A METHODOLOGY FOR ANALYZING COMPLEX MILITARY COMMAND AND CONTROL (C2) NETWORKS

ABSTRACT #099

David A. Jarvis

**Alidade Incorporated
31 Bridge Street
Newport, Rhode Island 02840**

This abstract and paper are UNCLASSIFIED

1.0 ABSTRACT

Military personnel are increasingly subject to multiple means of electronic communication for command and control (C2). The means are both synchronous and asynchronous and include email, chat, voice over IP and others. The analytical methodology offered through the study of complex networks such as the Internet, power grids, transportation networks, and patterns of social interaction can aid in the understanding of C2 systems used by military organizations. By analyzing the topologies of communication networks and developing metrics; leadership, patterns of communication, vulnerabilities, and the level of collaboration in the network can be discerned. This paper provides a condensed version of the results from a "discovery analysis" of a military email system used during a recent US/UK naval exercise. Additional topics for discussion include collaboration patterns between the two country's networks, an analysis of various sub-network communication patterns, and questions regarding unique properties of military networks that are not seen in other social networks. This methodology can help engineers and knowledge managers design better C2 structures by incorporating information about how people actually use electronic communication networks.

2.0 BACKGROUND

Most traditional C2 analyses are limited to the performance of information technology systems and related human factors. This analysis is unique in that it used network traffic databases to examine how the arrangement of actors and their interactions within a segment of a C2 network affected performance. This was the first time this type of network analysis had been performed in an operational military context. Because of this fact, the analysis was treated as experimental and a proof of concept. As a note, when the word "network" is used it refers to a defined collection of actors and their connections, not necessarily the information technology connotation that the word typically has.

The goal of the analysis was to provide insight into how networks could be structured to provide adaptive, robust and effective command and control for a network-centric force. To accomplish this, how the email network was expected to perform was compared with how it actually performed during operations. By examining the structure, function, and characteristics of command and control networks and creating metrics for network comparison, better organizational and technological structures can be built for future exercises and military operations.

2.1 Background on Complex Networks

The proliferation of information technologies has enabled the creation of new networked social structures that were not feasible before. To study these networked structures this study used the principles of complex graph and network theory. Graph theory is the mathematical study of how a network can be described and measured. A graph is a simplified representation of a network, where the network is composed of nodes and links. New measures and characteristics arise as the network becomes more and more complex. The theories are typically used for problems that have a high degree of complexity and interaction between its components.

The first instance of the use of graph theory was in 1736 by Euler to solve the famous "Seven Bridges of Königsberg" problem. In this problem there is an island in the middle of two rivers connected by seven bridges, the questions is can one cross all the bridges exactly once and return to a starting point? The fundamentals of graph theory developed out of the proof of this problem.

The mathematics remained largely delegated to simple network structures until the late 20th century because the large-scale numerical computation required for complex systems was impossible. With the development of high-powered computers, large-scale statistical depictions of networks were now possible. This has lead to the discovery, exploration and application of new network properties and structures. The field of complex networks has been recently advanced by the research by many scientists and mathematicians, including the study of random networks by Erdös and Rényi, small world networks by Watts and Strogatz, and scale-free networks by Barabási and Newman. A number of popular scientific book have been written on the topic in the last few years including *Small Worlds* (1999) and *Six Degrees* (2003) by Duncan Watts, *Linked* (2002) by Albert-László Barabási, *Nexus* (2002) by Buchanan and *Emergence* (2002) by Steven Johnson.

With the recent introduction of the principles of network-centric warfare and the importance of information and communication to today's warfighter, complex network theory is emerging as an indispensable tool for application to military problems.

2.2 Background on the Analysis of Email Networks

Email is the primary asynchronous method of electronic communication for the Information Age. There are a large number of other computer-based channels available including chat, voice-over-IP, web logs, and websites, but email has remained the chief method despite these technological developments. Studying email networks can provide a large number of benefits to an organization. HP Labs' Joshua Tyler, Dennis Wilkinson and Bernardo Huberman describe a number of benefits in the study of email networks[1]. Email provides insight into personal communication behaviors and is often a key productivity and collaboration tool. The collection of email data can provide maps of relationships within an organization. Many corporations use email network analysis to identify communities of practice and other informal groups within their organization. Email data can also be obtained in very large quantities that can be easily processed and analyzed. From this large volume of data hidden patterns of organization and leadership can be discovered. Analyzing email networks showcases the power of informal networks and indirect connections which are sometimes more important than more formal relationships and command chains. This type of analysis can enhance knowledge of the military's social and C2 networks and patterns of communication, and expose the vulnerability of such networks to viruses, information warfare, system failures and combat loses.

2.3 Analysis Terms & Definitions

A unique vocabulary, that all readers may not be familiar with, was used for this analysis. The following are common complex network-related terms and their associated definitions.

- **Network, graph, sub-graph** – a network is a collection of individual entities that are connected together in some way, a graph is more mathematical term that is used for a network, a sub-graph or sub-network is a smaller collection of entities that exist within a larger one, networks have the following three properties: a structure, dynamics and evolution

- **Topology** – the physical arrangement of a network, network structure

---

[1] Joshua R. Tyler, Dennis M. Wilkinson, Bernardo A. Huberman, "Email as Spectroscopy: Automated Discovery of Community Structure within Organizations,"
<http://www.hpl.hp.com/research/idl/papers/email/index.html> [14 March 2005].

- **Social network** – a depiction of the patterns of relationships among social actors

- **Node** – an entity in a network, in this analysis the nodes were email addresses

- **Link** – a connection between nodes, in this analysis a link was defined an email message sent between two addresses

- **Link/node ratio** - helpful in comparing the structural similarity of networks with different sizes

- **Directed graph, undirected graph** – a directed graph is one in which the links in the graph have a direction, in the case of email networks the link goes from a sender to a receiver, an undirected graph's links have no specific direction and just denote a link between two nodes

- **Degree (in and out)** – Only applicable for directed graphs, in-degree is the number of incoming links a node has, out-degree is the number of outgoing links a node has, it is the number of a node's nearest neighbors

- **Degree distribution** - a representation of the connection pattern of a network, a degree distribution plot shows the number of nodes with specific degrees

- **Characteristic path length (CPL)** - the median of the average distance from each node to every other node in the network, CPL is useful in determining the diffusion rate of the network, the shorter the CPL the quicker information is transferred throughout the network

- **Clustering** - a measure of local cohesion in a network, measures the extent to which nodes that are connected to a particular node are also connected to each other (is the friend of my friend also my friend)

- **Susceptibility/Robustness/Resilience** - the extent a network can avoid catastrophic failure as links or nodes are removed and how other properties are affected by node or link removal

- **Betweenness** – a measure of a node's importance to dynamic behaviors in a complex network, measures the number of shortest paths that pass through a node

- **Random network** - a network of nodes connected in a random fashion, random networks have particular properties including a random topology, low CPL, and low clustering

- **Scale-free network** – a network of nodes where a large percentage of nodes have very few connections and a small percentage of nodes, known as hubs, have a large number of connections, scale-free networks exhibit a power-law distribution of the nodes' degrees, a large number of real-world networks have this property including airline routes, the physical structure of the Internet, the World Wide Web, and connections between scientific publications

- **Assortative mixing** – the tendency of nodes to selectively link, the principle states that nodes with many connections will tend to link with other nodes with many connections, in other words hubs link to hubs, this is primarily a property of social networks[2]

---

[2] M.E.J. Newman, "Assortative mixing in networks," <u>Physical Review Letters</u>, 89 (2002): 208701.

- **Neutrality rating** – A measurement of the amount of additional, latent structure in a complex network, this additional latent structure, where properly configured , is the source of networked effects, adaptability, and modularity in complex networks

- **Nucleus** – A region of a social network with the highest concentration of links between nodes

- **Fringe** – A region of a social network with a low concentration of links between nodes

- **Coefficient of the power-law distribution (γ)** – Scale-free networks are governed by a power law distribution of a node's degree, γ is the scaling exponent in the equation that governs this distribution

- **Reciprocal communication** – Communication between two nodes is considered reciprocal if Node A sends to Node B and Node B also sends to Node A, this is used as a method to define a link in a network

- **Threshold** – A threshold is a set level of interactions between nodes used as a method to define a link in a network (e.g. a link does not exist unless twenty messages are sent between two nodes)

3.0 ESSENTIAL ELEMENTS OF ANALYSIS

The goal for the C2 network analysis was by analyzing the structure, dynamics and evolution of the email network employed by coalition participants, lessons on how to design adaptive command and control structures that are robust and match natural usage patterns could be derived. To support this goal, the analysis focused on five questions:

1. *Does the introduction of new email software tools change previously established operating structures?* Does the email flow match with formal chains of command and pre-established information transfer protocols or do new ones emerge? Do informal problem solving groups develop during operations and do they maintain their cohesion throughout the exercise or dissolve at the end of a particular event? Can we expose hidden patterns of organization and leadership?

2. *Who are the key nodes for email traffic flow?* In the old method of intra-coalition communication, liaisons were used. Do new types of liaison arise within the email network? Does the coalition email network function as one US-UK collective or as two separate entities connected by "gatekeeper" nodes?

3. *How robust is the email network in light of the removal of nodes and/or links (either due to combat or to technical failure)?* This question will help to evaluate how the email network may perform under stress. Can new connections be formed to maintain the integrity of the network? Does coalition data sharing increase as operational tempo increases?

4. *How does the structure of the email network evolve over the course of the exercise?* By looking at how the network was structured during different time periods (events) during the course of the exercise, we could show network evolution. Do the two coalition email networks merge over time? How are sub-graphs created and disassembled?

5. *What are the internal dynamics of select sub-networks and how to the sub-networks interact with each other?* Do any definitive collaborative groups emerge in the sub-networks? If so, what are the groups based on? Function? Rank? To aid in the development of ways to break up staffs based on natural network usage patterns, where are the potential cut-points? What is the level of interaction between sub-networks and who are the connecting nodes?

4.0 METHOD

The method followed to investigate the essential elements of analysis consisted of a number of different stages. The first stage was a familiarization and accumulation of knowledge about the setup of the exercise and the expected behavior of the email network. The second stage was data collection and the sorting, parsing and formatting of the data to use in the analysis tool that was selected. This third stage was the analysis. The analysis was divided into two parts, a general analysis that looked at network statistics over the entire exercise and a detailed analysis that examined two interesting time periods in greater detail. Finally, conclusions were drawn that had military significance and could aid in designing of military C2 structures and organizations.

To fully analyze the email system there were three characteristics of the network that had to be examined. They were the network's structure, its dynamics, and evolution. Network diagrams were generated of the actual topologies that emerged during the selected timeframes of the exercise. The table below shows the questions answered by this analysis and the associated metrics that were generated to address each question.

EEA	Question	Metrics
1	Does the introduction of new email software tools <u>change</u> previously established <u>operating procedures</u>?	▪ Link/node ratio ▪ Degree distribution ▪ Characteristic path length
2	Who are the <u>key nodes</u> for email traffic flow?	▪ Identify hubs ▪ Clustering coefficient ▪ Betweenness centrality
3	How <u>robust</u> is the email network in light of the removal of nodes and/or links?	▪ Betweenness centrality ▪ Characteristic path length
4	How does the <u>structure</u> of the email network <u>evolve</u> over the course of the exercise?	▪ Graphic visualizations of network structure at different time periods during the exercise ▪ Select metrics over time
5	What are the <u>internal dynamics</u> of select sub-networks and how to the sub-networks interact with each other?	▪ Graphic visualization of the sub-networks over the entire exercise ▪ Nucleus/fringe nodes

4.1 Overview of Tools Used for Analysis

To perform this analysis the commercial software package UCINET[3] was used. UCINET is comprehensive social network analysis software, used mainly in sociology. It is a Windows-based, menu-driven program that can calculate social network statistics and metrics through the

[3] S.P. Borgatti, M.G. Everett, and L.C. Freeman, "Ucinet for Windows: Software for Social Network Analysis," Harvard, MA: Analytic Technologies (2002). Used Version 6.53, June 2004.

processing large amounts of data. The application NetDraw (which comes with UCINET) was used to create all of the graphical visualizations of the network data in this report. Since the science of complex networks is relatively new, researchers many times write their own applications to perform the specific mathematical calculations. A large number of commercial, shareware and freeware application were examined prior to the selection of UCINET.

