7th International Command and Control Research and Technology Symposium,

September 16 - 20, 2002
Quebec City, Canada

Topic:
Network-centric Applications

Project Metanet: Methods for Analysis of Complex Networks

Christian Carling[1], Henrik Carlsen[2]
Swedish Defence Research Agency
Division of Defence Analysis
[1]Department of Command and Control Studies,
[2]Department of Technology and Acquisition Strategy

Corresponding author:

Christian Carling
Swedish Defence Research Agency
Division of Defence Analysis
Department of Command and Control Studies
S- 172 90 Stockholm, Sweden

Telephone: +46 8 55 50 39 17
Fax: +46 8 55 50 38 68

E-mail: carling@foi.se

Project Metanet: Methods for Analysis of Complex Networks

Christian Carling[1], Henrik Carlsen[2]

[1]Department of Command and Control Studies,
[2]Department of Technology and Acquisition Strategy

Swedish Defence Research Agency
Division of Defence Analysis
S- 172 90 Stockholm, Sweden
E-mail: carling@foi.se, henrik.carlsen@foi.se

Abstract

The transformation of armed forces towards network oriented principles poses a number of methodological challenges for the field of defence analysis. This paper presents Project Metanet, an undertaking at the Swedish Defence Research Agency, with the aim to monitor developments within the broadly defined field of *Network Analysis*, and outlines three specific challenges. The first two have to do with extending the tools of network reliability theory to handle the case of complex, hybrid communication systems, where the set of nodes and the state of their communication links is rapidly changing over time. The other is the problem of how to find resources in such a dynamic, distributed system using only local topological information.
The paper concludes with a discussion of general-purpose *Network Information Systems*.

1. Introduction

A growing body of research, dramatically underscored by recent events, shows that network-oriented operations, while still a distant option for the armed forces of nation states, is an effective and continually evolving practice in many forms of criminal and terrorist activity[1]. Thus, a better understanding of network forms of organisation and related concepts of operation is required not only to transform our armed forces, but also to understand the character of future conflicts in general.

The Swedish Armed Forces is today officially set on a course towards a network-based defence[2]. Presently in Sweden, the *network* concept is either used rather loosely, in a figurative sense, or with a narrow emphasis on the technical aspects of communication networks. While we acknowledge the value of metaphorical reasoning about uncertain, future developments, there is now a need to proceed beyond this stage, going from metaphors to methods. There is also a need to understand the relationships between the technical, doctrinal, social and other aspects of network-oriented forms of military organisation.

[1] John Arquilla and David Ronfeldt have written extensively on this topic. See [Arquilla and Ronfeldt, 2001].
[2] [Swedish Defence Bill 2001]

Project Metanet, which is carried out by the Swedish Defence Research Agency with funding from the Swedish Armed Forces, seeks to identify, and further on, to develop analytical tools and concepts to meet the challenges that are specific to network forms of organisation. The task of this project is to *monitor* and *review* the developments within the nascent field of Network Analysis and assess their relevance for the transformation of the Swedish Armed Forces. The character of this project is to a large degree *integrative*: We seek to combine concepts, methods and tools taken from a broad scientific domain and then to match them with key methodological challenges that we can see in the evolution towards a network based defence.

While the general field of Network Analysis as alluded to above is very broad, ranging from sociology to random graph theory, this paper will focus on quantitative methods, with primary application towards the analysis of complex, distributed communication networks. The formal start of the project was in January 2002 so this is an early presentation of work still in progress.

2. Network Analysis: State of the art

The last couple of years have seen the rapid growth of a new area of research, whose objects of study are complex networks[3], drawing on examples from a broad spectrum of technological, and social or biological systems. A large part of this research has a purely explorative character, showing a striking universality of structural patterns across a very broad range of domains. Several researchers have examined the relation between network structure and dynamics, while others attempt to relate the structure and stability of growing network systems to the details of the growth mechanism. An issue that is of particular interest in a military context is of course that of robustness: What makes a network structure, robust against failures and deliberate attacks? How do we defend our own network resources and how do we identify and capitalise on the structural weaknesses of enemy networks?

