Using Cyber-Security Exercises to Study Adversarial Intrusion Chains, Decision-Making, and Group Dynamics

Aunshul Rege[1], Joe Adams[2], Edward Parker[1], Brian Singer[1], Nicholas Masceri[1] and Rohan Pandit[1]
[1]Temple University, USA
[2]Merit Network, USA
rege@temple.edu
wjadams@merit.edu
ed.parker@temple.edu
brian.singer@temple.edu
nicholas.masceri@temple.edu
rohan.pandit@temple.edu

Abstract: Increasingly adversaries are becoming more sophisticated and persistent in their cyber-attacks against critical infrastructures. Traditional incident management is response-driven, which is ineffective and costly, especially in countering adaptive adversaries. The security community has argued for a paradigm shift towards proactive and anticipatory cyber-security. Defenders thus need to understand adaptive behaviors and dynamic decision-making processes of adversaries. Using a cyber-adversarial intrusion-chain model and empirical evidence of observations done at a force on force ("paintball") exercise held at the 2015 North American International Cyber Summit (NAICS), this paper argues that understanding how adversaries adapt at various points in the intrusion chain is crucial in profiling adversaries and developing anticipatory cyber-security measures. Specifically, this paper highlights the *human aspects* of cyber-attacks, with three specific objectives: (i) providing a preliminary temporal assessment of the cyber-attack process, (ii) understanding adversarial decision-making, cyber-attack disruptions and corresponding adaptability, and (iii) comprehending group dynamics, such as structure and interdependencies; cohesiveness and conflict; and division of labor.

Keywords: anticipatory cyber-defense, cyber kill chain, human behavior, measurement and metrics, dynamic cyber-defense

1. Introduction

Advanced Persistent Threats (APTs) have increasingly been targeting growing numbers of organizations, routinely bypassing traditional security measures, and resulting in large and costly damages. Unlike traditional threats, which are generic, scattershot, and predictable, APTs are customized, surgical, and highly sophisticated (TrendMicro 2017). APTs use *Advanced* attacks, such as customized malware and 'zero-day' (not publicly known) vulnerability exploits, are organized, focused on specific targets, have well-defined plans and objectives, and implement well-rehearsed and coordinated attacks (DELL, 2012). These malicious actors are *Persistent* as they do not give up easily, are professional in their approach and planning, and engage in repeated, coordinated and adaptive attacks to improve chances of success (RSA Division of EMC, 2012; DELL, 2012). To be considered a *Threat*, adversaries must have intent, opportunity, and capability; an APT dedicates all of the cognitive abilities and resources at its disposal, to pursue specific objectives (DELL, 2012; Ingoldsby, 2013). Conventional cyberattack management is reactive, where organizations focus their efforts on detecting Indicators of Compromise, or threats. This response-driven approach is problematic as it does not capture APTs and the mutating techniques and tactics they use, and also because it is costly to remedy (Cloppert 2009, Kulkarni, 2016). A paradigm shift from reactive to anticipatory and predictive cybersecurity is essential. One key aspect underlying this shift is the human element of the cybercrime equation. As such, this paper highlights the *human aspects* of cyberattacks, with three specific objectives: (i) providing a preliminary temporal assessment of the cyberattack process, (ii) understanding adversarial decision-making, cyberattack disruptions and corresponding adaptability, and (iii) comprehending group dynamics, such as structure and interdependencies; cohesiveness and conflict; and division of labor.

The rest of the paper is organized as follows. The next section puts forth the cyber-adversarial intrusion-chain model used in this study. The third section discusses the data collection procedures for a real-time cybersecurity exercise, methodological limitations, and the significance of qualitative, social science research. In the fourth section, we analyze the intrusion chain using our cybersecurity exercise case study. The fifth section focuses on how adversaries make decisions, and manage disruptions to their attacks. The sixth section focuses on group dynamics, such as division of labor, cohesion and conflict issues, and structure. We conclude with a discussion of metrics and measurement, how future research should further develop measurement techniques, and how qualitative research methods can be translated to quantitative methods to gain a more thorough understanding of adversarial behavior and cyberattack processes.

