A Qualitative Exploration of Adversarial Adaptability, Group Dynamics, and Cyber-Intrusion Chains

A Rege, E Parker, B Singer, N Masceri

Department of Criminal Justice
Temple University
Philadelphia, PA, U.S.A.

E-mail: rege@temple.edu; ed.parker@temple.edu;
brian.singer@temple.edu; nicholas.masceri@temple.edu

Abstract: *Conventional cyber attack management is reactive, which is ineffective in curbing sophisticated adversaries, especially Advanced Persistent Threats (APTs). There is an immediate need for proactive cyber-security measures that reflect the adaptive and dynamic nature of these adversaries. Using empirical evidence of observations and interviews conducted at the Industrial Control Systems Computer Emergency Response Team's (ICS-CERTs) Red-Team/Blue-Team cyber-security training exercise held at Idaho National Laboratory (INL), this paper highlights the human aspects of cyber attacks, with a specific focus on adversarial intrusion chains, adaptability after attack disruptions, and group dynamics.*

Keywords: *Anticipatory Cyber Defence, Cyber-kill Chain, Human Behaviour, Group Dynamics, Adversarial Adaptability, Advanced Persistent Threat (APT)*

Introduction

Advanced Persistent Threats (APTs) are attack campaigns in which adversaries establish an unauthorised, long-term presence on an enterprise's or government's network and computer systems. These campaigns can pose a serious threat to intellectual property, sensitive information, critical infrastructures, and national security. APTs include individuals who are nation-state actors, organised-crime group members, cyber criminals, and hacktivists (Dell 2012). APTs often use simple tools, such as Remote Access Trojans (RATs), common password-dumping and system administration tools, and simple malware (Dell 2012). However, APTs can escalate their Techniques, Tactics, and Procedures (TTPs) as necessary; they can use advanced attacks, such as customised malware and 'zero-day' (not publicly known) vulnerability exploits (Dell 2012). Furthermore, APTs can exhibit organisational sophistication, focus on specific targets, and implement well-rehearsed and coordinated attacks (Dell 2012). These malicious acts (and their actors) are persistent, as they do not give up easily and engage in repeated and coordinated attacks that will eventually be successful (RSA 2012). Moreover, APTs are professional in their approach and planning, are not deterred by obstacles, and may reorient strategies to adapt (Dell 2012). To be considered a threat, adversaries must have intent, opportunity, and capability; if any of these elements are missing the threat is negated (Ingoldsby 2013).

APT trends for 2016 suggest a landscape in which threats are increasingly common, dynamic, and highly deceptive (F-Secure 2016). Cyber-security experts have recently identified the following five APT trends: (1) more attacks, (2) more obfuscation, (3) continued false attribution, (4) greater shifts from opportunity-based attacks to more targeted attacks by non-state politically motivated adversaries, and (5) more damage that ranges from data manipulation to data encryption or deletion (F-Secure 2016).

Conventional cyber attack management is response-driven, which is an approach destined to fail, especially in curbing APTs and addressing the above-listed future trends (Cloppert 2009). Cyber-security experts agree that there is an immediate need for *anticipatory* defence measures that reflect the adaptive and dynamic nature of APTs (Hutchins, Cloppert & Amin 2011; Barnum 2012). While technical research has been active in the area of proactive security, it typically gives little weight to understanding the human aspects of cyber attacks, that is, how APTs organise, strategise, adapt, and function effectively. This paper uses a social science approach with qualitative methodologies to highlight the human aspects of cyber attacks to address three specific objectives: (1) understanding adversarial attack trajectories or intrusion chains, and the time adversaries spend on these trajectories; (2) understanding how adversaries manage attack disruptions and adapt; and (3) understanding how adversaries work in group settings.

The next section of this paper discusses the intrusion-chain model that serves as the analytical framework for this study. It then details the data collection procedures for a real-time red-team/blue-team cyber-security exercise, methodological limitations and mitigations, and the significance of qualitative research to understand cyber adversaries. In the next section, the authors first analyse their cyber-security exercise case study using the chosen intrusion-chain framework. Then the discussion turns to how adversaries manage disruptions to their attacks and how (if at all) they adapt. Next, the paper presents the authors' findings on group dynamics, such as division of labour as well as power and conflict issues. Finally, the paper concludes by offering some points for discussion and corresponding directions for future research.

Cyber-intrusion Chains

Dell's intrusion-chain model offers 12 stages as shown in **Figure 1**, below.

First, adversaries select their targets. Second, they find partners that complement and supplement their own skill sets to form alliances. In the third stage, adversaries design and build their attack vectors and/or gather toolkits necessary to execute attacks. Fourth, adversaries obtain target infrastructure blueprints, identify target vulnerabilities, and employ social-engineering practices. Fifth, adversaries gather information on any security protocols set in place by defenders they may encounter. Doing so enables adversaries to create appropriate evasion and response plans (Dell 2012). Sixth, adversaries deploy attack vectors, skills, and knowledge to gain a foothold into the target environment. In the seventh stage, adversaries gain preliminary access to the targeted environment to install malware. Adversaries establish more access points in the targeted environment in the eighth stage, while obtaining credentials to gain greater system access that will increase their control in the ninth stage. Tenth, adversaries will strengthen their presence by moving laterally and deeper into the targeted environment. This pivoting and lateral movement allows adversaries to establish control over as many different parts of the system as possible. In the eleventh stage, adversaries accomplish their objectives, such as exfiltrating data or disrupting functionality. Finally, adversaries remove evidence of their presence and actions in the targeted environment.

