Analysis of Adversarial Movement Using Network Structure

Nima Asadi[1], Aunshul Rege[2], and Zoran Obradovic[1,3]

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

***Abstract*—Capturing the patterns in adversarial movement can provide valuable information regarding how the adversaries progress through cyberattacks. This information can be further employed for making comparisons and interpretations of decision making of the adversaries. In this study, we propose a framework based on concepts of social networks to characterize and compare the patterns, variations and shifts in the movements made by an adversarial team during a real-time cybersecurity exercise. We also explore the possibility of movement association with the skill sets using topological sort networks. This research provides priliminary insight on adversarial movement complexity and linearity and decision-making as cyberattacks unfold.**

***Keywords*—adaptive human behavior, network theory, social network, dynamic decision-making, mixed methods**

I. Introduction

Cyberadversaries execute their attacks in discernible stages, known as the intrusion chain model. There are multiple intrusion chain models in the open literature [1],[2],[3],[4],[5] all with varying details (number/depth of stages) and structure (sequential vs. iterative). For instance, the model provided in Figure 1 is thorough, cyclical, and even captures human aspects of cyberattacks (stages 2 and 4) [11]. While intrusion chain models were intended to provide incident responders with a framework for reasoning about intrusions, it can serve as a foundation to delve deeper into how cyberadversaries progress through a cyberattack. Furthermore, sophisticated attacks may be conducted by groups of cyberadversaries; Advanced Persistent Threats, such as nation-state actors, organized crime groups, cybercriminals, and hacktivists are a case in point [4]. How might an intrusion chain model capture multiple adversaries acting as a single group? This paper uses data from a cybersecurity exercise to examine how cyberadversaries working as a group progress through intrusion chains, whether their skill set impacts movement across the chain, and whether there are similarities in the group member movements.

This paper is structured as follows. In the next section, we discuss the mixed-methods approach to this paper. We discuss the qualitative data collected during a real-time cybersecurity exercise. We also discuss topological sort networks, graph similarity measures, and structural comparisons techniques. We discover that adversarial movement is not linear and is not necessarily associated with skill sets.

II. Methodology

A. Case Study Data

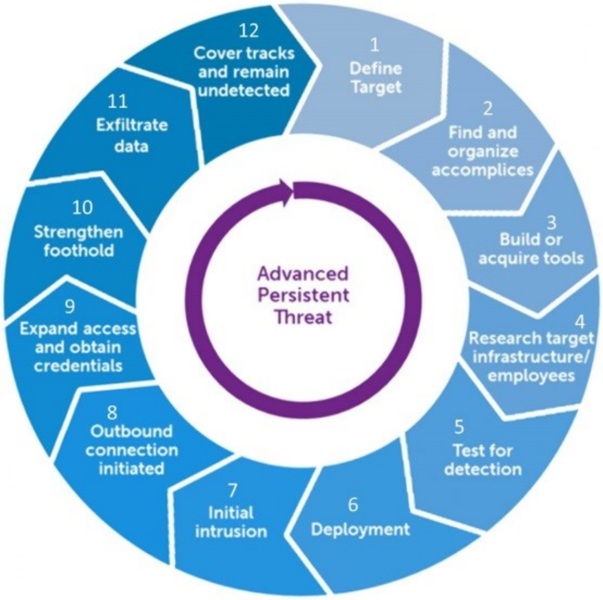
In September 2014, a five-day cybersecurity training event was run by the Industrial Control Systems-Cyber Emergency Readiness Team (ICS-CERT) held at Idaho National Laboratory(INL), which is henceforward referred to as ICS-CERT/INL. The first three days covered basic training for all participants, such as understanding networks, identifying vulnerabilities and how to exploit them, and comprehending defense tactics for critical infrastructure. Participants then implemented their training by participating in an eight-hour attack-defense cybersecurity exercise. The data used in this paper are from time-stamped observations of the attack team during this exercise.

