Vulnerability Assessment on Adversarial Organization: Unifying Command and Control Structure Analysis and Social Network Analysis

Il-Chul Moon
Institute for Software Research
School of Computer Science
Carnegie Mellon University
icmoon@cmu.edu

Kathleen M. Carley
Institute for Software Research
School of Computer Science
Carnegie Mellon University
carley@cs.cmu.edu

Alexander H. Levis
Department of Electrical and
Computer Engineering
George Mason University
alevis@gmu.edu

ABSTRACT

People often look at social networks as a way of explaining and understanding the design of an organization. The structure of an organization, in terms of workflow, can itself be assessed for feasibility, strength and robustness. Currently, tools for assessing organizations from a social network and from a workflow perspective are completely separate. Thus, we show how you can infer the workflow from the social network and what additional information can be extracted. This enables you to assess organizations from multiple perspectives at once and to gain a depth of understanding of this organization.

Keywords: Social network analysis, C2 structure analysis, Centralities, Inferred organizational structure

1. INTRODUCTION

Understanding an organizational structure is critical when we attempt to understand, intervene in, and destabilize the organization [3, 8, 9, 19]. However, there are different types of organizational structures according to various perspectives. For instance, we can partially reveal a terrorist network structure from email transactions. However, such an email transaction network is not a critical decision making structure since it contains contacts who are not significant or relevant to their tasks. On the other hand, the command and control (C2) structure [1] of the terrorist network is a critical decision making structure which organizes and directs the individual terrorists. This C2 structure means the organizational structure displaying relationships such as information sharing, response sharing, task result report, or command from the upper level. C2 structure concept emerged from military decision making studies, but we can apply it to adversarial groups.

However, the real-world adversarial C2 structure often differs from its known formal C2 structure [6, 7], and sometimes the members of the C2 structure hide the structure with various types of social interactions and communications. Furthermore, when we observe their command relations, the observed dataset is often noisy, containing misleading and uncertain information [4]. For instance, the C2 structure of a terrorist network may not have a formal hierarchy, but just a task force team that does not have clear cooperation. Also, this structure is usually hidden in friendly civilian communities [2, 14, 17]. The communities may include individuals who are not relevant to the terrorist network or their tasks, yet they have interactions with each other. Finally, the nature of relations among terrorists may be various, i.e. sharing information, reporting result or commanding orders.

To identify the C2 structure of an adversarial group, we introduce a framework which largely consisted of two steps. First, we use C2 structure extractor in Organization Risk Analyzer (ORA) [16] to extract the command structure from a social network of a target organization. Next, we analyze the extracted command structure with the social network analysis approach. Then, we can see the different key personnel lists and clustered members between the original social network and the extracted command structure. These differences imply that the analysis result can be richer if we investigate not only the existing social network, but also the inferred structures from it.

This C2 structure extraction will benefit a number of relevant or subsequent analyses. For instance, Rabasa et al [15] think that al-Qaeda is more relying on loose networks of operatives to conduct operations, which means that the operatives may be embedded in a social network of a community including civilians and operatives at the same time. Although they co-exist in the social network, it is certain that the group needs C2 activities among the operatives. Then, the C2 structure extraction will reduce or limit the relevant personnel in the social network, help setting the scope of investigations, and produce various analysis results from different organizational structure viewpoints.

2. Background

Our framework is in two steps: finding a potential C2 structure from a social network and analyzing the extracted structure with social network analysis metrics and algorithms. Therefore, the theories behind our approach may be enumerated in two folds. First, we explain the complex nature of a social network and how the complex nature is related to C2 structure. Second, we describe the used social network analysis metrics and algorithms.

2.1 Complex system as a meta-network

Alberts and Hayes [1] state that C2 implies the existence of multiple individuals and entities just as the nature of a complex system. On top of this complex system idea, they conceptualize the roles, responsibilities and relationships among the individuals. Their argument is that these three concepts serve to enable, encourage and constrain specific types of behavior through a C2 structure. Therefore, we may hypothesize that a C2 structure may exist and can be extracted from a complex system.

In fact, the organizations of interest in this paper exhibit the characteristics of complex system. According to Morel and Ramanujam [13], there are two commonly observed characteristics of a complex system: large number of interacting elements and emergent properties. We are particularly interested in the large number of interacting elements in this organizational domain since we are not plan to analyze the over-time organizational evolution. A terrorist network is a collection of heterogeneous entities interacting with and assigned to each other. Though a terrorist network was regarded as a simple terrorist-to-terrorist network traditionally [11, 12], recent observations and analyses [5, 18] assert that the terrorist network includes resources, information, tasks, locations as well as terrorists. Also, the assignment between terrorists to tasks or resources is a type of interaction between two heterogeneous entities. As these organizations are complex systems, we use meta-matrix [10] format to represent and analyze a target organization. Meta-network is an extended version of social network including various types of nodes and heterogeneous links, which follows the nature of complex system. Thus, we locate a potential C2 structure from a meta-network under the assumption that the complex nature of the meta-network enables locating the structure.

2.2 Social network analysis to find the vulnerabilities of an organization

Social network analysis has been one of the most useful tools in analyzing adversarial organizations, i.e. terrorist network. It is able to find key personnel and embedded clusters. Also, it assesses the characteristics, such as degree of centralization and levels of hierarchy, of the organizations. For instance, Kreb [11] visualized the terrorist network responsible for 9/11 attack, and he calculated centralities of terrorists. In this paper, we follow the basic analysis that he did in the paper, but we analyze both the inferred C2 structure and original social network.

Carley [5] analyze the organizational structure with a meta-matrix. As explained in the earlier previous research, meta-matrix enables to investigate the complex system including resources, tasks as well as personnel. Since she expands the analysis scope, she provides a set of new metrics measuring cognitive demand, resource/information exclusivity, etc.