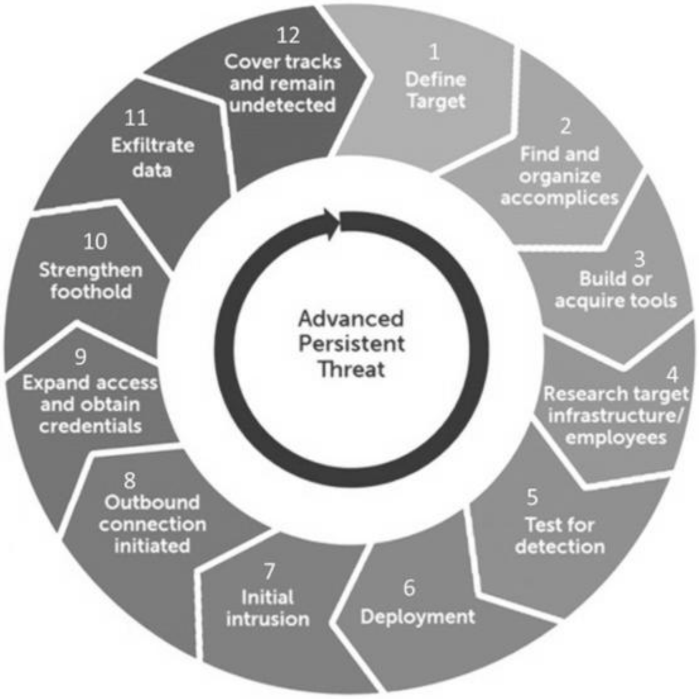
1
Define Target
2
Find and organize accomplices
3
Build or acquire tools
4
Research target infrastructure/ employees
5
Test for detection
6
Deployment
7
Initial intrusion
8
Outbound connection initiated
9
Expand access and obtain credentials
10
Strengthen foothold
11
Exfiltrate data
12
Cover tracks and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

Figure 1: Intrusion-chain model (Dell 2012)

This model serves as the analytical framework for the current discussion because it (1) provides greater depth on the intrusion stages, (2) incorporates some human aspects of the cyber attack process (for instance, stage 2: finding and organising accomplices), and (3) has a cyclical structure which addresses the possibly iterative nature of cyber attack processes.

Cyber-Security Training Exercises as Platforms for Qualitative 'Field Research'

Red-Team/Blue-Team Exercises (RTBTEs) are often used in the cyber-security arena for training purposes and involve one group of security experts (red team) attacking a computer system, while the opposing group (blue team) defends it (Mejia 2008). RTBTEs are beneficial, as they shed light on the various ways that systems can be targeted and the different TTPs that can be used in cyber attacks. Red team participants can better understand vulnerabilities, points of attacks, and best methods to secure systems. Blue team participants can learn how to defend systems in real time; how to manage limited employee and monetary resources; and how to better manage system confidentiality, integrity, and availability. RTBTEs vary in sophistication (computer systems can be simple or complex), duration (as short as a few hours to as long as two days), and players (from students and novices to seasoned security personnel or penetration testers). While RTBTEs have burgeoned for training purposes in the technical domain, they have not been widely leveraged for research purposes in the social science domain (Aoyama *et al.* 2015; Branlat *et al.* 2011; Branlat, Morison & Woods 2011). RTBTEs offer a rich platform from which to conduct 'field research' because researchers can observe human behaviour, decision-making, group dynamics, and adaptations in real time.

The United States Industrial Control Systems Computer Emergency Response Team (ICS-CERT) offers five-day cyber-security training exercises regularly, which are hosted at Idaho National Laboratory (INL), which is henceforth referred to as ICS-CERT/INL. The data presented in this paper comes from observations of the red team during days three and four (planning and RTBTE, respectively) of ICS-CERT/INL's September/October 2014 training event. The event included topics such as understanding networks, identifying and exploiting vulnerabilities, and understanding defensive tactics for critical infrastructure. For this exercise, teams were formed on day two, planning ensued on days two and three, and the RTBTE occurred on day four.

The red team was randomly created and consisted of ten members (referred to as S1 to S10 in this paper) who had not previously met one another. Team members had an assortment of jobs, such as system administrators, control systems engineers, and information technology specialists. Days three and four occurred in an enclosed room. The red team had to complete a set of predetermined tasks that varied in difficulty; each task was assigned points proportional to the level of its difficulty. Composition of the blue team was unknown to the red team (and to the authors).

The observed data were analysed by focusing, simplifying, and transforming the written-up field notes into visual representations (tables and charts), which facilitated reviewing large amounts of data efficiently (DeWalt & DeWalt 2010). Doing so allowed making comparisons, summarising patterns, drawing conclusions, and presenting effective arguments. Finally, to achieve interpretation and verification, interviews with the red team members were conducted where possible and compared to the exercise debriefing that occurred on day five. This approach was the best means of ensuring that observed data matched what the participants had experienced during the exercise.