B. Topological Sort Networks

Capturing and analysis of adversarial movement can provide crucial information about the decision making process of the cyber crimes. In order to capture the characteristics of the adversarial team members'movements during the attack, we propose a network representation of their activities. This representation is based on a concept known as topological ordering. A topological ordering is a linear ordering of the nodes of a graph such that for every directed edge uv from node u to node v a directed edge is drawn from u to v, meaning that u comes before v in the ordering. [7],[8]. In our case study, the vertices of the graph represent intrusion chain stages to be performed, and the directed edges denote the constraint that one intrusion stage is performed by subject S_1 before another. For instance, if subject S_1 performs intrusion stage A, and then preforms stage B, we draw a directed edge from A to B for the topological sort graph corresponding to that subject. Through this criteria, we create a topological sort for each subject in the Red team. Therefore, we obtain a directed acyclic graph (DAG) for each subject which we can analyze and compare with the graphs belonging to other subjects. In the next sections we discuss the methodology for measuring the similarity of the graphs created for each subject with each other. This measurement can help us gain further information about adversarial movements through their commonalities or differences.

C. Graph Similarity Measure

Measuring the structural similarity between the topological representation among the members of the adversarial team



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

Fig. 1. 12-stage Intrusion Chain Model [1]

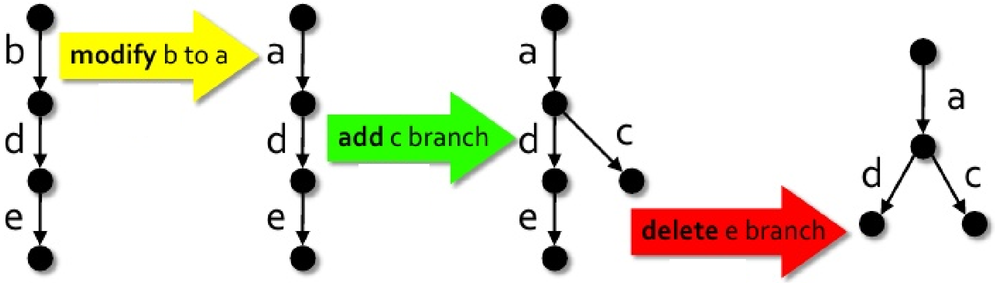


Fig. 2. An example of edit distance graph transformations (distance between the leftmost and the rightmost graphs is 3) [10].

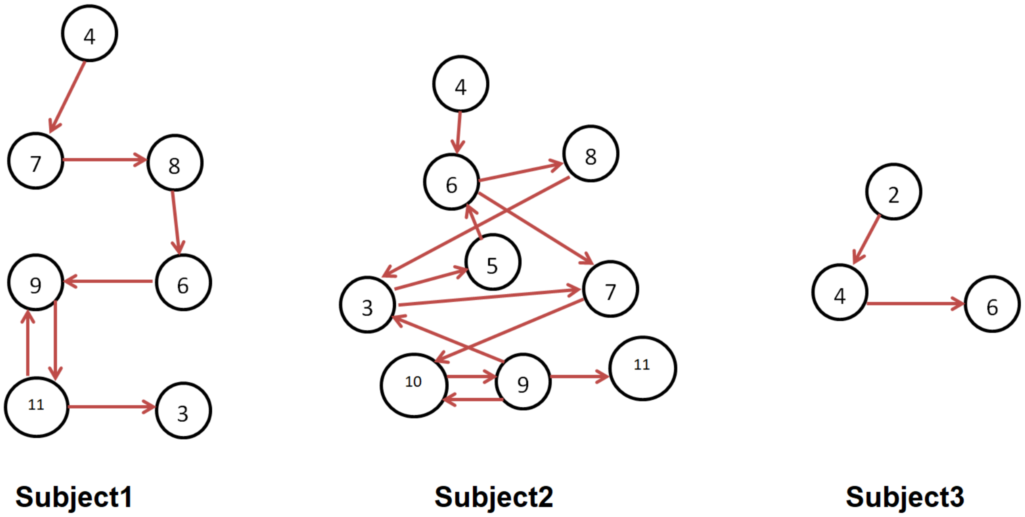


Fig. 3. Topological sorting graph of the activities of the first three subjects. The numbers inside the nodes denote the intrusion chain stage and the arrow from intrusion stage A to B represents the order of the subject's movement from stage A to stage B.