3. Dataset

Throughout this paper, we use a dataset collected from 1998 US Embassy bombing incident in Kenya. The dataset is a meta-network of a terrorist organization. Initially, this dataset is from a network text analysis on open-source documents, but later, the dataset went through corrections by human analysts. This meta-network is appropriate for this analysis in three reasons. First, it has a directed terrorist-to-terrorist network required for inferring a Command Interpretation structure, which will be explained later, included in the expected C2 structure. Second, it has a detailed task network. With inputs from human analysts, the dataset has a detailed task procedure of the incident, so it is particularly appropriate when we extract a C2 structure for the completion of a certain task. Third, this case was investigated by a group of analysts, and they found the C2 structure responsible for this incident. Therefore, we can compare our output C2 structure to theirs and qualitatively validate the model.

This meta-network can be from other cases, such as 9/11 terrorist attack or the 1998 US embassy bombing in Tanzania. Also, the introduced approach can be applied to other meta-networks as far as it contains required networks enumerated in the above paragraph. These potential applications to other datasets are possible because this approach displays and implements subject matter experts' general view about adversarial C2 structure.

As our framework starts with a meta-network, the initial input dataset is a collection of terrorists, information and resources for the bombing, and related

Table 1. the meta-matrix of the dataset, a terrorist group responsible for 1988 US embassy bombing in Kenya, This is an adjacency matrix of different types of nodes, the cells represent the sub-networks and the numbers in the cells are the density of the sub networks.

	Terrorist	Expertise	Resource	Task
Terrorist (17 terrorists)	Social Network (0.147)	Information Distribution Network (0.095)	Resource Distribution Network (0.088)	Task Assignment Network (0.126)
Expertise (8 expertise)		Not used	Not used	Required Information Network (0.048)
Resource (8 resources)			Not used	Required Resource Network (0.076)
Task (13 tasks)				Task Precedence Network (0.121)

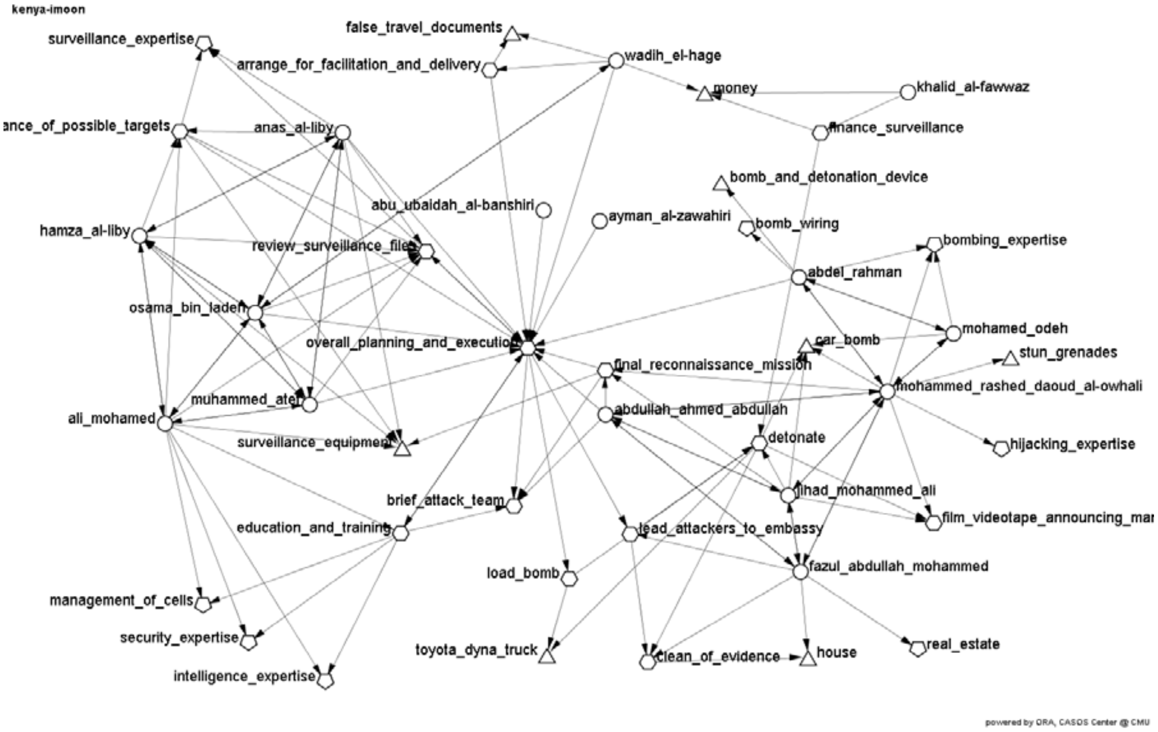
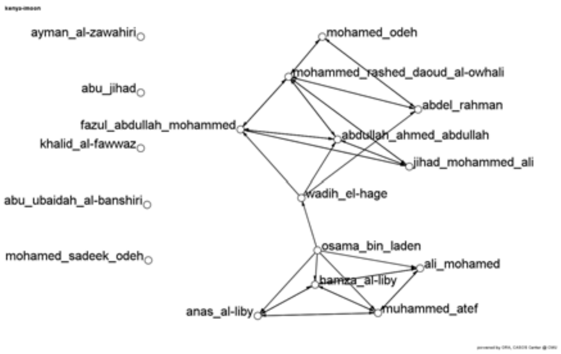
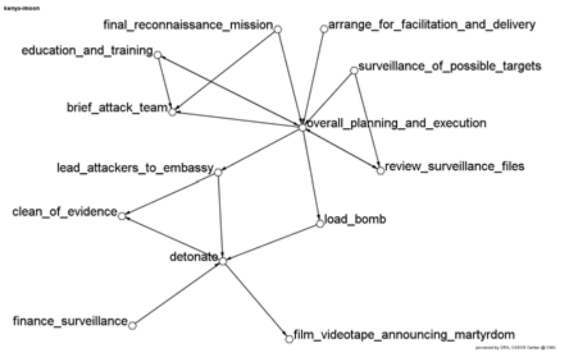


