A Temporal Assessment of Cyber Intrusion Chains Using Multidisciplinary Frameworks and Methodologies

Aunshul Rege[1], Zoran Obradovic[2,3], Nima Asadi[2], Brian Singer[1], and Nicholas Masceri[1]

[1]Department of Criminal Justice, Temple University
[2]Computer and Information Sciences Department, Temple University
[3]Data Analytics and Biomedical Informatics Center, Temple University

***Abstract*—Current approaches to cybersecurity are response-driven and ineffective as they do not account for adaptive adversarial behavior and dynamic decision-making. Using empirical evidence of observations done at the US Industrial Control Systems Computer Emergency Response Team's (ICS-CERT) Red Team-Blue Team cybersecurity training exercise held at Idaho National Laboratory (INL), this paper identifies how adversaries carry out, and adapt during, cyberattacks. This paper employs a unique mixed methods approach of qualitative observations and quantitative data science to address three objectives: (i) providing a quantitative framework for temporal analysis of the cyberattack processes by creating a time series representation of the qualitative data, (ii) employing data science methods, such as hierarchical clustering analysis, on the generated time series data to complement and supplement our understanding of cyberattack processes, and (iii) understanding how adversaries adapt during the disruptions by defenders.**

***Keywords*—adaptive human behavior, dynamic decision-making, mixed methods, temporal analysis, clustering**

I. Introduction

In 2016, the cyberthreat landscape showcased advanced attack techniques, escalated attack frequency, and high levels of adversarial sophistication [12]. Conventional cyberattack management is response-driven, with organizations focusing their efforts on detecting Indicators of Compromise, or threats [12]. This reactive approach has limited efficacy, as it does not capture advanced and sophisticated adversaries, mutating or unknown malware, living-off-the-land techniques or new variants being deployed [5],[12]. Furthermore, responding to incidents after the attack has occurred is costly for two reasons. First, the attack has successfully taken place and damage has occurred in the form of data theft, system manipulation, service/functionality disruption, or the like, which is costly to fix [2]. Second, during the attack, the adversary may have established several footholds in different parts of the targeted system. Identifying and eradicating these footholds are costly with regards to manpower and time [2]. The average time taken to identify and contain data breaches caused by malicious or criminal attacks was 229 and 82 days respectively and cybercrime detection and recovery activities accounted for more than 55 percent of total internal company activity costs in FY 2016 [11]. US organizations had the highest average cost of cybercrime ($17.36 million), with cybercrime costs in Germany and the UK averaging at $7.84 million and $7.21 million respectively [11].

There is thus an immediate need for a paradigm shift in the area of cybersecurity; security experts are calling for anticipatory or proactive defense measures that focus on Indicators of Attack that identify adversarial behavior and movement [2], [10], [12]. Doing so requires an understanding of the human agents conducting cyberattacks and their adaptive decision-making capacities, which are currently downplayed in existing technical research.

Using a criminological framework and empirical evidence of observations done at the US Industrial Control Systems Computer Emergency Response Team's (ICS-CERT) Red Team-Blue Team cybersecurity training exercise held at Idaho National Laboratory (INL), this paper addresses three objectives: (i) providing a quantitative framework for temporal analysis of the cyberattack processes by creating a time series representation of the qualitative data, (ii) employing data science methods, such as hierarchical clustering analysis, on the generated time series data to complement and supplement our understanding of cyberattack processes, and (iii) understanding how adversaries adapt during the disruptions by defenders.

This paper is structured as follows. Section 2 offers a brief overview of the Criminological framework of crime scripts and the corresponding technical model of intrusion chains to discuss adversarial attack paths. The third section outlines the mixed methodology of observations and time series analysis. Next, the observational, time series, and clustering results are discussed and what these might mean for adversarial adaptations. Finally, this paper discusses relevant findings and possible implications for the intrusion chain model, as well as the importance and temporal characteristics of certain intrusion stages.