The structural properties of networks are naturally described in terms of graphs. This gives access to a vast number of analytical concepts and a rich set of tools for quantitative analysis. When exploring empirical networks, measuring some properties of its graph representation is the first step in understanding its structure. Using those measures, it is possible to make structural comparisons between different networks. Another possibility is to make the comparison against the expected values for some random graph model. For networks that are growing or otherwise changing over time, a possible next step is to try to formulate a graph process model, in the form of an algorithm that generates graphs that are similar to the reference case, in a statistical sense. This will hopefully give some insight into the processes that is driving the systems structural evolution. Ultimately, the lessons learned from these explorations can be brought to bear on the question of design: How do we create, maintain and evolve efficient networks within the context of network-oriented defence?

The current surge in the study of complex networks represents the confluence of (at least) two developments: an empirical tradition, starting with Morenos studies of social networks in the

[3] Two good review articles are [Strogatz, 2001] and [Albert *et al.*, 2002]. A popular account is given in [Barabási, 2002].

1930s, and giving rise to the school of Social Network Analysis [Wasserman and Faust, 1994]. The other, theoretical tradition can be traced to the work of Paul Erdös, who together with Alfred Renyi in the 1950s formulated and studied a simple, yet rich model of random graphs.

2.1 *Small world networks*

A recurrent feature found in practically all real world networks is the existence of short paths between pairs of nodes: the average shortest paths scales as the logarithm of the number of nodes, so that the average separation for networks with millions of nodes is around 10. This is just what one would expect from the predictions of random graph theory, but surely those networks are far from random. A fundamental difference between simple random graph models and real world networks is that the latter often are locally clustered: people (or other networked entities) tend to associate in groups, forming dense clusters and cliques that are more loosely connected to the rest of the network. A simple measure of this is the *clustering coefficient*, defined as the probability that two nodes that each are connected to a third node also are connected directly to each other. Another way to state it is as the density of triangles in the graph. Thus defined, clustering is absent[4] in the Erdös-Renyi random graphs.

In 1998, Watts and Strogatz introduced the so-called the Small World model, which combines local clustering with short average separation. The starting point is regular grid, where every node is connected to its k nearest neighbours, thus having a high degree of local clustering (but large average node separation). The model then randomly rewires each link with probability p. The limiting case of $p = 1$ effectively recreates the random graphs. The rewiring process creates shortcuts that even for small values of p give the distance scaling of random graphs, without destroying the local clustering. Apart from providing a better match with real-world networks, small world networks have interesting properties in terms of information propagation, synchronisability etc. The book by Watts [Watts, 1999] is a good introduction to the sociological motivations behind the search for such models, while [Newman, 2000] gives a short review of the theoretical properties of Small World models.

2.2 *Scale-free networks*

Recent studies have shown that many complex networks, with the Internet and the World Wide Web serving as the prime examples, have a very heterogeneous topology: The majority of nodes have only a few links while some nodes have a very large number of links. The actual form of the distribution of links per node (called the degree distribution) often resembles a power-law[5]. Since a power-law is a broad distribution without a pronounced peak and thus lack a scale fixing a "typical" value, they are often referred to as scale-free networks [Albert and Barabási, 2001]. As will be noted later, this has far-reaching consequences for how such networks respond to failure and attack, and how information propagates across the network.

---

[4] That is, the clustering coefficient goes to zero in the limit of very large graphs with constant average degree.

[5] The probability that a node has exactly k links is proportional to k^{-g}, where γ is a parameter that falls in the range 2-3 for an amazingly broad set of real-world networks.

2.3 ***Network models***

The simple random graph models are very limited as models of real world networks. It is quite easy to formulate more general models, so that one can define random graph models with arbitrary degree distribution [Newman, 2001], including directedness and correlations. The finding that many real world networks have a power-law degree distribution led to the development of *graph growth* models. These differ from equilibrium random graph models in that they start with a small set of nodes and then add new nodes sequentially, which attach to the earlier ones through simple rules[6]. By suitable choice of attachment rules, one can tune many aspects of the resulting networks. Specifically, a scale-free degree distribution results for the case of *preferential attachment*: this means that new nodes attach to old ones with a probability proportional to their current degree. Thus nodes that have a head start with many connections will continue to attract ever more connections, leading to a degree distribution that is heavily skewed.