Study Assumptions, Scope, and Limitations

The authors recognise that there are some assumptions made in this research. The lack of attack disclosure in the open literature, the covert and dynamic nature of cyber attacks, issues with attribution, and unknown adversarial characteristics collectively compound the difficulty of truly understanding the nature of APTs. However, existing research has indicated a high level of sophistication, intelligence, adaptation, and persistence (Hutchins, Cloppert & Amin 2011; Dell 2012; Barnum 2012; Ingoldsby 2013; F-Secure 2016). As such, this paper assumes adversaries are intelligent, adaptive, work in groups, and engage in dynamic decision-making. Thus, the scope of this work is within the APT landscape.

One methodological limitation is the single instance of data collection; this study is based on a single case study. Additionally, there are issues with subject availability and sampling. Researchers had no control over member selection for the red team. Red team members had never worked together, had different skill sets and comfort levels, and were working with an unfamiliar environment in a compressed time frame. Collectively, these issues may have impacted the overall performance of the red team. The authors acknowledge that different red teams, as well as different exercise structures and durations, may have generated a very different set of behaviours, group dynamics, operational strategies, and overall exercise outcomes. Furthermore, the authors recognise that a different case study may have resulted in different findings than those presented in this paper.

Finally, the findings and analysis here cannot be generalised, and are not intended to capture all possible attacks, attackers, motivations, cultures, and organisational sophistication. As with any cyber-security exercise, the ICS-CERT/INL exercise was compressed and expedited over days three and four, which is certainly not representative of how cyber attacks occur in the real world. Cyber criminals may have unlimited time and resources, elements which simply cannot be reproduced in cyber-security exercises.

While these are all legitimate shortcomings and inhibit the generalisability of the findings, the authors make the case that these limitations are typical of quantitative/hard-science research, which the current research is not intended to represent.

Significance of qualitative/social science 'cyber-field' research

This paper neither offers the typical hard-science approach of stringent quantitative or experimental research design that is replicable, nor statistical analysis that can be generalised. The work, however, is critical to advancing the human behaviour and social science research aspects of cyber security, areas that are often downplayed. 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 processes and mechanisms of human interactions, group dynamics, and adversarial intrusion chains.

The authors use a qualitative approach here, which is useful for exploratory research; they are not aware of any studies in the open literature, qualitative/social science, or quantitative/hard science that focus on the temporal analysis of adversarial intrusion chains, adaptability to disruptions, and group dynamics. As such, this research is unique and innovative, and offers a preliminary dialogue toward understanding the human element in cyber attacks. While the research analyses a single case study, the authors emphasise that access to high-quality, well-structured, government red-blue cyber-security exercises (as is the case study used here) is highly protected and rarely open to academic researchers.

Intrusion-Chain Analysis

Rege (2016) found that some intrusion stages might be more relevant than others and that this relevance could be determined by several factors, such as time, money, resources, effort, and the overall attack technique reliability/familiarity. Given the assortment of relevant factors listed, this research focuses on *one* relevant factor, namely time. Do adversaries spend more time on certain intrusion-chain stages than others?

As noted earlier, the third day of the ICS-CERT/INL five-day cyber-security training exercise focused mostly on training, preparation, and reconnaissance. More than half of the day was dedicated to building/acquiring tools (stage 3) and included activities such as undergoing tutorials on penetration techniques and sharing information on these techniques. With regards to preparation, approximately 27% of the day was spent organising accomplices (stage 2). Members were grouped based on skills and comfort zones, as detailed below in the 'Group Dynamics' section. Finally, researching target infrastructure/employees (stage 4) comprised 11% of the third day, during which red-team members worked on identifying information about the blue team and its systems. This temporal breakdown is shown in **Figure 2**, below.