II. Criminological Crime Scripts and Technical Adversarial Cyber-Intrusion Chains

In the criminological discipline, *crime scripts* identify every stage of the crime-commission process and the decisions and actions that are needed at each stage [3], [6], [7]. Several crime scripts have been produced to account for robbery and vehicle theft [6], employee cybercrimes [17], explosive attacks [4], organized crime [8], illegal waste dumping [16] and wildlife poaching [9]. However, the application of crime scripts to cyberattacks as they unfold remains understudied.

Interestingly, the technical domain offers intrusion chain mod-

els that capture the step-by-step process of cyberattacks [2], [5], [10]. We use the 12-step cyberintrusion chain model by [5] (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 [1]. (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 the target's security controls and procedures that they are likely to encounter, so that they can create appropriate evasion and response plans [1]. (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: Cleanup 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.

Fig. 1. Intrusion Kill Chain Model [5]

III. Methodology

We employ a mixed methodology combining qualitative methods of observations coupled with quantitative data science methods. The United States Industrial Control Systems Computer Emergency Response Team (ICS-CERT) offers cybersecurity training events hosted at Idaho National Laboratory (INL) (henceforward referred to as ICS-CERT/INL). Data were collected at ICS-CERT/INLs five day September/October 2014 training event, which covered topics such as understanding networks, identifying vulnerabilities and how to exploit them, understanding defense tactics for critical infrastructure. The training culminated in a Red Team/Blue Team exercise (RTBTE) where participants could apply their training, knowledge and skills. For this particular 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 created randomly, had ten members who were a mix of system administrators, control systems engineers, and information technology specialists. The data presented in this paper are from observations of the Red Team during days three and four (planning and RTBTE respectively). The data were analyzed by transforming the written up field notes into tables, which allowed for comparisons, summarizing patterns, drawing conclusions, and presenting effective arguments.

The temporal analysis of a process is aimed to reveal the actionable trends, patterns, and variations within the process. Data mining techniques can then be used to extract discriminative patterns and characteristics in the data. In order to develop such a framework to characterize the Red Team's activities throughout the exercise, the collected qualitative observational data were converted to time series using the time stamps and durations of the intrusion stages. The idea behind this representation is to achieve a quantitative temporal analysis of various aspects of the data, including the adaptation strategies adopted by the Red Team in order to avert disruptions from the Blue Team, and the trends in the teams general decision making and planning behavior. This conversion provides a new perspective into the

process which is computationally more instrumental for data mining techniques such as clustering, feature selection, and classification.

In order to obtain the time series, we used the time stamps of the start and end times of the intrusion stages which were recorded in the observational data. Each time point in the time series represents 15 minute time spans throughout the exercise. Therefore, for each time point, the value of each time series is determined by accumulating the number of minutes spent by the Red Team on its corresponding intrusion stage. Figure 2 shows an example of a time series generated based on this approach. After achieving the time series data, we were able to perform temporal analyses of the intrusion stages using data mining techniques. Measuring temporal correlations between the time series representation of intrusion stages can reveal valuable knowledge about the codependence of intrusion stages, which might in turn be used to develop a more substantial intrusion chain or to understand the team's movements throughout the attack period. In our study, clustering of temporal signals is used as a tool for achieving an interpretable and verifiable quantitative measurement of such correlations. Through the process of clustering, the time series are partitioned into several groups based on their similarity. In our case, the similarity in time series is measured by comparing the total amount of time allocated to each intrusion stage by the Red Team within each 15 minutes time span. These comparisons are then summed throughout the whole exercise time to achieve a similarity value between each pair of time series, and therefore, place them in groups of similar time series. Therefore, a high similarity between the time series representation of the intrusion stages A and B is an indication of the fact that the time allocation for stages A and B showed similar patterns within the 15 minute time spans throughout the exercise. In other words, similar time series have a closer amplitude than other time series throughout the exercise period, i.e. whenever intrusion stage A occurs, the possibility of occurrence of stage B during the same 15 minute time span with a close total amount of allocated time is higher than the possibility of occurrence of any other intrusion stage. This analysis provides a better perspective into the temporal patterns of the intrusion stages throughout the exercise period which is difficult to obtain via pure observation. Especially, other studies with larger datasets can benefit from this computational approach due to the fact that discovering knowledge form mere observation can be rather difficult in their case.