3. **Examples of methodological challenges**

Current ideas for future C^2 systems call for a complex interconnected network of sensors, decision support systems and weapon systems. The dynamics of a network centric battlefield with a rapidly changing population of nodes, communication links that go down and are re-established continually, creates formidable challenges for the design of such networks. In this section we outline three specific examples:

1. Vulnerability of command- and control networks.
2. Cascading failures and epidemic spreading in network systems.
3. Local search in distributed systems.

3.1 ***Vulnerability of command- and control networks***

Many accounts of Network Centric Warfare simply take the integrity of networks for granted. In reality, it is obvious that the network itself will become a primary target for enemy operations. Realistic models for assessing the robustness and survivability of such networks is therefore of critical importance in evaluating different architectures.

Ever since the groundbreaking work of Paul Baran in the 1960s, most work on robust communication networks has been focused on the case of homogenous topology, where all nodes have approximately the same number of links. As several research groups have shown[7], the degradation of a network subjected to deliberate attacks and random failures depends critically on details in the connection pattern, even for the same overall level of link redundancy. If the network has a scale-free topology, with decentralised hubs, a targeted attack against the hubs will destroy the network very fast. On the other hand, such networks will be much more robust against random destruction than homogenous structures.

---

[6] The models can also be extended to include rules for rewiring links between old nodes.

[7] Albert, R., Barabási, L-A., Jeong, H. *Error and attack tolerance of complex networks*, Nature **406**, 2000.

Network reliability is of course a rich and well-developed field, with a vast literature[8]. However, most of this is focused on problems related to the case of a fixed connection topology: The standard methods model a communication system as a fixed graph, where individual nodes and links break down with given probabilities. The *reliability polynomial* then gives the probability that the system is in a state represented by a (fixed) subgraph of working nodes and links. For instance, the probability of finding a spanning tree gives the probability that all nodes are still connected through some path. This is called all-terminal connectivity, and many variations of this are of course possible.

This standard approach is relevant for the case of fixed infrastructure systems, but quite unsatisfactory for the complex case of hybrid communication systems, where a large proportion of mobile users connect through ad-hoc multi-hop radio networks, or some other technology. The main method of analysing the reliability and robustness of such networks is through (Monte Carlo-type) software simulation models. However, such simulations could, and in our view, should be complemented by other means. One such alternative approach would be to model the network on a coarse level with some suitable chosen random graph model. The effects of mobile nodes entering and leaving the network, with individual connections going up and down as a function of movements, terrain, random failure et c. is then "wrapped up" by an ensemble of such random graphs. Of course, in reality such topological perturbations propagate locally in space and time, inducing subtle correlations that are not adequately captured by simple ensemble averages, but the point is that such models could give a rough estimate of overall characteristics that can be studied in the limit of extremely large networks, which are effectively intractable through software simulation.

The challenge here is to construct a random graph model that captures the essentials of the dynamical topology, which at the same time is consistent with realistic military operational patterns. This gives us a baseline model for the network under "blue sky" conditions. Antagonistic attacks are then superimposed upon this model. The actual measures to use in describing the degradation of a network under attack require some consideration. Classic connectivity measures such as described above (e g all-terminal connectivity) can be estimated by standard percolation methods [Stauffer and Aharony, 1994], [Callaway *et al.*, 2000]. Since the basic military functions are to be generated by many distributed components acting together temporarily, full global connectivity is an unnecessarily stringent requirement. One could therefore also try to estimate the probability of finding small surviving functional chains or sub-networks that can still perform their mission, as a function of the intensity of attacks. This would be of value in finding the optimal trade-off between a fully distributed system of systems, versus autonomous, integrated platform systems.

The universality of sharp transition phenomena in percolation theory indicates that all realistic networks will exhibit graceful degradation up to some critical level of destruction, and then fail abruptly. The actual point of the percolation transition, and the shape of the transition curve, depend on details of the network topology, and can be analysed both through numerical simulation and analytically with random graph models.

[8] The excellent review article [Ball, 1992] lists over 400 references.

