UNITED STATES MILITARY ACADEMY

WEST POINT, NEW YORK

HOLLIS AWARD SUBMISSION

War Gaming Cyber Conflict Effects on a Stryker Infantry Company

by

CDT Matthew T. Moellering
CDT Stuart R Topp

May 2014

Advisor: Dr. Chris Arney

War Gaming Cyber Conflict Effects on a Stryker Infantry Company

CDT Matthew T. Moellering
CDT Stuart R. Topp
United States Military Academy
West Point, New York 10996

KEYWORDS: Cyber, Python Simulation, Stryker Company, Mission Command, Communication

CONTACT: **Matthew T. Moellering**, United States Military Academy, West Point, New York 10996. **Email:** matthew.moellering@usma.edu **TEL:** 925-963-0508.

Stuart R. Topp, United States Military Academy, West Point, New York 10996. **Email:** stuart.topp@usma.edu **TEL:** 847-406-0412.

ADVISOR: Chris Arney, Mathematics Department
Email: david.arney@usma.edu TEL: 845-938-4429

ABSTRACT

Securing the passage of information is a critical task for all military units in contemporary warfare. As critical systems and communications increase in their reliance on networked and linked devices, their vulnerability to a crippling cyber attack also increases. Stryker units' increased reliance on these systems allows for the sabotage and compromise of their communications networks. Using a five-stage, connection-focused approach, the war game looks at several different scenarios of cyber attacks by different actors on the Stryker Company's Lower Tactical Internet to examine the effects of cyber conflict on a Stryker Company's communications networks. Leaders can use the results from the simulations to assess key network weaknesses, and then apply the Army leadership principles of Mission Command to ensure unit effectiveness in a contested cyber environment.

INTRODUCTION

With the growing importance of the internet, our world is shrinking. As we increase our reliance on critical systems and our communications over networked and linked devices, we also increase our vulnerability to a crippling cyber attack. This level of attack could destroy key weapon systems and eliminate our ability to successfully operate our military by eliminating our ability to communicate and ultimately command and control. A full-scale Cyber war has yet to happen, so the United States is unsure how devastating such a war would be to its large, complex, and high-tech military arsenal. However, we do know that the number of nations that have offensive cyber capabilities is growing every day. Nations such as Iran, China, North Korea, and Russia have developed impressive cyber capabilities and those capabilities are expanding in scope and effectiveness.[1]

However, the success of the US Army through history at key battles such as D-Day, Bastogne, Desert Storm, have often been credited to the ability of the American commanders to adapt by delegating command authority to the lower levels. With the revolution of the internet and our ability to network and connect our entire military, we need to make sure that this flexible; "Mission Command" capability remains and thrives in our modern US Army. If the enemy hijacks or destroys our critical systems, our Army must have multiple contingencies and additional communication methods so we are not cyber-fully reliant on any one piece of equipment or network.

BACKGROUND

Cyber is the newest, and perhaps the most pervasive, battlespace. This battlespace encompasses more than just military information systems and networks. National infrastructure, the finance industry, and all of the world's "connected" civilian populations are, in one way or another, a part of the military's Cyber domain. Therefore, Cyber has the potential to affect billions of lives on a daily basis. Society's growing dependence on cyber support makes it a very attractive target for criminals, terrorists, and competing nations. Cyber activities can range from "hacktivism" and electronic

[1]Richard Clarke, "Cyber War," 2010, HarperCollins: New York.

vandalism, to crime directed at private citizens, private industry, or government agencies, to covert "grey" state-sponsored espionage or attacks, to overt cyber attacks in conjunction with military operations or infrastructure utility. Richard Clarke paints a depressing picture in his book *Cyber War* on the ability of the enemy to use already emplaced logic bombs and trapdoors to destroy our key weapon systems before a kinetic war even starts.[2] These cyber weapons are most likely already sitting dormant in our networks, ready to degrade or even cripple our ability to command and control our military with a push of a button.

In addition the US Army has also acknowledged that globalization of network communications and the IT marketplace has produced increased vulnerability and acknowledges the potential use of logic cyber weapons to disable our weapon systems during both peace and war.[3] More importantly the army has acknowledged that these, "threats to the information systems and networks relied upon by strategic and operational forces exist from various sources, and they exist on a continual basis".[4] This increased reliance has created, "vulnerabilities to attack from various sources. Networks and information systems are vulnerable to attack from adversaries who can quickly take advantage of weaknesses in design, ineffective or lax security procedures, or insufficient internal controls."[17] FM 6-02.71 also notes that this reliance makes us vulnerable to actors who may not have the same level of advanced computing technology but are still advanced enough to complete a cyber attack.[5] Unfortunately these weaknesses are only becoming larger as we became more reliant on off-the shelf technologies. An example of this vulnerability happened in 2009 when insurgents in Iraq were able to hack into drone footage using simple video capturing devices to figure out where our drones were and what they were targeting.[6]

---

[2] Clarke, "Cyber War," 2010, HarperCollins.