Figure 1. the visualization of the meta-matrix of the terrorist group responsible for the 1988 US embassy bombing in Kenya




kenya-imoon
final_reconnaissance_mission
arrange_for_facilitation_and_delivery
education_and_training
surveillance_of_possible_targets
brief_attack_team
overall_planning_and_execution
lead_attackers_to_embassy
review_surveillance_files
clean_of_evidence
load_bomb
detonate
finance_surveillance
film_videotape_announcing_martyrdom

(Left) Figure 2. the terrorist social network in the meta-matrix, (Right) Figure 3. the task network in the meta-matrix

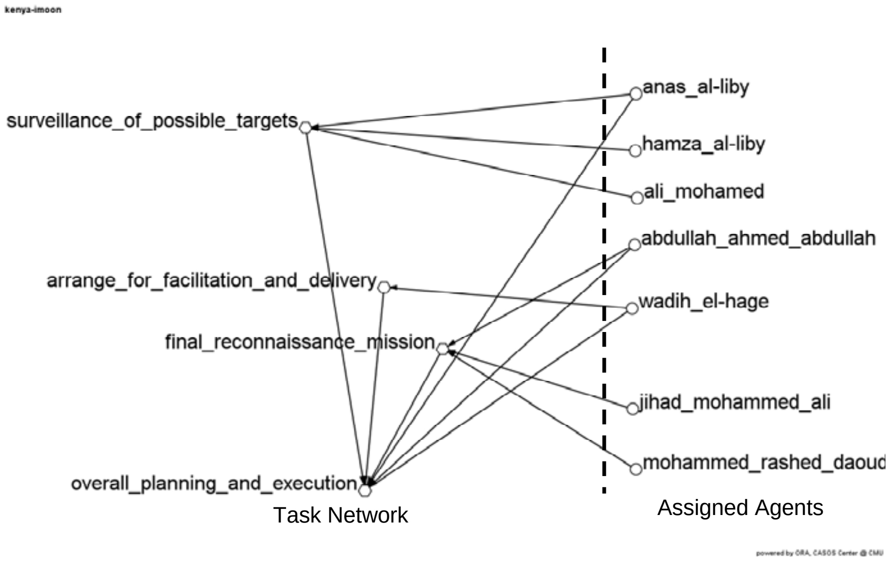

kenya-imoon
surveillance_of_possible_targets
arrange_for_facilitation_and_delivery
final_reconnaissance_mission
overall_planning_and_execution
anas_al-liby
hamza_al-liby
ali_mohamed
abdullah_ahmed_abdullah
wadih_el-hage
jihad_mohammed_ali
mohammed_rashed_daoud
Task Network
Assigned Agents
powered by ORA, CASOS Center @ CMU

Figure 4. the partial visualization of the task precedence network (task-to-task) and the task assignment network (terrorist-to-task). When user setup *overall_planning_and_execution* as a final task for the task-oriented C2 structure, the visualized tasks and terrorists are the components of the sub-task network and the accompanying decision makers respectively.

tasks. Figure 1 is the visualization of the meta-network of the Kenya case. Also, we visualized two sub-networks, a terrorist social network in Figure 2 and a task precedence network in Figure 3. The basic statistics of this network is listed in Table 1. For each of the sub-networks, there is an interpretation for the links. For instance, the link in a social network represents that the two terrorists interacted or communicated with each other, and the link in a task assignment network shows that the terrorist was assigned to completion of the linked task.

4. Method

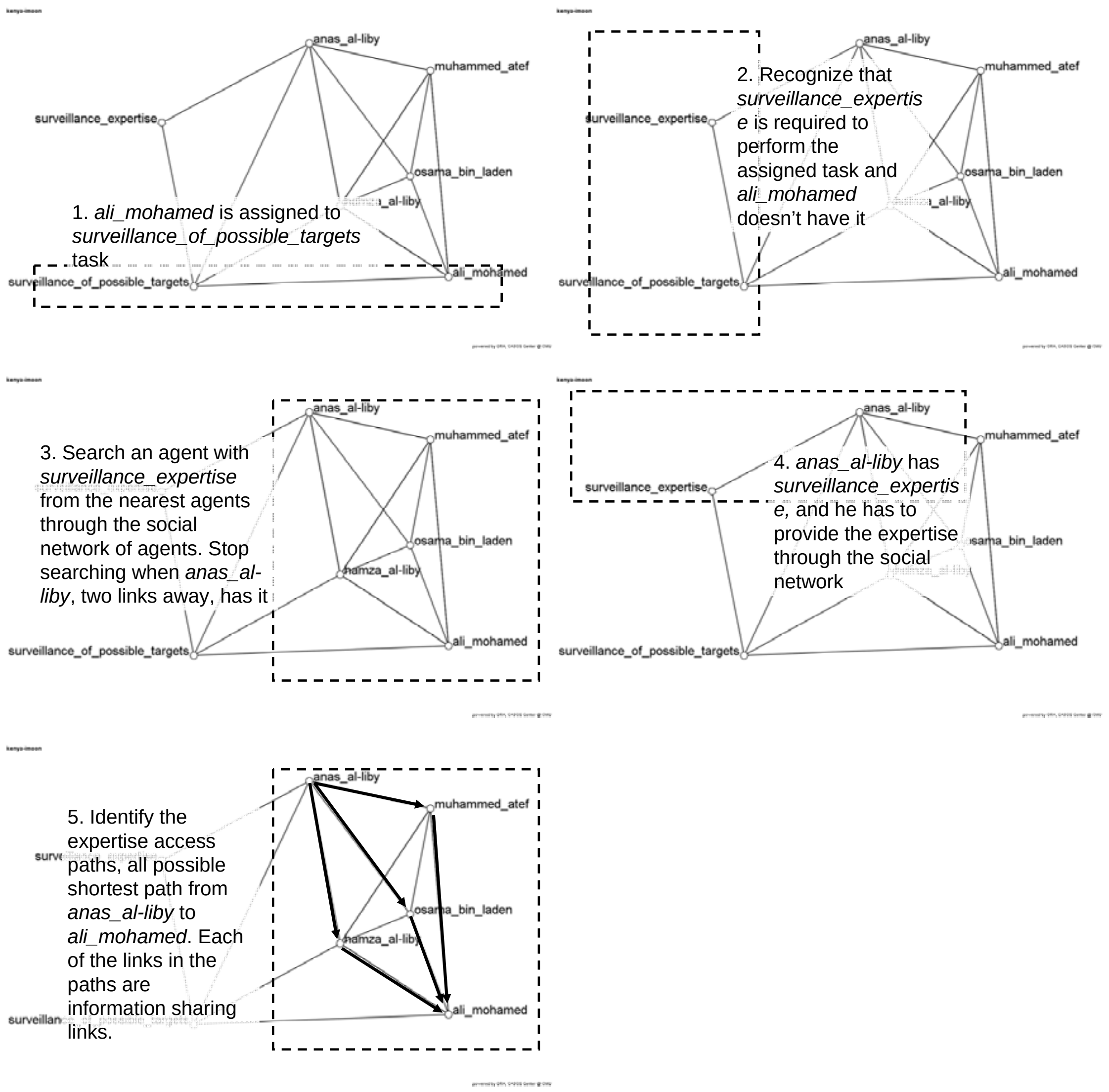
Our framework is in two folds: extracting a potential C2 structure from a meta-network of an adversarial group and analyzing the extracted C2 structure and the original social network. We performed this two-staged analysis with Organization Risk Analyzer (ORA). ORA extracts a task-based potential C2 structure, and it also calculates various social network analysis metrics and clustering algorithms. Since the used network analysis metrics and algorithm in the second stage are well-known, in this section, we only introduce how to infer a potential C2 structure, the key research method in the first stage.