can provide the level of commonalities in their movement. One of the common network similarity measurement methods is the edit distance method which measures the minimum number of graph operations (e.g. edge additions or deletions) needed to transform one graph to another. [12]. The smaller the distortion needed, the more similar the two graphs are. The set of elementary edit operators commonly includes: introducing a new node to a graph, replacing the label of a node with new label of a given vertex, removing a node from a graph, inserting a new edge between a pair of nodes, deleting an edge between a pair of nodes. A simple example of graph edit distance method is illustrated at Figure 2 where the operators needed to transform the leftmost graph to the rightmost graph include one edge modification, one edge addition and one edge deletion. The effectiveness of edit distance-based pattern recognition relies on the adequate definition of cost functions for the basic edit operations. In case of unlabeled graphs, the cost is usually defined via unit cost for all deletions and insertions of both nodes and edges, while substitutions are free of cost.

D. Structural Comparisons

After creating the DAGs for each subject of the Red team, we can perform further analysis through structural characteristics of the generated networks [6]. One of the structural characteristics that we measure and compare for this work, is the longest path in the networks. The longest path in a given network is defined as the length of the simple path of maximum length in it(A path is called simple if it does not have any repeated vertices) [9]. In this work, the length of the path between node A and node B is measured by the number of edges that it takes to traverse from A to B. Note that since we have directed graphs, the graph traversal can only take place along the direction of the edges. This means that there can be a case where there is a path from A to B, but no paths from B to A. To understand this scenario in our case study, one can think about be the case where subject S_i performs intrusion stage B after intrusion stage A, and never goes back to A again. The reason we use longest path as a measurement is that it can show the level to which the adversarial movement of a subject is linear, i.e. does not contain a loop back to a previously performed stage. An extreme case can be the completely linear movement where each intrusion stage happens only once, and every stage takes place after its previous stage. In that case, the longest path is maximized.

The other structural feature measured in this study is the number of edges, which indicates the frequency of movement from one stage to another by the subject. A DAG with high edge density indicates high level of alterations in the subject's focus from one intrusion chain to other.

The results of the case study are discussed in the next section.