[3] United States of America, Department of Defense, Department of the Army, *Network Operations*, Vol. 6-02.71, Washington, DC: Department of the Army, 2009, Print, 2-7.

[4] Ibid.

[5] Ibid.

[6] Gorman, Siobhan, Yochi J. Dreazen, and August Cole. "Insurgents Hack U.S. Drones." *Wall Street Journal* [New York] 17 Dec. 2009: Print.

MISSION COMMAND

From Army Doctrine Publication 6-0, Mission Command "is the exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of unified land operations."[7] The principle of mission command is based off the German concept of Auftragstaktik, which translates to mission-type tactics.[8]The Germans used this principle to allow their German officers to make decisions based off their close view of the battlefield. When thinking in terms of the advent of cyber war, and our reliance on information technology, the use of Mission Command becomes extremely important. Primarily because Mission Command attempts to find the perfect balance between what the U.S. Army defines as the Art of Command and the Science of Control.[9] The networked ability of our new communications devices gives new possibilities to the Science of Control as it allows commanders to communicate to subordinate commanders at faster intervals. Using Network Science centrality measures the Principles of Mission Command can be measured by figuring which actors of the network have the greatest ability to communicate to and control the unit.

NETWORK SCIENCE OVERVIEW

At the most abstract level, network science "is the organized knowledge of networks based on their study using the scientific method."[10] Network science draws on theories from many disciplines, including graph theory and social science, and can be applied to almost any discipline where there are actors or other "things" and relationships, or links, between them.[11]

Graph theory provides the basic foundation for modeling a network:

$$G = \{N, L, f\}$$

---

[7] United States of America, Department of Defense, Department of the Army, *Mission Command*, ADP 6-0, Washington, DC: Department of the Army, 2009, Print,1.

[8] USA, DOD, *Mission Command*, v.

[9] USA, DOD, *Mission Command*, 2-17.

[10] Committee on Network Science for Future Army Applications, 2005, p. 26

[11] Lewis, 2009.

"where N is a set of nodes, L a set of links, and $f: N \times N$ a mapping function that defines the structure of G—how nodes are connected to each other through links."[12] When the model incorporates time, G becomes:

$$G(t) = \{N(t), L(t), f(t): J(t)\}$$

where t is time, N is a set of nodes (also referred to as vertices or actors), L is a set of links (also referred to as edges), $f: N \times N$ is a mapping function that connects nodes, and J is an "algorithm for describing [the] behavior of nodes and links versus time".[13]

Lewis identifies eight general principles of network science: structure, emergence, dynamism, autonomy, bottom-up evolution, topology, power, and stability. First, "networks have structure," and "are not random collections of nodes and links".[14] Second, "a network property is emergent if it changes by a factor of 10 as a consequence of a dynamic network achieving stability".[15] Third, a network's "dynamic behavior is often the result of emergence or a series of small evolutionary steps leading to a fixed-point final state of the system".[16] Fourth, "a network forms by the autonomous and spontaneous action of independent nodes that 'volunteer' to come together (link), rather than through central control or central planning". [17] Fifth, "networks grow from the bottom or local level up to the top or global level".[18] Sixth, "the architecture or topology of a network is a property that emerges over time as a consequence of distributed—and often subtle—forces or autonomous behaviors of its nodes".[19] Seventh, "the power of a node is proportional to the number and strength of its nodes and links".[20] Finally, "a dynamic network is stable if the rate of change in the state of its nodes/links or its

[12] Ibid, 6.

[13] Ibid, 9.

[14] Ibid, 19.

[15] Ibid.

[16] Ibid, 20.

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] Ibid.

topology either diminishes as time passes or is bounded by dampened oscillations within finite limits"[21]

Depending on the discipline utilizing network science, *N* can be a set of actors, vertices, points, nodes, or agents, and *L* can be a set of the relationship between actors, edges, links, or connections. There are several ways to measure these connections. For the purposes of the following definitions, *N* will be a set of nodes, and *L* will be a set of edges. The **degree** of a node is the sum of the links connecting that node to the graph, and whichever node has the largest degree in a graph is called the **hub**. The longest path from a node to all the other nodes is the **radius** of the node, and the **diameter** of a graph is the length of the longest radius (whose respective nodes are called **peripheral nodes**), while the **center** of the graph is the node or nodes with the shortest radii. The **betweenness** of a node is the number of paths that link all of the other nodes to each other that pass through the original node. The **closeness** of a node is the number of direct paths that link all of the other nodes to each other that must pass through the original node.[22] These measures are used to identify relationships and the relative level of importance of different nodes within the graph.

Cyber science encompasses the cyber domain: information systems, the data on those systems, communications between systems, etc. Cyber scientists can use network science to mathematically describe the disposition of information systems and their networks, identify relationships between information systems, identify critical nodes, and determine the broader structural effects of modifications to elements of information systems.