3.2 *Cascading failures and epidemic spreading in network systems.*

Large infrastructure systems constitute an area where network analysis can provide powerful tools in terms of analysing system integrity and critical dependencies between different systems. The technological convergence between public systems based on open architectures and mission-specific C^2 systems create attractive options for antagonists. The perils of system-wide, cascading failures is very real and cannot be understood solely as a function of individual subsystem integrity. Another issue is of course the spread of malicious code or false information in communication systems. Simple models[9] based on infective spreading can give interesting insights into the global dynamics of such events, and the relation between network structure and contagion/failure dynamics.

The standard models for such processes all rest on the simple assumption of homogeneity, which means that all nodes are "typical", having roughly the same number of links and the same transmission probability. The central result from these models is the presence of thresholds: If the effective spreading probability is below a certain threshold value, the perturbation will die out. If it exceeds the threshold, a system-wide cascade, or an epidemic state, is possible. Removing this assumption of homogeneity to account for the scale-free topology found in many designed and evolved systems, the threshold virtually disappears: Any disturbance, however small, runs a risk of saturating a large part of the system. Infections are thus much more likely to spread, but the expected prevalence is lower than for classical epidemic models. Including the effects of finite size, clustering and higher-order correlations will affect the position of thresholds, but the main lesson to be learned is that the resilience and integrity of network systems is determined to a large degree by the connection pattern.

3.3 *Local search in distributed systems*

Knowing the position and the status of both enemy and friendly resources has always been a critical ingredient in military operations. A key ingredient of the "Revolution in Military Affairs" is the supposition that advances in technologies, especially in ICT (information, communication and telecommunication), will bring about a transformation in battlespace awareness. By "lifting the fog of war" [Owens, 2000], commanders will be able to apply the right kind of force at the right target at the right time.

The vision of superior battlespace awareness is problematic for at least two reasons[10]. First, if information superiority is our main asset compared to the enemy, we can be certain that the systems that supply battlespace knowledge will be one of enemy's main targets. Second, the inherent complexities of such systems will inevitably contribute some "fog" of their own.

When thinking of networks, one usually pictures a graph with a number of nodes connected by links. Implicit in this view is the premise that we have complete information on the status of the

[9] For a nice example, see [Watts, 2000].

[10] Of course, there are a number of other critical aspects of this development, e.g. man-system interaction, which deserves attention. Here, however, we focus on the more intrinsic technological aspects of the vision.

whole network at any instant of time. We will argue that this will rarely be the case in a military context: the networks we imagine will exhibit complicated dynamical behaviour, e.g. temporary dedicated networks[11] will be configured out of the "underlying" network of systems from which all the possible configurations are built. Of course, one could try to create a complete picture of the network by broadcasting information trough the network concerning the status of nodes and their relationships. The possibility to do so is dependent on the capacity of the system and this information is transmitted at the cost of other needs, so the attempt of a global picture comes at the price of efficiency. In the hypothetical case we do get complete information of the network status, it will anyhow very soon be outdated.

Given the above, if is safe to say that a global picture of the network is unattainable. The prudent approach then is that communication and search protocols should be designed from the premise that we only have local and temporary information on network topology. This shift is illustrated in Fig. 1.