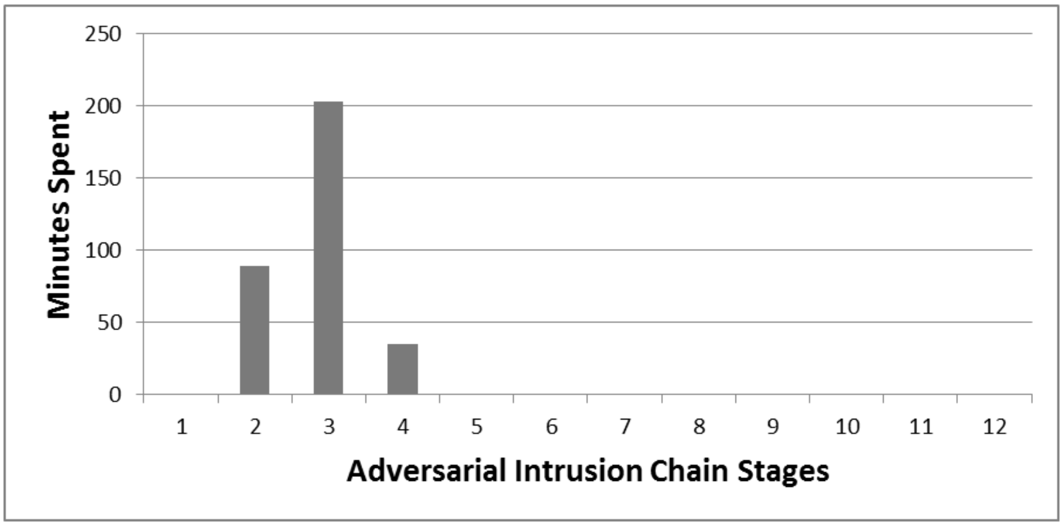

Figure 2: Time allocated to the intrusion stages on day three: planning

The actual RTBTE occurred on the fourth day. The first half of the fourth day was like the previous day, and the red team spent approximately 40% of its time on preparation, specifically on organising accomplices (stage 2), building and acquiring tools (stage 3), and researching target and infrastructure (stage 4). (See dotted box in **Figure 3**, below.) However, reconnaissance had a different flavour from the previous day as red team members performed tasks such as gathering information on, and locating IP addresses for the blue team's servers, and doing social engineering calls to deceive blue team members. Another 50% of the morning was evenly spent on expanding access (stage 9), deploying hacks (stage 6), and initial intrusions (stage 7), which is collectively shown in **Figure 3**'s solid box. Covering tracks (stage 12) and exfiltrating data (stage 11) took up minimal time, with roughly 2% and 3% respectively.

During the afternoon, the observed data indicates a shift from earlier stages to later stages of the intrusion-chain model. Only 19% of exercise time was dedicated to organising accomplices (stage 2), building and acquiring tools (stage 3), and researching target and infrastructure (stage 4), which might be indicative of the fact that most preparation, training, and forming of sub-groups based on skills and tasks had been well-established by this point in the exercise. More than 50% of the time was spent on the middle phases like deployment (stage 6), initial intrusions (stage 7), and expanding access and credentials (stage 9), which may suggest that the cyber attack was well in progress and the red team members were actively trying to accomplish their objectives (solid box in **Figure 4**, below). The authors' analysis indicated that the red team spent almost 16% of the afternoon on covering its tracks (stage 12). However, much like the morning, little time (8%) was spent on exfiltrating data (stage 11).