In this work we used Agglomerative hierarchical clustering[13] to discover temporal similarities between different stages. The Agglomerative hierarchical clustering is a bottom up approach where pairs of clusters are merged to move up the similarity hierarchy. In order to quantify the similarities among the stages, we measured the Euclidean distances between the time series of the stages. As depicted in Figure 3, the Euclidean distance between two time series is calculated by measuring the distance between the amplitudes of the two time series at each time point, and then adding the distances together to obtain one value, which is the distance value. The distances between the time series are then compared by the clustering model to find the pair of time series (stages) with the smallest distance, which corresponds to the largest similarity value. The

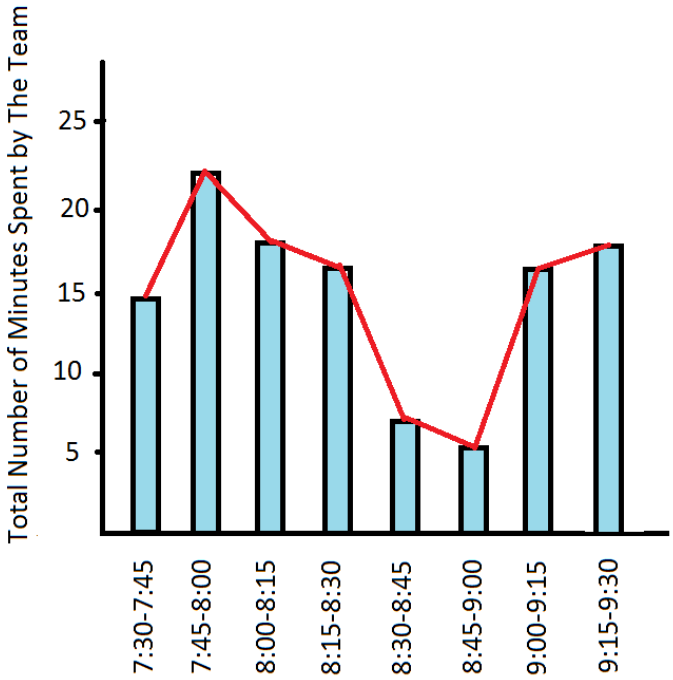

Fig. 2. Time series generated using the accumulated number of minutes spent by the entire team on an intrusion stage within each 15 minutes time interval

reason behind selecting this clustering technique is its power in providing an interpretable depiction of the clusters which includes the order and hierarchy of the clusters, and the fact that no apriori information about the number of clusters are required.

We then focused on creating a quantitative framework for understanding the adaptation measures that the Red Team chose to take when facing disruptions from the Blue Team. In order to achieve this goal, we employed the time series representations of the intrusion stages that we created previously by detecting their local peaks. From a mathematical point of view, a local peak in the time series of the intrusion stages represents a local maxima in the total number of minutes allocated by the Red Team to the intrusion stages. For this study, we used the Peak-Valley detection algorithm [14], [15] for detecting the peaks. The quantitative framework for peak detection can also be of high value for other studies where the observational data is large or the observation time span is longer, and thus, it is difficult to observe the local maxima in the data easily. The peak analysis is beneficial for understanding the adaptation measures that the Red Team decided to take. Therefore, we can observe the shifts in focus from one stage to another by

$$D(Q,C) \equiv \sqrt{\sum_{i=1}^{n}(q_i - c_i)^2}$$

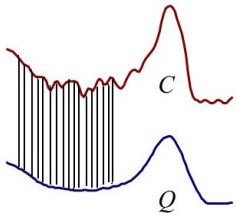

Fig. 3. Measuring the Euclidean distance for two time series Q and C

the Red Team when encountering a disruptive attempt by the Blue Team. This observation helps us pinpoint and focus on the intrusion stages which are of more importance during the adaptation process. The main reason for putting our emphasis on the selected intrusion stages is that the recurrence of only those stages upon discovering a disruption can provide a more focused and precise framework for understanding the attackers adaptation process.
In order to select the intrusion stages that occurred during the adaptation period, we focused on the peak values that were above the global mean of the time series. The global mean of the time series is measured as the average of the mean of all time series within each 15 minute time span. The reason for selecting this global mean value as the threshold is to filter out the values that are small (i.e. the Red Team put little time on them) and keep the significant values for further analysis.