This is a procedural approach that is not similar to the data-mining on terrorist networks. This framework implements what human analysts would do to reorganize the dataset and to infer the underlying organizational structure of a terrorist network. Therefore, we provide the rational about the inference heuristics and concepts behind them, rather than listing algorithms in formulas.

4.1 Extracting a C2 structure from a meta-network

The scope of the C2 structure is limited to the task-oriented C2 structure that is a part of overall C2 structure and that performs a specific task. This limits the number of terrorists consisting of the C2 and makes the other terrorists as the outside collaborators. By applying this limitation, we can focus on the investigation of a specific task performance and keep the generated structure recognizable by human analysts. Also, in C2 community, these selected terrorists regarded as decision makers, so this limitation differentiates between a social agent and a decision maker in the target C2.

After selecting the decision makers, we infer the various C2 relations by utilizing not only the terrorist social network, but also the task assignment, the information and the resource distribution networks. For instance, when two members are connected with a communication path and one has a resource required for the other one, the shortest path may be a resource sharing path in terms of C2 relations. With similar methods, in addition to the resource sharing relations, we infer information sharing relations and command interpretation relations.



1. *ali_mohamed* is assigned to *surveillance_of_possible_targets* task

2. Recognize that *surveillance_expertise* is required to perform the assigned task and *ali_mohamed* doesn't have it

3. Search an agent with *surveillance_expertise* from the nearest agents through the social network of agents. Stop searching when *anas_al-liby*, two links away, has it

4. *anas_al-liby* has *surveillance_expertise,* and he has to provide the expertise through the social network

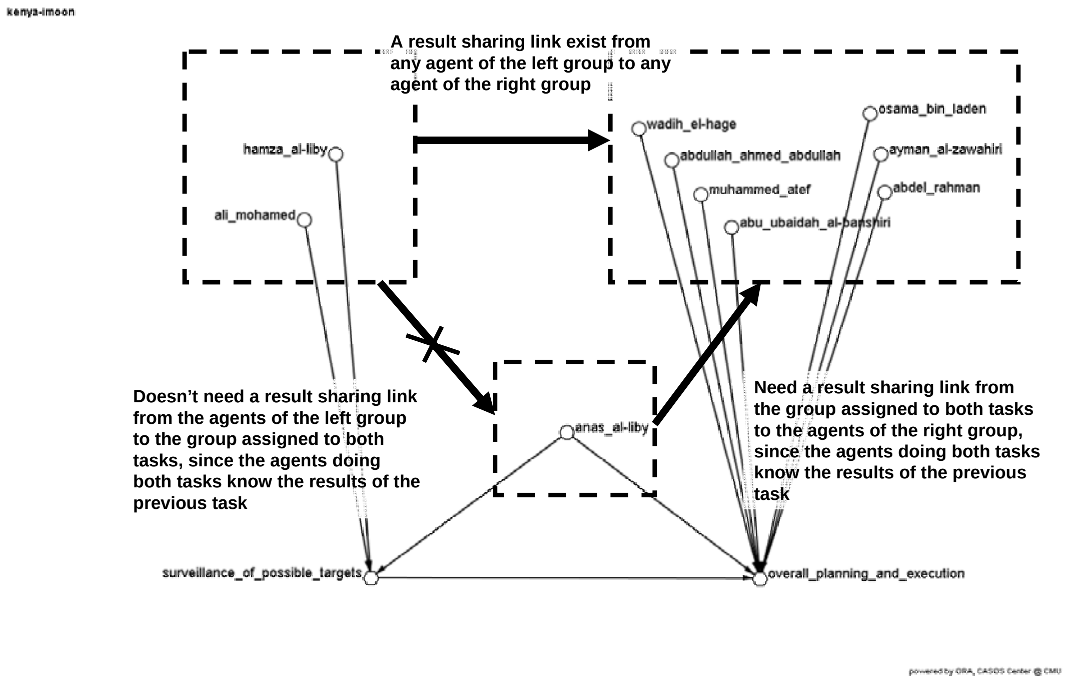
5. Identify the expertise access paths, all possible shortest path from *anas_al-liby* to *ali_mohamed*. Each of the links in the paths are information sharing links.