4.2 Assumptions & Limits of Analysis

Since this was an exploratory exercise, a number of assumptions needed to be declared and understood before delving into the results of the analysis.

- What is a node? – For the purposes of this analysis a node was considered to be an email addresses (not the same thing as an individual). An email address may have multiple people associated with it, or none at all. Also, sometimes individuals do not use their own email account but have others manage it for them.

- What constitutes a link? – The email network analyzed was a directed network. A link existed between two nodes if an email had been exchanged between two addresses. The links did not discriminate between addresses that are in a message's "to:" or "cc:" field. For example, if there is a message sent from "Sample@navy.mil" and "X1@navy.mil" is in the "to:" field and "X2@navy.mil" is in the "cc:" field, links existed from Sample to X1 and from Sample to X2.

- In the examination of how the sub-networks interacted, different ways of defining a link were tested to see how they changed the structure of the network. For some of the graphical depictions of the sub-networks a link was assumed to exist if there was reciprocal communication, in others, if a certain number of messages were exchanged between two nodes (a threshold).

- The general analysis data was broken into timeframes of six hours. Six hour segments were chosen in order to follow the battle rhythm of the exercise. The analysis looked at the evolution over these timeframes. The metrics are derived from static timeframe snapshots.

- This analysis looked solely at message connection patterns. The intent, content or importance of the information in the emails did not play a factor. Also, the personalities of the email address owners were not considered, some individuals are more apt to communicate via email than other methods.

- A military email network does not have to worry about external messages entering the system, or the generation of spam or junk email. However, there are questions regarding how individuals who broadcasted informational messages to large number of addresses during the exercise affected the system. Since this analysis did not look at the content of messages, it is impossible to gauge the importance of messages sent to a large number of individuals.

- The email network was only one component of the entire C2 structure. There were many other traditional and digital layers that contributed to the total C2 structure as well.

- Every effort was made to remove email addresses from the system that acted as artifacts. A number of email addresses in the network either auto-forwarded other messages, were

automatically generated messages, or were messages from the email server. These nodes did not contribute the structure of the social network.

5.0 ANALYSIS

5.1 General (Overview) Analysis

The general analysis was geared towards developing an understanding of how the email network evolved over the course of the exercise. The data was divided into four, six hour periods for each day, 0000-0600, 0600-1200, 1200-1800 and 1800-2400. By looking at the following metrics for each timeframe the specific type of network the pattern of email interactions formed could be determined.

- Number of nodes in the network
- The number of links in the network
- The ratios of links to nodes
- Characteristic path lengths
- Clustering coefficients

Different properties belong to different network types. Once the specific structural archetype was known a basis for the detailed analysis of specific timeframes could be performed. In most email and other computer networks that have been studied in the scientific literature, the structure has been found to be scale-free. That is, the degree distribution of nodes follows a power-law (as opposed to the more common regular distribution). In this type of network there are very few nodes with a large number of links and a large number of nodes with just a few links. Through this analysis it was determined whether or not this military email network was scale-free.

First, the number of nodes (n) participating in the network over time was determined and graphed (see Appendix Figure A-1). There was a distinct cyclical pattern that emerged in the number of nodes during each time period. During the active part of the exercise the number of nodes participating in the network remained fairly constant across each timeframe. Since this was a closed military network, and there were not large loses in the number of addresses, this behavior was understandable.

Next, the number of links in the network needed to be plotted over time. In this case there are two metrics to look at, the total number of links (k) and the distinct number of links (k_d) in the network during each timeframe (see Appendix Figure A-2). The distinct number of links was determined by taking the list of all the links and filtering out the unique pairings. If one address sent five messages to another address during the time period, the number of links would be five but the number of distinct links would only be one. The link plots also follow a similar cyclic pattern like that of the nodes, with the peak traffic during the 0600-1200 and 1200-1800 timeframes, which matched with the most active parts of the exercise.

With just these two statistics, the number of nodes and number of links, network behaviors can be derived. The number of nodes was plotted against the number of distinct links, with each point one particular timeframe (see Appendix Figure A-3). As shown the in the graph, the metric follows a linear pattern. That is, as the number of nodes in the network grows the number of distinct links grows in a linear fashion. This was an important evolutionary statistic. This can help network managers gauge potential usage patterns, and network traffic could be estimated by just looking at how many addresses (nodes) were participating in the system.

In general, the most adaptive complex networks have twice as many links as nodes.[4] Some network-centric warfare theories state that every node should be connected to every other node in the network to have the best performance (n^2), exploiting the principles of Metcalfe's Law.[5] On the contrary, having fewer links provides an economy of resources while the structure still can maintain robust, adaptable behavior. Having a higher link to node ratio may provide more robustness which is a desirable to a military network but, if it gets to high, there may be too much excess structure in the system. The ratio for this analysis's email network lies between 1.5 and 3.0 for the duration of the exercise (see Appendix Figure A-4).

The next metric that was derived and plotted for the network was characteristic path length. As stated in Section 2.3 characteristic path length is the median of the average distance from each node to every other node in the network. In adaptive, robust complex networks the CPL should be approximately the logarithm of n.[6] CPL is useful in determining the diffusion rate of the network, the shorter the CPL the quicker information is transferred throughout the network. It is a good measure of what the strongest, quickest and most probably path between two nodes is. The CPL for the email network generally ranged between four and six and a half (with a few outliers) (see Appendix Figure A-5). This is above the optimum number [$\log(n)$], meaning that information may flow more slowly on this particular network than a network that was fully optimized. There is extra structure in the network but, as mentioned before, this is good for a military network because is promotes adaptability by having alternative information routing patterns available if certain nodes are eliminated. There is a fine balance that must be struck, enough latent structure should be available to promote adaptation, but not so much that it is economically and physically impractical.

The final metric that was generated for the overview analysis was the clustering coefficient (see Appendix Figure A-6). The clustering coefficient was used to determine the amount of local node cohesion. The clustering coefficient measures the number of a node's direct neighbors that are also direct neighbors of each other. The higher the clustering coefficient, the higher the amount of collaboration in the network. Note the timeframes where the coefficient is highest [Day 4 0600-1200 (0.23), Day 5 1800-2400 (0.20), Day 6 1200-1800 (0.28), Day 8 1800-2400 (0.20), Day 10 1200-1800 (0.20)]. These high clustering numbers could denote that during those timeframes communications in the network were tightly coupled and a high degree of collaboration was occurring.

Figure 5.1-1, is a graphical depiction of how the email network changed over the course of one day. These diagrams may look like a Rosarch test or astronomical chart, but valuable information can be gained though the visualization of complex networks. It is difficult to make broad generalizations about the network by just looking at the diagram or the individual statistics. Complex networks are just that, complex. There is rarely a simple correlation that can be made between statistics. A parallel can be made between how a doctor diagnoses a patient and how complex networks are analyzed. Doctors look at multiple measurements (blood pressure, pulse,

---

[4] Derived from M.E.J. Newman, "The Structure and Function of Complex Networks," <u>SIAM Review</u>, 45 (2003): 167-256.
[5] Network-Centric Warfare: Developing and Leverage Information Superiority, 2nd Edition Revised, David S. Alberts, John J. Garstka, Frederick P. Stein, CCRP, 1999. - "Metcalfe's Law (Figure 4) describes the potential value of a network. It states that as the number of nodes in a network increases linearly, the potential 'value' or 'effectiveness' of the network increases exponentially as the square number of nodes in the network."
[6] Derived from M.E.J. Newman.

etc.), symptoms, and other factors before making a diagnosis. All of the statistics and the pictures must be examined simultaneously in order to understand the topology of a complex network.

Table 5.1-1 lists the major statistics for Day 5 of the exercise. The 0000-0600 timeframe had the fewest number of nodes and links so the structure of the network is more evident in the diagram. There are some noticeable "tree" patterns throughout the center of the network. This indicates that one person sent an email to a group of individuals. There are a few heavily connected hubs and a large number of simple recipients. In the second time period, this hub and spoke pattern was even more evident. The two large "blooms" at the top and in the middle of the network are instances where a few individuals sent messages to a large number of recipients. The top "bloom" belongs to the UK system and the middle "bloom" to the US. If you remove all of the nodes with a degree of one, most of the "bloom" will disappear. Note that the clustering coefficient for the timeframe was the lowest of the day, probably due to fact that there was increased simple information broadcast.

The final time period of the day had the highest clustering coefficient (0.20). The diagram gives clues to this fact. The "rings" that are seen in the other diagrams aren't as pronounced. The rings are a symptom of a less cohesive network. From looking at diagrams throughout the exercise, this class of network had a highly connected core that broadcasted messages to an inner ring, who then in tern broadcasted to an outer ring. This network structure lends itself to a hierarchical organizational structure. This was not the case for the 1800-2400 timeframe which has a larger number of indirect connections.

Date	Time (EDT)	N	k	k_d	k/n	k_d/n	CPL	$\log(n)$	C
Day 5	0000-0600	557	2636	984	4.73	1.77	5.02	2.99	0.08
Day 5	0600-1200	2069	16,700	5558	8.07	2.69	4.78	3.74	0.05
Day 5	1200-1800	1449	13,209	4329	9.12	2.99	4.52	3.64	0.12
Day 5	1800-2400	1183	8867	2928	7.50	2.48	4.83	3.47	0.20

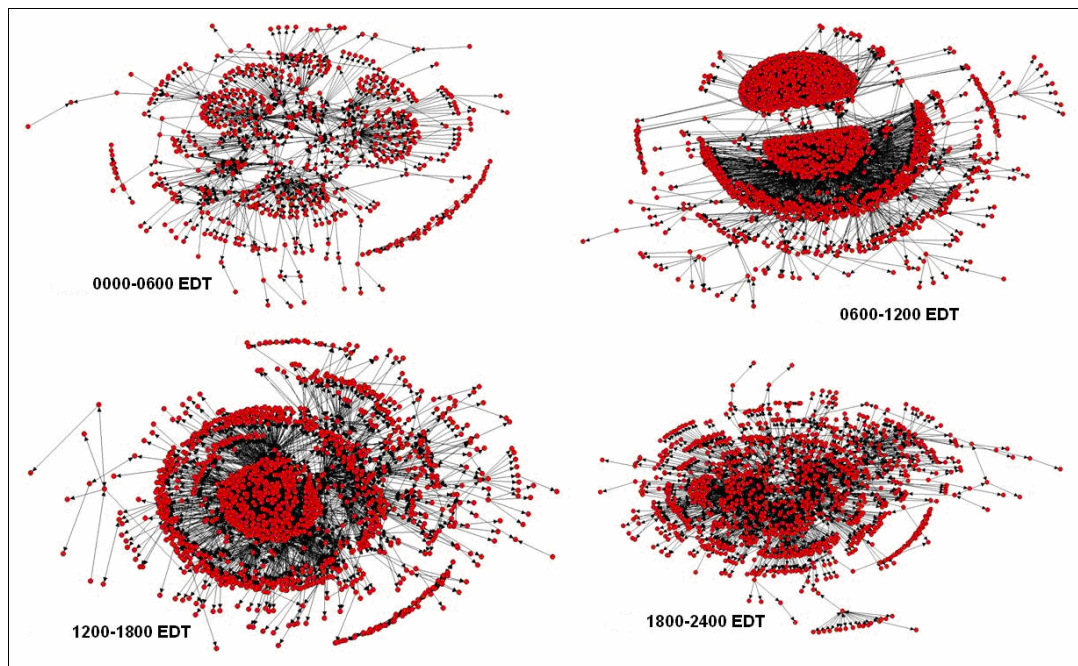**Table 5.1-1: Select Statistics for Email Network on Day 5**