Cyberspace has been used for everything from simple pranks gone wrong, to industrial and military espionage, to widespread denial of service attacks in conjunction with military operations, to target-specific viruses designed to destroy nuclear equipment without a trace. Because of the broad nature of cyberspace, both military and civilian critical infrastructures are vulnerable to the same style of attacks, which are much easier to conduct than they are to prevent or attribute.

[21] Ibid

[22] Ibid.

METHODOLOGY

To date, there has been no known active cyber conflict, where combatants on both sides actively sought to degrade or destroy each other's information systems capabilities, and there is no accompanying body of sound, strategic though on cyber conflict. Policymakers need tools to develop sound and legitimate cyber policies based on possible actions and outcomes, and not derived from policies in other battlespaces. During any conflict, maintaining communication and the flow of information is critical for coordination and success. In a cyber conflict, communication and connectivity between information systems and users are especially important, because without either, systems lose their value. For this model we recreated the current communications structure of a Stryker Infantry Company arguably the most advanced Infantry unit in the world, and used it to look at the outcomes of a Cyber attack on the communication structure of such a unit.

POLICY EXPLORATION

We developed a five stage model for cyber conflict based on an amalgamation of Engebertson's methodology and historical case studies, outlined in Table 1, below. The first stage is the battlespace preparation stage, where both sides have the opportunity to prepare the battlespace by emplacing logic bombs, backdoors, and other malicious code within their opponent's networks. Based on each side's internal security posture, there is a possibility that some or all of these preparations might be discovered. The second stage is the first wave of attacks, where the attacker initiates his initial exploits, and the defender's network responds automatically, if at all. The third stage is the first response stage, where the defender develops a deliberate response to the specific exploits launched against his network, but the attacker is able to respond in real-time. The fourth stage consists of two parts. In the first part of Stage IV, the attacker launches his second wave of exploits, while the defender responds in real-time. In Stage IVa, the defender launches a counterattack (as dictated by the defender's cyber policy). In the final recovery stage, both sides rebuild or enhance their capabilities. This methodology is a simplification of the dynamic and real-time realm of cyber conflict, but, due to the limited pool of data to draw from, must currently suffice.

Stage	Stage I	Stage II	Stage III	Stage IV	Stage IVa	Stage V
Name	**Battlespace Preparation**	**First Wave**	**First Response**	**Second Wave**	**Counterattack**	**Recovery**
Events	Preparation of the battlespace	Initial exploits initiated	Defender's deliberate responses	Second wave of exploits initiated	Defender initiates exploits	Both sides rebuild or enhance capabilities
	Emplacement and discovery of malicious code	Automated network responses	Automated attacker network responses	Automated network responses	Policy dependent	
	Active/passive security		Real-time attacker responses	Real-time defender responses	Automated and real-time attacker responses	

Table 1: Simulation Stages

MODELING THE SBCT COMMUNICATION NETWORK

The network model used in this project was gathered from the United States Army's table of organization and equipment for a Stryker Brigade Combat Team. Using the Table of Organization the key actors were selected from the 167 members inherit to the Stryker company. Using the Table of Organization and Army Field Manuals the six primary networks of communication for a Stryker Company were recreated as adjacency matrices in order to create a larger meta- that encompassed the entire communication picture. In order to create a workable model key assumptions were made about the nature of the Stryker Company in question.

The key assumptions that were made were that the Stryker Company was operating in a conventional warfare environment, against a cyber equipped enemy nation state, and operating at intervals where only Squad leaders can communicate by using their voice. These assumptions were made in order to emphasize reliance on the communication networks and emphasize Mission Command leadership principles by decentralizing control. Finally, the conventional warfare assumption was made to simplify the network to the SCBT's lower tactical internet.

The lower net consists of all the systems for inter, and intra communications between all of the fighting platforms.[23] These are connected through a variety of various networks most notably the Enhanced Position Location Reporting System, and the Single Chanel Ground and Air Radio System (SINGGAR) (See Figure 1 for the layout of the SCBT Communication System).[24] For this model, the focus is on the Lower TI of a Stryker Communications network. Therefore, this acknowledges communications problems that occur at just the level of the Lower TI The emphasis on the Lower TI system applies for the emphasis placed on a unit that is conducting land warfare maneuver, and will be happening within at the Company level and below.

The lower tactical internet consists of 4 different communication networks. At this level, this focuses on three different Company level FM radio networks.[25] In addition to radio communications, the Stryker Company is augmented via digital communications. The primary digital communication for a Stryker infantry company is the Force XXI Battle Command Brigade and Below (FBCB2), which is an ad-hoc network of computers located in all vehicles, inherit to the Stryker company. A Stryker company will inherently use three or two radio networks to communicate amongst each other depending on the variant of Stryker vehicle available.[26] A Company Command Net, a Company Fires Net, and Platoon level nets, In addition to the radio net a company level Stryker unit will have access to FBCB2 to link their family of Stryker vehicles together, and finally they have the ability to communicate by internal radio communication devices with in a Stryker, and by voice if dismounted. A fifth voice network was created to demonstrate that if all communication devices are eliminated an inherent command and control still exists. The diagram of this meta-network is below.

