On the Optimal Distribution of Risk and Information Exchange in Star Networks

Roy Lindelauf
Military Operational Art & Science
Netherlands Defense Academy
P.O.Box 90002, 4800 PA Breda
The Netherlands
CentER and Department of Econometrics and OR
Tilburg University
P.O.Box 90153, 5000 LE Tilburg
The Netherlands.

Iris Blankers
Peter Borm
Herbert Hamers
CentER and Department of Econometrics and OR
Tilburg University
P.O.Box 90153, 5000 LE Tilburg
The Netherlands.

Abstract

Terror cells and military units represent entities in different networked organizations facing a common goal: the organizational structure has to be chosen such that it allows for flexible information exchange while simultaneously providing the necessary secrecy. These kind of organizations have been studied extensively from a qualitative perspective. However, quantitative approaches are less frequent, even though they can provide guidelines for policy makers on future courses of action in either counter-terrorism and counter-insurgency or in choosing organizational designs for covert action. A theoretical framework on the optimal communication structure of homogenous covert networks based on cooperative game theory exists (Lindelauf, Borm, and Hamers 2008a). A test and extension of this framework incorporating heterogeneity of the risk interactions present is presented in (Lindelauf, Borm, and Hamers 2008b). In that paper interactions were considered that are heterogeneous with respect to the risk they present to the organization, but homogeneous with respect to the amount of information exchange they provide. In this paper the star network structure will be analyzed taking both information and secrecy heterogeneity into account. We will derive the optimal distribution of risk and information exchange over the links of this graph.

Introduction

Much has been said in recent years on the organizational transformation of terrorist organizations such as Al Qaeda. For instance it is known that Al Qaeda shifted from a bureaucratic, hierarchical organization into an ideological umbrella for loosely coupled jihadi networks (Mishal and Rosenthal 2005). As another example consider Hezbollah's organizational structure during the 2006 IDF war in southern Lebanon. Hezbollah acted as an informal and adaptive distributed network of small cells and units that were acting with considerable independence and were capable of rapidly adapting to local conditions (Cor 2007). They showed the ability of a non-state actor to use and exploit network centric warfare concepts. Arquilla and Ronfeldt (Aro 2001) discuss the importance of the network centric paradigm for reasoning about warfare, from a military as well as non-state actor perspective. It is recognized that the essential feature distinguishing such covert organizations from overt ones is the need to take secrecy into account when conducting operations (Baker and Faulkner 1993), (Raab and Brinton Milward 2001). These organizations consisting of loosely coupled networks interact with each other in varying degrees.

In Lindelauf et al. (Lindelauf, Borm, and Hamers 2008a) a theoretical framework on homogeneous covert networks is established. Measures of secrecy and information for graphs are defined and optimal communication structures using game theoretic bargaining are derived. In another paper this framework is put to the test and extended. In Lindelauf et al. (Lindelauf, Borm, and Hamers 2008b) not only optimal communication structures are investigated but the influence of varying degrees of risk interactions present to the organization are analyzed. This resulted in a first approach to heterogeneity in covert networks. It is assumed that high risk interactions affect the exposure probability of individuals in the organization (and hence the secrecy measure), not the amount of information that potentially could be exchanged. For instance consider the delivery of bomb making materials between individuals of the organization. This interaction presents a higher risk to the organization than individuals discussing target sites. However, it bears no influence upon the amount of information exchange inside the organization: there either is such a risky interaction or there is not. Therefore the information measure in Lindelauf et al.(Lindelauf, Borm, and Hamers 2008b) is not adapted.

Next to giving a short survey on the above mentioned theoretical frameworks the focus of this paper is on secrecy and information heterogeneous star networks. This prototype network can represent an arms smuggling network where the center of the network for instance corresponds to the agency distributing arms between its various outposts. The real world exhibits many (non-covert) networks shaped as stars. Consider for instance a hub and spoke network of aircarriers or sensor networks where there is one base station and several sensors communicating with it. Thus the study and analysis of such star networks could yield results directly applicable to real world problems. In addition there are also covert networks adopting star topologies: an actual covert network that adopted the star network structure is that

of the Dutch National Clandestine Service's so-called 'stay behind organization'. This organization consisted of a group of single agents equipped with radio systems connecting to a central hub. The single agents where unaware of each other and thus the adopted network structure was a perfect star. In this paper we will investigate the optimal distribution of risk and information exchange in such a star network.