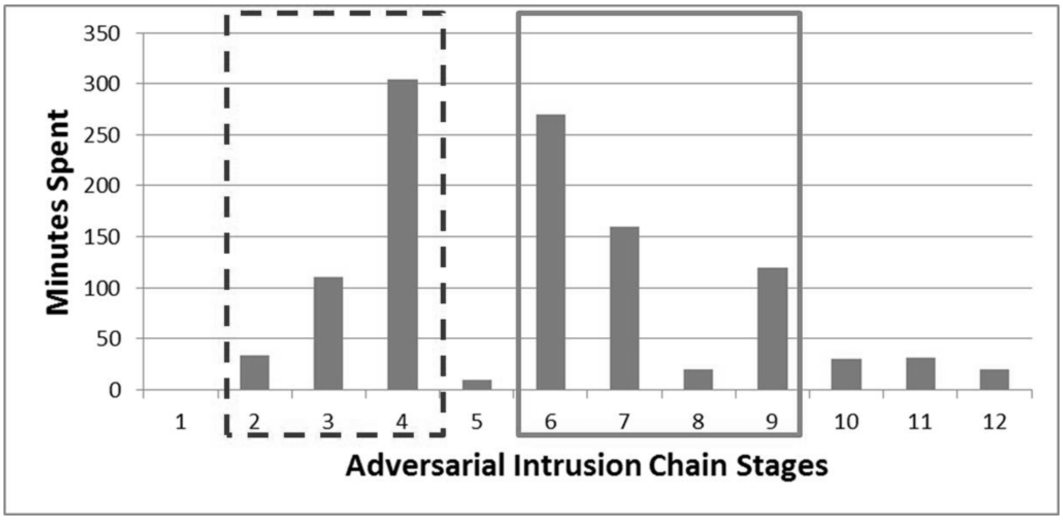

Figure 3: Time allocated to the intrusion stages on the morning of day four

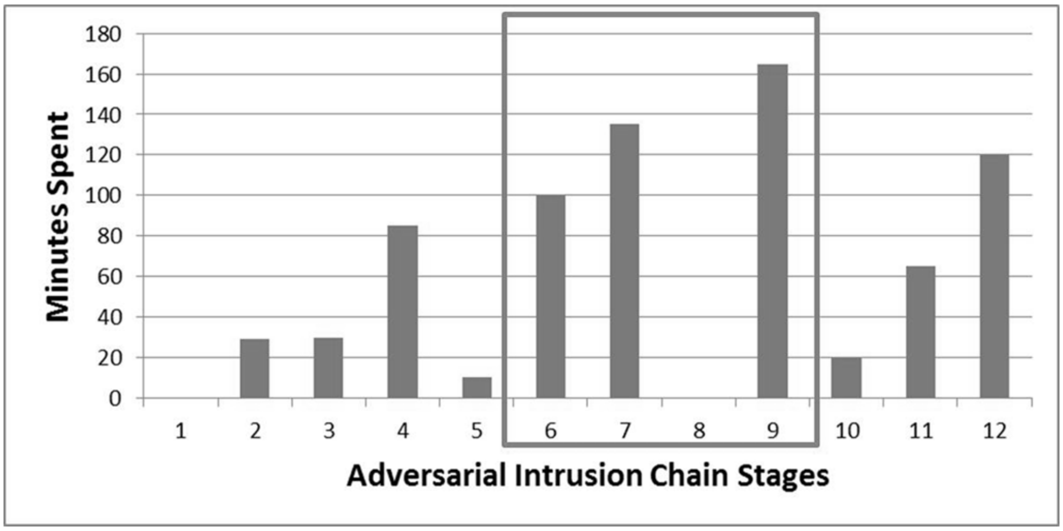

Figure 4: Time allocated to the intrusion stages on the afternoon of day four

To summarise, the cumulative temporal relevance of each stage over the third and fourth days suggests that system exploitation (deployment, initial intrusion, establishment of outbound connection, and acquisition of credentials, as shown in **Figure 5**'s solid box, below) took up roughly 44% of the exercise time. This was followed closely by reconnaissance/preparation (organising accomplices, building and acquiring tools, and researching target and infrastructure, as shown in **Figure 5**'s dotted box), which took up approximately 42% of the total exercise time. Both findings are not surprising; understanding and attacking the target system are critical to the success of any cyber attack.

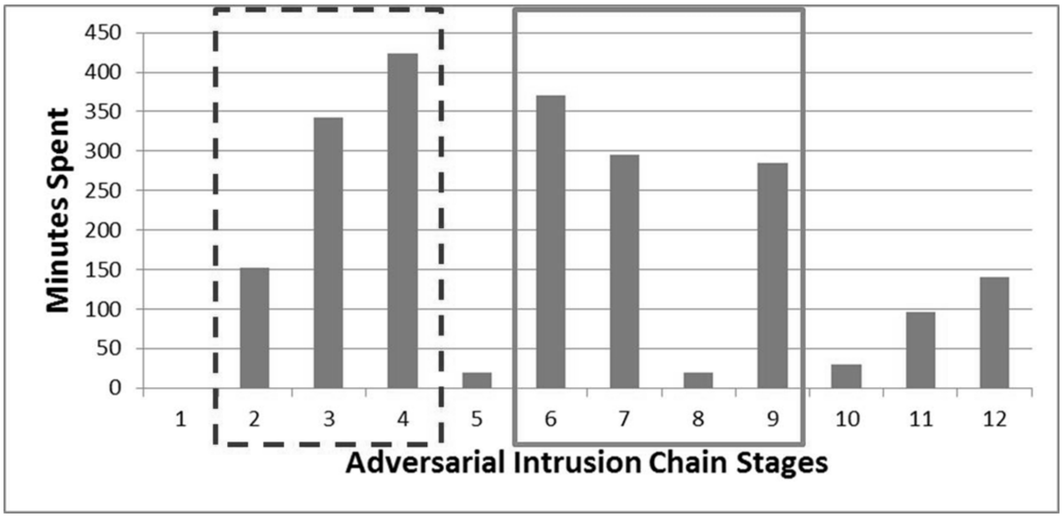

Figure 5: Combined time allocated to intrusion stages on days three and four

This research yielded some interesting findings. Prior research by Rege (2016) found that penetration testers have attributed roughly 50-75% of their temporal efforts to reconnaissance (stages 2, 3, and 4). In this research, reconnaissance only accounted for 42%. This discrepancy, however, might be indicative of methodological limitations. The dataset for this research comprises observations only; researchers did not speak with the red team members to get a better estimate of how much time they spent on reconnaissance.

Another interesting finding was the limited amount of time spent on covering tracks (stage 12 – 6%), strengthening foothold (stage 10 – 1.5%), finding and organising accomplices (stage 2 – 7%), and exfiltrating data (stage 11 – 4%). Several explanations could account for the minimal time dedicated to these stages: the attack was structured as an expedited, compressed exercise, which is not representative of reality and thus did not require covering tracks; the red team was formed randomly and members were forced to work with one another rather than having the liberty of finding the most compatible members based on skill and prior partnerships; red team members had limited knowledge bases (perhaps this particular team did not have enough knowledge of how to cover tracks, strengthen footholds, or exfiltrate data); and the exercise structure and points system were lacking (it is very likely that the exercise did not have challenges that required the red team to exfiltrate data, or did not allocate enough points to exfiltration to make it attractive for the red team to pursue).

There were three stages that had little observational data and, therefore, could not be analysed. The ‘define target’ stage was already completed before the exercise began, as the target was predetermined for the red team, and, hence, it did not spend any time on this stage. Likewise, observation did not uncover any traces of the ‘test for detection’ stage, which may be a result of the nature of the exercise. Given that there were no actual consequences resulting from being detected by the blue team, and that the exercise was compressed and expedited, the red team may not have seen the value in investing time or effort to identifying the blue team’s detection capabilities. Finally, the ‘outbound connection initiated’ stage appeared only minimally in the observational data. A possible explanation is that this stage overlapped with the ‘initial intrusion’ and ‘expand access and obtain credentials’ stages.

Adversarial Chain Disruptions and Adaptability

The red team exhibited several instances of adaptability over days three and four. The team was forced to adapt to three main types of disruptions: (1) the blue team's (defender) responses, (2) the limited knowledge possessed by its members, and (3) errors it made through its own actions. Each of these is discussed below.

Disruptions by blue team

The blue team disrupted the red team's attacks on several occasions. For instance, on Day 3 at 10 a.m., S2 reported that the blue team shut down one of his shells, which was used to maintain access to the blue team's servers. Later in the exercise, there were two reported instances of subjects being kicked off the servers they had gained access to. These blue-team disruptions and red-team adaptations are summarised below in **Table 1**.