Figure 5.1-1: Graphic Progression of Network on Day 5

To complete the overview analysis, data needed to be generated that helped to answer how well the two email systems were connected during the exercise (EEA #1 and #2). To do this, the database of email connections from the entire exercise was filtered to only include those links that occurred either between UK addresses or between US and UK addresses. The result of that filtering was plotted in NetDraw, and the results are shown below in Figure 5.1-2. From a cursory inspection the two networks did exhibit a level of interaction, though not a complete merger. A handful of nodes provided the majority of connections between the two systems. The diagram was visually inspected to see who acted as connectors between the two systems. A numerical analysis of these connections was not performed as part of this analysis, but metrics could be developed in the future to accomplish a more qualitative approach.
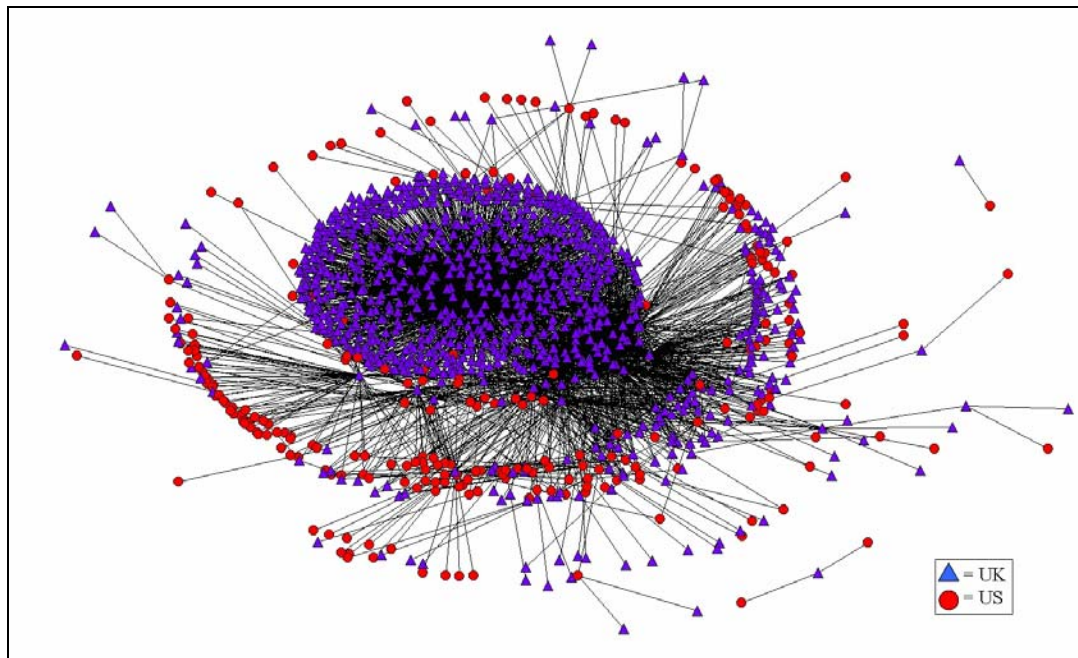

Figure 5.1-2: US-UK Interactions for Entire Exercise

5.2 Detailed Analysis of Select Exercise Timeframes

The overview analysis in Section 5.1 provided a look into how the exercise's email network evolved of the course of thirteen days. In order to gain more insight into the structure and dynamics of the network a more detailed analysis was required. Two interesting timeframes were chosen for further study. These specific timeframes were chosen firstly because they fell during the middle of the exercise, so biases caused by the exercise personnel warming up or winding down wouldn't occur. Secondly, so comparisons could be made, the same timeframe for both days (1200-1800) was selected. A number of additional statistics were examined for the detailed analysis including:

- In and out degree distributions
- Betweenness centrality
- Collaboration metrics
- Random and targeted robustness measurements
- More detailed annotated network diagrams

11

Date	Time (EDT)	N	K	k_d	k/n	k_d/n	CPL	$\log(n)$	C
Day 6	1200-1800	1217	10,819	3331	8.89	2.74	4.80	3.52	0.28
Day 8	1200-1800	1546	14,275	4104	9.23	2.65	4.63	3.61	0.14

Table 5.2-1: Network Statistics for Detailed Timeframes

Degree Distribution

Since the email networks were treated as directed graphs each node had both an in-degree and an out-degree. The degree distribution of a network is a representation of the connection pattern of a network. The more connections a node has the more important it is to spreading information through a network. By plotting a histogram of degrees, the class of a network (regular, random, scale-free, etc.) can be determined. In Figure 5.2-1 (and Appendix Figure A-7) the number of email addresses with a particular degree was plotted on a log-log scale. If the network was scale-free this distribution will be linear. The graphs show that both the in and out-degree for both timeframes follow a linear pattern when plotted. A very few number of nodes have very large degrees and a large number of nodes have small degrees. This provides evidence that the exercise's email network was indeed scale-free.
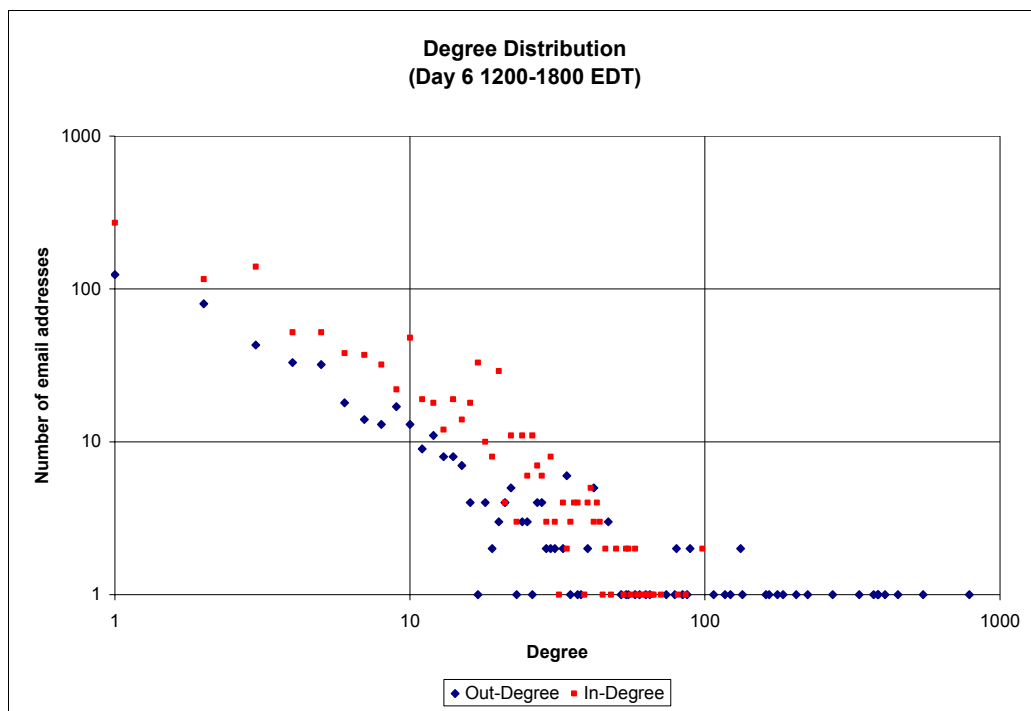

Figure 5.2-1: In and Out-Degree Distributions for Day 6 1200-1800 EDT

For real, scale-free networks the degree distribution decays as a power law governed by the equation: $p_k \sim k^{-\gamma}$. By determining what γ is for the degree distributions for the exercise's email networks, a comparison can be made with other real-world networks. Table 5.2-2 shows the γ's for the selected timeframes. For networks such as the Internet, metabolic reaction networks, telephone call graphs, and the WWW, γ is approximately between 2.1-2.4.[7] Why the discrepancy? It is unknown at this time. Further mathematical investigation outside the scope of this analysis might provide some answers. Another email network, from a university, that has been studied has

---

[7] Steven H. Strogatz, "Exploring complex networks," Nature, 410 (8 March 2001).

shown smaller exponents, along the lines of less than two.[8] These are closer to the exponents for the exercise's network. Diagrams of the original degree distribution plots and the equations from which the γ's were derived are in Appendix Figures A-8 and A-9.

Timeframe	Out-Degree γ	In-Degree γ
Day 6 1200-1800	1.3	1.4
Day 8 1200-1800	1.2	1.4

Table 5.2-2: Coefficient of Power-Law Distributions

So what were the most important addresses (hubs) to the email network? For a complete listing of the top ten in, out and total degree nodes see Tables A-1 and A-2 in the Appendix. The individual node with the highest total degree in each detailed case was an individual who was involved with intelligence. The individual in charge of the exercise also ranked high, which was expected. Please note that for classification reasons the actual email addresses for these individuals were removed from this report.

Collaboration

In this analysis it was assumed that someone who collaborates both sends and receives email. In Figure 5.2-2 a notional way of computing this is demonstrated. Those nodes that have a high out-degree and a low in-degree are considered "broadcasters" (send lots of email). Those that have a high in-degree and low out-degree are "receivers" (receive lots of email). Those who send and receive a comparatively equal amount are the collaborators in the network. The data generated from the analysis of the two detailed timeframes was used to test this new measure. When this data was plotted, there was not as clear a distinction as would have be expected between receivers, broadcasters and collaborators in the diagrams.
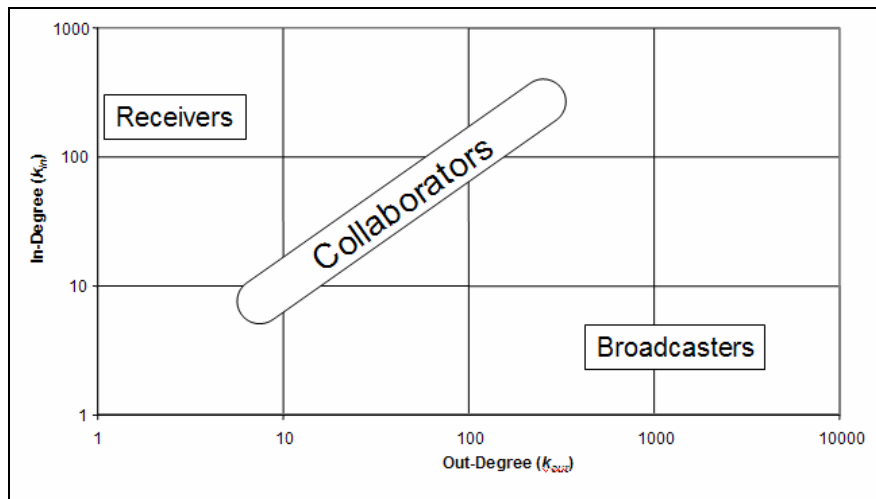
Figure 5.2-2: Collaboration Graph

Different ways of manipulating the data before plotting it could make the distinction clearer. In these graphs someone who sends and receives one or two emails is treated the same as someone who sends and receives tens or hundreds of emails. By weighting the nodes this bias could be corrected. Statistics that are more telling than the collaboration graphs are located in Table 5.2-3.