Quantitative Frameworks on Covert Networks

It is important for a covert organization to take the network structure explicitly into account. In Lindelauf et al. (Lindelauf, Borm, and Hamers 2008a) several basic scenarios concerning covert networks are defined and analyzed. Furthermore, this framework is extended by introducing the fact that the *nature* of interaction influences the exposure probability of individuals in the organization. Hence, the secrecy measure is adapted and the resulting first approach to heterogeneous covert networks can be found in Lindelauf et al. (Lindelauf, Borm, and Hamers 2008b).

To be more specific imagine two agents, one responsible for network secrecy and the other one for information efficiency, bargaining over the set of all connected networks of certain order. The information measure corresponding to network g is denoted by $I(g)$. Similarly, the secrecy measure is denoted by $S(g)$, and it is defined as the *expected* fraction of the network that remains unexposed under the assumption of a certain exposure probability of individuals in the network. Explicit values of S(g) and I(g) can be found in Lindelauf et al. (Lindelauf, Borm, and Hamers 2008a). The tradeoff between secrecy and information is modeled using cooperative bargaining theory. The optimal network in the sense of the Nash bargaining solution is the network that maximizes the product of S(g) and I(g).

Assume that individuals in the network are exposed uniformly and that the fraction of the network that an individual exposes is equal to the expected number of neighbors in the network that will be detected if communication on links is detected independently and identically with a certain probability. In this first scenario Lindelauf et al. (Lindelauf, Borm, and Hamers 2008a) show that for a low value of this link detection probability the complete graph is optimal and for a high value of this probability the star graph is optimal, indicating that in certain cases the star network topology is an important one.

In a second scenario Lindelauf et al. (Lindelauf, Borm, and Hamers 2008a) assume that the probability of exposure of an individual in the network depends on his centrality with regard to the exchanging of information in the network. It is argued that setting this exposure probability equal to the equilibrium distribution of a random walk on the graph is an adequate choice. Optimal graphs for larger order are approximated by computer simulation and generally speaking it is shown that cellular structures emerge: each individual is connected to a limited member of network members.

In Lindelauf et al. (Lindelauf, Borm, and Hamers 2008b) the assumption is made that certain interactions present a higher risk to the organization than others. However no distinction is made on the amount of information exchange interactions provide. For instance, the interaction representing the delivery of bomb making materials presents a higher risk to a covert organization than discussing target information in codewords. This risk is evaluated by assigning a higher weight to the link representing such an interaction. It is shown that optimally the pair of individuals in the organization to conduct the interaction that presents the highest risk to the organization is the pair that is the least connected to the remainder of the network. In addition the situation is analyzed where only a single risky interaction is present and the organizational form is either that of a star, path or ring graph. Given a certain amount of risk the interaction presents either the path or star graph is optimal, where the transition depends on the order of the graph. The higher the risk this interaction presents becomes, the higher the transition point (in terms of number of individuals in the network) becomes. Hence, the potential secrecy breach this interaction presents is dealt with by adopting the path graph structure and locating the risky interaction at the periphery of the organization. Only if the organization becomes very large will it become more profitable to adopt the star graph structure.

However, the information exchange in the framework of Lindelauf et al.(Lindelauf, Borm, and Hamers 2008b) is still considered to be homogeneous: there either is such an interaction or there is not. If a distinction is made in the amount of information exchange, i.e., if certain individuals deliver higher amounts of bomb making material than others, we arrive at secrecy *and* information-heterogeneous covert networks, which will be discussed in detail further on in case of the star network topology.

To recapitulate: the risk an interaction presents is modeled by assigning 'weights' to the links, representing the risk of that interaction. This weighting function is defined such that a higher weight on one link with respect to another is interpreted in the following way. The interaction between the pair of individuals with high weight presents a higher risk to the organization than the interaction between the individuals corresponding to the other link. The secrecy measure S(g) is adapted accordingly. The exposure probability of individuals in the network is adjusted to incorporate this heterogeneity of interactions with respect to risk. For it can be argued that the probability of detection not only depends on *the number* of individuals this individual is connected to but also on the nature of that interaction. Hence, if an individual is engaged in interactions that present a higher risk to the organization than another individual his exposure probability will be larger.