Figure 5. a partial visualization explaining the formation of information sharing links. *ali_mohammed* requires *surveillance_expertise* hold by *anas_al-liby*. This information demands produce three information sharing paths and links in the paths.

4.1.1 Limiting task network and finding decision makers

Since the C2 structure in this paper is task-oriented, our framework aims to extract a C2 structure responsible for completing a certain final task. This task is a user defined parameter. With the given final task, we can retrace a sub-task network from a meta-network by following the prerequisite tasks repeatedly starting from the final task. For example, in Figure 4, the final task is *overall planning and execution*, then its sub prerequisite tasks are *surveillance of possible targets*, *final reconnaissance mission* and *arrange for facilitation and delivery*. These four tasks consist of the sub-task network for extraction, and the 12 terrorists assigned to those tasks are the decision makers of this task-oriented C2 structure.

After limiting the involved decision makers, we aggregate the uninvolved agents as an outside organization. It is typical to see a C2 structure interacting with outside organizations. If we configure a task-based sub C2 structure, some of the terrorists will be excluded since they are not doing the tasks in the sub-task network. However, still it is possible that the excluded terrorists hold required resources or information, and this will demand the communication between the selected decision makers of a C2 structure and the outside organization which is the group of the excluded terrorists. Thus, finding assigned decision makers is not just limiting the personnel of the C2 structure, but also specifying the boundary decision makers interacting with outside organizations. In this example, we have total 17 terrorists, and 12 terrorists

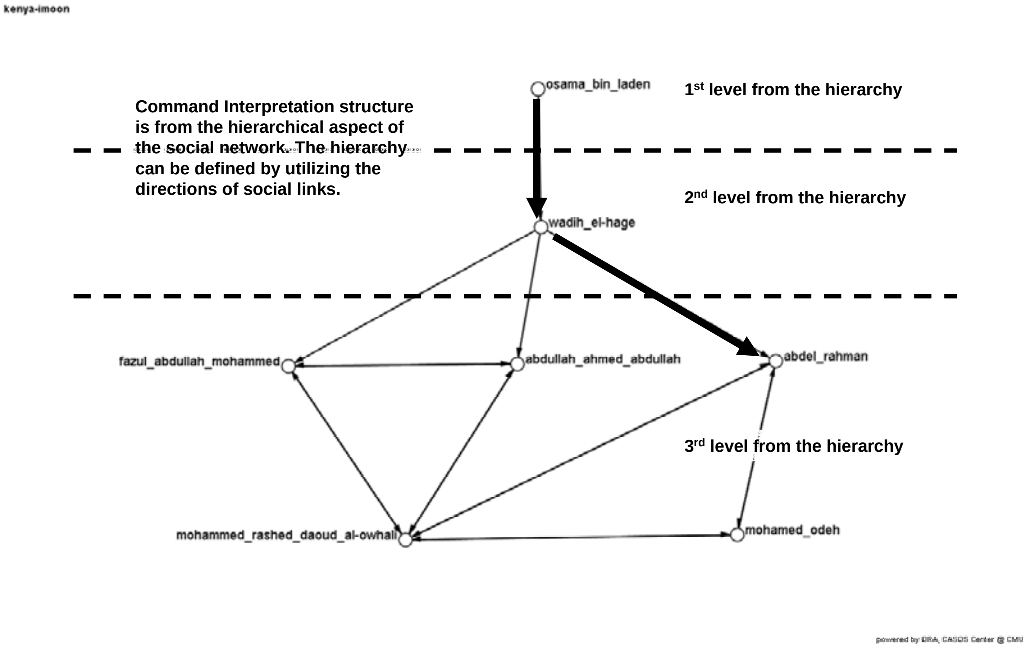


A result sharing link exist from any agent of the left group to any agent of the right group

Doesn't need a result sharing link from the agents of the left group to the group assigned to both tasks, since the agents doing both tasks know the results of the previous task

Need a result sharing link from the group assigned to both tasks to the agents of the right group, since the agents doing both tasks know the results of the previous task

Figure 6. a partial visualization of two tasks and ten assigned agents. This precedence task relation will result 21 result sharing links between the agents doing the prior task and the agents performing the next task. One agent who is doing both does not need any result sharing link.


kenya-imoon
osama_bin_laden
wadih_el-hage
fazul_abdullah_mohammed
abdullah_ahmed_abdullah
abdel_rahman
mohammed_rashed_daoud_al-owhali
mohamed_odeh
1st level from the hierarchy
2nd level from the hierarchy
3rd level from the hierarchy
powered by ORA, CASOS Center @ CMU

Command Interpretation structure is from the hierarchical aspect of the social network. The hierarchy can be defined by utilizing the directions of social links.

Figure 7. a partial visualization of the agent-to-agent network. From the directions of links, we can identify the hierarchy of the network. After configuring the hierarchy, we can see the Command Interpretation relations between two agents at the adjacent level.

are selected as decision makers. Thus, the other 5 terrorists form the outside organization of this C2 structure.