[23] Wayne, and Garfinkle, "Maintaining the Information Flow," 3.

[24] Ibid.

[25] Stryker Platoon and Squad 2-2

[26] Ibis

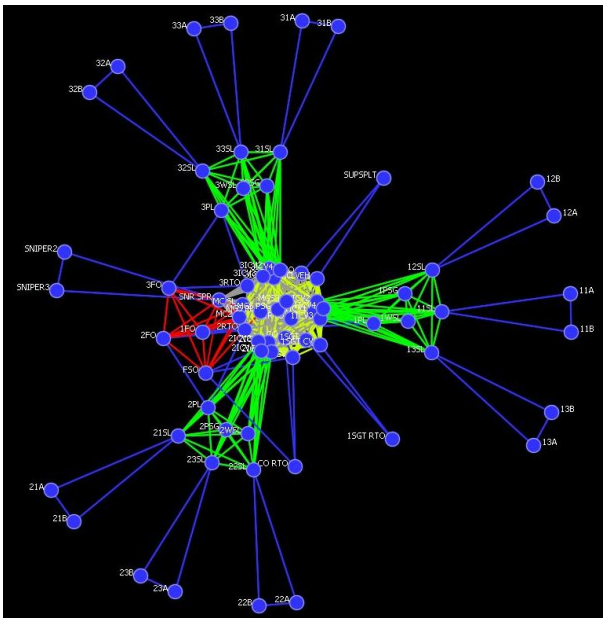

Figure 1: Graph of the full connected SCBT Rifle Company

SIMULATION DESIGN AND ALGORITHM DEVELOPMENT

We developed a simulation program in Python called the Cyber Conflict Network Simulator (CCNS), based partially on the Python-based Advanced Network Targeting (ANAT) social network analysis program.[27] The ANAT program reads in a network from a comma separated value file, builds the component networks and metanetwork, uses bridging to create social networks, and then produces a targeting report. The CCNS borrows the ANAT's module for reading the source file and building the metanetwork and uses the same modules for calculating network centrality and centralization measures, but the similarities end there. After creating the metanetwork, the CCNS executes a module for each simulation stage, based on the designated skill level of the attacker and defender. The skill levels are found in Table , below. Currently, there has not been any development of the Stage IVa module, and Stage V only has one "standard" level.

In order to capture the cumulative effects of cyber conflict on a network's connectivity, we developed a connectivity measure, or "connectivity probability," that represents the likelihood that a message sent from an originator arrives at the recipient.

[27] Johnson, McCulloh, Curwin, & Topp, 2013

The connectivity probability exists for each edge in a given network, and can be different for messages traveling in opposite directions. This measure combines the results of various cyber attack techniques, and generalizes conflict in order to allow the simulator to work for most networks, instead of becoming highly tailored for specific types of networks and conflicts.

Factor			Levels		
			Low	Medium	High
Stage I	Battlespace Preparation	Attacker	None	Limited	Active
		Defender	Passive	Limited	Active
Stage II	First Wave	Attacker	Basic	x	Advanced
		Defender	None	Basic	Advanced
Stage III	First Response	Attacker	None	Basic	Advanced
		Defender	Basic	x	Advanced
Stage IV	Second Wave	Attacker	Basic	x	Advanced
		Defender	None	Basic	Advanced
Stage IVa	Counterattack	Attacker	None	Basic	Advanced
		Defender	Basic	x	Advanced
Stage V	Recovery	Attacker	None	Basic	Advanced
		Defender	None	Basic	Advanced

Table 2: Simulation Factors and Levels

SIMULATION ALGORITHMS

Each simulation stage follows the same pattern. First, the stage selects a target or target list. Then, the simulator identifies the location of each target in the incidence and connectivity value matrices. Next, the simulator "attacks" each target by locating the edges connected each target, and multiplies the connectivity value for each edge by a given multiplier that represents the net effects of the stage's cyber attacks and the defenders' repairs. If any connectivity values are reduced to below 0.5, the edge is considered to not be reliable, and the edge is removed from the network. If the connectivity value of an edge that was previously removed from the network is restored above the 0.5 threshold, the edge is added back to the network. Finally, the simulator calculates the new network centralities.

Target selection is based on node centrality measurements (calculated at the end of the previous stage). One or more targets may be selected. When a single target is

selected, the node with the highest selected centrality becomes the target. Degree centrality selects the most connected target, while betweenness centrality identifies gate-keepers within the network, closeness centrality indicates how "close" a node is to the other nodes in the network, and Eigenvector centrality identifies nodes connected to other, important nodes (McCulloh & Johnson, 2011). When multiple targets are required, a given number of nodes with the highest indicated centralities are selected (a node can only be selected as a target once, even if it appears on the top of multiple centrality lists). In Stage V, targets can be selected from the list of edges removed from the network, or from a list of edges with the lowest connectivity values (and therefore need to be restored), and the multipliers are always greater than one.