---

[8] H. Ebel, Mielsch, L.-I., and Bornholdt, S., "Scale-free topology of e-mail networks," Phys. Rev. E, 66 (2002): 035103.

In this simple table, the number of nodes that receive only, transmit only, and both transmit and receive are listed. For both timeframes only approximately one-third of all nodes in the email network during the six hours of the detailed timeframe collaborate at any level. The vast majority of nodes are apparently just receiving informational email. This does not play to the strengths of the technology of email. Perhaps a different way to communicate with these receivers should be investigated, such as a public webpage or message board.

Timeframe	Receive Only	Xmit Only	Xmit & Receive
Day 6 1200-1800	684 (56%)	91 (7%)	441 (36%)
Day 8 1200-1800	894 (58%)	146 (10%)	504 (33%)

Table 5.2-3: Transmit and Receive Statistics for Detailed Timeframes

Betweenness

Another statistic that helps to determine what the most important nodes to the system are is the betweenness centrality. The betweenness measures the number of shortest paths that run through a particular node. It really tells us what the most "well-worn" node is. It is different than degree in that degree only measures the origination and termination of paths through the network but betweenness measures those nodes that are most important to facilitating information flow. To apply an Industrial Age metaphor to an Information Age process, those nodes with high betweenness act as the most important cogs in a machine, they might not start or end processes but they enable them to happen. Those nodes with the highest betweenness also have a measured effect on robustness, by removing nodes with high betweenness the path lengths through the network will lengthen, slowing information flow. Appendix Table A-3 lists the betweenness ranking for the two detailed timeframes.

Robustness

An important property of any network, not only military ones, is its robustness. Robustness is the ability of a network to continue to function effectively while withstanding the removal or nodes or links. Knowing from the degree distribution plots that the exercise's email network is scale-free, hypotheses about the resilience of the network to attack or failure could be made. Scale-free networks, in general, are very robust in the light of random attack or failure but more susceptible to the targeted removal of hubs.[9] The Internet is a scale-free network, it has a small percentage of well connected hubs (routers) and a very large percentage of sparsely connected nodes. Random failure occurs very frequently when viruses attack systems and technical problems with routers occur. If the well-connected routers were removed one by one from the network, soon the Internet would become fragmented and unable to function properly. The exercise's email network, like many other information networks, should follow the same course.

To test the theory, two sets of calculations were performed on each detailed time period. In the first set, twenty nodes were removed in order of highest total degree (in plus out degree). For the second set twenty nodes were selected at random for removal from the network. Appendix Tables A-4 and A-5 are a comparison between those sets of calculations. The key metric is how the CPL changed as the nodes were removed. For both cases as the targeted nodes were removed the CPL increased, meaning the information would diffuse more slowly in networks that were under this type of targeted attack. As each highly connected hub was removed other nodes were also removed from the network since they were connected to that hub, and only that hub. In both

---

[9] Réka Albert, Albert-László Barabási, "Statistical mechanics of complex networks," Reviews of Modern Physics, 74 (January 2002): 47-97.

cases by removing approximately two percent of the total nodes in the network, between eighteen and twenty percent of the total network was lost. This shows the power hubs have to assist the flow of information. In the random case, CPL did not change and the percentage of nodes lost was in line the percentage of nodes removed from the network. Figures 5.2-5 illustrates the dramatic difference between the targeted and random removal of nodes and their affect on network structure. Notice that the degradation of the system is not linear. Just like all nodes, all hubs are not created equal, some hubs have more degree one nodes connected to them than others. The roller-coaster like downward path that the size of the network takes as the high degree nodes are deleted exemplifies this. This analysis assumes that damage control does not take place while the nodes are being deleted from the network.

Social networks (like email networks) exhibit an interesting property that other types of networks do not share. Assortative mixing occurs when nodes in a network show preferential linking to other nodes in the network. In social networks, hubs tend to connect with hubs. This makes sense, people who know a lot of people know people who know a lot of people. This property should be taken in account when studying the resilience of a network.
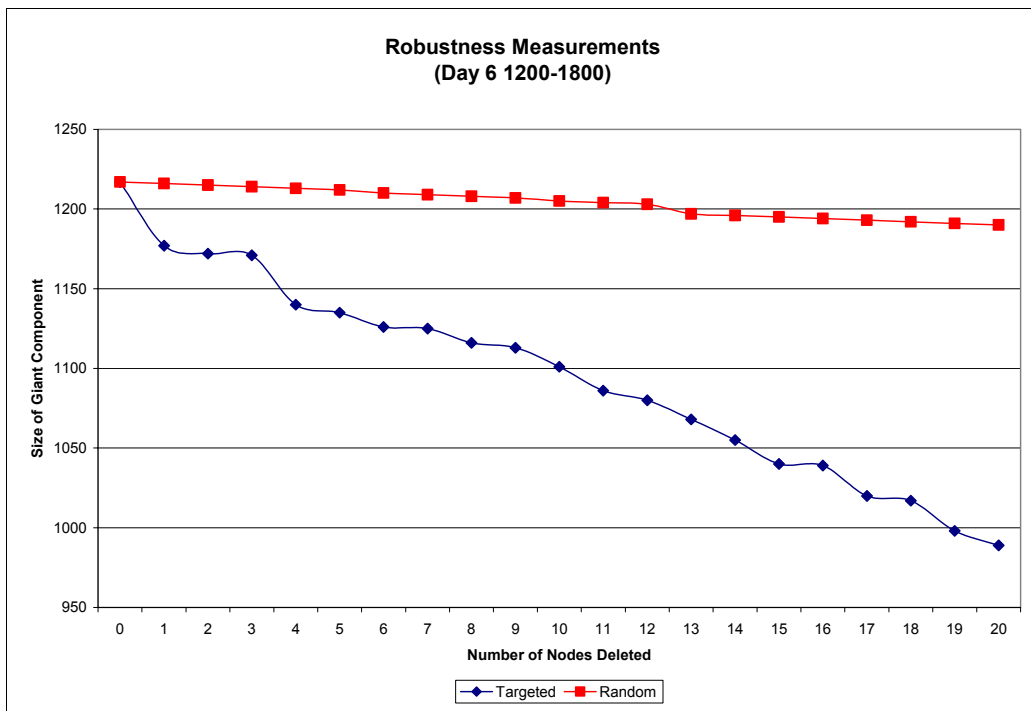
Figure 5.2-5: Targeted and Random Robustness Measurements for Day 6 1200-1800 EDT

5.3 Sub-Network Communications

In order to answer EEA #5, three staffs participating in the exercise were selected for detailed study. The customer of this analysis wanted to investigate potential strategies to deliberately divide staffs between different ships or ships and shore-based facilities. Understanding the dynamics of how the various staffs communicated was required before specific recommendations could be made.

Intra-Sub-Network Communications

For intra-sub-network communications (communications within a sub-network) for the three selected sub-networks, network diagrams were generated to help understand their patterns of communication. In addition, similar network statistics to what were in generated in the overview and detailed parts of the analysis (in Sections 5.1 and 5.2) were also generated. Table 5.3-1 lists statistics for the sub-networks and compares them to the statistics for the overall exercise's email network. The numbers of nodes in the sub-networks are a small fraction of the total number found in the entire network, which makes comparison somewhat difficult. In general, Staff #1 and Staff #2 showed levels of collaboration on a much greater level than the network as a whole. They had characteristic path lengths that were short and on par with what the thumb rule dictates. They also had very high clustering and high amounts of neutral structure. The distinct link to node ratios were between fifteen and twenty, meaning that the sub-network members communicated with lots of different individuals in their sub-network. The difference in statistics between the entire exercise network and the Staff #1 and Staff #2 sub-networks could be due to the fact that there are a large number of unimportant nodes in the exercise's network, including external addresses, artifacts and other non-exercise related email traffic. The sub-networks were very well defined and only included email that members of each staff generated. Staff #3 did not have enough email traffic to perform an adequate analysis.

Network	N	K	k_d	k/n	k_d/n	CPL	$\log(n)$	C	N
Entire Exercise	6,096	344,382	37,941	56.49	6.22	3.79	4.58	0.09	5.2
Staff #1	295	36,068	6,087	122.3	20.6	2.25	2.47	1.48	19.6
Staff #2	52	8,636	812	166.1	15.6	1.75	1.72	6.7	14.6
Staff #3	59	130	71	2.2	1.2	NA	NA	NA	NA

Table 5.3-1: Network Statistics for Sub-Networks

Staff #1

The diagrams of the sub-network interactions were very detailed and full of complicated interaction patterns. They have not been included in this report due to the fact that they contain exercise participants' names.

The first diagram generated showed all of the interactions between the 295 nodes in the Staff #1 sub-network. Because of the diagram's complexity, we can't get much useful information out of this diagram except that there was a "nucleus" of individual nodes at the center of the sub-network communications. To create a clearer, a more useful picture, changing the definition of a link could be helpful. The second diagram generated showed the sub-network interactions using a reciprocal link definition. This cleared the picture up quite a bit. The structure of Staff #1 became more evident. There was a clear "nucleus" of nodes in the center of the diagram. There were 160 (out of the 295) nodes that participated in the reciprocal network. This meant that approximately fifty-four percent of the total Staff #1 nodes participated in two-way communication. Running an algorithm in UCINET provided us with a list of which nodes were in the nucleus (representing 9% of the total network). The twenty-seven nucleus nodes and their rank and functional position were determined.

Another different link definition was tried and a diagram of interactions generated. This time a link only existed if greater than fifty messages were sent between nodes. This link definition was based more on volume of communication than on level of collaboration. The diagram showed that the members of the Staff #1 nucleus were located in two groups in the center of the diagram.

Staff #2

16

Staff #2 was much smaller than the Staff #1, thus the structure of the network was more evident in the diagrams. There was a significant amount of interaction between all the nodes in the sub-network and it did not show the typical characteristics of a scale-free network that were prevalent in the detailed views of the entire exercise's email network. A diagram was generated that showed Staff #2 sub-network interactions with a standard link definition. Another diagram showed the same network, but with a reciprocal link definition. Seventy-seven percent of the Staff #2 nodes were in the reciprocal network. The nucleus of Staff #2 represented a much larger percentage of the total network than Staff #1 did (31% for Staff #2 vice 9% for Staff #1). Bearing in mind that a higher percentage of nodes were in Staff #2's reciprocal network than in Staff #1's (77% versus 54%), and that a higher percentage of nodes were in Staff #2's nucleus, Staff #2 collaborated at a greater level than Staff #1. This could be because a smaller team like Staff #2 might be predisposed to greater collaboration and teamwork.

Staff #3

Staff #3's sub-network was so sparse that accurate generalizations could not be made about it. The reason for this sparseness could be due to the fact that Staff #3 was a combination of three dissimilar staffs combined together just for the purposes of the exercise. Since these staffs did not have common standard operating procedures, they may have relied on other methods of communication (face-to-face, chat, etc.).

Inter-Sub-Network Communications

A secondary goal of this part of the analysis was to analyze how the various sub-networks interacted with each other. Interactions between Staff #1 and Staff #2 were selected for a more in-depth look. All of the intra- and inter-sub-network interactions for the two sub-networks were plotted. In the diagram, it appeared that the two nuclei of the two sub-networks were highly connected, as would be expected. Additional plots and metrics could have been generated just showing inter-sub-network interaction, or just the interactions between the nucleus nodes of the two sub-networks.

