the need to protect leaders by reducing visibility. We find that this debate misses some of the subtleties of covertness; visibility of what? To whom? Over which time period?

It is worth considering some of the theoretical debates and what we may term 'real-world' practicalities of controlling covert networks. Leadership is a vague concept, but many identified studies discuss network leadership as though they had 'birds' eye views' of the network, and were thus able to manipulate and design it to adapt the network according to external pressures. The control of a network will vary widely with the types of activities carried out by members. For example, covert social movements driven by ideological or political aims are likely to need to need some overt leadership who define the aims and means of the movement – one thinks of the video statements made by Osama bin Laden, or the political speeches of the Pankhursts. However, networks in which individuals seek activities of a different kind - drug users or individuals engaging in sexual practices - are perhaps in less need of control for the sake of the network overall.

Campana and Varese (2013) add another layer of complexity by considering the use of overtness and covertness as a means of control (Campana and Varese 2012, 15:13-30). Again, we return to the problem of what is kept secret, by whom, how, and for what reason – and the effects of these facets of secrecy on network structure. They discuss the effect of shared acts of violence on the structure of the network, and show that committing acts of violence (e.g. executions) together, participants are bound by shared overt knowledge of the act, which also segregates them from others by having to keep their activities concealed. The role of trust in control, by minimising disputes and reducing the risk of exposure is also hypothesised by Raab and Milward (2003) who discuss how breaking ties in networks is prevened by actual or threatened use of force (Raab and Milward 2003, 13:413-439).

Roles and specialisation

Research has also been focused on the relationship between functions within networks and structural properties of networks.

As described above, some argue that covert networks try and avoid formation of brokerage structures or highly centralised actors in order to protect themselves and members, although Carley et al (2002) argue that peripheral individuals act as brokers between networks and spread information (Carley, Lee, and Krackhardt 2002, 24:79-92). More generally, it is argued that members of covert networks tend to develop and cluster around specialised roles, leading to functional differentiation within covert networks (Calderoni 2011;Malm and Bichler 2011, 48:271-297). This differentiation may become more acute the higher up the hierarchy one goes (Bouchard 2007, 8:325-344), over time (Raab and Milward 2003, 13:413-439) and may lead to development of specialised cliques (Raab and Milward 2003, Crossley 2012). Klerks (2001) argues however, that this does not happen, based on his analysis of organised crime over 8 years in the Netherlands, and may reduce resilience (Klerks 2001, 24:53-65).

A few studies comment on the role of women in covert networks. Varese (2013) finds that wives relay orders on behalf of the husbands, approaching structural equivalence (Varese 2013, 29:899-909). Others show that women can occupy important positions because of pre-existing ties (Gimenez-Salinas Framis 2011)or that they form new ties and strength existing contact, leading to greater cohesion (Klerks 2001, 24:53-65).

Summary

The effects of network position on roles of individuals in covert organisations – and vice versa – is still unclear. Some evidence suggests that there are resilience implications in role specialisation and differentiation.

8. Network evolution, disruption and dissolution

While network analysis is a useful tool to describe and analyse covert organisations, it usually offers snapshots rather than a dynamic model of the formation, evolution and dissolution of these organisations, which are naturally dynamic themselves (Sparrow 1991, 13:251-274)). However, reflecting the interests of funders in shutting down criminal and terrorist organisations, theories about the nature of these changes, and techniques to create changes abound.

Covert networks may aim to evolve deliberately; in response to increased risk for example, by changing activities (e.g. from dealing heroin to dealing cocaine) (Bouchard 2007, 8:325-344). Helpfully, Crenshaw presents geneologies of organisational development of covert networks (e.g. cohesive/homogenised, or fragmented/specialised) (Crenshaw 2010). Or covert networks may evolve or end due to targeted action. Fragmentation of covert networks may result from changes over time (Milward and Raab 2006, 9:333-360) or in response to some kind of disruption (Koschade 2006, 29:559-575).