Multipliers are used to modify the network connectivity values. The multipliers for each stage are determined based on the quotient of the defender's and attacker's skill level values. The skill level values are numerical approximations for the skill level of the attacker or defender. The formula for determining the multiplier is:

$$M = c * \frac{D}{A}$$

where *M* represents the multiplier, *D* represents the defender's skill level, *A* represents the attacker's skill level, and *c* is a constant. For example, a defender with a skill level of 3, an attacker with a skill level of 5, and a constant of 1 yields a stage multiplier of 0.6. Each stage has a unique constant that reflects the nature of the cyber activities during that stage.

WARGAMING THE COMMUNICATIONS OF A STRYKER COMPANY

We selected three different potential cyber attacks on a Stryker Company communications network. In the first scenario, the enemy disrupts FM communications using a frequency-jamming device. The multipliers for Stages I-V were (in order): 0, 0.25, 0, 0.7, and 150. The entire Fires, Command, and Platoon FM networks were targeted based on the nature of frequency jamming. In the second scenario, the enemy targets digital communications through offensive cyber means. The multipliers for Stages I-V were (in order): 0.85, 0.25, 0, 0.5, and 150. The key company leadership was targeted in Stage I, and the entire FBCB2 network was targeted in the other stages. In the third scenario, both attacks occur simultaneously. The same multipliers and targeting systems were applied simultaneously. We estimated these multipliers (instead of using the

traditional formula) by determining the effectiveness of each type of attack. We assumed that the Stryker Company is engaged in a modern, conventional fight against comparable enemy ground forces and that the Stryker Company is on the move and can only access its Lower TI communication devices. We do not examine communication above the company level.

RESULTS

We executed one run of each data point in the CCNS, and saved the results to a comma separated value file in order to compile and analyze the outcome of each stage. Since there are no stochastic elements to my model, each run of the same data point produces the same data. We exported each network's centralization and centrality measures and connection strengths after each stage, and a list of the deleted links. We then calculated the average centrality measures for each stage:

$$ACM_k = \frac{\sum_{i=1}^{n} C_i}{n}$$

where ACM_k is the average centrality measure (degree, closeness, betweenness, and eigenvector) of Stage k, C_i is the centrality of the i^{th} node in the network, and n is the total number of nodes in the network. The averages of the centrality measures represent the cumulative effects of cyber attacks on each network.

Design Point 1 (Electromagnetic Frequency Jamming Attack) targeted three networks: the Company Command, Platoon Radio, and Company Fires FM networks. During Stages II-IV, these networks were rendered completely inoperable. The effects on the Company Command FM network are representative of the effects on the other two networks.

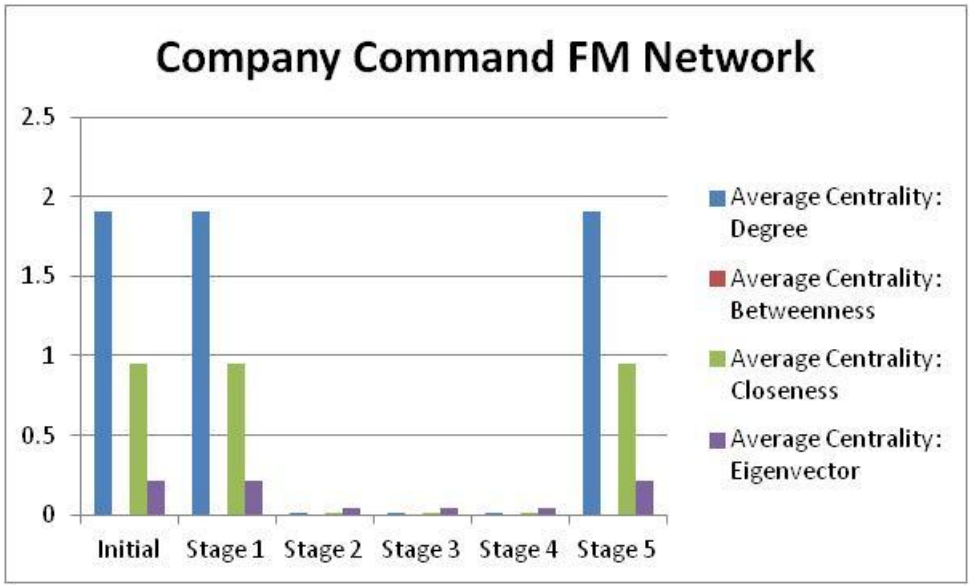

Figure 2: DP1: Company Command FM Network Average Centrality Measures

The jamming attack prevents the Stryker Company from being able to communicate with its FM radios. The attack greatly affects closeness, as the commander is no longer able to contact all if his leaders. In this scenario, the commander should use a closeness analysis to facilitate a restructuring of the company's forces may be necessary. One such restructuring would involve consolidating the platoons together to allow for better command and control. From a mission command perspective, this arrangement allows for more control from the squad leaders and vehicle commanders since they are now limited to voice communication.