IV. Results

A. Characterization of the Adversarial Intrusion Chain Using Observational Data

The total amount of time spent by the Red Team on each intrusion stage throughout the whole exercise period is provided in Figure 4. The observational data suggest that system exploitation (deployment, intrusion, outbound connection or expand access and obtain credentials) took up roughly 44% of the exercise time or 970 minutes. This was followed closely by reconnaissance/preparation (organize accomplices, build and acquire tools, and research target and infrastructure), which took up approximately 42% of the total exercise time. Both of these are not surprising as understanding and attacking the target system are critical to the success of any cyberattack.

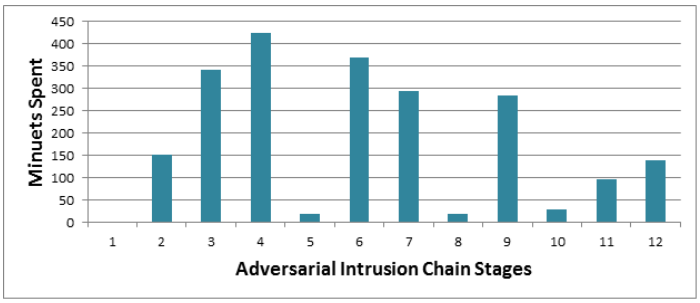

Fig. 4. Adversarial Intrusion Chain Stages: 1. Define Target; 2. Find and Organize Accomplices; 3. Build or Acquire Tools; 4. Research Target Infrastructure/Employees; 5. Test for Detection; 6. Deployment; 7. Initial Intrusion; 8. Outbound Connection Initiated; 9. Expand Access and Obtain Credentials;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

B. Conversion to Time Series

For temporal data analysis, the time stamps of the observed events were converted into time series. Figure 5 shows the resulting time series created for each stage of the RTBTE, where each time interval represents a 15-minute time span, and the value in each interval represents the total time spent by the entire team on that specific stage within the time span. The time series span from the morning until the evening of the RTBTE. This figure excludes the time series belonging to stage 1 (Define Target) described in Figure 1, as the target was predetermined by the exercise coordinators and thus the Red Team did not spend any time on this stage. The start time of the RTBTE shown at Figure 5 is 7.30am until 4.45pm. Please note that in this representation more than two hours were spent on doing research within the initial 60 minutes of the exercise. This is because the number of minutes each of the ten Red Team members spent doing research was added together. Thus, if first member spent 30 minutes, the second spent 10 minutes, the third spent 20 minutes, the fourth spent 10 mins (and so on), the total time spent would amount to well over an hour.

C. Clustering Results

The clustering results are presented in the dendogram in Figure 6 where the Euclidian distances between the time series are measured and used to create the clusters. The vertical axis in the dendogram corresponds to the Euclidian distance between each pair of time series within the clusters. This distance measure is explained in the methodology. When two time series Q and C are placed in one cluster, it means that the intrusion stage Q has the most similar temporal pattern to intrusion stage C as compared to other intrusion stages. In other words, similarity in temporal patterns of two intrusion stages means that the two time series have overall close shapes throughout the length of the time series, i.e. the peak/valley patterns in the two time series are more similar than other time series. Therefore, the result of this clustering analysis provides a measure for the correlation between the intrusion stages throughout the exercise period.
To choose which cluster stages should finally be considered as one group depends on our selection of the clustering threshold. We place the threshold at the middle of the largest distance which results in the red threshold line in Figure 6. This means that we can consider the clusters under this threshold as one cluster which includes stages 3, 4, 6, and 7 in one cluster, 9 and 10 in another one, and finally 11 and 12 in a yet another cluster due to fact that the distance between these three groups falls under the clustering threshold. These results show that there are similarities in the temporal peak/valley patterns among the mentioned time throughout the exercise period. In other words, for instance, the occurrence of intrusion stage 3 (a peak in its time series), is more likely to be accompanied by the occurrence of the stages 4, 6, and 7 than any other intrusion stages.
This analysis provides new demonstrable knowledge about the relations and dependencies among intrusion processes, which can help us with developing more precise and efficient anticipatory measures as well as suggesting more substantial and realistic intrusion models.