4.1.2 Information Sharing structure

In a meta-network, a piece of information is represented as a knowledge node. Thus, we assume that producing information is represented as a link

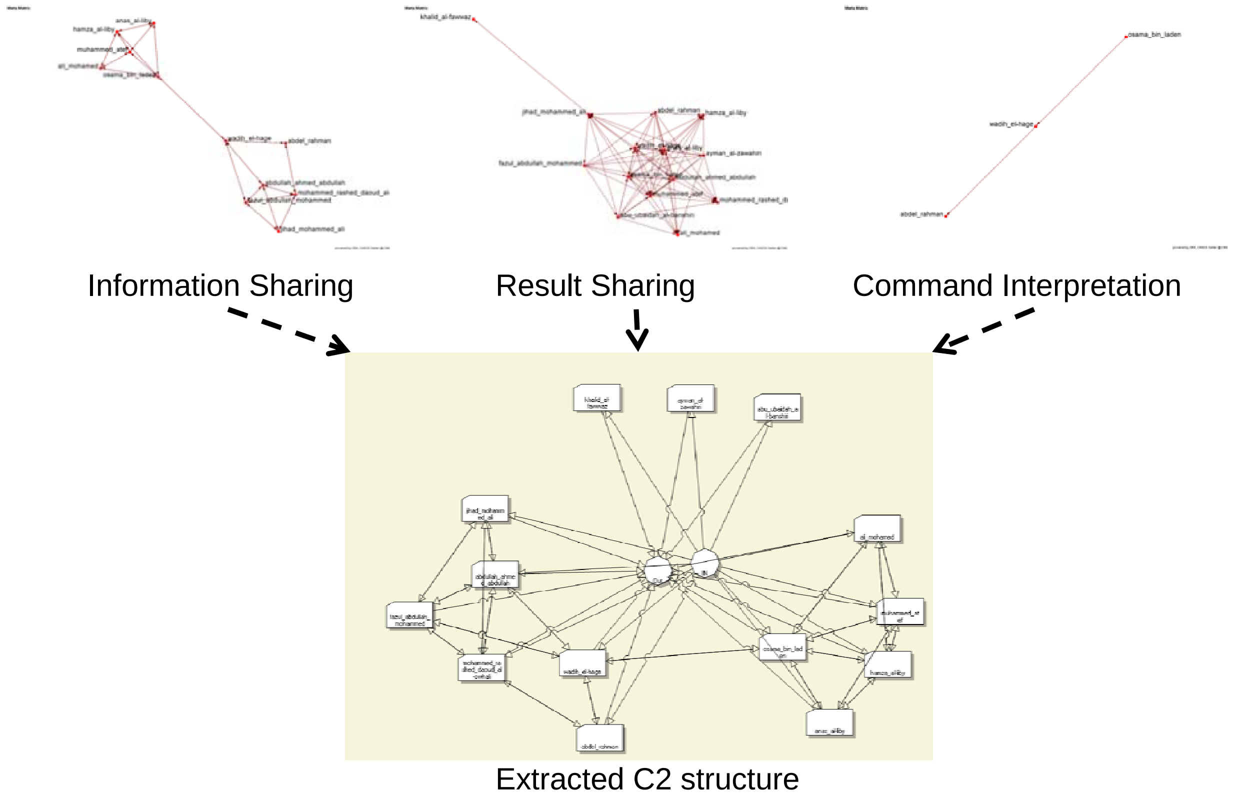


Figure 8. (top) Three inferred C2 structures and (bottom) the aggregated C2 structure for *detonation*

from an agent node to a knowledge node. Also, we infer that one decision maker will acquire an information piece through an information sharing path if 1) he needs the information to perform his assigned tasks, 2) he does not have the information, and 3) the information sharing path is the shortest path from the nearest decision maker holding the information to him. Figure 5 describes the case of information sharing links. According to the sub-network in the figure, *ali mohamed* is assigned to *surveillance of possible targets* which requires *surveillance expertise*. However, *surveillance expertise* is not available to *ali mohammed*, but available to *anas al-liby*. Then, *ali mohamed* finds possible shortest paths to *anas al-liby*, and he finds shortest paths with two social links going through *osama bin laden*, *hamza al-liby* or *muhammed atef*. Then, the links in these three shortest paths will be the information sharing links.

4.1.3 Result Sharing structure

Result Sharing (RS) is communication from a decision maker finishing his assigned task to a decision maker with a task that required the previously done task. For instance, there is a RS communication from a terrorist who finished *surveillance of possible targets* to a terrorist who will perform *overall planning and execution*. Figure 6 shows the above two tasks and their assigned agents. *Surveillance of possible targets* has three assigned agents, and *overall planning and execution* has eight agents. Then, there will be 21 result sharing links originating from the three agents to the seven agents, excluding the agent who is assigned to the next task and already knows the results of the previous task.

4.1.4 Command Interpretation structure

Command Interpretation (CI) is command relation from a decision maker who completed his task and sent an order to a lower ranking decision maker. We infer this relation by reconstructing the hierarchy in the social network based on the direction of agent communication links. We assume that the directions of communications are the representation of who-reports-to-whom relation. Subsequently, the directions will provide a basis for extracting hierarchical structure. For instance, *osama bin laden* has a one-way link to *wadih el-hage*, and *wadih el-hage* has a link to *abdel rahman*. These one-way social links imply a command chain. On the other hand, *abddel rahman* and *Mohamed odeh* are linked with a bi-directional link that does not mean any explicit command interpretation relation. Therefore, they remain at the same level in the hierarchy. When we observe such command interpretation relations, we add a link to C2 structure.

5. Result

The described C2 structure extraction scheme is applied to the US embassy bombing in Kenya case. First, we describe and visualize the extracted C2 structure. Next, we calculate two social network metrics, degree centrality and betweenness centrality, on the social network and various C2 relation networks. Comparisons on the calculated metrics provide an insight into who stands out in different settings and why.