The most commonly-discussed type of disruption of covet networks is removal of central nodes (leaders; although see discussion above for reflections on the appropriateness of this metric). Carley defines disruption as being networks where information cannot flow, individuals cannot take decisions or reach consensus, or cannot perform tasks accurately (Carley, Lee, and Krackhardt 2002, 24:79-92). Crenshaw argues that networks with strong leaders are more cohesive and less prone to factioning. Therefore, removal of these nodes may disrupt the networks effectively ((Crenshaw 2010;Tsvetovat and Carley 2002). Westlake showed that removal of the five most central nodes in a network on child exploitation websites lead to a decrease in their newly-developed metric ‘Network Capital’ (Westlake, Bouchard, and Frank 2011, 3:1-32). This may apply less in decentralised or highly adaptable networks, or in networks where there are several well-connected individuals (Carley, Lee, and Krackhardt 2002, 24:79-92;Cockbain, Brayley, and Laycock 2011, 5:144-157). Conversely some have argued that the best way to target covert networks would be to identify the complete node set and roll the whole network up simultaneously (Helfstein and Wright 2011).

Few studies exist on the ending of covert networks. Descriptive accounts of terror groups show they end if they have loose goals, the leader killed or imprisoned, or the groups achieve its goals (Lauchs 2012, Gupta 2008), but this is an area for more work.

Summary

Most studies theorise about the need to disrupt networks without modelling the effect or showing empirical case studies. Few empirical studies exist on the evolution or dissolution of covert networks.

9. Methodological questions

This broad range of studies into covert networks have given rise to methodological problems and solutions. These are summarised below:

Missing data and boundary specification

- Covert network data are incomplete, unobserved and unrecorded (Sparrow 1991).
- Sampling in covert networks misses data in four ways: underestimating existence of and strength of ties, number of edges, scope (geodesic) and centrality measures are inaccurate (Gill and Freeman 2013, 1:68-94)
- Measurement of covert networks is affected by missing data (peripheral actors, multiplex relationships, boundary specified by time, actors' exogenous factors, processes) (Keegan, Ahmed, Williams, Srivastava, and Contractor 2010:201-208;Keegan, Ahmed, Williams, Srivastava, and Contractor 2011:24)
- Covert networks can be estimated using subsamples using link-tracing (Liben-Nowell and Kleinberg 2007, 58:1019-1031;Rhodes and Jones 2009, 60:1373-1383;Thompson and Frank 2000, 26:87-98) and respondent-driven sampling/chain-referral technique (Salganik and Heckathorn 2004, 34:193-239)
- Use of automated web crawlers to describe network boundary (Westlake, Bouchard, and Frank 2011, 3:1-32;Zhou et al. 2005, 20:44-51), tested on child exploitation websites and US extremist groups

Estimating destabilisation

- Use of algorithm to test removal of specific nodes (Memon et al. 2006:26)), tested on idealised and Krebs network data

Microstructures

- Clique analysis can be used to examine dual-mode structures in covert networks (Krikorian and Ludwig 2003).

Identification of key players

- Use of centrality measures based on number of introductions which would be required for replacement, nearest replacement and number of paths on which the node lies (Toth, Guly+ís, Legendi, Duijn, Sloot, and Kampis 2013, 222:1413-1439)
- Use of Laplacian centrality to identify and sensitivity-test removal of central nodes (Qi et al. 2012, 194:240-253)
- Use of network efficiency measure quantifies how efficiently the nodes of the network exchange information and can be used to identify the most important nodes in the network (Latora and Marchiori 2004, 20:69-75)
-

Edges

- edge prediction can be done on the basis of qualitative information (Gill and Freeman 2013, 1:68-94), tested using data from UK soap opera, Eastenders.
- Covert ties are multiplex (Reed 2007;Varese 2013, 29:899-909)

10. Conclusion

In conclusion, we argue that covertness is under-theorised in the literature on covert networks. We argue that covertness could be developed into sets of variables which could be used with exogenous and endogenous factors to develop and test hypotheses about the structures and processes of covert networks.

We have shown that there is a lack of comparable empirical data in the field, and that theories about some types of covert network, even if empirically verified may not be generalizable to other types. We show that network aims and activities and context may affect the types and formation of covert ties, which themselves may be multiplex. Contextual and endogenous factors are said affect network structure in quantifiable ways, but we have shown that these may not be uni-directional relationships. Covert networks may form, be controlled, evolve and dissolve in consistent ways, but we currently lack the empirical basis for statements of this kind.