Star Networks

Motivated by the fact that in the baseline scenario as described in the previous section and analyzed in Lindelauf et al. (Lindelauf, Borm, and Hamers 2008a) the star network

is optimal we further analyze the star network topology. We assume that not only is it possible to have interactions that are heterogeneous with respect to secrecy but also that there are interactions that provide an opportunity in varying the amount of information exchange. We analyze the optimal distribution of this risk and information exchange over the star network topology.

Example: Consider an arms smuggling organization consisting of five regional outposts and a central distributing agency in the form of a star graph, see figure 1. The central distributing agency is denoted by 'C' and the outposts are indexed 'K' through 'O'. If the situation is such that the exposure probability of each vertex is equal, for instance if the organization is located deep in a jungle and military incursions are rare, and secrecy and information are considered homogeneous Lindelauf et al. (Lindelauf, Borm, and Hamers 2008a) showed that the star structure is optimal. However, now consider the same organization in a transnational setting. Additionally assume that the exchange of weapons between the distributing agency and its outposts may vary. Thus looking at figure 1 (Right) twice as much weapons are smuggled on link CM with regard to link CL. Similarly, three times as much weapons are smuggled on link CO with respect to link CL, etc. It can be argued that

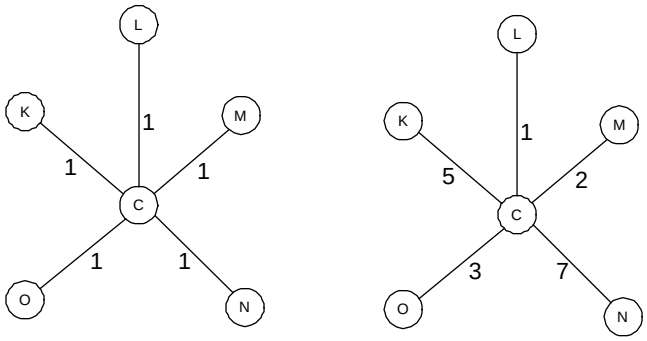

Figure 1: Homogeneous star (Left) and heterogeneous star (Right).

the risk of shipping weapons between the agency and an outposts depends linearly on the amount of goods shipped. In addition the more material that can be exchanged the better the performance of the organization from the perspective of the smugglers. Thus we could say that the numbers corresponding to the links in figure 1 (Right) 'represent' the risk and information exchange in this casus. It is these kind of considerations that force us to extend the model.

In general, a graph g is an ordered pair (V, E), where V represents the finite set of vertices and the set of edges E is a subset of the set of all unordered pairs of vertices. An edge $\{i, j\}$ connects the vertices i and j and is also denoted by ij. The order of a graph is the number of vertices $|V| = n$ and the size equals its number of edges $|E| = m$. We define a function to represent the *risk* an interaction presents by $t : E \mapsto [1, \delta_S]$. Here δ_S is the maximum value a risky interaction can attain. In the context of smuggling this could be representative of the fact that there is a maximum smuggling capacity. Another function, $c : E \mapsto [1, \delta_I]$ is defined to represent the amount of information exchange between the respective vertices, with similar considerations on δ_I. In addition of course $c_{ij} > c_{kl}$ with $ij, kl \in E$ implies that the amount of information exchanged between individuals (terror cells, military units, human traffickers) i and j is higher than the amount of information exchanged between individuals k and l (similar considerations hold for the risk function). We denote the graph $g = (V, E)$ with risk weighting function t and information weighting function c explicitly by $g(t, c)$. Note that 'information exchange' depends on the context under consideration. For instance, in the context of human trafficking an interaction represents humans being smuggled: i.e., in that context a higher amount of information exchange corresponds to more humans being trafficked.

The function representing the risk of an interaction and the function representing the amount of information exchange need not be equal in general. An interaction may be risky but not provide any possibility in increasing the amount of information to be exchanged. However, there are types of interactions such that the more information is exchanged the riskier the interaction becomes. It may be argued that this is the case for human trafficking. The interaction between entities in the trafficking network consists of exchanging people. The more people that are exchanged over a link in the network the 'better', preferably yielding a higher information measure. However, the possibility of link detection also becomes higher, hence the influence on secrecy. In this situation it can be argued that $t = c$, or at least that there is some positive linear relation between them.