5.1 Extracted C2 structure from the Kenya case

Figure 8 is the visualization of the extracted C2 structure for *detonation* task. Whereas the original social network has 17 members, the extracted structure has only 14. The removed members are not related to the task network of *detonation*. As the figure shows, there are three groups, one group with six members, the other group with five members, and another group with three members. The third group has members only interacting with others not included in this structure. This is shown as the only links between the third group member and IN/OUT nodes. The other two groups have dense C2 structure relations. There should be more investigations to reveal why there was a split between the two groups. The reasons can be 1) the result sharing relations coming from the structure of task network, 2) the information sharing relations from the information and the resource distributions of the original social network. Given only two command interpretation links, they might not be the reason of the split. We cannot say that the organization was better or worse off by having two cells. The terror network

Table 2. two social network metrics on the social network from the meta-matrix and the three different C2 relational structures

	Total degree centrality				Betweenness centrality			
Node	Social Net.	Info. Share	Result Share	Comm. Interpret.	Social Net.	Info. Share.	Result Share	Comm. Interpret.
Abdel Rahman (A1)	0.1563	0.1538	0.3846	0.0385	0.0111	0.0256	0.0064	0
Abdullah Ahmed Abdullah (A2)	0.2188	0.3077	0.6154	0	0.0069	0.0641	0.0064	0
Abu Jihad	0	Not included in C2 structure			0	Not included in C2 structure		
Abu Ubaidah Al-banshiri (A3)	0	0	0.3846	0	0	0	0.0064	0
Ali Mohamed (A4)	0.1563	0.2308	0.3077	0	0	0	0	0
Anas Al-liby (A5)	0.1563	0.2308	0.6154	0	0	0	0.0064	0
Ayman Al-zawahiri (A6)	0	0	0.3846	0	0	0	0.0064	0
Fazul Abdullah Mohammed (A7)	0.2188	0.3077	0.3462	0	0.0069	0.0641	0.2051	0
Hamza Al-liby (A8)	0.2188	0.3077	0.3077	0	0.0042	0.0043	0	0
Jihad Mohammed Ali (A9)	0.1875	0.2308	0.3846	0	0	0	0.2436	0
Khalid Al-fawwaz (A10)	0	0	0.0385	0	0	0	0	0
Mohamed Odeh	0.125	Not included in C2 structure			0	Not included in C2 structure		
Mohamed Sadeek Odeh	0	Not included in C2 structure			0	Not included in C2 structure		
Mohammed Rashed Daoud Al-owhali (A11)	0.3125	0.3077	0.3077	0	0.05	0.0256	0	0
Muhammed Atef (A12)	0.2188	0.3077	0.6154	0	0.0042	0.0043	0.0064	0
Osama Bin Laden (A13)	0.1563	0.3846	0.6154	0.0385	0	0.312	0.0064	0
Wadih El-hage (A14)	0.125	0.3077	0.6154	0.0769	0.025	0.3333	0.0064	0.0064

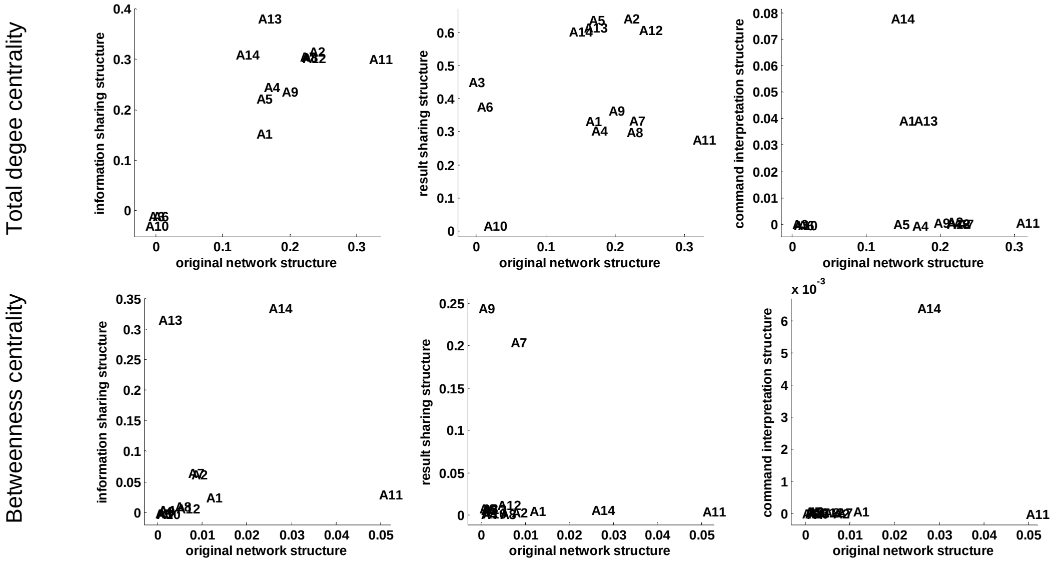


Figure 9. scatter-plots showing the network metrics from the original structure by those from the three C2 structures. jittering within 5% of mean is applied to the values.

could be better off by splitting its organization into smaller pieces because it is widely known that a terrorist network has a cellular network after adaptation. However, from the C2 structure analysis viewpoint, an organization can perform better by unifying a C2 structure.

Table 2 shows degree centrality and betweenness centrality values for each of the involved agents. Three agents are excluded since they were not in the *detonation* task C2 structure. Figure 9 is the visualization of the values from Table 2. For both metrics, the figure has three scatter plots displaying the metrics from the original structure by those from the three C2 structures. In degree centrality, *Osama Bin Laden* (A13) has the highest degree centrality in the information sharing and the result sharing, but a medium degree in the command interpretation and the original structure. If we only considered the original structure for the analysis of this organization, we may just conclude A13 has only a medium level of degree centrality. However, he is a key person in terms of degree centrality when it comes to information and result sharing. Also, *Al-owhali* (A11) has the highest betweenness centrality in the original network. Yet, in the information sharing and the command interpretation structures, *Wadih El-hage* (A14) has the top betweenness centrality, and in the result sharing structure, *Jihad Mohammed Ali* (A9) has the biggest betweenness centrality. Therefore, by analyzing the different structure generated from different perspectives, we can identify multiple key personnel sets.