D. Adaptation Analysis via Peak Detection

The local peaks in the time series can also be observed in Figure 5 as well as the global mean value which is depicted by the horizontal red line in Figure 6. To understand the Red Team's decision making process during the adaptation, we analyze the time series data in the one hour time span after two disruptive events, caused by the Blue Team, create difficulties for the Red Team. The first disruption by the Blue Team was an attempt to mislead the Red Team with a decoy within the 10:00-10:15 AM time span. The second disruption occurred when a shell was shut down by the Blue Team, within

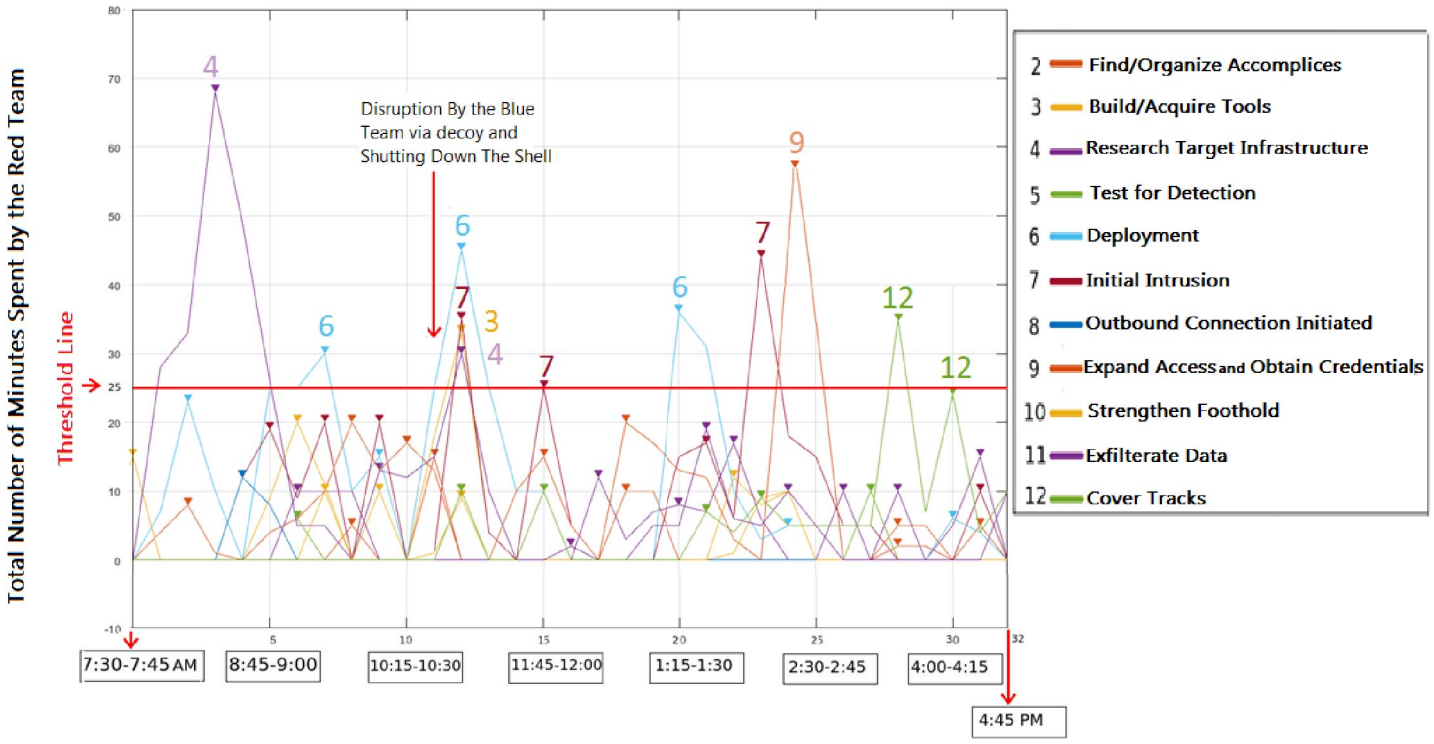

Fig. 5. Time series representation of the Red Team's data for the RTBTE. The numbers on the time series correspond to their intrusion stage in the legend. The values on the vertical axis correspond to the total number of minutes spent by the Red Team within each 15 minute time span.

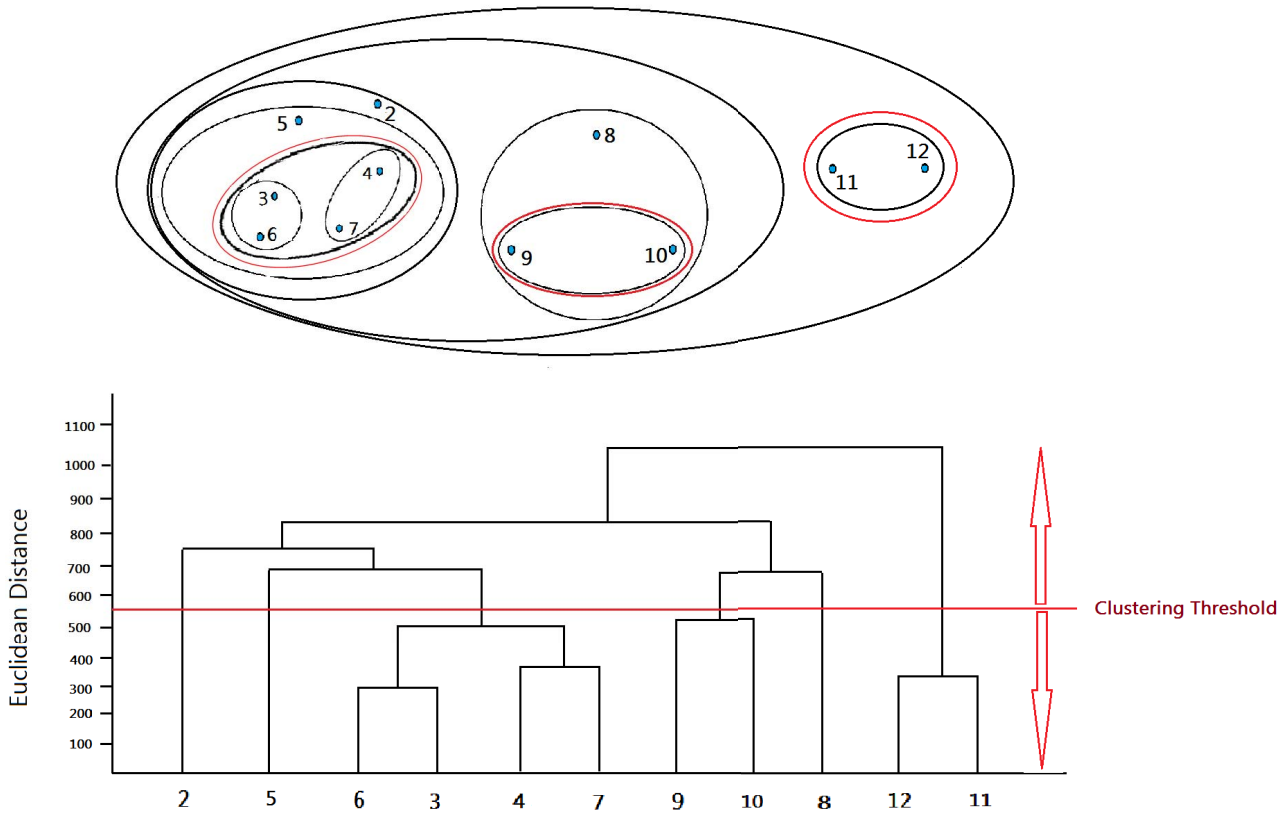

Fig. 6. Hierarchical clustering of the time series where each number corresponds to the intrusion stage number (refer to Figure 1). The clustering threshold is the middle value of the maximum distance. The red clusters in the top figure are the ones within the clustering threshold.