Design Point 2 (Targeted Digital Attack) targeted the FBCB2 network. During Stages II-IV, the network was rendered completely inoperable. The effects of the attack on the FBCB2 network are shown in Figure 3. The other networks are not affected, and their network structure remains unchanged. Figure 4 shows the new FBCB2 network structure after this attack.

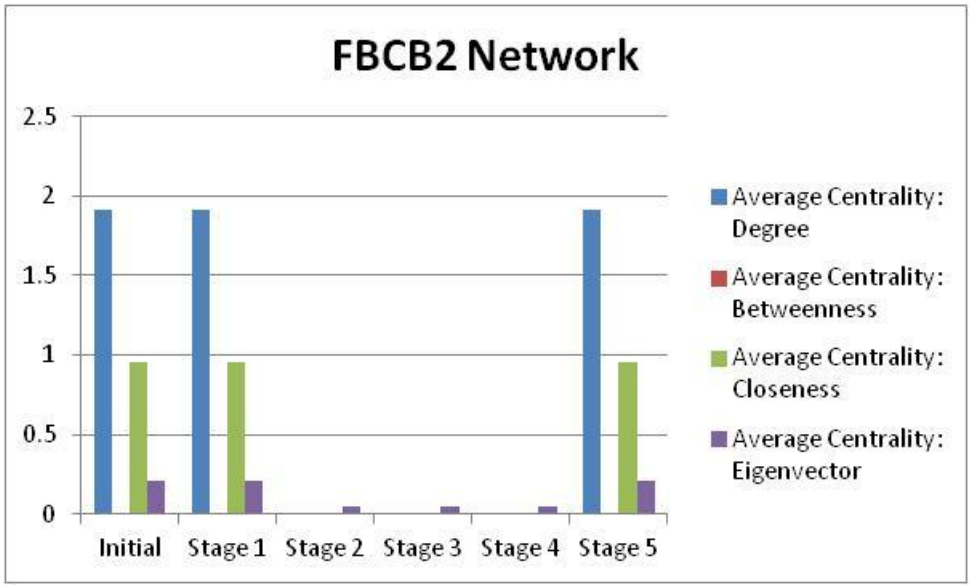

Figure 3: DP2: FBCB2 Network Average Centrality Measures

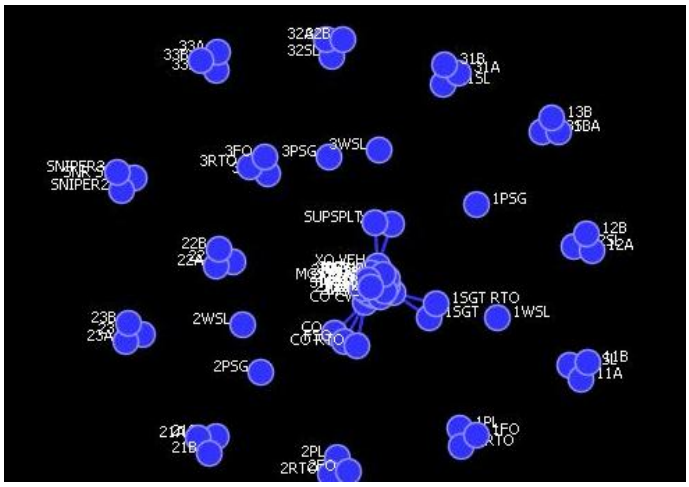

Figure 4: Enemy Compromises Digital Communications

The Stryker FM mentions the importance of not relying too heavily upon digital platforms such as the FBCB2. Even though the FBCB2 network is incapacitated, the FM radios allow the company to continue communicating with minimal disruptions. All units are still able to use the radios to communicate and command and control is still enforced.

Design Point 3 (Electromagnetic Frequency Jamming and Targeted Digital Attack) targeted the three FM networks and the FBCB2 network. During Stages II-IV, all networks were rendered completely inoperable. The effects of the attack on the Platoon Radio FM network, which are representative of the effects on the other networks, are shown in Figure 5Figure . Figure 6 shows the effects on the overall network structure.