Subject	Blue-team Disruption	Red-team Adaptation
S4	Red team misled by a Blue decoy (10 a.m., Day 3)	Searched for connection but no other adaptation; S4 encouraged by teammates to stay on task
S2	Shut down one shell (10 a.m., Day 3)	Backtracked and changed administrative password to bolster security and access
S2	"May have kicked me off" (4:10 p.m., Day 4)	No adaptation, just shrugged it off, laughed
S7	"Someone knocked me out" (3:21 p.m., Day 4)	Assessed impact level ("Good thing I deleted things when I did"); regained access, changed IP address to secure his foothold

Table 1: Blue-team disruptions and red-team adaptations

Disruptions due to limited knowledge

During the preparation and attack execution, the red team exhibited several instances of failure. Some team members had limited knowledge of when to deploy certain types of attacks and limited target knowledge, as shown in **Table 2**, below. For example, S7 was unable to gain access to one of the blue team's servers due to his limited skill level. He drew on the experience of more skilled team members to continue his task. When S4 was unsure of how to complete the task he was working on, he searched online for potential options. When S2 and S10 needed direction early on day three, S8 assumed a supervisory role and affirmed the courses of action.

Example of seeking advice from more experienced team members for limited skill set	Example of seeking confirmation from team members for limited target knowledge
S2: "Send phishing?" S10: "Should I do this?" S8: "Yes, yes do what you must!"	S2: "Are they [XYZ].com?" S1: "Don't know yet"

Table 2: Examples of limited red-team knowledge (Day 3: 7:34 a.m.)

Thus, when lack of information was the cause for poor progress, team members immediately leaned on other members for assistance or actively sought novel solutions. However, this collaboration may have been limited by the fact that the red team was randomly formed; members did not know each other and, thus, may have experienced some discomfort while seeking assistance.

Disruptions due to red team's own errors

The red team disrupted its own intrusion chains (independent of the blue team's actions), thereby, hindering its own progress. On Day 3, at roughly 1:23 p.m., S7 accidently disconnected from a server he had broken into and immediately reconnected to continue operations; he thus had to restart his task of gaining and maintaining access to the target server. Other red-team failures included members getting stuck on specific techniques and tactics, as illustrated in **Table 3**, below. Some red team members could adapt along similar techniques and tactics.

Subject	Hurdle	Adaptation
S7	Shut down his own access (1:23 p.m., Day 3)	Reconnected immediately
S6	Failed Password Attempt (1:38 p.m., Day 4)	None
S9	Failed Remote Desktop Protocol (2:40 p.m., Day 4)	None
S3, S8, & S10	Failed phishing phone call (10:20 a.m., Day 4)	Pivoted from the failed attempt and developed other phishing techniques

Table 3: Self-inflicted red-team disruptions and corresponding adaptations

Group Dynamics

Many APT cyber attacks are not conducted by individual cyber criminals, but rather by highly organised groups. Yet, very little is known about how group decision-making occurs during the planning and execution of attacks. For instance, what is the division of labour? How do power and status dynamics between team members occur? How are conflicts and tensions managed? How are threats and failures handled? How does group-member cohesiveness and interaction occur? How does the group make decisions as a whole?

Division of labour, organisation, and cohesion

At the ICS-CERT/INL event, the red team was formed randomly and members had not previously met one another (and hence had never worked together). On Day 3, which was dedicated to planning, team members discussed and assessed their backgrounds, strengths, and expertise (collectively shown in **Table 4**, below), which determined the division of labour. Tasks were mostly completed on an individual basis.

Team member S8 emerged as the team leader and requested status updates from different subgroups about the specific tasks they were working on. Interestingly, he lacked technical expertise and thus served a managerial role by engaging in task delegation, organising sub-teams based on skills and familiarity, and encouraging communication among team members to ensure that the group functioned effectively. At the same time, S8's supervisory role was rather infrequent and informal in nature. Furthermore, red team members had full autonomy on their sub-team tasks, indicating that the hierarchy of supervision was a mere symbolic token; rather, the red team exhibited a networked structure.

Subject	Backgrounds and Skill Sets
S1	Linux, Sniffing
S2	Metasploit
S3	Programmable Logic Controller (PLC) Programming, Minimal Linux, Strategy Planning
S4	Project Supervisory Control and Data Acquisition (SCADA), Metasploit, Several Capture The Flag (CTF)
S5	Cyber Security Compliance, Management, Minimal Industrial Control Systems (ICS), Networking, Switching Configurations
S6	Cyber security, Distributed Control Systems (DCS) Networks, Networking, ICS Pen Testing, Metasploit
S7	Critical Manufacturing, Systems Engineering, Programming PLC, Minimal Linux
S8	Threat Advisories/Warnings, Broad Cyber Security Knowledge
S9	PLC Connectivity, Remote iOS
S10	Network Engineering

Table 4: Red-team member backgrounds and skill sets

Sub-group membership, while initially based on common or complementary skill sets, was transient and shifting. Red team members often moved from one sub-group to another depending on where their skills or assistance were needed. A 'tag-team' operation existed, where members completed their portion of the larger task, which they handed off to the other members or sub-teams. On Day 4, for instance, S2 created a malicious Adobe PDF and handed it to S6 to upload onto a blue team's server that the latter had already compromised. This example also illustrates that continuous face-to-face and virtual communication was used. Consider the following example as well. S8 used a whiteboard to brainstorm and collaborate on hypothetical game plans and recon techniques with fellow red team members. However, he also created a group wiki to better facilitate intergroup communication.