6.0 MILITARY SIGNIFICANCE

A large amount of statistics and diagrams were generated in order to better understand how the email network operated and evolved over the course of the exercise. So how does all the information in the analysis translate to the real world operation of similar information networks? This analysis attempted to measure things that had not been measured before in command and control structures. The essential elements of analysis (EEAs) focused those measurements into a series of questions that could shed some light on how better to engineer command and control structures. The majority of the analysis dealt with observing, measuring, describing and understanding. However, the true power is its usefulness is in the engineering of new systems. Below, evidence is presented in order to answer the EEAs. Conclusions are then drawn from the evidence.

EEA #1: *Does the email cross domain solution change previously established operating procedures?*

Evidence: Various network interaction diagrams that were generated provided graphical representations of how the cross domain solution functioned. Little information was known about email traffic flows in prior exercises. It was assumed that in the past individual liaisons handled all of the communications between US and UK networks. In the two time periods investigated a

level of integration existed between multiple hubs however, a mathematical measurement that could be used for comparisons was not generated.

Conclusion: There is insufficient evidence to determine the level to which the new software tools altered organizational structures from prior experiments. Individual interviews with participants might be useful in this case. The diagrams show that there was some level of integration between the two networks. The clustering coefficient could be a useful metric for comparisons, as the time period with the higher clustering coefficient appeared to have more mixing between the US and UK networks.

EEA #2: *Who are the key nodes for email traffic flow?*

Evidence: There were many important nodes is this network. In identifying a small handful of individuals as the most important nodes the analysis was not implying that other nodes in the network were not performing necessary tasks. The question that was asked was who was most important to the structure of the system? To determine who the most important nodes were for the two detailed time periods, the nodes that were in the top five for in- and out-degree and betweenness were identified. Three nodes met these criteria. They were the head of the exercise, the J2 ACOS, and an individual involved with information operations.

Conclusion: The individuals identified were the most important to the structure of the network, they should be protected more so than other less important nodes. It is difficult to deem importance by just looking at one statistic, multiple statistics should be considered when identifying "important nodes". One noticeable individual ranked very high in in-degree and much less so in out-degree and betweenness. That node probably broadcasted a large amount of informational messages, but was not as crucial as other nodes were to the structure of the network. When looking at collaboration patterns in the two detailed timeframes, the vast majority of nodes were apparently just receiving informational email. Perhaps a different way to communicate with these receivers should be investigated, such as a public webpage or message board.

EEA #3: *How robust is the email network in light of the removal of nodes and/or links?*

Evidence: Appendix Tables 4 and 5 and Figure 5.2-5 provided the evidence of how robust the exercise's email network was at particular times.

Conclusion: Like all scale-free networks and many email networks, the email network that evolved over the course of the exercise was resilient to random node removal and susceptible to targeted node removal.

EEA #4: *How does the structure of the email network evolve over the course of the exercise?*

Evidence: All of the analysis in Section 5.1 was done in order to understand how the email network evolved of the course of the exercise. The statistics for this evolution are located in Appendix Table A-6, the Master Statistics Table.

Conclusion: The email network's statistics and structure tended to follow the rhythm of the exercise with the highest periods of activity occurring between 0600 and 1800. The CPL remained in a fairly consistent band expect for some peripherals when the network size was small. The CPL was higher than it needed to be, but the redundancy may add to the robustness of the network, which is a desirable property for military systems. The network tended to grow and

recede in a linear fashion which can help predict resource requirements. The clustering was not dependent on network size and sometimes was higher when the size of the network was smaller, probably due to more broadcast emails being transmitted when the network was larger.

EEA #5: *What are the internal dynamics of select sub-networks and how do they interact with each other?*

Evidence: Numerous figures provided graphical depictions of the structure of the Staff #1, Staff #2 and Staff #3 sub-networks. Different link definitions (including reciprocal and threshold) were used to help understand the interaction patterns better. It was hoped that these diagrams would provide insight into how the staffs could be split if the need arose. Members of the nucleus in the Staff #1 and Staff #2 sub-networks were also determined.

Conclusion: These techniques can be used to aid in the distribution of staffs, in particular how to distribute a staff based on coordination needs. Sub-networks that coordinate a lot would need to be co-located, while groups who do not can be distributed. For Staff #1 and Staff #2 there were no obvious splits in the network where the staffs could be easily subdivided. There was a nucleus of dense communication surrounded by a fringe of lesser amounts of communication for both sub-networks. This leads to a challenge, if we subdivide the staff based solely on who is the nucleus and who is in the fringe and place all of the nucleus nodes in one location, we have just made the protection of that location more important. However, if we split the sub-network's nucleus into two pieces and place them at different locations, the level of communication within the nucleus might not be as great. It would ruin the established collaboration pattern of the sub-network.

All of Staff #2 was highly connected and collaborative, more so than Staff #1. This is probably due to the smaller size of Staff #2. In the case of Staff #3, there was not enough communication within the sub-network to make any generalizations. This could be due to the fact that there were not enough computers for the staff and individuals were sharing accounts. It could also be because the three different component staffs that were pooled together to form Staff #3 didn't have experience working together before. In examining the diagrams plotting the connections between Staff #2 and Staff #1 is was obvious that the two nuclei of the networks were connected. It is worth mentioning that only approximately 400 nodes out of the 6000 in the entire exercise's email network were in the staff sub-networks. This leads us to the conclusion that there were a large number of external nodes affecting the structure of the overall exercise's network.

7.0 CONCLUSIONS

There are three items that should be understood and applied in the future based on the results of this analysis of a US/UK naval exercise email network.

1. The exercise's email network was scale-free, showing a skewed degree distribution. There were a small number of nodes with a large degree and a large number of nodes with a very small degree. This puts the power of the network in the hubs. They provide the majority of the robustness of the network. This means that to protect the flow of information through those hubs they should not be physically located all on the same platform. If the platform were damaged or destroyed, not only has a physical combat asset been lost but a large component of the information system has as well. The importance of the hubs also means that they should probably get preferential treatment in relation to nodes that do not greatly contribute to the structure of the network. Since the majority of information on the email network flows through the hubs, they are very

susceptible to physical malfunctions and attacks by computer viruses. The hubs should get preferential treatment for bandwidth, technical support and virus protection.

2. The purpose of this analysis was to observe and analyze a particular email network during a particular exercise. This can be taken to the next level where the lessons learned from analyzing informal C2 networks can applied to the design of new C2 structures that would have more beneficial properties. If the robustness of the network needs to be improved, certain elements of the topology can be changed. If the diffusion of information needs to occur at a greater rate, other things can be done to facilitate that. Most of the academic research has looked at applying complex network analysis techniques to pre-existing networks. Industry and the military are increasingly interested in moving beyond just describing what already exits, and moving toward exploiting network properties in the design of new systems. It should be understood that this is a very new field of study.

3. Part of the goal of this analysis was to see what could be learned from the exercise by just looking at simple connection patterns. Ignorance regarding the context of the exercise was deliberately pursued. Why do this? It was an attempt to determine what happened during the exercise and to figure out who was important without initially knowing any of the players and nothing of the timeline. Besides helping design and understand our own C2 systems these analysis tools could be useful in examining hostile countries' or terrorist networks' email logs. By developing the same types of network diagrams and statistics, valuable information could be learned without knowing the content of the messages or the context in which is was sent. Email network analysis could prove to be a powerful intelligence tool.

Through discussions with representatives of the Navy Warfare Development Command (NWDC) and Navy Network Warfare Command (NNWC) a number of militarily significant findings were discussed. The recommendations fell in the following three categories:

1. Information Operations / Information Assurance
   – Focus network defense on most important nodes
   – Improve node counter-targeting
   – Examine use of method to exploit adversary networks and C2 structure

2. C2 Structure and Information Flow
   – Support decision of critical nodes placement in distribution of staff
   – Develop alternate C2 paths
   – Measure and understand key command and staff relationships to more effectively use Collaborative Information Environment

3. Network and Information Management
   – Assist warfighter in defining requirements and providing feedback on engineering design parameters
   – Provides metrics for evaluation and design of information management practices
   – Provide input to plans for graceful degradation of capability

8.0 LESSONS LEARNED AND NEXT STEPS

This section offers a high-level overview of some of the lessons learned from this discovery analysis process and suggests where immediate improvements could be made. Overall, this

analysis showed that the value provided though analyzing network topology is essential to the development of any modern command and control system. The email system was just one segment of a larger C2 network. This method would prove useful for any or all of the additional segments (chat, voice-over-IP or others). The analysis also showed how two separate networks (US and UK) collaborated and began to merge.

There are three main areas to look at for prospective variations and improvements to this analysis's method, they are: data collection and formatting issues, additional software tools and changing network definition parameters. The data made available for this particular analysis came from the Microsoft Outlook logs that were generated during the exercise, only information in those logs could be used. Additional nodal information such as nationality, position and rank would have been additional properties that could have been analyzed. The information was available through other sources but it was difficult and cumbersome to integrate it into the pre-existing data and software tools.

Other software tools could have brought an additional level of understanding to the exploration of the email network. HP Labs has developed an application called Zoomgraph to be used as a network visualization tool. Most of its functionality is similar to NetDraw, save for one feature. Zoomgraph has the ability to generate network evolution movies by extrapolating between fixed network diagrams. Time constraints prevented the examination of this program in developing network evolution movies for the exercise. There has also been some preliminary research into dynamic network visualization tools, where network structure and properties were measured as a function of time. Specific nodes could be targeted for monitoring and their degree, betweenness, and position in the topology could be tracked.

A potential variation of the analysis would involve just looking at specific sub-networks of interest. For example, just look at the nodes that sent email across networks, US to UK or vice versa. Some research has been done by Valdis Krebs[10], a social network researcher best known for his terrorist network diagrams, into how the merger of two companies occurs by only studying their email systems. These theories might be applicable to these military efforts. Finally, one way to alter the analysis would be to change the assumptions of the network. How many connection should there be to make a link? In most of this analysis the answer was one. What would the networks look like if this was changed to five or ten? Some of these potential improvements were studied preliminarily in the sub-network analysis found in Section 5.3.

---

[10] Valdis Krebs' website is http://www.orgnet.com

SOURCES & ADDITIONAL RESOURCES

Albert, Réka, Albert-László Barabási. "Statistical mechanics of complex networks." Reviews of Modern Physics, 74 (January 2002): 47-97.

Barabási, Albert-László. Linked: How Everything Is Connected to Everything Else and What It Means. New York: Plume, 2003.

Boyd, John P., William J. Fitzgerald, and Robert J. Beck. "Computing Core/Periphery Structures and Permutation Tests for Social Relations Data." Institute for Mathematical Behavioral Sciences, Paper 16 (September 28, 2004).

Braha, Dan, Yaneer Bar-Yam. "Topology of large-scale engineering problem-solving networks." Phys. Rev. E, 69 (2004): 016113.

Ebel, H., Mielsch, L.-I., and Bornholdt, S. "Scale-free topology of e-mail networks." Phys. Rev. E, 66 (2002): 035103.

Gloor, Peter A., Yan Zhao, Scott B.C. Dynes. "Temporal Visualization and Analysis of Social Networks." <http://ccs.mit.edu/pgloor%20papers/CKN4NAACSOS.pdf> [14 March 2005].

Huberman, Bernardo A., Lada A. Adamic. "Information Dynamics in the Networked World." <http://www.hpl.hp.com/research/idl/papers/infodynamics/index.html> [14 March 2005].

Newman, M.E.J. "The Structure and Function of Complex Networks." SIAM Review, 45 (2003): 167-256.