We now define the information measure $I(g(t, c))$. Intuitively the optimal graph in the sense of heterogeneous information exchange is the complete graph $g_{comp}(t, c)$ with maximum weight on all its edges. We define *resistances* on the edges. The resistance of edge $ij \in E$ is defined to be the reciprocal of the measure for information exchange, i.e., $r_{ij} = \frac{1}{c_{ij}}$. Denote a path between vertex i and j in graph g by $P_{ij}(g)$. The 'distance' between vertex i and j is defined as the shortest *resistance-weighted* path between i and j:

$$l_{ij}(g(t, c)) = min_{P_{ij}(g(t,c))} \sum_{kl \in P_{ij}(g(t,c))} r_{kl}.$$

The associated total distance is $T(g(t, c)) = \sum_{i,j \in V \times V} l_{ij}(g(t, c))$. The information measure of graph $g(t, c)$ is defined by,

$$I(g(t, c)) = \frac{\frac{1}{\delta_I} n(n-1)}{T(g(t, c))}. \quad (1)$$

The function $c : E \mapsto [1, \delta_I]$ that assigns the maximum weight to all edges of graph $g = (V, E)$, i.e, $c_{ij} = \delta_I$ for all $ij \in E$, is denoted by $\bar{c}$. Since $T(g^n_{comp}(t, \bar{c})) = \sum_{i,j \in V \times V} l_{ij}(g^n_{comp}(t, \bar{c}) = n(n-1)\frac{1}{\delta_I}$, the complete graph with maximum weight w.r.t. information at all its

edges attains the highest information measure, in accordance with intuition, i.e., $I(g^n_{comp}(t,\bar{c})) = 1$. In addition, graph $g(t,\bar{c})$ performs better in the sense of information than a graph $g(t,c)$, i.e., $I(g(t,\bar{c})) \geq I(g(t,c))$.

The total risk individual i is engaged in is defined by $t_i = \sum_{j\in\Gamma_i(g)} t_{ij}$, where
$\Gamma_i(g) = \{j \in V | ij \in E\}$. The heterogeneous secrecy measure (Lindelauf, Borm, and Hamers 2008b) with risk function t and total weight $W_t = \sum_{i\in V} t_i = 2\sum_{ij\in E} t_{ij}$ is

$$S(g(t,c)) = \frac{n^2 - 2m - n + W_t(n-1) - \sum_{i\in V} d_i t_i}{n(W_t + n)}. \quad (2)$$

The value of W_t can be interpreted as the total risk the organization is engaged in. Given a value for W_t the question then becomes how to optimally distribute this total risk among its edges.

In Lindelauf et al. (Lindelauf, Borm, and Hamers 2008a) it was argued that a good criterion for optimality of a graph g is the Nash bargaining value, i.e., the graph g that maximizes $\mu(g) = S(g)I(g)$. For graph $g(t,c)$ this value is given by

$$\mu(g(t,c)) = \frac{n-1}{\delta_I T(g(t,c))} \cdot \frac{n^2 - 2m - n + W_t(n-1) - \sum_{i\in V} d_i t_i}{(W_t + n)}.$$

We analyze the star graph with equal weighting functions corresponding to secrecy and information interactions, i.e, $t = c$. Thus we assume that the interaction is of such a type that if the information exchange it presents increases the risk increases accordingly. In case of arms smuggling this relation seems a good first approximation.

In fact, in case of a star graph organizational design,with the nature of interactions such that the risk and information weighting functions are equal, it follows that optimally a given total amount of information exchange (and hence risk) should be distributed equally among the links:

Proposition 0.1 *Let* $g = g^n_{star}$.
Then $argmax_{t\in[1,\delta_I]^m : W_t = W}\{\mu(g(t,t))\} = (\frac{\frac{1}{2}W}{n-1}, \frac{\frac{1}{2}W}{n-1}, ..., \frac{\frac{1}{2}W}{n-1})$.

Proof: It readily follows that $\sum_{i\in V} d_i(g)t_i(g) = \frac{1}{2}nW$. In addition it can be seen that
$T(g) = 2(n-1)\sum_{kl\in E} \frac{1}{t_{kl}}$, such that
$\mu(g) = \frac{n^2 - 3n + 2 + W(\frac{1}{2}n-1)}{2\delta_I(W+n)\sum_{kl\in E}\frac{1}{t_{kl}}}$. Hence, given the constraint that $\sum_{i\in V} t_i = 2\sum_{ij\in E} t_{ij} = W$, $\mu(g(t,t))$ is maximized if $\sum_{kl\in E}\frac{1}{t_{kl}}$ is minimized.