Clearly, there remain a great number of untested and unvalidated hypotheses about the formation, structure, evolution and dissolution of covert networks of all types. The question of whether covert networks are substantially different from overt networks remains moot. Clearly, the diversity of metrics generated by analysis of covert networks tells us more about the heterogeneity of the data and ties studied that any intrinsic property of covert networks. However, the role of secrecy in the formation and evolution of networks is not yet well-understood. In conclusion, as remarked by many colleagues, the importance of divining appropriate methods and metrics to analyse covert networks is clear to us all. The next steps are to gather covert network data to allow a comparative testing of these hypotheses in an attempt to understand the nature and effects of secrecy on networks.

Literature Cited

Acosta B, and Childs SJ. 2013. Illuminating the global suicide-attack network. *Studies in Conflict & Terrorism* 36 (1): 49-76.

Asal V, and Rethemeyer RK. 2008. The nature of the beast: Organizational structures and the lethality of terrorist attacks. *The Journal of Politics* 70 (02): 437-449.

Baker WE, and Faulkner RR. 1993. The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry. *American sociological review*: 837-860.

Bakker RM, Raab J, and Milward HB. 2012. A preliminary theory of dark network resilience. *Journal of Policy Analysis and Management* 31 (1): 33-62.

Barnett G, Ruiz J, Hammond J, and Xin Z. 2013. An examination of the relationship between international telecommunication networks, terrorism and global news coverage. *Soc. Netw. Anal. Min.* 3 (3): 721-747.

Bouchard M. 2007. On the Resilience of Illegal Drug Markets. *Global Crime* 8 (4): 325-344.

Calderoni F. 2011. Strategic positioning in Mafia networks.

Campana P, and Varese F. 2012. Listening to the wire: criteria and techniques for the quantitative analysis of phone intercepts. *Trends in organized crime* 15 (1): 13-30.

Carley KM, Lee JS, and Krackhardt D. 2002. Destabilizing Networks1. *Connections* 24 (3): 79-92.

Carrington PJ, and van Mastrigt SB. 2013. Co-offending in Canada, England and the United States: a cross-national comparison. *Global Crime* 14 (2-3): 123-140.

Caselli GC, and Della Porta D. 1991. The history of the Red Brigades: organizational structures and strategies of action (1970-82). *The Red Brigades & Left-Wing Terrorism in Italy*.

Clutterbuck L. 2008. Rethinking Al Qaeda: Leaderless jihad: terror networks in the twenty-first century.

Cockbain E, Brayley H, and Laycock G. 2011. Exploring Internal Child Sex Trafficking Networks Using Social Network Analysis. *Policing* 5 (2): 144-157.

Coleman JS. 1990. Rational action, social networks, and the emergence of norms. *Structures of power and constraint*: 91-112.

Crenshaw M. 2002. The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice in Terrorism and Counterterrorism: Understanding the New Security Environment, Reading & Interpretations. Connecticut: Mc-Graw-Hill Companies.

-----. 2010. Mapping terrorist organizations. *Unpublished working paper*.

Crossley N, Stevenson R, Edwards G, and Harries E. 2010. Covert Social Movement Networks: A Report for the British Home Office.

Crossley N, Edwards G, Harries E, and Stevenson R. 2012. Covert social movement networks and the secrecy-efficiency trade off: The case of the UK suffragettes (1906ΓÇô1914). *Social Networks* 34 (4): 634-644.

Della Porta D. 1992. Political socialization in left-wing underground organizations: Biographies of Italian and German militants. *International Social Movement Research* 4: 259-290.

-----. 1995. Social movements and the state: Thoughts on the policing of protest.

Demiroz F, and Kapucu N. 2012. Anatomy of a dark network: the case of the Turkish Ergenekon terrorist organization. *Trends in organized crime* 15 (4): 271-295.

Diani M. 1997. Social Movements and Social Capital: A Network Perspective on Movement Outcomes. *Mobilization: An International Quarterly* 2 (2): 129-147.

Düring M. 2014. **The dynamics of helping behavior for Jewish refugees during the Second World War: The Case of the Segal family**.