2. Intrusion chain models

There are multiple cyber-adversarial intrusion-chain models in the open literature (Hutchins et al., 2011; Barnum, 2013; Cloppert, 2009). We use Cloppert's (2009) 12-step intrusion-chain model (displayed in Figure 1 below): (1) *Define Target*: During this stage, adversaries identify their targets, such as businesses, power grids, financial sectors, or other critical infrastructures. (2) *Find and Organize Accomplices*: Adversaries often have specific areas of expertise and lack the complete skill set that is needed to execute a successful attack. In this stage, adversaries find partners and form alliances that complement and supplement their own skill sets. (3) *Build or Acquire Tools*: In this stage, adversaries build their attack vectors, gather toolkits, and set the technical groundwork to execute attacks. The infrastructure needed to implement and execute the attack will vary based on the target and the objective, but the necessary resources will be identified and prepared ahead of the direct action against the target (DELL 2012). (4) *Research Target Infrastructure/Employees*: This stage typically involves obtaining target infrastructure blueprints, identifying target vulnerabilities, and social engineering practices. (5) *Test for Detection*: In this stage, adversaries gather intelligence on security controls and procedures set in place by the targets that they are likely to encounter to create appropriate evasion and response plans (DELL 2012). (6) *Deployment*: After the preceding preparatory stages, adversaries attempt to gain a foothold into the target environment by deploying their attack vectors, skills, and knowledge. (7) *Initial Intrusion*: Here adversaries gain preliminary access into the targeted environment. Adversaries typically accomplish this via (spear) phishing with malicious links or attachments, which when clicked, install malware payloads. (8) *Outbound Connection Initiated*: Once an initial foothold is attained, adversaries attempt to establish more points of access into the targeted environment. (9) *Expand Access and Obtain Credentials*: In this stage adversaries gain access to additional systems and authentication material that will allow access to further systems. (10) *Strengthen Foothold*: Adversaries want to persist in the targeted environment as long as it takes them to achieve their objectives. Doing so requires that they strengthen their presence inside the targeted environment, which is typically done by gaining credentials, using these to move laterally and deeper into the targeted environment, and establishing control over as many different parts of the system as possible. (11) *Exfiltrate Data*: Here, adversaries remove resources that can be used for future exploit(s), steal documents and data that have financial or other perceived worth, or take everything (every document, email and other types of data) from the network that might be of interest. (12) *Cover Tracks and Remain Undetected*: Clean-up efforts involve removing evidence of the intrusion, what systems/data were targeted, planting or manipulating data in the environment for the purpose of misdirection, and eliminating evidence of the adversarial identity and location. We use this model as the framework for our analysis as it offers a thorough description of the attack phases and its cyclical structure addresses the possibly iterative nature of the cyberattack process.

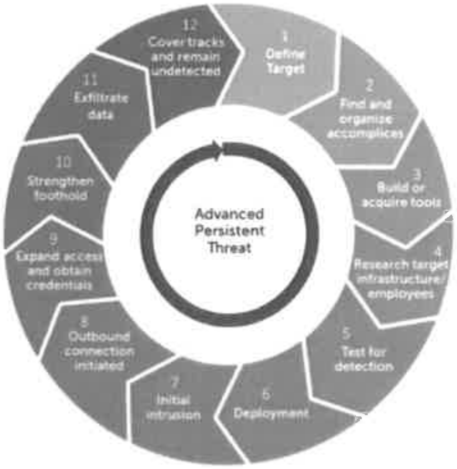
12 Cover tracks and remain undetected
1 Define Target
2 Find and organize accomplices
3 Build or acquire tools
4 Research target infrastructure/ employees
5 Test for detection
6 Deployment
7 Initial intrusion
8 Outbound connection initiated
9 Expand access and obtain credentials
10 Strengthen foothold
11 Exfiltrate data
Advanced Persistent Threat

Figure 1: Cyber-adversarial Intrusion-chain model (Cloppert, 2009)