Within and between sub-groups, there was a good overall cohesiveness despite members' having never worked together before. Even though there was some hierarchy (team leader overseeing operations and more skilled members coaching less skilled ones), it was minimal and informal; all members had an equal say in research, task execution, and determining the best courses of action.

Frustration and conflict

Team members experienced frustration throughout the exercise. S3 expressed his frustration over his limited knowledge base during the post-exercise interview, stating "Learning the IT tools while expecting to implement them quickly is frustrating. I will be of great use if we get into the ICS network". Also S3's minimal skill set was evidenced in the statement that he was "unable to establish a shell through Metasploit". However, this frustration was managed as best as possible in two main ways. First, higher-skilled team members coached lesser-skilled subjects both before and during the exercise. For instance, on Day 3, S1 trained S2, S4, S5, and S10 on how to conduct penetration testing. Second, members who became stuck during the exercise resorted to researching via Google and learning 'on-the-fly'.

On other occasions, red team members were upset when they could not continue their attacks against the blue team's systems. Some red team members were upset with their shell/access experiences. For instance, the blue team shut down S2's shell access, which S2 indicated was frustrating.

There were minor conflicts between sub-teams as to the best courses of action to achieve their specific tasks. S3 noted during an interview on Day 4, "Between myself and the other ICS guy—he claims outrageous skills but the approach is flawed". However, these conflicts were addressed quickly, with members eventually agreeing on a single course of action.

Discussion and Directions for Future Research

This paper has argued that understanding the dynamic and adaptive adversarial decision-making processes is necessary to better profile adversaries, anticipate their movements, and effectively deploy the limited security and monetary resources available to counter cyber attacks. While certainly not representative of reality, the RTBTE at ICS-CERT/INL was instrumental in gaining preliminary insights into how adversaries might adapt and manage disruptions during their attacks, and how group operations and decision-making occur to effectively maintain operations. This line of research does not intend to offer the typical statistical findings of existing empirical work; rather, it hopes to initiate a dialogue, provide a basis for further discussion, and set the context for future research.

Measuring intrusion chains

The researchers offered one means of measuring adversarial intrusion chains, namely temporal. However, the authors are aware that this was an unscientific means of measurement based solely on observations. The major limitations of the observed timestamps were the durations between them and their non-descriptiveness. For example, one observed timestamp might have been at 3:30 and the next one at 3:45, but several tasks may have occurred during these 15 minutes. Thus, accurately calculating the exact amount of time spent on any one task was problematic, resulting in time calculations which might be inaccurate. This lack of clarity, in turn, impacts discussions regarding the amount of time spent on different intrusion-chain stages.

Another issue (although not a limitation per se) was that the observations were for a group and so each timestamped observation covered 10 players. Thus, at any given timestamp, each player might have been working on a separate intrusion chain or similar ones or even multiple ones; observations simply cannot help unravel these complexities, which further impact temporal measurement.

One means of mitigating these problems in the future is to take more detailed timestamps during observations. Ideally, future research should obtain technical RTBTE logs and overlay these with the observational timestamps to better capture durations and frequencies of intrusion stages.

Measuring human behaviour

There are many other metrics that can be used to determine individual and group-based performance and decision-making. Some possible factors that impact decision-making might be the time required to execute a tactic, the amount of effort required, the monetary costs involved in implementing the tactic, and the overall reliability of that tactic to guarantee success (Rege 2016). How might these aspects be measured and used to predict adversarial behaviour (Ingoldsby 2013)? For instance, how could a cost-benefit analysis be conducted for various TTPs to identify the best one? Would it be possible to assess which intrusion-chain stages adversaries spend more time and effort on? In addition to the time spent on various stages, how do adversaries choose the optimal attack path from several different available intrusion chains? Finally, how could these different metrics be standardised, which would allow them to be effectively compared and used in computations?

RTBTEs, such as those run by ICS-CERT/INL, can be modified in future research with permutations and combinations designed to study adversarial movements and the underlying decisions associated with those movements. For instance, RTBTE experiments can be set up with different objectives, teams, and roadblocks to better comprehend the complexity of human decision-making. More specifically, these experiments could manipulate: (1) adversary-specific variables, such as time, effort, skills, knowledge, and motivations; (2) system-specific variables, such as architecture and vulnerabilities; and (3) defender-specific variables, such as response time, response action, and adversarial deception. Manipulating these variables over several different experimental designs can generate larger datasets that could shed light on adversarial behaviours and movements.