_____. "Assortative mixing in networks." Physical Review Letters, 89 (2002): 208701.

Newman, M.E.J., Stephanie Forrest, Justin Balthrop. "Email networks and the spread of computer viruses." Phys. Rev. E, 66 (2002): 035101.

Tyler, Joshua R., Dennis M. Wilkinson, Bernardo A. Huberman. "Email as Spectroscopy: Automated Discovery of Community Structure within Organizations." <http://www.hpl.hp.com/research/idl/papers/email/index.html> [14 March 2005].

Watts, D. J. Six Degrees: The Science of a Connected Age. New York: Norton, 2003.

_____. Small Worlds: The Dynamics of Networks Between Order and Randomness. Princeton, NJ: Princeton University Press, 1999.

Strogatz, Steven H. "Exploring complex networks." Nature, 410 (8 March 2001).
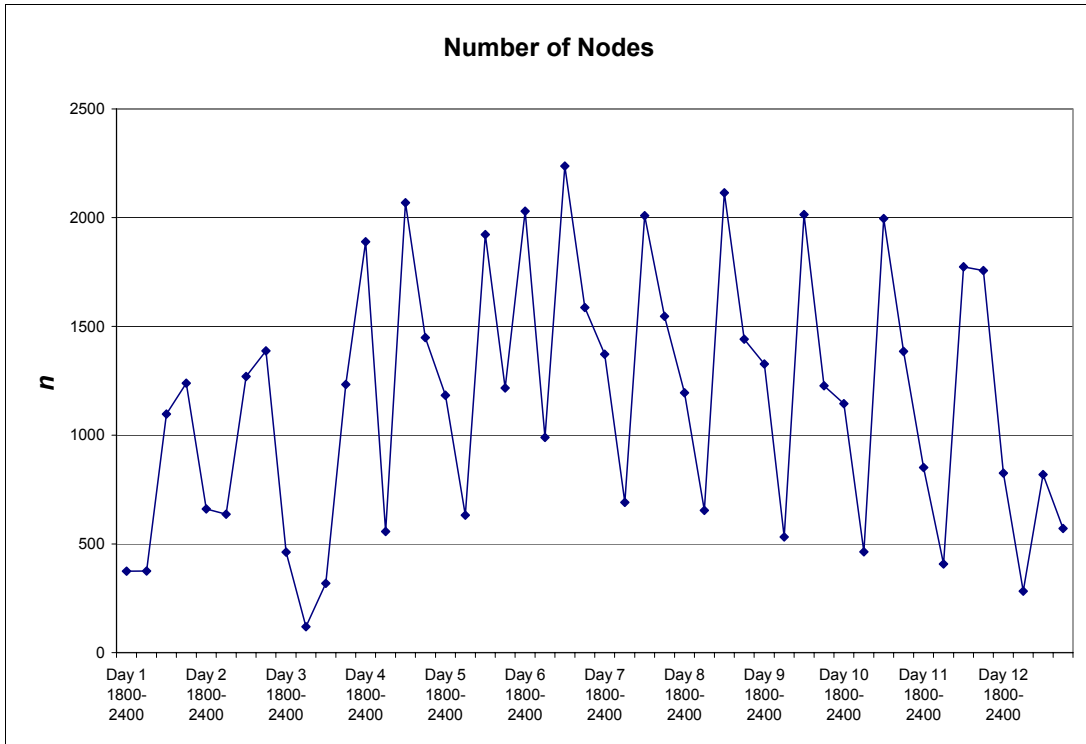
Figure A-1: Number of Nodes
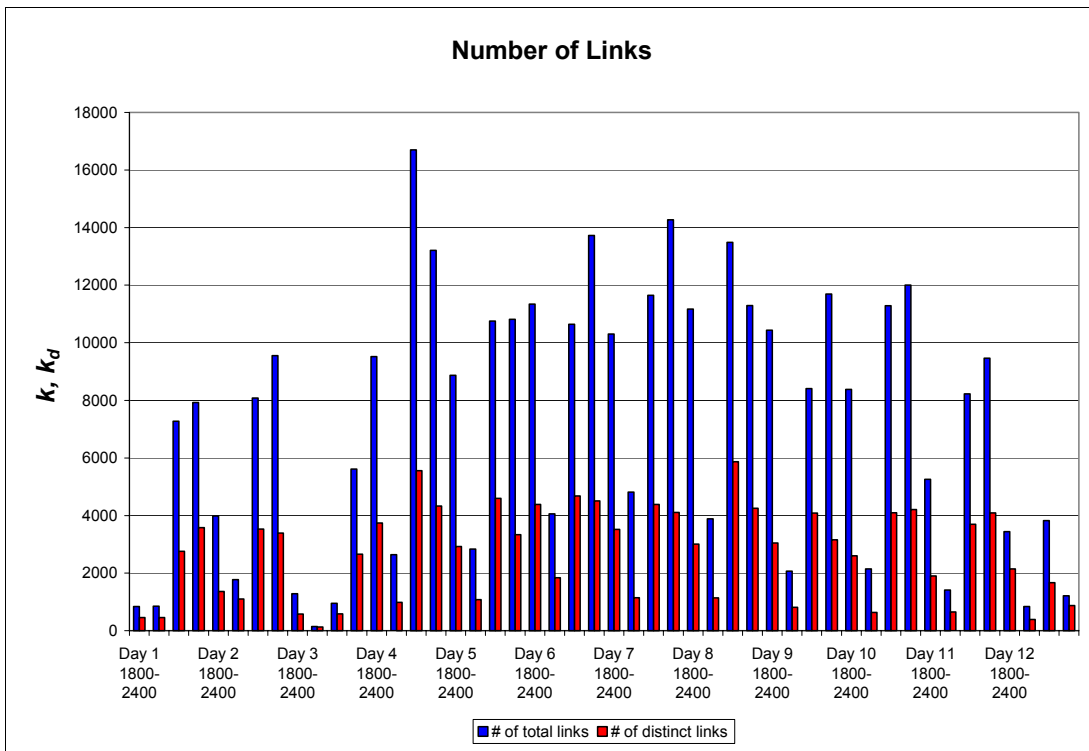
Figure A-2: Number of Total and Distinct Links
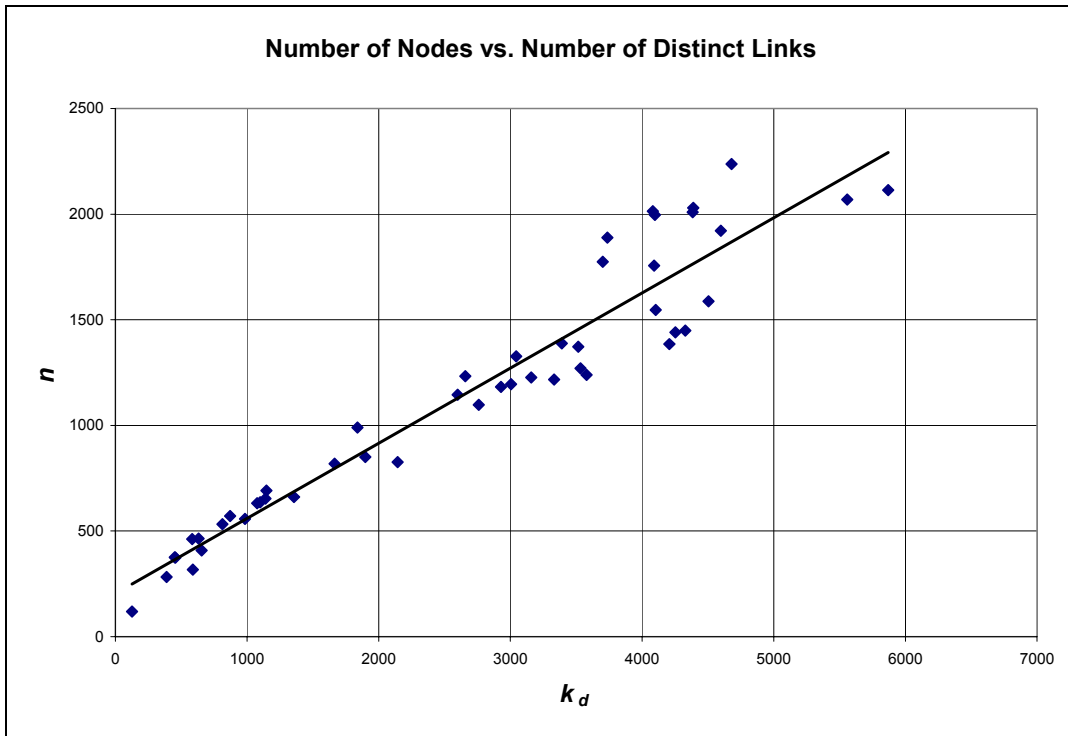
Figure A-3: Number of Nodes vs. Number of Distinct Links
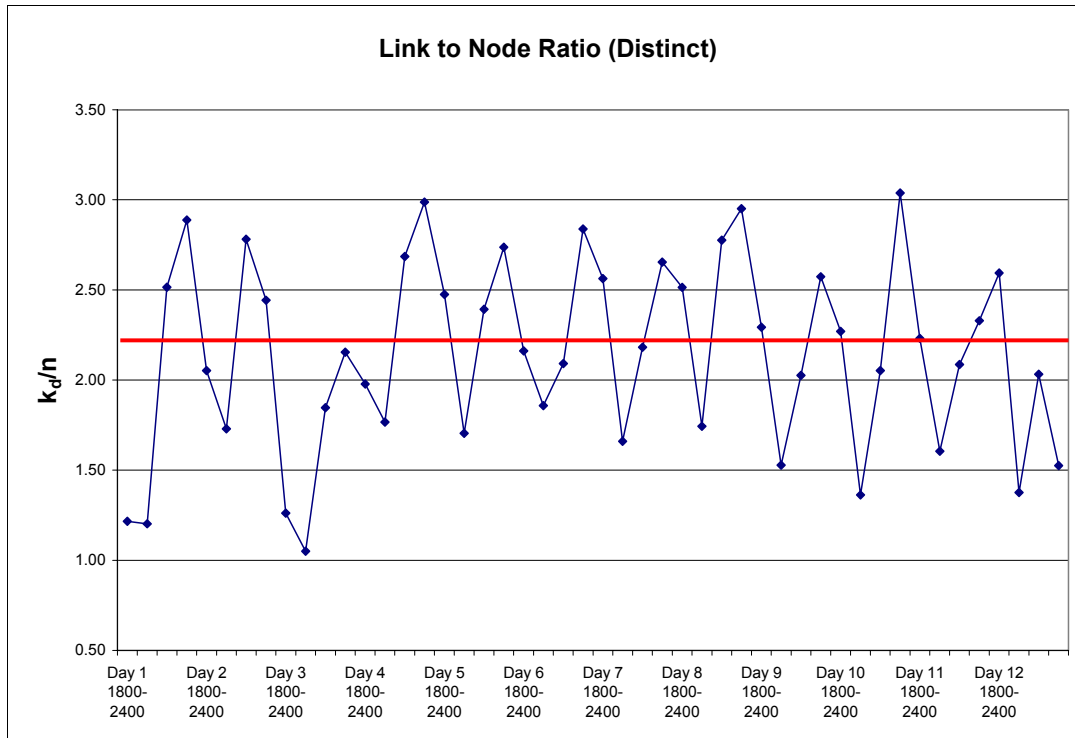
Figure A-4: Distinct Link to Node Ratio