3. Using real-time cybersecurity exercises to do "field research"

Merit Network and the Michigan Cyber Range provide a robust virtual environment, henceforth called Alphaville, for CTFs and other cyber exercises. The Michigan Cyber Range was created in 2012 as a network accessible training platform specializing in cyber security. Alphaville debuted in March 2013 and has been improved and expanded continually since then. Created to emulate the services and information commonly found in small cities, Alphaville consists of over 200 virtual machines that present a CTF participant with a complete spectrum of challenges in an environment of realistic servers, firewalls, and networks. Alphaville consists of five "locations:" a school, a library, a city hall, a small business with a manufacturing facility, and a power company. Each of these locations contains servers and firewalls with intentional vulnerabilities. Some servers and services are more secure than others. Most importantly, information found in one site might be used to break into another site. Since Alphaville is completely virtual, the Michigan Cyber Range can operate up to 30 instances of the environment at the same time, either isolated from each other or combined to communicate through a wide area network added to the environment. Alphaville is used in a variety of force on force exercises, experiential classroom labs, and product development test programs every day. In 2015, almost 30 exercises used Alphaville for a wide range of professional, academic, and government participants. Some exercises are designed to test individual skills, such as CTFs at a conference, while others pit teams of participants against each other, as in the Collegiate Cyber-Defense Competition (CCDC) or the North American International Cyber Summit (NAICS). During the 2015 NAICS, researchers observed a force on force exercise colloquially called "paintball." In this type of exercise, teams of five participants battle to claim Alphaville's network by controlling critical servers and firewalls. A team marks its control of an asset by planting an encrypted beacon and defending that asset against other teams. The 2015 NAICS featured six teams operating in the same environment. Teams were spread across the globe, with seven time zones between some participants. Their progress was displayed on a scoreboard, which was visible to all teams. Dots on the scoreboard represented the assets in the different locations, with the dot's color signifying which team had control of it in that 5 second segment. The team we observed consisted of four members (henceforward referred to as Subjects S1, S2, S3 and S4). Two members had worked with each other before, which facilitated team organization and division of labor. The exercise lasted for 5 hours, during which the team attempted to control various parts of Alphaville's infrastructure as described above. Composition of the other teams was unknown to the team observed (as well as the researchers). The observed data from the exercise was analyzed and verified, when possible, by interviewing the participants separately (Dunning, 2008).

3.1 Study limitations and significance of qualitative/social science research

There are some obvious limitations to this study. First, interviews were only minimally conducted; the researchers did not wish to break the team members' concentration as they were too focused on the exercise to explain their actions and thought processes. Second, this was a public event and participants were expected to speak with attendees, which not only impacted the researchers' observational capacity, but also the team group dynamics and strategies. Third, the lack of exercise logs made it difficult to gauge how the observed team reacted to the other teams' actions. Fourth, the findings and analysis here are by no means intended to address all possible attacks, motivations, cultures, attackers and organizational sophistication. This study is based on a single instance of data collection, and it is likely that a different set of team members may have generated a very different set of behaviors, group dynamics, and operational strategies. Additionally, this cyber-security exercise was compressed and expedited, which is certainly not representative of how cyberattacks occur in reality, as cyber-criminals may have unlimited time and resources. While these are all legitimate limitations and inhibit the generalizability of the findings, we argue that *these limitations are typical of quantitative/hard science research, which our research is not*. Our work is qualitative in nature and critical to advance the human behaviour and social science research aspects of cyber-security, areas that are often downplayed in the technical domain. First and foremost, our research is based on a *qualitative case study*; we emphasize that access to high quality, well-structured cyber-security exercises involving professionals (as is the case study used here) is highly protected and rarely open to academic researchers. Human behaviour in group settings is a complex and rich social phenomenon, one that *requires* a qualitative and social science approach to unpack the underlying process mechanisms of human interactions, group dynamics, and adversarial intrusion-chains. Second, qualitative approaches are very useful for *exploratory* research; we are not aware of any research in the open literature, qualitative/social science or quantitative/hard science, which focuses on the temporal analysis of adversarial intrusion chains, adaptability to disruptions, and group dynamics. As such, this research is unique, innovative, and offers a preliminary dialog on unpacking cyber intrusion-chains and group dynamics. Finally, to achieve interpretation and verification, the observations were compared to the debriefing session that occurred at the end of the exercise. This approach was the best means of ensuring that observed data matched what the participants had experienced during the exercise.