Edwards G. 2014. Infectious innovations? The diffusion of tactical innovation in social movement networks, the case of suffragette militancy. *Social Movement Studies* 13 (1): 48-69.

Edwards G, and Crossley N. 2009. Measures and meanings: exploring the ego-net of Helen Kirkpatrick Watts, militant suffragette. *Methodological Innovations Online* 4 (1).

Enders W, and Su X. 2007. Rational Terrorists and Optimal Network Structure. *The Journal of Conflict Resolution* 51 (1): 33-57.

Erickson BH. 1981. Secret Societies and Social Structure. *Social Forces* 60 (1): 188-210.

Everton SF. 2011. Network Topography, Key Players and Terrorist Networks. *Connections* 32 (1): 12.

Feld SL. 1981. The focused organization of social ties. *American Journal of Sociology*: 1015-1035.

-----. 1982. Social structural determinants of similarity among associates. *American sociological review*: 797-801.

Gill J, and Freeman JR. 2013. Dynamic elicited priors for updating covert networks. *Network Science* 1 (01): 68-94.

Gimenez-Salinas Framis A. 2011. **Illegal networks or criminal organizations*: Power, roles and facilitators in four cocaine trafficking structures*** .
Universidad Autónoma de Madrid .

Goffman E. 1959. *The presentation of self in everyday life*. Oxford, England: Doubleday.

Granovetter M. 1973. The strenth of weak ties. In: American Journal of Sociology, 78. *American Journal of Sociology* 78.

Harris-Hogan S. 2012. Anatomy of a terrorist cell: a study of the network uncovered in Sydney in 2005. *Behavioral Sciences of Terrorism and Political Aggression* 5 (2): 137-154.

Helfstein S, and Wright D. 2011. Covert or Convenient? Evolution of Terror Attack Networks. *Journal of Conflict Resolution* 55 (5): 785-813.

Horowitz MC, and Potter PB. 2013. Allying to Kill Terrorist Intergroup Cooperation and the Consequences for Lethality. *Journal of Conflict Resolution*: 0022002712468726.

Jackson JL, Herbrink JC, and Jansen RW. 1996. Examining criminal organizations: Possible methodologies. *Transnational Organized Crime* 2 (4): 83-105.

Keegan B, Ahmed MA, Williams D, Srivastava J, and Contractor N. 2010. Dark gold: Statistical properties of clandestine networks in massively multiplayer online games.

-----. 2011. Sic transit gloria mundi virtuali?: promise and peril in the computational social science of clandestine organizing.

Kirby A. 2007. The London bombers as ΓÇ£self-startersΓÇØ: A case study in indigenous radicalization and the emergence of autonomous cliques. *Studies in Conflict & Terrorism* 30 (5): 415-428.

Klerks P. 2001. The network paradigm applied to criminal organizations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands. *Connections* 24 (3): 53-65.

Koschade S. 2006. A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence. *Studies in Conflict & Terrorism* 29 (6): 559-575.

Krebs VE. 2002. Mapping terrorist networks. *Connections* 24 (3): 43-52.

Krikorian D, and Ludwig G. 2003. Advances in network analysis: Over-time visualization, dual-mode relations, and clique detection methods.

Latora V, and Marchiori M. 2004. How the science of complex networks can help developing strategies against terrorism. *Chaos, Solitons & Fractals* 20 (1): 69-75.

Lauchs M, Keast R, and Yousefpour N. 2011. Corrupt police networks: uncovering hidden relationship patterns, functions and roles. *Policing & Society* 21 (1): 110-127.

Liben-Nowell D, and Kleinberg J. 2007. The link–Éprediction problem for social networks. *Journal of the American society for information science and technology* 58 (7): 1019-1031.

Lindelauf R, Borm P, and Hamers H. 2009. The influence of secrecy on the communication structure of covert networks. *Social Networks* 31 (2): 126-137.

Malm A, and Bichler G. 2011. Networks of collaborating criminals: Assessing the structural vulnerability of drug markets. *Journal of Research in Crime and Delinquency* 48 (2): 271-297.

Memon N, Hicks DL, Harkiolakis N, and Rajput AQK. 2008. Small world terrorist networks: a preliminary investigation. In *Applications and Innovations in Intelligent Systems XV*, 339-344. Springer.