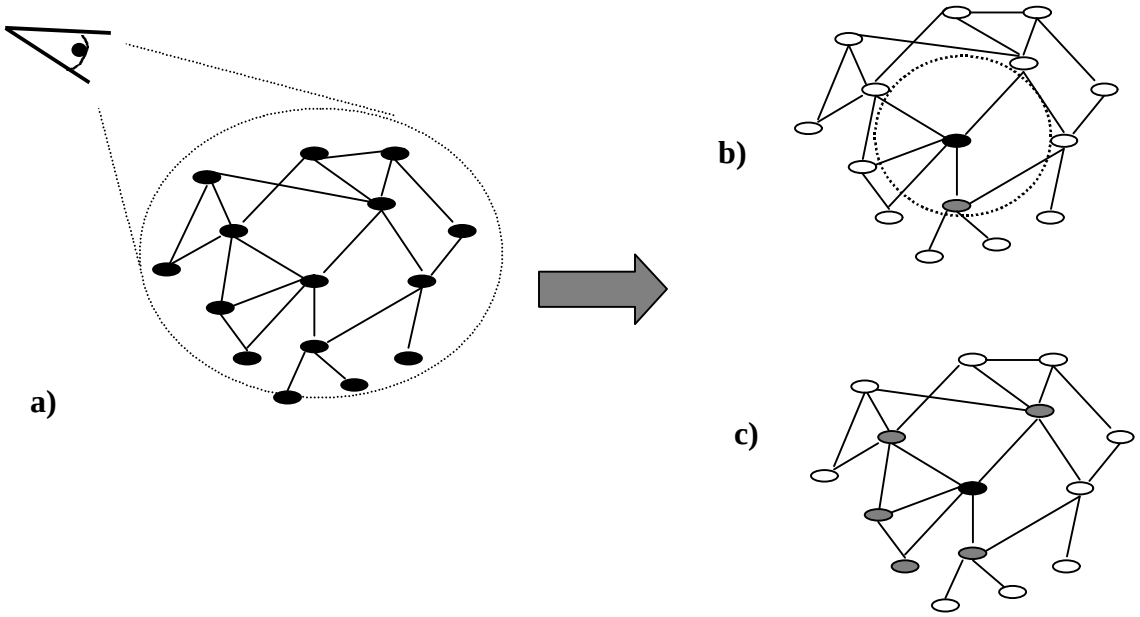

Figure 1: From a global to a local view. Complete knowledge of the network is present in a). Figures b) and c) show partial knowledge from two perspectives: in b) the grey nodes represent represents partial knowledge limited by geometry (the dotted circle), and in c) a topological local knowledge via nearest neighbours.

[11] As an example think of a sensor-to-shooter chain where the systems only participate in the chain during the actual mission. To enable efficient reuse of shared resources, it is of course of interest to limit the time each system participates in the chain.

So how do we find things in a network using only local information? The *existence* of short paths between nodes is of little use if we have no effective procedure for their discovery [Kleinberg, 2000]. The performance of a communication system thus depends ultimately on the routing algorithms used *and* on the actual connection topology. Most research and development efforts today concentrate on the algorithmic part of this equation. This is easily justified, since the network topology has fewer design degrees of freedom: it is constrained by technology, environment and operational requirements. Still, the lesson to be learned from the study of existing complex networks tells us that the details of the connection topology may matter just as much as the algorithms. This has two important consequences:

a) Algorithms have to be tested on realistic network topologies.
b) Optimal design requires that algorithms not only match but also take advantage of the actual topology.

As mentioned above, many complex networks have a scale-free topology. This feature has been shown to be important for finding short paths with only local information. The search algorithm utilizes the high degree nodes by passing a message to the nearest neighbour with most links. This strategy agrees well with intuition since well-connected nodes should give access to a larger portion of the network. In simulations on large systems these algorithms show high efficiency [Adamic *et al.*, 2001].

Gnutella is system that could serve as a model for the basic problems raised in this section. This is a distributed filesharing system without a central server that stores file location information. The lack of a central server gives the system high robustness at the cost of efficiency. If a user wants a particular file, she sends a query to all her neighbours within a given radius. This process continues until the file is found or the radius is exceeded. This is of course a very costly way of searching and it does not use the special features of the topology. However, in networks with a scale-free structure, the search can be made efficient with a procedure as described above. This shows that complex ad-hoc networks can be made searchable and that robustness and efficiency is not an impossible combination if the characteristics of the network are used properly.

Designed for different purposes, systems like FreeNet [Clarke *et al.*, 2002], do share some key features with the requirements for future command and control system, notably robustness, information integrity and the ad-hoc nature of operation. We think this is only one of many examples where Peer-to-Peer networks [Oram, 2001] could serve as inspiration and test bench when thinking about future command and control systems.