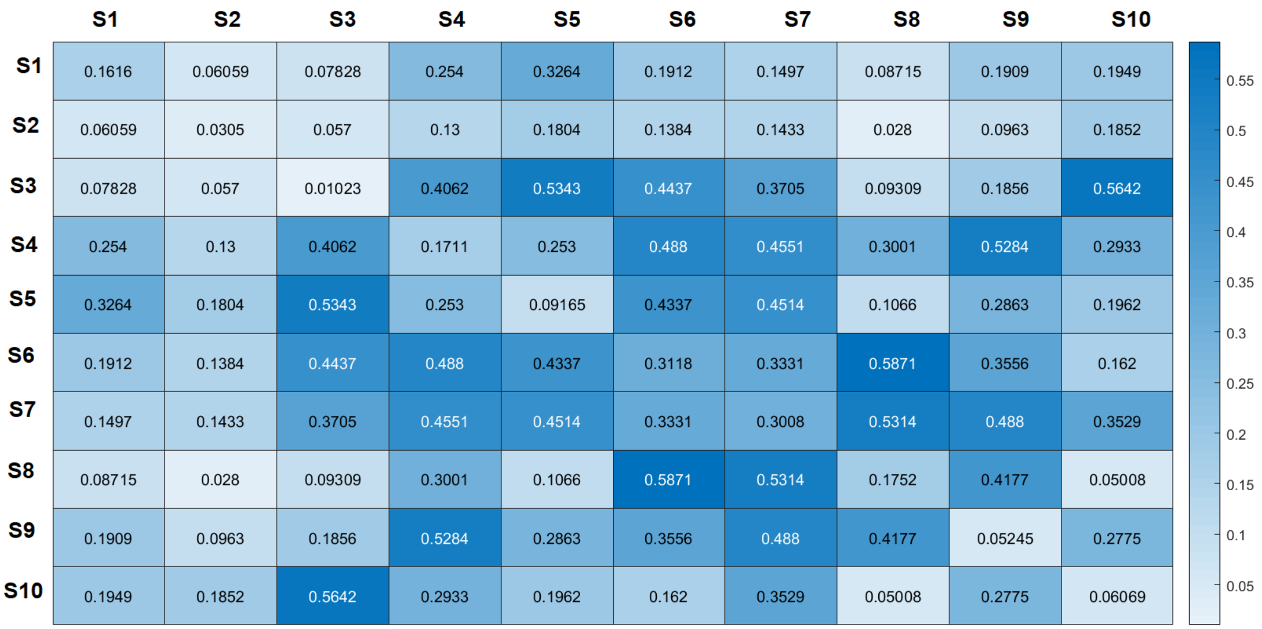
III. Results

The background and expertise of each member of the Red team is provided in Table 1. The third column shows the number of different intrusion stages that each member was involved in throughout the exercise. For instance, Subject S_1 was involved in 7 different intrusion stages out of the 12 stages in Dell's kill chain model. This observation is provided to create a comparison between each member's skill set and the number of different intrusion stages that they were engaged in. As can be seen in Table 1, subject 2 had the highest involvement in various stages followed by subject 1. As can be seen in that table, the rest of the subjects were involved in smaller number of stages, meaning that their focus was mainly on a specific stages.

The topological sorting for each member was performed and their corresponding directed graphs were created using the observation field notes. An example of the graphs generated for subjects one, two, and three are depicted in Figure 3. As explained in the methodology, the directed edges show the movement of a subject from one intrusion stage to the next one as the exercise progresses. In some cases, such as for stages 9 and 11 for subject 1, directed edges are drawn between both stages. This means that the subjects put their focus back on the previous stage after spending time on the current stage. This can be seen for subject 2 as well. As one can conclude, the stages without any incoming nodes are the stages that the subjects begin working on. For subjects 1 and 2, this is stage 4 (Research Target Infrastructure) and for subject 3 this is stage 2 (Find/Organize Accomplices). The same conclusion can be made for the final stage focused by the subjects, which is the stage without any outgoing edge. This is the stage 3 (Build/Acquire Tools) for subject 1, stage 11 (exfiltrate data), and for subject 3, stage 6 (Deployment).

Also, as mentioned through column 3 of Table 1, we can see that the focus of subject 2 was placed on more unique stages than subjects 1 and 3. Therefore, the topological ordering graph in fact provides information complementary to Table 1. Another point worth mentioning is that the final movement of subject 1 from stage 11 (exfiltrate data) back to stage 3 (Build/Acquire Tools) can indicate a failure that occurred in the subject's effort to advance to the final step. Another possible explanation for this could be the fact that necessary tools are required to cover tracks therefore, this stage was performed. Yet another possibility is that subject 1 started a new objective after completing stage 11, which required different tools. This is an example analysis that can be done through the topological ordering graphs of the adversarial movement of the members of the Red team.

After creating the directed networks for each subject, we employed the graph similarity measure explained in the methodology to find the similarities between the adversarial movements among the team members. The result of this analysis is provided as a heat map in Figure 4 where the higher values mean the higher similarity between the movement of the subjects. As an example in that figure, the similarity between the adversarial movement order of subject 2 and other subjects is lower, whereas there is a higher similarity among subjects 6 and 8. The topological graph of subjects 6 and 8 are provided in Figure 5 where the similar sub-pattern between the two networks is marked with dashed lines. Due to this similarity, the edit distance transformation does not need many operations. In fact, by adding node 2, replacing node 11 with node 6, and adding one edge from node 6 to node 7 we can convert the graph of subject 6 to the graph of subject 8. Therefore, the movement patterns of these two subjects show higher similarity. This analysis provides further insight into the association between the skill set of the subjects and their