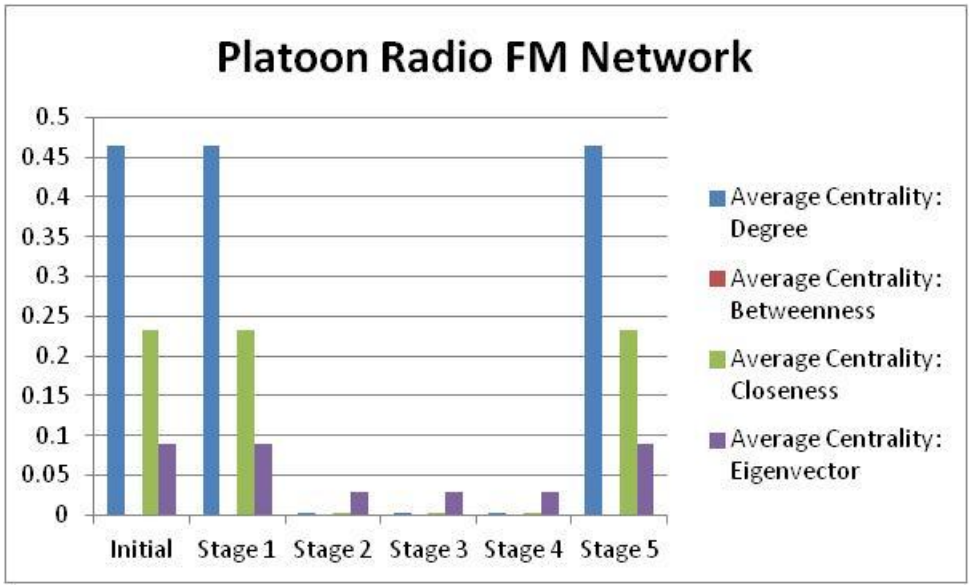

Figure 5: DP2: FBCB2 Network Average Centrality Measures

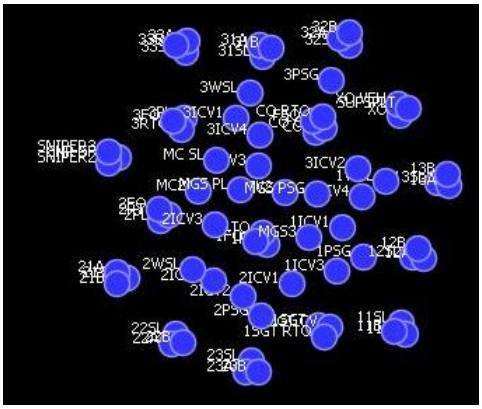

Figure 6: Enemy Compromises Digital and FM Communications

This scenario emphasizes the importance of the voice network. The Stryker Company has two options: it can reconsolidate its forces and maneuver in larger formations in order to rely on greater command and control, or delegate more control to subordinate commanders since communication will not be able to keep up with the potential pace of combat.

CONCLUSION AND FURTHER RESEARCH

Cyber adds another level of fog of war. Combat commanders must be aware of it and the threats it poses to the specific type of unit and the type of communications that the specific unit uses. That way when the fog of war does hit they can properly use mission command principles to limit the effects of the cyber attack. Cyber attacks should not limit the level of communications that a unit has. With a high variety of communication devices available to a unit this should be an extremely small limiting factor to any unit. Doctrine holds that company commanders should practice a proper level of training between computer technologies and basic soldier redundancy training using traditional navigation and communication devices.[28]

We did not create a counter-attack module during my research. The biggest question that we faced while exploring possible ways to create a counter-attack targeting algorithm exposed a significant limitation in my model and test dataset: the model does not distinguish between attacker- and defender-controlled nodes, and the dataset only includes defender-controlled nodes. Further research should examine whether or not it is realistic to include the attacker-controlled portion of the network. If it is realistic, then the current targeting algorithms would need to be adjusted to differentiate between attacker- and defender-controlled nodes, and the attacks themselves would need to become more specific than our current multiplier system is. Also, the results should report the effects on attacker and defender nodes separately, in order to provide a better understanding of the conflict's effects. If it is not realistic to include the attacker-controlled portion of the network, then we believe the placement of the counter-attack stage in our cyber conflict model should be reevaluated. We believe the best way to model a counter-attack without including attacker nodes would be to degrade the capabilities of the attacker in the next stage. The model currently places the counter-attack stage before Stage V, where we do not believe the effects of the counterattack would have a significant effect. The counter-attack might be better placed before Stage IV, instead. We also did not fully develop the recovery module during my research. Currently, the recovery model has one "standard"

[28] Stryker Company F-2

setting. Further research should develop my proposed Stage V skill levels for implementation in the simulation.

We noticed one major bug in my program, and several design flaws that could create issues in the future. The bug, which is referred to as the "Stage V Bug," restores all of the connectivity values above the 0.5 threshold for removing edges from the network, but not all of the edges are added back into the network. Further research should attempt to identify what is causing this situation. The first design flaw is the lack of a failsafe that would prevent edges that have been removed from the network from still being affected when one of the nodes from that edge is attacked. This is closely related to a second design flaw, where the simulator does not identify nodes that are isolated from the network or prevent them from being added to targeting lists. A third design flaw is the ability for connectivity values to exceed a value of one. Since the connectivity value is a probability, the values need to be constrained to fall between zero and one.