Figure A-5: Number of Nodes vs. Characteristic Path Length

Figure A-6: Clustering Coefficient
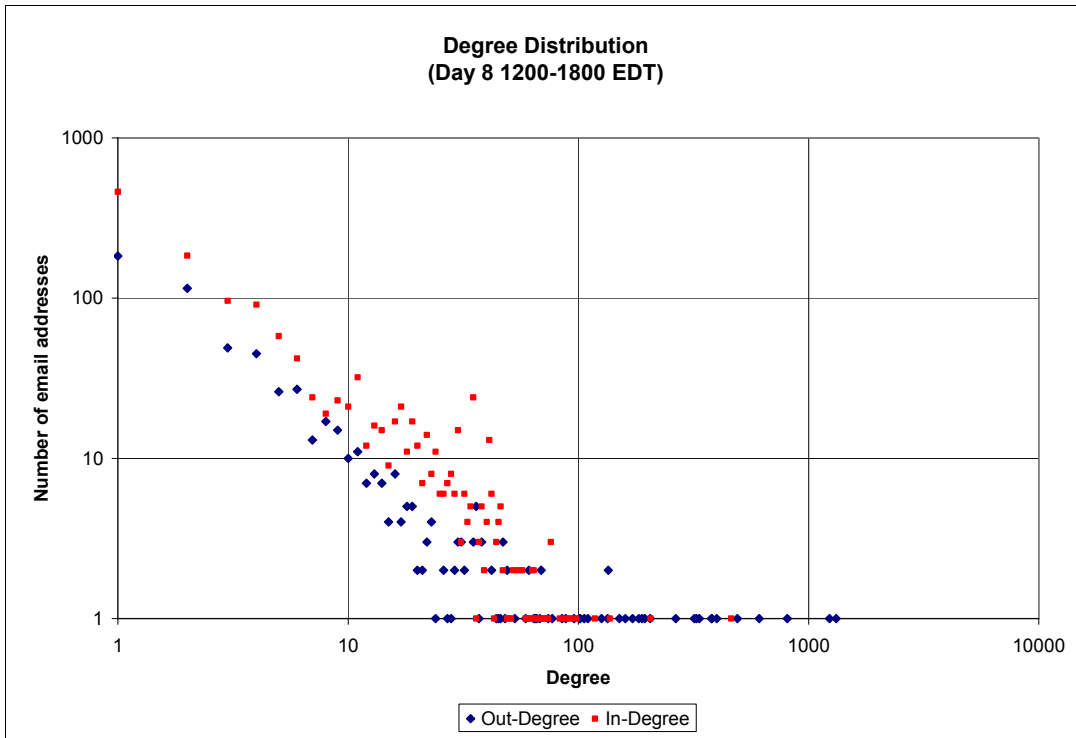
Figure A-7: In and Out-Degree Distributions for Day 8 1200-1800 EDT
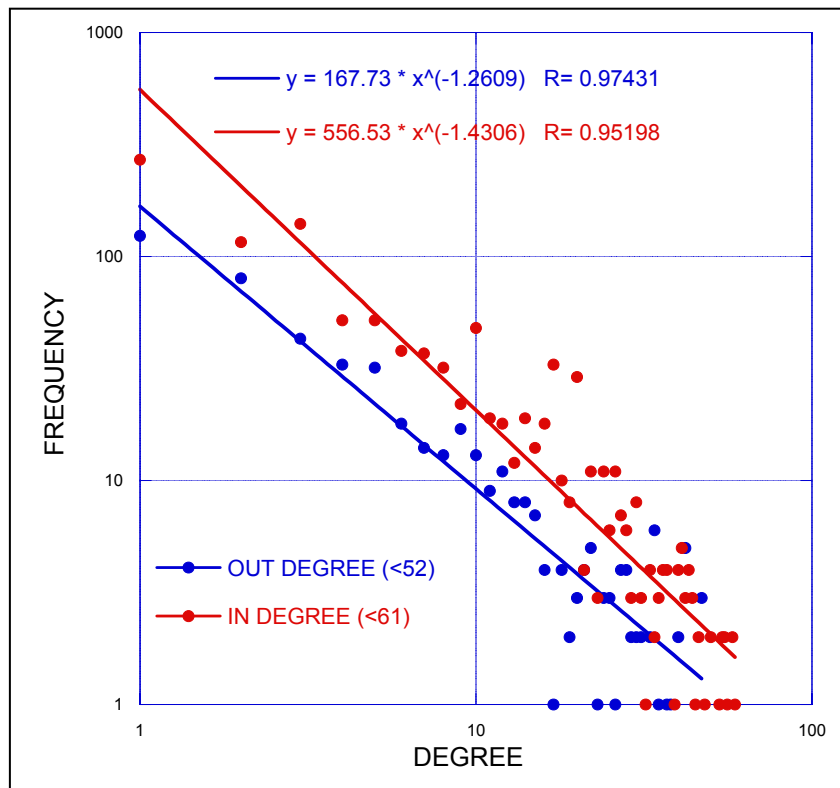
Figure A-8: In and Out-Degree Distributions for Day 6 1200-1800 EDT
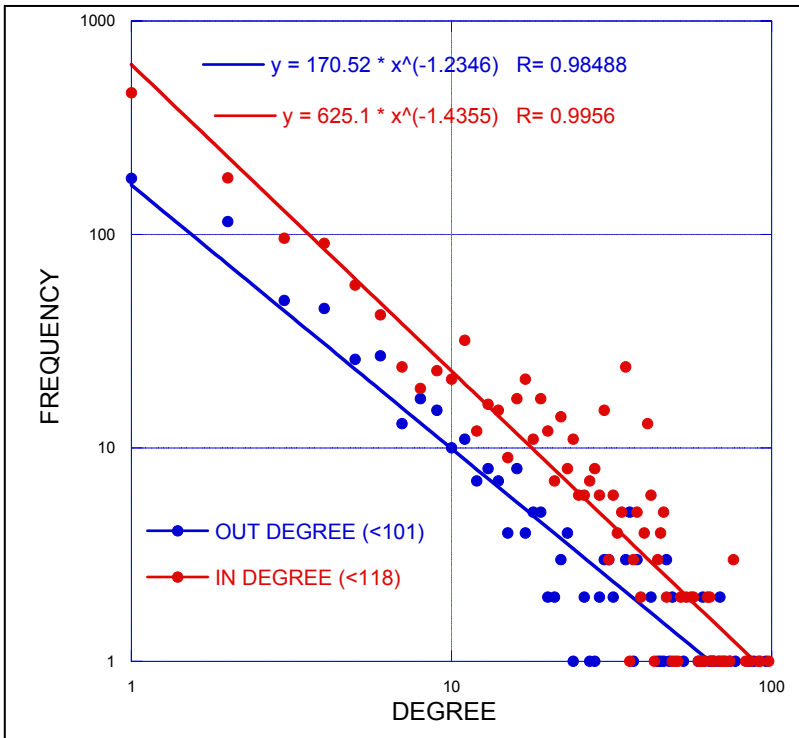
Figure A-9: In and Out-Degree Distributions for Day 8 1200-1800 EDT

Table A-1: Out-, In- and Total Degree Rankings for Day 6

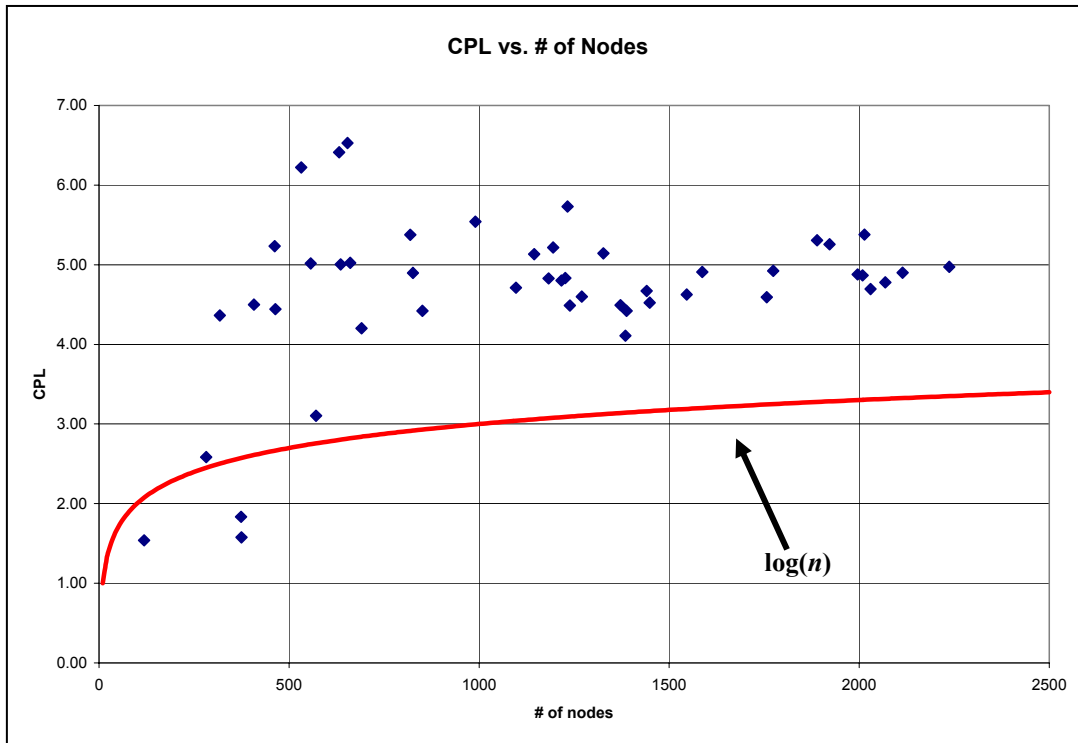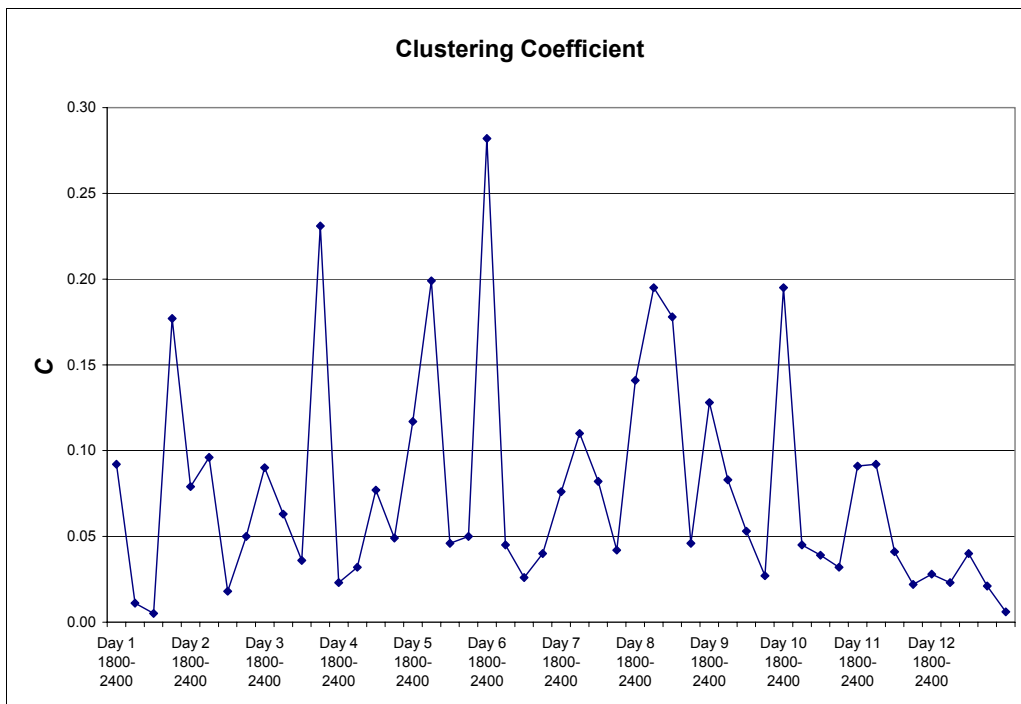|	DAY 6 1200-1800 EDT		
	OUT-DEGREE	**IN-DEGREE**	**TOTAL DEGREE**
#1	Intel	CFMCC, COPS Dir	Intel
#2	Battle Watch Commander (CFMCC)	Artifact	BWC
#3	Asst. JOC Watch	J3A	Asst. JOC Watch
#4	CJTF 950, DACOS Training and Exercise	JOC Watch (JTF BWC)	CJTF 950, DACOS Training and Exercise
#5	CJTF 950, J2 ACOS	CJTF 950, ACOS Operations	CJTF 950, J2 ACOS
#6	Maritime Ops	CFMCC, Ops	CJTF 950, OPSEC/CNO Officer
#7	CJTF 950, OPSEC/CNO Officer	JTF2024	Maritime Ops
#8	CJTF 950, ???	CJTF 950, J2 ACOS	CJTF 950
#9	CJTF 950, Logistics Support	CJTF 950, DACOS Training and Exercise	CJTF 950, Logistics Support
#10	J2CI, Intel	Intel	CJTF 950, Dep. IO Officer