4. **Network Information Systems**

The history of warfare is intimately connected to the history of mapmaking. There is a straight line from the earliest field maps, passing through our present-day Geographic Information Systems, and leading on towards the various technologies proposed for building battlespace awareness in the future. However, moving away from traditional ways of conducting military operations, there is also a need to transform the concepts and ultimately, the tools we use to create and communicate this awareness. If the future of armed conflict is truly network-centric, then battlespace awareness is, in relative terms, less about knowing where things are in physical space, and more about how things are connected to each other. This represents a subtle shift from geography to topology, from G*eographic Analysis* to *Network Analysis.*

While it is true that current Database Management and Geographic Information Systems (GIS) can handle many elementary operations of Network analysis, we firmly believe that a full transformation towards network-centric warfare requires the development of generic software tools, in close analogy with the development of Geographic Information Systems. The term *Network Information Systems* (NIS) suggests itself and is indeed already used to describe certain existing domain-specific systems for management of computer communication and energy distribution networks. What we propose here is a generic class of tools, designed for a broader range of applications.

As was the case for GIS, early instances of NIS will most likely support off-line, back-office tasks such as research, design and development. In the long run, as the technology matures one can visualise its incorporation into command and control systems deployed in the field, serving as on-line, integrated components in force management and decision support systems.

Today there exist a large number of software tools and utilities for network analysis, all developed to help solve various small and well-defined problems. The majority of these tools fall in a category one could call ”academic software”, developed by an individual or small group of researchers, for a particular research project and then distributed as-is, for free. Support and further development is often non-existent or severely limited. At the other end of the spectrum, there exists a number of highly specialized, high cost, commercial systems aimed primarily at operators of public infrastructure systems in the telecom and energy distribution sector. In between these extremes there is a small, but growing number of companies, providing generic building blocks (code libraries) for component-based software development.

The rapidly growing field of bioinformatics is arguably all about network analysis: In the post-genome sequencing era, the challenge ahead is to understand the complex interactions of proteins inside cells (proteomics), and gene regulatory dynamics, how individual genes control each others activity in a complex network of epistatic interactions. Thus, it is a safe bet that the large resources invested in bioinformatics will continue to push the envelope of network analysis tools and methods in the near future.

4.1 ***Basic features of Network Information Systems***

The main features envisioned in a full-fledged Network Information System are the following:

Data storage and handling
The user should be able to interactively edit both graph structure and node/link attributes.
There is a need for translation filters, enabling the system to import and export data in a broad range of formats. All network and attribute data can reside in a standard relational database engine. This provides a scalable platform and makes it possible to work with large data sets and to maintain an easily accessible archive of different networks. Another important feature is search and query operations, combining both topology and node/link attributes. This will for instance make it possible to search for specified patterns of topological relations (embedded subgraphs), in combination with node and link attribute data.

Visualisation
An essential feature in a NIS is interactive visualisation, supported by automated graph drawing algorithms in 2 and 3 dimensions. The resulting graph layouts can either be displayed with normal Euclidean metric or in, for example, a hyperbolic projection. The user should be able to navigate the graph by panning and zooming (changing display scale). It is also desirable to have functions for hiding / revealing selected nodes and links, and to collapse / expand entire substructures as compound nodes.

Analysis
A NIS should include a large set of standard graph-theoretical algorithms, such as finding minimum spanning trees, connected components and shortest paths. Other obvious examples are topological sorting, breadth-first/depth-first search, as well as algorithms for partitioning and clustering the graph and solving flow-related problems. The list can be made long and the important requirement is that this toolbox is extensible. There is also a need for functions calculating various attribute and network statistics.

Extensibility
A fully developed NIS should incorporate a standardised scripting language, thereby providing a platform to build higher-level functionality. A simple use of this is to write macros, performing sequences of statistical and graph theoretical operations on multiple data sets. Examples of higher-level functionality may range from implementations of cognitive maps/influence diagrams to more complex applications such as Monte Carlo-simulation of network dynamics.

5. **Further work**

Social Network Analysis is a mature field of study, drawing participants from sociology, epidemiology, criminology and statistics, to name a few. In the present context the applications towards criminology and intelligence analysis are particularly relevant. Tools and methods from this field has been brought to bear on the analysis of transnational terrorist organisations[12].