Our test of the CCNS maintained the same attacker and defender skill levels across each data point. Further research should examine whether this is a realistic combination of settings for the simulator, since defender's abilities should become degraded after a prolonged attack, or the defender's abilities could become enhanced if skilled cyber warriors were sent to reinforce the network. This research should determine if the simulator should account for fatigue and skill degradation, or if the user should be responsible for incorporating these types of situations by selecting the appropriate settings from the simulator.

The CCNS does not identify critical edges that connect the attacker to the defender, nor does it select targets based on the ability of the attacker to reach those targets, nor does it account for the effects on intermediary nodes and edges when the attacker reaches targets deep within the defender's network. Further research should examine how to identify and protect critical edges in order to ensure the attacker doesn't cripple its own ability to reach the defender's network, and whether or not the target selection algorithm chooses appropriate targets.

Further research should determine how much recovery is appropriate across the various levels of Stage V? Is total recovery realistic? If so, what does the attacker gain if the attacks inflict no lasting damage? Does the motivation for a cyber attack come from

the opportunities the attacker is able to exploit while the defenders' networks are down, or does the attacker benefit from the time, resources, and money that the defender spends on restoring the network? Answering these questions may require the development of different variations of the CCNS to model different types of attackers—military, patriotic hackers, hacktivists, and criminals.

Improvements of the model could allow the FM networks all to be on one FM network since in theory one FM could be used to switch and hop between all radio frequencies. In addition the addition of battalion level assets increases the amount of nets drastically better demonstrating the important commanders as we continue to add more players and decision makers. Another process that is worth considering is reversing the game process on an enemy communications network. At this level, the network could be used to determine which of the enemy networks could be eliminated in order to cripple or limit their communication options in order to cripple enemy forces. With this addition it could be worth considering cyber capabilities at the unit level.

Finally, further research using data from actual cyber conflicts should adjust the multipliers we used for the initial test of the CCNS. The current multipliers generate the general trends in network connectivity degradation that we would expect to see, but are not actually supported by other data. The validation of the multipliers would give the CCNS a significantly greater amount of applicability.

LIST OF REFERENCES

Alberts, David S., John Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC: National Defense UP, 1999. Print.

Anderson, B. Wayne, and Gerald S. Garfinkle. "Maintaining the Information Flow: Signal Corps Manpower And Personnel Requirements For The Battlefield." *US Army Research Laboratory* (2002): Print.

Barzashka, I. (2013, April 28). Are cyber-weapons effective? *The RUSI Journal*, 158(2). doi:10.1080/03071847.2013.787735.

BBC. (2013, December 19). NSA: White House task force recommends surveillance curbs. Retrieved from http://www.bbc.co.uk/news/world-us-canada-25439544.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. 2nd ed. New York: Ecco, 2010. Print.

Committee on Network Science for Future Army Applications. (2005). *Network Science*. Retrieved from http://site.ebrary.com/lib/usma/.

CDX 2009 network USMA. (2009, April 02). Retrieved from http://www.westpoint.edu/crc/SiteAssets/SitePages/DataSets/CDX_2009_Network_USMA.pdf .

Gorman, Siobhan, Yochi J. Dreazen, and August Cole. "Insurgents Hack U.S. Drones." *Wall Street Journal* [New York] 17 Dec. 2009: Print.

Healey, J. (Ed.). (2013). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* [Kindle version]. Retrieved from Amazon.com.

Johnson, A., McCulloh, I., Curwin, E., & Topp, S. (2013). Advanced Network Analysis and Targeting Report (Version 2.0) [Computer software]. West Point, NY: United States Military Academy.

Leiner, B. M., Cerf, C. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (n.d.). *Brief History of the Internet*. Retrieved from http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

Lewis, T. G. (2009). *Network science: Theory and applications*. Retrieved from http://site.ebrary.com/lib/usma/.

McCulloh, I., & Johnson, A. (2011). *Advanced network analysis and targeting course: A social network approach to targeting*. Wiley Preprint.

Thompson, Loren B. "The Twilight Of Network-Centric Warfare." *Lexington Institute*. N.p., 06 Aug. 2010. Web. 8 Oct. 2013.

Spafford, E. H. (1988, December 8). The internet worm program: An analysis. West Lafayette, IN: Purdue. Retrieved from http://spaf.cerias.purdue.edu/tech-reps/823.pdf.

United States of America. Department of Defense. Department of the Army. *Brigade Combat Team*. FM. 03-90.6. Washington, DC: Department of the Army, 2010. Print.

United States of America. Department of Defense. Department of the Army. *Mission Command*. ADP 6-0. Washington, DC: Department of the Army, 2009. Print.

United States of America. Department of Defense. Department of the Army. *Network Operations*. FM 6-02.71. Washington, DC: Department of the Army, 2009. Print.

United States of America. Department of Defense. Department of the Army. *SBCT Infantry Rifle Platoon and Squad*. FM 3-21.09. Washington, DC: Department of the Army, 2010. Print.

United States of America. Department of Defense. Department of the Army. The *SBCT Rifle Company*. FM 3-21.11. Washington, DC: Department of the Army, 2003. Print.