4. Temporal assessment of the cyber intrusion-chain

The cyber intrusion-chain offers a mechanism to understand the many stages of the cyber-attack process. However, there are many components of the intrusion chain that remain unknown. Are some intrusion chain stages more relevant than others? Rege (2016) states that stage relevance could be determined by several factors, such as time, money, resources, effort, and the overall attack technique reliability/familiarity. While the exercise did not have monetary aspects, a points system was used for each challenge that the red-team had to complete. However, there was no means to obtain information on monetary incentives and attack technique reliability/familiarity as the structure of the exercise did not permit the researchers to speak with the red-team during the exercise. As our research was limited to observations, we can only offer the *temporal relevance* of the various phases in the cyber intrusion-chain model. Time was evenly distributed throughout most of the stages of the intrusion-chain. However, there were two stages that were more temporally taxing than the other stages. First, roughly 20% (55 minutes) of the group's time was spent at the beginning of the exercise on the "Finding and Organizing Accomplices" stage, where group members familiarized themselves with each other. The other stage, "Expand Access and Obtain Credentials" accounted for about 21% (60 minutes) of the group's time, which could be due to the difficulty and duration of the tasks associated with this stage. For instance, S3 took roughly 20 minutes to obtain access to one of the rival team's machines. S1 needed approximately 20 minutes to put a beacon in Alphaville's school's server. The "Initial Intrusion" stage was next with regards to time commitment and took up approximately 12% (35 minutes) of the overall time. Like the "Expand Access and Obtain Credentials" stage, the tasks involved with this stage also appeared to be difficult and time-consuming. For instance, S3 spent roughly 15 minutes trying to infiltrate one of the rival team's boxes. There were several stages that required similar temporal dedication. The "Build and Acquire Tools", "Research Target Infrastructure", "Test for Detection", "Deployment", "Outbound Connection Initiated", and "Strengthen Foothold" required roughly 7-9% of their overall exercise time.

Interestingly, there were three stages of the cyber intrusion-chain that did not appear to have get any of the observed team's time. First, "Define Target" did not get any attention because the target (Alphaville) was predetermined and discussed prior to the start of the exercise. Next, "Exfiltrate Data" did not appear to take up any of the team's time; this could be because this particular exercise did not require data exfiltration. The team was more concerned with gaining access to Alphaville's systems and controlling servers. In a similar vein, the "Cover Tracks" stage was not given any time, which may be indicative of the nature of the exercise. Given that the exercise was compressed and expedited, and that there were no consequences for being detected, the team may not have been concerned with covering its tracks and thus could not justify dedicating any time to this stage. To summarize, the "Find and Organize Accomplices", "Expand Access and Obtain Credentials" and "Initial Intrusion" stages required the most amount of time in this particular exercise, which may indicate that these stages involve tasks that are more difficult and thus time-consuming. Figure 2 summarises the temporal breakdown of each of the cyber-adversarial intrusion-chain stages across the entire exercise.

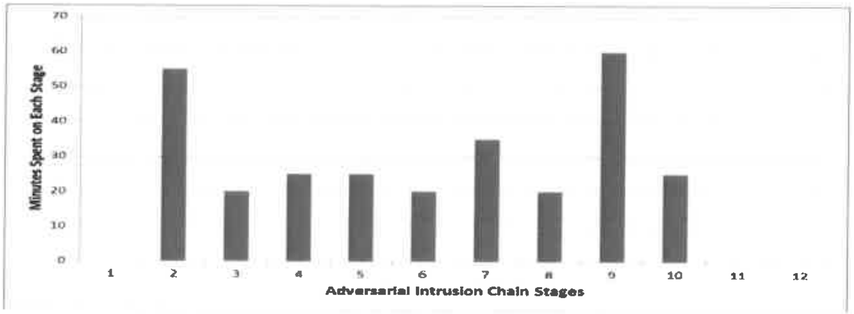

Figure 2: Temporal Breakdown for Cyber Intrusion Chain Stages: 1. Define Target; 2. Find and Organize Accomplices; 3. Build or Acquire Tools; 4. Research Target Infrastructure/Employees; 5. Test for Detection; 6. Deployment; 7. Initial Intrusion; 8. Outbound Connection Initiated; 9. Expand Access and Obtain Credentials; 10. Strengthen Foothold; 11. Exfiltrate Data; and 12. Cover Tracks and Remain Undetected (Cloppert, 2009)

5. Adversarial decision-making, intrusion chain disruptions, and adaptability

A rational model of group decision-making involves four stages: (i) orientation, where the group defines the problem and discusses any steps that could be taken to solve the problem, (ii) discussion, where the group gathers and processes information relevant to the decision, (iii) decision-making, where the group chooses a solution via a variety of mechanisms, such as averaging individual inputs, voting, and consensus, and (iv) implementation, where the group implements the decision and then evaluates it (Forsyth, 2006).