Bringing qualitative research into the cyber-security domain

Experimental methods are touted as being the preferred strategy for causal investigations, while qualitative methods are considered descriptive and rudimentary and, therefore, best used to merely supplement scientifically rigorous quantitative methods (Maxwell 2004; Howe 2004; Dunning 2008; Prowse & Camfield 2013). However, this viewpoint largely ignores the unique contributions that qualitative methods make to causal investigation. First, qualitative research is process-oriented and answers the ‘Why?’ or ‘How is something happening?’ questions, unlike randomised experiments, which merely offer a very “gappy, black box account” by answering questions such as ‘What is happening?’ and ‘Is there a systematic effect?’ (Howe 2004, p. 47;

Maxwell 2004; Dunning 2008; Prowse & Camfield 2013). Qualitative research is ideal for acquiring a better understanding of how adversaries engage in a strategic, decision-making process in cyber attacks (Prowse & Camfield 2013). Qualitative research is effective in unpacking these process mechanisms, offering insights into unanticipated relationships, and developing new insights (Maxwell 2004).

Merging qualitative research methods, such as field research, observations, and interviews, with quantitative methods, such as agent-based modelling, simulations, and time-series analysis, could offer unique insights into understanding adversarial behaviour, movement, and adaptability. There is already multidisciplinary research that marries observed data with time-series analysis on the dataset used in this paper. This joint research provided preliminary answers to the following questions:

- Do adversaries move to certain stages when their actions are disrupted?
- If so, how much time do they spend on these stages?
- If adversaries are interrupted at different points in the intrusion chain, do they focus on different stages, and how much time is spent on these stages (Rege *et al*. forthcoming)?

Future research should embrace such multidisciplinary approaches as they offer unique insights which cannot be attained by siloed disciplines and methods alone. Understanding and anticipating adversarial behaviour is essential to generating a cyber-security paradigm shift, one that moves away from reactionary measures and embraces predictive or anticipatory ones. Doing so will allow defenders to be as dynamic and adaptive as the adversaries they are trying to manage.

Acknowledgements

This material is based upon work supported by the National Science Foundation (NSF) CAREER Award No. 1453040 and partially by NSF Award No. 1446574.

The authors thank the Industrial Control Systems Computer Emergency Response Team (ICS-CERT) and Idaho National Laboratory (INL) for allowing data collection at their September/October 2014 Red-Team/Blue-Team cyber security training exercise.

References

Aoyama, T, Naruoka, H, Koshijima, I, Machii, W, & Seki, K 2015, 'Studying resilient cyber incident management from large-scale cyber security training', *Proceedings of the IEEE 10th Asian Control Conference (ASCC)*, pp. 1-4.

Barnum, S 2012, *Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™)*, MITRE Corporation, viewed 5 March 2014, <http://www.mitre.org/sites/default/files/publications/stix.pdf>.

Branlat, M, Morison, AM, Finco, GJ, Gertman, DI, Le Blanc, K, & Woods, DD 2011, 'A study of adversarial interplay in a cybersecurity event', *Proceedings of the 10th International Conference on Naturalistic Decision Making*.

Branlat, M, Morison, A, & Woods, DD 2011, ‘Challenges in managing uncertainty during cyber events: lessons from the staged-world study of a large-scale adversarial cyber security exercise’, *Proceedings of the Human Systems Integration Symposium*, pp. 10-25.

Cloppert, M 2009, ‘Security intelligence: attacking the cyber kill chain’, viewed 2 February 2014, <http://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain>.

Dell 2012, ‘Lifecycle of an Advanced Persistent Threat’, viewed 19 September 2013, <http://www.redteamusa.com/PDF/Lifecycle%20of%20an%20Advanced%20Persistent%20Threat.pdf>.

DeWalt, KM & DeWalt, BR 2010, *Participant observation: a guide for fieldworkers*, Rowman Altamira, Plymouth, U.K.

Dunning, T 2008, *Natural and field experiments: the role of qualitative methods*, viewed 24 November 2012, <http://www.thaddunning.com/wp-content/uploads/2009/12/DesignBased_QualMethods_v2.pdf>.

F-Secure 2016, ‘5 Advanced Persistent Threat trends to expect in 2016’, viewed 7 April 2017, <https://business.f-secure.com/5-advanced-persistent-threat-trends-to-expect-in-2016>.

Howe, K 2004, ‘A critique of experimentalism’, *Qualitative Inquiry*, vol. 10, no. 1, pp. 42-61.

Hutchins, E, Cloppert, M & Amin, R 2011, *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains,* viewed 25 January 2012, <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, Calgary, Alberta, Canada.

Maxwell, JA 2004, ‘Causal explanation, qualitative research, and scientific inquiry in education’, *Educational Researcher*, vol. 33, no. 2, pp. 3-11.

Mejia, R 2016, ‘Red team versus blue team: how to run an effective simulation’, viewed 15 February 2016, <http://www.csoonline.com/article/2122440/disasterrecovery/emergency-preparedness-red-team-versus-blue-team-how-torun-an-effective-simulation.html>.

Prowse, M & Camfield, L 2013, ‘Improving the quality of development assistance: what role for qualitative methods in randomized experiments?’, *Progress in Development Studies,* vol. 13, no. 1, pp. 51-61.

Rege, A 2016, ‘Incorporating the human element in anticipatory and dynamic cyber defense’, *Proceedings of the IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, pp. 1-7.

——, Obradovic, Z, Asadi, N, Singer, S & Masceri, N forthcoming, ‘A temporal assessment of cyber intrusion chains using multidisciplinary frameworks and methodologies’, *Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, IEEE, Xplore Digital Library.

RSA 2012, ‘Stalking the kill chain’, viewed 31 March 2014, <http://www.emc.com/rsa>.