Table A-2: Out-, In- and Total Degree Rankings for Day 8

	DAY 8 1200-1800 EDT		
	OUT-DEGREE	**IN-DEGREE**	**TOTAL DEGREE**
#1	Intel	Joint Intel Watch Officer	Intel
#2	CJTF 950, DACOS Training and Exercise	CFMCC/CDS, COS	CJTF 950, DACOS Training and Exercise
#3	CJTF 950, OPSEC/CNO Officer	CFMCC, Current Ops Dir	CJTF 950, OPSEC/CNO Officer
#4	Watch account for CFMCC Comms Watch	Intel	Watch account for CFMCC Comms Watch
#5	J6 ACOS	J3A	J6 ACOS
#6	JTF2024	JTF2024	JTF2024
#7	Artifact	JOC Watch	Joint Intel Watch Officer
#8	JOC Watch	CJTF 950, OPSEC/CNO Officer	JOC Watch
#9	Maritime Ops	Asst. JOC Watch	Maritime Ops
#10	CJTF 950, Logistics Support	CJTF 950, Dep. IO Officer	Artifact

Rank	Day 6 1200-1800	Day 8 1200-1800
#1	CJTF 950, DACOS Training and Exercise	J6 ACOS
#2	CJTF 950, J24 ISR&T/SSO	J3A
#3	CFMCC, AIR/GAT	CJTF 950, DACOS Train. and Exer.
#4	CJTF 950, J2 ACOS	CJTF 950, J2 ACOS
#5	CFMCC, KM/COMMO	CJTF 950, Subsurface Train. and Exer.
#6	Asst. JOC Watch	CJTF 950, ACOS Operations
#7	CFMCC, OPS	CJTF 950, OPSEC/CNO Officer
#8	CJTF 950, J25 Plans/Policy	CFMCC, KM/COMMO
#9	BWC	Intel
#10	CFMCC, COPS Dir	CJTF 950, Fleet Comms

Table A-3: Betweenness Rankings for Detailed Timeframes

DAY 6 1200-1800 EDT						
	Targeted*			Random*		
n deleted	CPL	*n* left	% *n* lost	CPL	*n* left	% *n* lost
0	4.8	1217	0%	4.8	1217	0%
1	4.8	1177	3.3%	4.8	1216	0.1%
2	4.9	1172	3.7%	4.8	1215	0.2%
3	4.9	1171	3.8%	4.8	1214	0.2%
4	5.2	1140	6.3%	4.8	1213	0.3%
5	5.2	1135	6.7%	4.8	1212	0.4%
6	5.2	1126	7.5%	4.8	1210	0.6%
7	5.3	1125	7.6%	4.8	1209	0.7%
8	5.4	1116	8.3%	4.8	1208	0.7%
9	5.4	1113	8.5%	4.8	1207	0.8%
10	5.4	1101	9.5%	4.8	1205	1.0%
11	5.4	1086	10.8%	4.8	1204	1.1%
12	5.5	1080	11.3%	4.8	1203	1.2%
13	5.5	1068	12.2%	4.8	1197	1.6%
14	5.5	1055	13.3%	4.8	1196	1.7%
15	5.7	1040	14.5%	4.8	1195	1.8%
16	5.7	1039	14.6%	4.8	1194	1.9%
17	5.7	1020	16.2%	4.8	1193	2.0%
18	5.8	1017	16.4%	4.8	1192	2.1%
19	5.8	998	18.0%	4.8	1191	2.1%
20	5.8	989	18.7%	4.8	1190	2.2%

*Only removing ~1.6% of the total number of nodes
Table A-4: Robustness Statistics for Day 6 1200-1800 EDT

DAY 8 1200-1800 EDT						
	Targeted*			Random*		
n deleted	CPL	*n* left	% *n* lost	CPL	*n* left	% *n* lost
0	4.6	1546	0%	4.6	1546	0%
1	4.6	1511	2.3%	4.6	1545	0.1%
2	4.7	1505	2.7%	4.6	1544	0.1%
3	4.8	1486	3.9%	4.6	1543	0.2%
4	4.8	1480	4.3%	4.6	1542	0.3%
5	4.9	1310	15.3%	4.6	1541	0.3%
6	5.0	1306	15.5%	4.6	1540	0.4%
7	5.0	1301	15.8%	4.6	1539	0.5%
8	5.0	1300	15.9%	4.6	1538	0.5%

9	5.1	1299	16.0%	4.6	1537	0.6%
10	5.1	1299	16.0%	4.6	1536	0.6%
11	5.1	1286	16.8%	4.6	1535	0.7%
12	5.2	1252	19.0%	4.6	1534	0.8%
13	5.2	1249	19.2%	4.6	1533	0.8%
14	5.3	1243	19.6%	4.6	1532	0.9%
15	5.3	1226	20.7%	4.6	1531	1.0%
16	5.3	1221	21.0%	4.6	1530	1.0%
17	5.4	1214	21.5%	4.6	1529	1.1%
18	5.7	1205	22.1%	4.6	1528	1.2%
19	5.8	1175	24.0%	4.6	1527	1.2%
20	5.8	1161	24.9%	4.6	1523	1.5%

*Only removing ~1.3% of the total number of nodes
Table A-5: Robustness Statistics for Day 8 1200-1800 EDT

Table A-6: Master Statistics List

Date	Time (EDT)	n	k	k_d	k/n	k_d/n	CPL	log(n)	C
All	All	6096	344382	37941	56.49	6.22	3.79	4.58	0.09
Day 1	1800-2400	374	839	455	2.24	1.22	1.84	2.66	0.01
Day 2	0000-0600	375	854	451	2.28	1.20	1.58	2.65	0.01
Day 2	0600-1200	1097	7274	2760	6.63	2.52	4.71	3.44	0.18
Day 2	1200-1800	1239	7924	3578	6.40	2.89	4.49	3.55	0.08
Day 2	1800-2400	661	3984	1357	6.03	2.05	5.02	3.13	0.10
Day 3	0000-0600	636	1770	1100	2.78	1.73	5.01	3.04	0.02
Day 3	0600-1200	1270	8081	3533	6.36	2.78	4.60	3.55	0.05
Day 3	1200-1800	1388	9555	3390	6.88	2.44	4.42	3.53	0.09
Day 3	1800-2400	462	1283	583	2.78	1.26	5.23	2.77	0.06
Day 4	0000-0600	119	145	125	1.22	1.05	1.54	2.10	0.04
Day 4	0600-1200	318	951	587	2.99	1.85	4.36	2.77	0.23
Day 4	1200-1800	1233	5610	2657	4.55	2.15	5.73	3.42	0.02
Day 4	1800-2400	1889	9524	3737	5.04	1.98	5.31	3.57	0.03
Day 5	0000-0600	557	2636	984	4.73	1.77	5.02	2.99	0.08
Day 5	0600-1200	2069	16700	5558	8.07	2.69	4.78	3.74	0.05
Day 5	1200-1800	1449	13209	4329	9.12	2.99	4.52	3.64	0.12
Day 5	1800-2400	1183	8867	2928	7.50	2.48	4.83	3.47	0.20
Day 6	0000-0600	632	2831	1077	4.48	1.70	6.41	3.03	0.05
Day 6	0600-1200	1922	10759	4598	5.60	2.39	5.26	3.66	0.05
Day 6	1200-1800	1217	10819	3331	8.89	2.74	4.80	3.52	0.28
Day 6	1800-2400	2030	11344	4388	5.59	2.16	4.69	3.64	0.05
Day 7	0000-0600	990	4056	1839	4.10	1.86	5.54	3.26	0.03
Day 7	0600-1200	2237	10643	4679	4.76	2.09	4.97	3.67	0.04
Day 7	1200-1800	1587	13725	4504	8.65	2.84	4.91	3.65	0.08
Day 7	1800-2400	1372	10303	3516	7.51	2.56	4.49	3.55	0.11
Day 8	0000-0600	691	4813	1147	6.97	1.66	4.20	3.06	0.08
Day 8	0600-1200	2009	11649	4384	5.80	2.18	4.87	3.64	0.04
Day 8	1200-1800	1546	14275	4104	9.23	2.65	4.63	3.61	0.14
Day 8	1800-2400	1195	11171	3005	9.35	2.51	5.22	3.48	0.20
Day 9	0000-0600	654	3883	1140	5.94	1.74	6.53	3.06	0.18

Day 9	**0600-1200**	2114	13487	5869	6.38	2.78	4.90	3.77	0.05
Day 9	**1200-1800**	1441	11294	4253	7.84	2.95	4.67	3.63	0.13
Day 9	**1800-2400**	1327	10438	3044	7.87	2.29	5.14	3.48	0.08
Day 10	**0000-0600**	532	2067	813	3.89	1.53	6.22	2.91	0.05
Day 10	**0600-1200**	2014	8411	4082	4.18	2.03	5.38	3.61	0.03
Day 10	**1200-1800**	1227	11699	3158	9.53	2.57	4.83	3.50	0.20
Day 10	**1800-2400**	1145	8383	2599	7.32	2.27	5.13	3.41	0.05
Day 11	**0000-0600**	464	2143	632	4.62	1.36	4.44	2.80	0.04
Day 11	**0600-1200**	1996	11291	4097	5.66	2.05	4.88	3.61	0.03
Day 11	**1200-1800**	1385	11999	4208	8.66	3.04	4.11	3.62	0.09
Day 11	**1800-2400**	851	5255	1899	6.18	2.23	4.42	3.28	0.09
Day 12	**0000-0600**	408	1416	655	3.47	1.61	4.50	2.82	0.04
Day 12	**0600-1200**	1774	8226	3701	4.64	2.09	4.92	3.57	0.02
Day 12	**1200-1800**	1757	9463	4092	5.39	2.33	4.59	3.61	0.03
Day 12	**1800-2400**	826	3438	2143	4.16	2.59	4.90	3.33	0.02
Day 13	**0000-0600**	282	838	388	2.97	1.38	2.58	2.59	0.04
Day 13	**0600-1200**	819	3828	1665	4.67	2.03	5.38	3.22	0.02
Day 13	**1200-1800**	571	1210	871	2.12	1.53	3.10	2.94	0.01

n = number of nodes
k = number of total links
k_d = number of distinct links
k/n = link to node ratio (mean degree)
k_d/n = distinct link to node ratio
CPL = characteristic path length
log(n) = a metric used for network CPL comparisons
C = clustering coefficient