In the group observed, the overall decision-making process was very fast. The orientation stage occurred at the very beginning of the exercise where all members had a quick discussion about strategy and goal. S2 made the overall decisions and assigned tasks to the other members, and for the most part, each member was trying his best to stay true to the objective of controlling as many systems as possible. Even though S2 acted as the clear leader, all members had discussions about what, when, and how to attack/defend each server, indicating communication was relevant.

Throughout the exercise, however, split-second decisions were constantly being made by individual members (rather than the group) to either attack or defend. Instead of always being able to implement their strategies against the other teams, the subjects had to react to the decisions made by the opposing teams. Due to the back and forth nature of this exercise, the implementation stage was structured more as an implementation and decision-making stage combined, where members had to respond very quickly based on what had just occurred rather than long thought processes and strategies.

In this observed exercise, it appears that the team did exhibit all stages. However, the orientation phase was the shortest, while the discussion, decision-making, and implementation stages occurred concurrently as members were toggling between proactive and reactive approaches to gain and maintain control over systems respectively.

There were several occasions where rival teams disrupted the observed team's attacks, as identified in Table 1 below. Most of the rival teams' actions were noticed by the observed team well after the damage had been done. The observed team did not notice anything different with its systems until the rival teams had either killed their chains or taken over their systems, which typically resulted in arguments, visible frustration or desire to get back at the rival teams.

Table 1: Rival team disruptions and corresponding (observed) adaptations

Subject	Disruption	Observed Adaptation
S2	Rival team 3 gains control of S2's beacon **(11:25)**	Acts to counteract action, retakes beacon, responds with humor: "I gave them hope"
S1	"They found ... boxes – killing me out there" **(10:00)**	Gets help from other members on what to do and how to get around it.
S2	Acknowledges that rival teams are fighting back **(10:03)**	Keeps an eye on rival team and attempts to toughen security on controlled systems
S2	"They came in and closed out boxes" **(11:46)**	Attempts to regain access to their boxes, asks for help from teammates.
All Subjects	Team loses more than half their beacons **(11:57)**	Subjects begin to argue, S2 reprimands S3 for "being a **** to everyone"

During the exercise, the observed team exhibited several instances of failure due to limited experience. For instance, some team members had little knowledge on both when to deploy certain types of attacks and also on target knowledge as shown in Table 2 below. Team members exhibited lack of knowledge and confidence in several instances. One example was when S3 lacked the knowledge to complete a task assigned to him and therefore S1 had to step in and help.

Table 2: Examples of the observed team's limited knowledge/experience

Example of more experienced team member helping less experienced members			
8:04 S2: "Problems setting up?" S3: "Got it, I guess" S2: "I wouldn't try that yet"	8:41 S2 helps S1 make a backdoor	8:41 S2 checks in with S4 for his status	11:12 S2 moves closer to S3 to assist with a command
Example of a member questioning what is happening because of a lack of knowledge			
8:40 S2 "Why do I keep losing my shell"	9:44 S2's visibly frustrated trying to get into Alphaville	10:00 S1: "Still not able to get in"	11:40 S2 denied root access to known IP address
Example of backtracking to locate command required for progress 9:55 S2: "I have to go back and find that specific command, all that stupid scroll back."			

Finally, the observed team disrupted its own intrusion-chains (independent of its rivals' actions), thereby hindering its progress, as shown in Table 3 below. Each member of the observed team had to manage firewalls and/or login credentials to ensure interaction with the network. Once the team accessed the system, it changed all of the login credentials so that its competition would require extra effort to gain access. When a team member locked himself out, another teammate would alter the system to allow access. The only significant failure to adapt came when they locked everyone out of the firewall at one time. No one from any team could find a way to interact with the system so the exercise organizers had to step out of the normal game bounds and reset the system.