Denote the number of elements t_{kl} of $t \in [1,\delta_I]^m$ such that $t_{kl} = \frac{\frac{1}{2}W}{m}$ with $k(t)$ (clearly $k(t) \leq m$) and let $f(t) = \sum_{ij\in E}\frac{1}{t_{ij}}$. Take $\hat{t} \in [1,\delta_I]^m$ such that $k(\hat{t}) < m$. We will construct a $\hat{t}'$ such that $f(\hat{t}') < f(\hat{t})$ while $k(\hat{t}') > k(\hat{t})$. Iterating this procedure yields the result.

Now consider $\hat{t}_{ab}$ and $\hat{t}_{cd}$ such that $\hat{t}_{ab} < \frac{1}{2m}W$ and $\hat{t}_{cd} > \frac{1}{2m}W$. Assume $\frac{1}{2m}W - \hat{t}_{ab} < \hat{t}_{cd} - \frac{1}{2m}W$ (the other case can be dealt with similarly). We set $\hat{t'}_{ab} = \frac{1}{2m}W$ and $\hat{t'}_{cd} = \hat{t}_{cd} - (\frac{1}{2m}W - \hat{t}_{ab})$. This mapping clearly has a unique fixed point: $(\frac{\frac{1}{2}W}{m}, \frac{\frac{1}{2}W}{m}, ..., \frac{\frac{1}{2}W}{m})$. It also readily follows that $f(\hat{t'}) = f(\hat{t}) - (\frac{1}{\hat{t}_{cd}} + \frac{1}{\hat{t}_{ab}}) + \frac{1}{\frac{1}{2m}W} + \frac{1}{\hat{t}_{cd} - \frac{1}{2m}W + \hat{t}_{ab}}$. Easy calculus yields $(\frac{1}{\hat{t}_{cd}} + \frac{1}{\hat{t}_{ab}}) > \frac{1}{\frac{1}{2m}W} + \frac{1}{\hat{t}_{cd} - \frac{1}{2m}W + \hat{t}_{ab}}$ and hence $f(\hat{t'}) < f(\hat{t})\square$.

Consider the example of arms trafficking again. It was argued that in this case the information and risk weighting functions can be considered equal. If such an organization adopts a star graph design, i.e., a central 'distributing agency' distributing weapons from one place to another, they would perform best by distributing the number of weapons (shipments) evenly across each link. See the figure below.

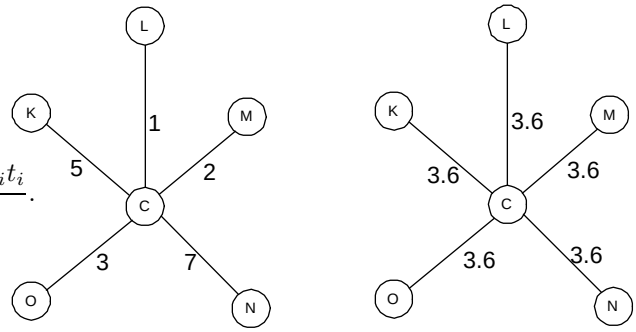

Figure 2: A star network with total risk of 18 (Left and Right), optimally distributed (Right).

References

2001. *Networks and Netwars*. RAND monograph MR-1382.

Baker, W., and Faulkner, R. 1993. The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry. *American Sociological Review* 58(12):837–860.

2007. *Lessons of the 2006 Israeli-Hezbollah War*. Center for Strategic and International Studies: Washington D.C.

Lindelauf, R.; Borm, P.; and Hamers, H. 2008a. The influence of secrecy on the communication structure of covert networks. *CentER Discussion Paper* 23:1–18.

Lindelauf, R.; Borm, P.; and Hamers, H. 2008b. On heterogeneous covert networks. *CentER Discussion Paper* 46:1–13.

Mishal, S., and Rosenthal, M. 2005. Al qaeda as a dune organization: Toward a typology of islamic terrorist organizations. *Studies in Conflict & Terrorism* 28(4):275–293.

Raab, J., and Brinton Milward, H. 2001. Dark networks as problems. *Journal of Public Administration* 13(4):413–439.

ICCCD 2008 Proceedings

This paper was published in the *Proceedings of the Second International Conference on Computational Cultural Dynamics,* edited by V. S. Subrahmanian and Arie Kruglanski (Menlo Park, California: AAAI Press).

The 2008 ICCCD conference was held at the University of Maryland, College Park, Maryland, USA, 15–16 September, 2008.