Memon N, Hicks DL, Larsen HL, and Rajput AQK. 2006. How investigative data mining can help intelligence agencies in understanding and splitting terrorist networks. *Data Mining Case Studies*: 26.

Milward HB, and Raab J. 2006. Dark networks as organizational problems: Elements of a theory. *International Public Management Journal* 9 (3): 333-360.

Morselli C, Giguire C, and Petit K. 2007. The efficiency/security trade-off in criminal networks. *Social Networks* 29 (1): 143-153.

Natarajan M. 2000. Understanding the structure of a drug trafficking organization: a conversational analysis. *Crime Prevention Studies* 11: 273-298.

-----. 2006. Understanding the structure of a large heroin distribution network: a quantitative analysis of qualitative data. *Journal of Quantitative Criminology* 22 (2): 171-192.

Phillips BJ. 2013. Terrorist Group Cooperation and Longevity. *International Studies Quarterly*: 1-12.

Qi X, Fuller E, Wu Q, Wu Y, and Zhang CQ. 2012. Laplacian centrality: A new centrality measure for weighted networks. *Information Sciences* 194: 240-253.

Raab J, and Milward HB. 2003. Dark Networks as Problems. *Journal of Public Administration Research and Theory: J-PART* 13 (4): 413-439.

Rapoport DC. 2002. The four waves of rebel terror and September 11. *Anthropoetics* 8 (1): 42-43.

Reed B. 2007. A social network approach to understanding an insurgency. DTIC Document.

Rhodes CJ, and Jones P. 2009. Inferring missing links in partially observed social networks. *Journal of the operational research society* 60 (10): 1373-1383.

-----. 2009. Inferring missing links in partially observed social networks. *Journal of the operational research society* 60 (10): 1373-1383.

Sageman M. 2004. *Understanding terror networks*.: University of Pennsylvania Press.

Salganik MJ, and Heckathorn DD. 2004. Sampling and estimation in hidden populations using respondent-driven sampling. *Sociological methodology* 34: 193-239.

Sedgwick M. 2007. Inspiration and the origins of global waves of terrorism. *Studies in Conflict & Terrorism* 30 (2): 97-112.

Simmel G. 1906. The Sociology of Secrecy and of Secret Societies. *American Journal of Sociology* 11 (4): 441-498.

Sparrow MK. 1991. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks* 13 (3): 251-274.

Stevenson R, and Crossley N. 2014. Change in Covert Social Movement Networks: The ΓÇÿInner CircleΓÇÖof the Provisional Irish Republican Army. *Social Movement Studies* 13 (1): 70-91.

Thompson SK, and Frank O. 2000. Model-based estimation with link-tracing sampling designs. *Survey Methodology* 26 (1): 87-98.

Toth N, Guly+ís L+, Legendi RO, Duijn P, Sloot PM, and Kampis G. 2013. The importance of centralities in dark network value chains. *The European Physical Journal Special Topics* 222 (6): 1413-1439.

Tsvetovat M, and Carley K. 2002. Knowing the enemy: A simulation of terrorist organizations and counter-terrorism strategies.

van der Hulst ReC. 2009. Introduction to Social Network Analysis (SNA) as an investigative tool. *Trends in organized crime* 12 (2): 101-121.

van Mastrigt SB, and Carrington P. 2013. Sex and Age Homophily in Co-offending Networks. *Crime and Networks*: 28.

Varese F. 2010. *Organized crime: critical concepts in criminology*.: Taylor & Francis.

-----. 2013. The Structure and the Content of Criminal Connections: The Russian Mafia in Italy. *European sociological review* 29 (5): 899-909.

von Lampe K. 2009. The study of organised crime: an assessment of the state of affairs. *Organised crime: norms, markets, regulation and research. Oslo, UNIPUB.*

Westlake BG, Bouchard M, and Frank R. 2011. Finding the key players in online child exploitation networks. *Policy & Internet* 3 (2): 1-32.

Zhou Y, Reid E, Qin J, Chen H, and Lai G. 2005. US domestic extremist groups on the Web: link and content analysis. *Intelligent Systems, IEEE* 20 (5): 44-51.