Table 3: Self-Inflicted team disruptions and corresponding (observed) adaptations

Subject	Disruption	Observed Adaptation
S3	Kills S2's intrusion-chain **(8:33)**	S2 reacting with humor, not anger, to regroup and move on.
S3	Killed his own access and had trouble regaining access. **(8:45)**	Slightly frustrated humour and then refocusing on the task at hand
S3	Failed login attempt **(8:50)**	None
S3	Asks S1 for firewall exception for him **(10:48)**	Waited until S1 could give him access

6. Group dynamics

Group dynamics have been studied in several disciplines, such as Anthropology, Business and Industry, Clinical/Counseling Psychology, Communications, Education, Political Science, Psychology, Social Work, and Sociology (Forsyth, 2006). In the Criminal Justice arena, group dynamics have been used to analyze law enforcement agencies, gangs and jury deliberations (Forsyth, 2006). Research on crime groups, including cybercrime rings, is limited to organizational dynamics, such as structure and divisions of labor (Broadhurst, 2014; Wagen & Pieters, 2015; Wall, 2015). Member dynamics, power and status dynamics, conflicts and tensions, cohesiveness, and interdependencies in cybercrime rings/groups have received minimal attention. A main reason for this the difficulty in observing real-time interactions between members of cyber-crime groups, given the dispersed, covert, and dynamic nature of cyber-crimes.

6.1 Structure and Interdependencies

Groups typically create a state of interdependence, which is a mutual dependence or influence, where one member's outcomes, actions, thoughts, and experiences are determined in whole/part by other group members (Forsyth, 2006). These interdependencies could be unilateral (one member influences all others), sequential (one member influences the next member, who then influences the next), or reciprocal (members influence each other) (Forsyth, 2006). Group structure embodies the set of roles expected at different positions in the group and inter-member relations between the group members (Forsyth, 2006).

Subjects S1, S2, S3 and S4 all played different roles and worked on a variety of tasks. Throughout the exercise, S2 consistently exhibited characteristics of holding the position of leader, as he primarily designated tasks to each of the other subjects. In addition, S2 displayed the greatest skill set and knowledge base out of the four subjects, which may have further cemented his leadership role. Furthermore, S2 was comfortable with other members and acted as a common link for the whole team. Throughout the exercise, in addition to delegating tasks, S2 would get up from his seat to walk to each team member and provide instruction, advice, and help. Even though S2 served as the leader, he did not order the other members to complete tasks; rather he framed assignments as suggestions, which the members accepted.

S1 and S3 assumed similar roles, in that they took most tasks from S2. Their skill sets were not as extensive as S2 (but more so than S4, discussed below). Even though these subjects played a secondary role, they occasionally gave out both help and smaller task delegations to each other. S1 and S3 would also get out of their seats infrequently to walk and help S2 and S4.

S4 was relatively inexperienced and lacked many skills the other subjects had, and as such, he primarily worked alone. He did not assign any tasks of his own, only received assignments (infrequently), and he required more help than any other member.

In this context, it appears that the interdependencies between team members were of a very informal nature with a combination of unilateral and reciprocal, as illustrated in the Figure 3 below:

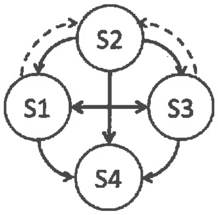

Figure 3: Unilateral and reciprocal interdependencies

6.2 Cohesiveness

Group unity is determined by its cohesion, which is the strength of bonds linking members to one another, and the degree to which members coordinate their efforts to achieve their goals (Forsyth, 2006). Cohesiveness varies across different groups, but all groups require a certain amount without which they would disintegrate.

Members of the group observed in this study were not all familiar with each other nor had they worked together much prior to the exercise. Normally this would hinder a team's cohesion but because of the informal nature of the structure, this effect was mitigated. As a group the members did not stick solely to their respective tasks, but (as noted earlier) often helped their teammates and did not hesitate to ask for aid in solving a problem.