Subject	Blue Team Disruption	Adaptation
Subject 4	Red Team misled by a Blue decoy (10am-10:15am)	Googled for connection but no other adaptation; no change in morale, met with encouragement from teammates to stay on task
Subject 2	Shut down one shell (10am-10.15am)	Backtracks and changes administrative password to bolster security and access

TABLE I. BLUE TEAM DISRUPTIONS AND RED TEAM ADAPTATIONS

the same time span, in order to block the Red Team's access to the system. These events are pointed out in Figure 5 as well as in Table 1 which includes the adaptation measures in the observational data. As we can observe in Figure 5, these disruptions led the Red Team to shift its focus and re-execute some of the stages with a different plan. We observe that during the one hour period after detecting the disruption (Blue Team decoy and shell shutdown), stage 3 (Build/Acquire Tools), 4 (Research Target Infrastructure), 6 (Deployment), and 7 (Initial Intrusion) were highly focused on. The possible reasons behind the reoccurrence of the mentioned four stages after the disruptions can be explained through the description of the stages provided in the introduction section of this paper. In this regards, one can reasonably hypothesize that when a shell is shut down by the Blue Team, the Red Team tries to regain its access to the system, therefore, stages 3 (Build/Acquire Tools) and 4 (Research Target Infrastructure) are noticeably emphasized on. Also, the decoy sent by the Blue Team was aimed to disrupt the Red Team's effort for deployment (stage 6), and initial intrusion (stage 7), thus these two stages were focused on within the one hour time span after the disruption. However, precise and verifiable distinction of the reasoning and motivations behind the significant reoccurrence of these four stages requires further inquiry.

The horizontal threshold line in Figure 5 indicates the threshold line (global mean of 25 minutes total engagement per 15-minutes interval). As discussed in the methodology, this threshold is used to methodologically filter out the negligible events within each time span. We can observe that during the adaptation process, within the hour after the disruption event, the amount of time allocated to the four mentioned intrusion stages was above this average value at multiple intervals while time devoted to other stages has never exceeded the average. This means that these four stages played the most important role in the adaptation period. This analysis provides empirically testable knowledge into the adaptation of the Red Team, which can be beneficial for understanding and predicting the adversarial teams behavior when encountering disruptions.

V. CONCLUSION

This paper offers a preliminary examination of real-time adversarial movement across the cyber intrusion chain. There are some obvious and unavoidable limitations. First, the analysis put forth in this paper is based on a single case study, which has obvious implications for generalizability and validity. There are many permutation and combinations of attack scenarios, adversarial types and motivations, objectives, and organizational dynamics, which cannot be accounted for by this single case study. Second, this study is based on very limited data and much more observations would be needed to better characterize the intrusion chain analysis. While these are indeed valid limitations, this paper is exploratory in nature with the goal of temporally characterizing intrusion chain stages via hierarchical clustering of multivariate longitudinal observations. Furthermore, while this paper uses a single case study, it is one of the most reputable and well-established Red Team/Blue Team exercises (RTBTE) in the United States.

More importantly, this research offers methodological innovation; it combines qualitative observations and quantitative data science techniques to temporally characterize the intrusion chains stages, which cannot be attained by either method alone. The observational data give insight into real-time human behavior and adaptation as the cyberattack unfolds. Researchers rarely get access to real cyberattacks as they occur. This case study, while compressed and expedited, offers a unique insight into the dynamics of adversarial movement and adaptability. When these observational data are translated to quantitative, data science methods are employed to obtain verifiable and substantial insights into the temporal characteristics of the intrusion process.