6. Conclusion

This paper demonstrates what can be achieved by integrating social network analysis and C2 structure analysis. Social network analysis has been a prominent tool in investigating an adversarial organization. However, it is also susceptible from errors embedded in the given network structure. Therefore, reorganizing the links is required to perform analysis correctly. This reorganization is often done by human analysts. We expect to reduce such efforts by utilizing the introduced methods.

Furthermore, the method produces a set of different C2 structures. They differ from each other in their natures. For instance, information sharing is a different relation compared to result sharing or command interpretation. When we only used a social network analysis, often the links are single-mode meaning that the links are not differentiable. Therefore, the above method will enable analysts to think the different types of links among the same entity types, and the analysts can reason deeper by asking questions like why these two agents have a command interpretation without any result sharing.

From the organizational structure perspective, a C2 structure and a social network are both organizational structures. Therefore, the analysis methods are interchangeable to some extent. For instance, we can apply social network metrics to a C2 structure and treat a social network as a part of C2 structure. These interoperability or interchangeability makes the analysis more comprehensive. For instance, we have different sets of critical personnel by analyzing various C2 relations and an original social network. We are not certain which set contains the true personnel of interests, but we can suggest a package of results to human analysts.

Future work on this integration will include two major components. First, we should strengthen the C2 structure extraction heuristics. Currently, the information sharing extraction generates a dense network that is not common in the C2 domain. Also, we have a too sparse command interpretation that we believe that there are more in the organization. Therefore, we develop the existing method furthermore or validate the current model by showing the dense information sharing and the sparse command interpretation is legitimate. Second, we need to include more C2 structure oriented analysis methods in the framework. The result in this paper is only from the social network analysis though it used the C2 structure for the analysis input. There are several C2 structure analysis methods, i.e. generating a set of feasible C2 structures under certain cultural constraints. In spite of these incomplete developments, this framework still shows its value by showing 1) trimming process of a noisy social network, 2) different vulnerability analysis results from the extracted C2 structure, and 3) opening a unified organization analysis framework integrating social network analysis and C2 structure analysis.

7. ACKNOWLEDGMENTS

This work was supported in part by the AirForce Office of Sponsored Research (MURI: Cultural Modeling of the Adversary, 600322) for research in the area of dynamic network analysis. Additional support was provided by CASOS - the center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the AFOSR.

8. REFERENCES

[1] Alberts, D. S. and Hayes, R. E. (2006) Understanding Command and Control, Department of Defense, CCRP

[2] Allanach, J., Haiying T., Singh, S., Willett, P. and Pattipati, K. (2004) Detecting, tracking, and counteracting terrorist networks via hidden Markov models, Proceedings of IEEE Aerospace Conference, Vol. 5, pp 3246-3257

[3] Arquilla, J. and Ronfeldt, D. (editors) (2001) Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, Calif.: RAND, MR-1382-OSD. www.rand.org/ publications/ MR/MR1382/

[4] Borgatti, S. P., Carley, K. M., and Krackhardt, D. (2006) On the robustness of centrality measures under conditions of imperfect data, Social Networks, Vol. 28, Issue 2, pp 124-136

[5] Carley, K. M. (2006) Destabilization of covert networks, Computational & Mathematical Organization Theory, Vol. 12, Issue 1, pp 51-66

[6] Fulmer W. E. (2000) Shaping the Adaptive Organization: Landscapes, Learning, and Leadership in Volatile Times. AMACOM, New York.

[7] Goolsby, R. (2006) Combating terrorist networks: An evolutionary approach, Computational Mathematical Organizion Theory, Vol. 12, Num. 1, pp 7-20

[8] Jenkins, B. (2002) Countering al Qaeda, Santa Monica: RAND, 5.

[9] Kansal, S. K., AbuSharekh, A. M. and Levis, A. H. (2007) Computationally Derived Models of Adversary Organizations, IEEE Symposium on Computational Intelligence in Security and Defense Applications, Apr 1-5, pp 92-99

[10] Krackhardt, D. and Carley, K. M. (1998) A PCANS Model of Structure in Organization, In Proceedings of the 1998 International Symposium on Command and Control Research and Technology, pp 113-119

[11] Krebs, V. E. (2002) Mapping Networks of Terrorist Cells, CONNECTIONS, Vol. 24, Num. 3, pp 43-52

[12] Mayntz , R. (2004) Organizational Forms of Terrorism: Hierarchy, Network, or a Type sui generis?, Max-Planck-Institut fur Gesellschaftsforschung Koln, MPIfG Discussion Paper 04/4,

[13] Morel, B. and Ramanujam, R. (1999) Through the Looking Glass of Complexity: The Dynamics of Organizations as Adaptive and Evolving Systems, Organization Science, Vol. 10, No. 3, Special Issue: Application of Complexity Theory to Organization Science

[14] Raab, J. and Milward, H. B. (2003) Dark networks as problems, Journal of Public Administration Research and Theory, Vol. 13, pp 413-439

[15] Rabasa, A., Chalk, P., Cragin, K., Daly, S., Heather S., Karasik, T. W., O'Brien, K. A. and Rosenau, W. (2006) Beyond al-Qaeda Part 1., Rand Corp., pp 27-29

[16] Reminga, J. and Carley, K. M. (2004) ORA:Organization Risk Analyzer, Tech Report, CMU-ISRI-04-106, CASOS. Carnegie Mellon University. Pittsburgh PA, http://www.casos.cs.cmu.edu/projects/ora/index.html

[17] Sageman, M (2004) Understanding terror networks, Philadelphia: University of Pennsylvania Press

[18] Urry, J. (2002) The Global Complexities of September 11th, Theory, Culture & Society, Vol. 19, No. 4, pp 57-69

[19] Levis, A. H. (2005) Executable Models of Decision Making Organizations, Organizational Simulation, William B. Rouse and Ken Boff, Eds., Wiley, NY