One of the reasons S2 was seen as a clear leader was because of how often he was getting up and helping or collaborating with the other members. This mainly occurred with S2 and S3. It seemed that S2 was more comfortable with S1's and S3's skill levels and assigning them tasks. Within this trend, there were more instances of S2 collaborating with S1 than anyone else. It is also worth noting that S2 was the person primarily interacting with S4, who was mostly withdrawn from the other members. This distancing could be attributed to skill level, unfamiliarity with the other subjects, or a combination of both. However, S4's inexperience was met with collaboration on the part of S2 and S3, rather than hostility.

There were also instances of S1 and S3 collaborating without the involvement of S2. This occurred especially in the moments where it seemed S2 was making a breakthrough or working hard at gaining or maintaining control of a system.

Overall, the observed team was very cohesive, informal and supportive, but there were moments of conflict that the team was able to overcome to continue operations.

6.3 Conflict

Conflict represents disputes and/or disagreements between group members (Forsyth, 2006). It is no surprise that the overall group unity is impacted by conflict and cohesiveness, where if the strength of the former may result in group discord and if the latter is eminent the group is more likely to remain intact.

There were two distinct conflicts that arose during the course of the exercise. The first arose when S3 kicked two other team members out of the school server inadvertently. It was interesting that while this was a conflict, it was very light-hearted in nature, as all members laughed when they realized it was S3 who had locked them out of the system (and not the rivals). This informal and friendly division of roles and labor further cemented the bonding between members and team unity.

The second, and more serious of the two conflicts, arose around the midpoint of the exercise. At this time the subjects became visibly and audibly frustrated with losses of beacons inside of the systems they had, up to this point, been controlling. This put a serious strain on their relationships, interactions lessened, and the overall team atmosphere became tense, and S2 noted that S3 was "being a d*** to everyone." Tensions eased as they learned from the exercise organizers that the problem lied with the scoreboard display and not with rivals dismantling the team's control over the systems.

Thus, whatever (minimal) conflict that emerged was resolved via open conversation. The fact that some members had known each other and had worked together before may have also assisted in smoother and quicker conflict resolutions.

6.4 Division of labor and organization

Team members employed specific strategies and took on certain roles so as to fulfil the group's overall mission (Forsyth, 2006). Some roles, such as task roles, were concerned with accomplishing the task at hand, organizing the group to attain goals, and providing administrative or technical support to other members (Forsyth, 2006). Other members adopted socio-emotional roles where they satisfied the emotional roles of the group (Forsyth, 2006).

The team's main strategy was to take control of the various systems in Alphaville, such as school, library, and business, and then change passwords and admin credentials so that they could lockdown the servers from other teams. After they gained access to the servers the subjects would then light their beacon, which was a program, inside the servers in a specific location on the system. In addition to this main strategy, the subjects changed firewall settings of the servers to only allow for specific IP addresses (their own) access.

S2 emerged as the team leader and assigned tasks to other members of the team. Another characteristic of S2's leadership role was that he helped the other members (S3, S4) when they were unable to complete a task. Finally, S2 also communicated with sub groups and other members, and ensured strong team cohesion by checking on team members (S4), by asking how they were doing. In addition to the leadership role, S2 also actively participated in the exercise. He created backdoor entrances to the servers in case other teams gained access. Additionally, S2 switched his team's beacon for another team's beacon and then changed the name to match that team's beacon so that the rival would not realize that they were running his beacon.

S3 attempted to flood a team with packets, to create a DDOS attack to control the business server. S1 changed username and password credentials in order to make the servers and systems much harder to hack into; he also changed the firewall settings. All the players used Kali Linux and its various built-in tools to attack, and defend from, the other teams.

In the observed team, S2 took on both task and socio-emotional roles by completing the specific tasks list above and maintaining an informal leadership (as noted in the earlier section) respectively. S1 and S3 mostly had task roles. Given S4's overall minimal involvement, limited skill set, and receipt of assignments, he also had a task role.

7. Measurement and metrics

This paper offered a rudimentary temporal assessment of the cyber intrusion-chain. We are aware that this was a rough estimate of measurement based solely on observational time-stamped data. The major limitations of this data collection and analysis process are the durations between them and their non-descriptiveness. For example, several tasks could occur between a single observational time stamp, which makes calculating the exact amount of time spent on any one task accurately problematic and different than what they actually were in the exercise. This lack of clarity, in turn, impacts our discussions on the amounts of time spent on different intrusion chain stages. One means of mitigating this problem is to take more detailed time stamps during observations. The ideal solution, however, is to obtain the technical exercise logs and overlay these with the observational time stamps to better capture durations and frequencies of the intrusion stages. The amount of resources and time required to tag the exercise logs with attack, tool, and objective would be substantial. Furthermore, analyzing the tagged logs would not yield the participants' intent and would require further interviews.