Another concern is how to develop and evolve a network-centric defence capability that can co-adapt to the changing requirements in an uncertain future. The intricate relationships between different technologies, suppliers, systems, operational concepts and security challenges form a complex web. Graph theoretical descriptions provide a formal representation of such *conceptual networks*. Bringing graph-theoretical tools to bear on this problem may yield interesting results that may ultimately be instrumental in enabling the transformation towards a network-oriented defence.

6. **References**

[Adamic *et al.*, 2001] Lada Adamaic, Rajan Lukose, Amit Puniyan and Bernardo Huberman. *Search in Power-Law Networks.* Phys. Rev. E **64**, 046135, 2001.

[Albert and Barabási, 2002] Reka Albert and Alberto-Lazlo Barabási, *Statistical Mechanics of Complex Networks*, Rev. Mod. Phys. **74**, 1, 2002.

[Albert *et al.*, 2000] Reka Albert, Alberto-Lazlo Barabási and Hawoong Jeong, *Error and attack tolerance of complex networks*, Nature **406**, 2000.

[Arquillla and Ronfeldt, 2001] John Arquilla and David Ronfeldt. *Networks and Netwar*, RAND MR-1382, Santa Monica, Calif., 2001.

[Barabási, 2002] Alberto-Lazlo Barabási. *Linked: The New Science of Networks.* Perseus Publishing, 2002.

[Ball, 1992] M. O. Ball, C. J. Colbourn and J. S. Provan. *Network Reliability*. Technical Report TR 92-74, Systems Research Center, University of Maryland, 1992.

[Callaway *et al.*, 2000] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, D. J. Watts. *Network robustness and fragility: Percolation on random graphs*. Phys. Rev. Lett. **85**, 5468-5471 (2000).

[Clarke *et al.*, 2002] Ian Clarke, Scott Miller, Theodore Wong, Oskar Sandberg and Brandon Wiley. *Protecting Free Expression Online with Freenet*. IEEE Internet Computing, January-February 2002, p 40, 2002.

[12] A simple yet illuminating example is the analysis of the links between Al-Quaeda members in [Krebs, 2001].

[Kleinberg, 2000] Jon Kleinberg, *Navigation in a Small World*, Nature **406**, 845, 2000.

[Kempe *et al.*, 2001] D. Kempe, J. Kleinberg, A. Demers. *Spatial Gossip and Resource Location Protocols*. Proc. 33rd ACM Symposium on Theory of Computing, 2001

[Krebs, 2001] Valdis Krebs, *Uncloaking Terrorist Networks*, First Monday **7**, no 4, April 2002. http://www.firstmonday.org/issues/issue7_4/krebs/index.html

[Newman, 2000] M. E. J. Newman. *Models of the small world.* J. Stat. Phys. **101**, 819-841 2000.

[Newman *et al.*, 2001] M. E. J. Newman, S. H. Strogatz and D. J. Watts. *Random graphs with arbitrary degree distributions and their applications.* Phys. Rev. E **64**, 026118 2001.

[Oram, 2001] Andy Oram (ed). *Peer-to-Peer: Harnessing the Power of Disruptive Technologies.* O´Reilly and Assoc., Sebastopol, Calif. 2001

[Owens, 2000] B. Owens, *Lifting the Fog of War*, Farrar, Straus and Giroux, New York, 2000.

[Stauffer and Aharony, 1994] D.Stauffer and A.Aharony *Introduction to Percolation Theory*, 2nd ed, Taylor and Francis, London 1994

[Strogatz 2001] Steven H. Strogatz, *Exploring complex networks*, Nature, vol. 410, p. 268-76, 2001.

[Swedish Defence Bill, 2001] *Continued Renewal of the Total Defence*, http://forsvar.regeringen.se/pressinfo/pdf/FB_2002_02_10_eng.pdf

[Wasserman and Faust, 1994] Stanley Wasserman and Katherine Faust. *Social Network Analysis: Methods and Applications.* Cambridge University Press, 1994.

[Watts, 1999] Duncan Watts, *Small Worlds: The Dynamics of Networks between Order and Randomness*. Princeton University Press, 1999.

[Watts, 2000] Duncan Watts, *A simple model of fads and cascading failures*, Santa Fe Institute Working paper 00-12-062, 2000.