Finally, this study also offers advancement in better assessing the intrusion chain model and the time spent by adversaries on the various stages. Based on this preliminary assessment, it appears that the intrusion stages 3 (Build/Acquire Tools), 4 (Research Infrastructure), 6 (Deployment), and 7 (Initial Intrusion) display similar overall temporal traits throughout the exercise period. This means that the occurrence of one of these four intrusion stages is more likely to be accompanied by the occurrence of the other three stages than any other intrusion stage. Identifying these temporal relations and dependencies among the intrusion stages provides a wider outlook into understanding and development of more accurate and informative intrusion models. Furthermore, the results of the peak analysis on the time series data can help with anticipating and pinpointing specific intrusion stages that play a significant role during the adaptation process, and thus dedicating the effort and attention on them, resulting in a more efficient and anticipatory defense mechanism against such cyberattacks.

ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation CAREER Award, Grant No. CNS1453040 and partially by National Science Foundation CPS Award, Grant No. 1446574. The authors thank the Industrial Control Systems Computer Emergency Response Team (ICSCERT) and Idaho National Laboratory (INL) for allowing data collection at their September/October 2014 Red Team/Blue Team Cybersecurity Training Exercise.

REFERENCES

[1] DELL 2012. *Lifecycle of an Advanced Persistent Threat*. http://www.redteamusa.com/PDF/Lifecycle\%20of\%20an\%20Advanced\%20Persistent\%20Threat.pdf. Accessed: 2016-12-20.

[2] S. Barnum. *Standardizing cyber threat intelligence information with the Structured Threat Information eXpression*. http://www.mitre.org/sites/default/files/publications/stix.pdf.

[3] H. Borrion. "Quality assurance in crime scripting". In: *Crime Science* 2.1 (2013), p. 1.

[4] R. Clarke, Victor G., and G. Newman. *Outsmarting the terrorists*. Greenwood Publishing Group, 2006.

[5] M. Cloppert. *Security Intelligence: Attacking the Cyber Kill Chain*. http://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain. Accessed: 2014-02-02.

[6] D. Cornish and B. Derek. "The procedural analysis of offending and its relevance for situational prevention". In: *Crime prevention studies* 3 (1994), pp. 151–196.

[7] D. Cornish and M. Felson. "Introduction: Criminology, Routine Activity, and Rational Choice." In: *Advances in Criminological Theory* 5 (2008), pp. 1–14.

[8] G. Hancock and G. Laycock. "Organised crime and crime scripts: prospects for disruption". In: *Situational prevention of organised crimes* (2010), pp. 172–193.

[9] J. Hill, S. Johnson, and H. Borrion. "Potential uses of computer agent-based simulation modelling in the evaluation of wildlife poaching". In: *Situational Prevention of Poaching* (2014), pp. 120–153.

[10] E. Hutchins, M. Cloppert, and Amin R. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed: 2012-01-25.

[11] Ponemon Institute. *2016 Cost of Data Breach Study: Global Analysis*. https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf. Accessed: 2017-10-01.

[12] A. Kulkarni. *The Five Core Components of Proactive Cybersecurity*. http://www.techzone360.com/topics/techzone/articles/2016/12/05/427743-five-core-components-proactive-cybersecurity.htm. Accessed: 2016-12-05.

[13] O. Maimon and L. Rokach. *Data mining and knowledge discovery handbook*. Vol. 2. Springer, 2005.

[14] Z. Nopiah et al. "Peak-valley segmentation algorithm for fatigue time series data". In: *WSEAS Transactions on Mathematics* 7.12 (2008), pp. 698–707.

[15] R Schneider. "Survey of Peaks/Valleys identification in Time Series". In: *Department of Informatics, University of Zurich, Switzerland* (2011).

[16] L. Tompson and S. Chainey. "Profiling illegal waste activity: using crime scripts as a data collection and analytical strategy". In: *European Journal on Criminal Policy and Research* 17.3 (2011), pp. 179–201.

[17] R. Willison and M. Siponen. "Overcoming the insider: reducing employee computer crime through Situational Crime Prevention". In: *Communications of the ACM* 52.9 (2009), pp. 133–137.