There are many other metrics that can be used to determine individual and group-based performance and decision-making, such as the PARE RISKS framework: **P**revention measures, **A**ttacks and Alliances, **R**esults, **E**ase of Access, **R**esponse & Recovery, **I**nterconnectedness and Interdependencies, **S**ecurity Testing, Assessments and Audits, **K**nowledge, Skills, Research and Development, and **S**ystem Weaknesses (Rege, 2014; 2016). How might these components be measured and used to predict adversarial behavior? How can the PARE RISKS framework be used to further study the complexities of intrusion-chain stages, to identify where adversaries might spend more time and effort? Future research should also address how these different metrics and components can be *standardized*, effectively *compared* to develop APT profiles that can aid in proactive and anticipatory cybersecurity measures. Future research should also identify mechanisms to translate qualitative, social science data obtained via observations and interviews, into hard science, quantitative computations, such as time series analyses, game theory applications, and statistical graph models to gain a multidisciplinary and a more plausible picture of cyber-attack processes.

Acknowledgements

This material is based upon work supported by the National Science Foundation CAREER Award, Grant No. CNS-1453040, and partially by National Science Foundation CPS Award, Grant No. 1446574.

The authors thank the Michigan Cyber Range, a virtual training and testing program created and maintained by Merit Network in partnership with the State of Michigan.

References

Barnum, S. (2013). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). MITRE Corporation, July. Online at http://www.mitre.org/sites/default/files/publications/stix.pdf

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An Analysis of the Nature of Groups Engaged in Cyber Crime. An Analysis of the Nature of Groups engaged in Cyber Crime, International Journal of Cyber Criminology, 8(1), 1-20.

Cloppert, M. (2009). "Security Intelligence: Attacking the Cyber Kill Chain". Retrieved February 2, 2014. Online at http://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain

DELL (2012). "Lifecycle of an Advanced Persistent Threat". Retrieved September 19, 2013. Online at http://www.redteamusa.com/PDF/Lifecycle%20of%20an%20Advanced%20Persistent%20Threat.pdf

Dunning, T. (2008). Natural and Field Experiments: The Role of Qualitative Methods. Retrieved
November 24, 2012. Online at http://www.thaddunning.com/wp-content/uploads/2009/12/DesignBased_QualMethods_v2.pdf

Forsyth, D. (2006). Group Dynamics. California: Cengage Learning.

Hutchins, E., Cloppert, M. & Amin, R. (2011). "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Retrieved January 25, 2012. Online at http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Ingoldsby, T. (2013). Attack Tree-based Threat Risk Analysis. Amenaza Technologies Limited.

Kulkarni, A. (2016). "The Five Core Components of Proactive Cybersecurity". Retrieved December 20, 2016. Online at http://www.techzone360.com/topics/techzone/articles/2016/12/05/427743-five-core-components-proactive-cybersecurity.htm#

Rege, A. (2016). "Incorporating the Human Element in Anticipatory and Dynamic Cyber Defense", Proceedings of the The 4th International Conference on Cybercrime and Computer Forensics (ICCCF). Institute of Electrical and Electronics Engineers (IEEE).

Rege, A. (2014). A Criminological Perspective on Power Grid Cyberattacks: Using Routine Activities Theory and Rational Choice Perspective to Explore Adversarial Decision-Making. Journal of Homeland Security and Emergency Management (JHSEM) 11(4): 463-487.

RSA Division of EMC (2012). "Stalking the Kill Chain". Retrieved March 31, 2014. Online at http://www.emc.com/collateral/hardware/solution---overview/h11154---stalking---the---kill---chain---so.pdf

TrendMicro (2017). "Combating Advanced Persistent Threats". Retrieved January 10, 2017. Online at http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/

Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. British journal of criminology, 55(2), 1-18.

Wall, D. S. (2015). Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime. The European Review of Organised Crime, 2(2).