	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
S1	0.1616	0.06059	0.07828	0.254	0.3264	0.1912	0.1497	0.08715	0.1909	0.1949
S2	0.06059	0.0305	0.057	0.13	0.1804	0.1384	0.1433	0.028	0.0963	0.1852
S3	0.07828	0.057	0.01023	0.4062	0.5343	0.4437	0.3705	0.09309	0.1856	0.5642
S4	0.254	0.13	0.4062	0.1711	0.253	0.488	0.4551	0.3001	0.5284	0.2933
S5	0.3264	0.1804	0.5343	0.253	0.09165	0.4337	0.4514	0.1066	0.2863	0.1962
S6	0.1912	0.1384	0.4437	0.488	0.4337	0.3118	0.3331	0.5871	0.3556	0.162
S7	0.1497	0.1433	0.3705	0.4551	0.4514	0.3331	0.3008	0.5314	0.488	0.3529
S8	0.08715	0.028	0.09309	0.3001	0.1066	0.5871	0.5314	0.1752	0.4177	0.05008
S9	0.1909	0.0963	0.1856	0.5284	0.2863	0.3556	0.488	0.4177	0.05245	0.2775
S10	0.1949	0.1852	0.5642	0.2933	0.1962	0.162	0.3529	0.05008	0.2775	0.06069

Fig. 4. Heat map of similarities between the topological network corresponding to each subject.

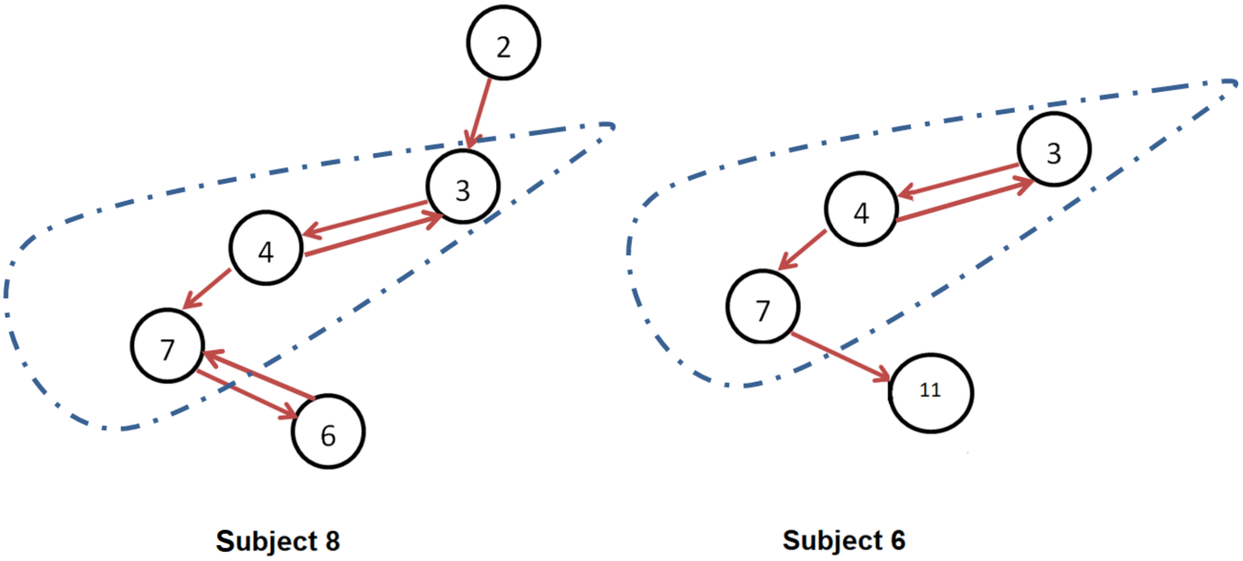


Fig. 5. Heat map of similarities between the topological network corresponding to each subject.

adversarial movement.

As explained in the methodology section, the longest path in the directed graph generated for each subject shows the level of linearity in their movement and the number of intrusion stages. performed by them. This information is included in Table 2. Also, the edge density of the graphs are provided in that table. Comparable to Table 1, we can observe that the adversarial movement of subject 2 has the highest edge density followed by subject 1. However, the longest path length of subject 1 was higher than that of subject 2. This further shows that subject 2 did more frequent back-and-forth between various intrusion stages. One possible explanation for this could be the difference between the approaches that the two subjects decided to take: subject 1 was more focused on an intrusion stage before moving to another stage while subject 2 made quicker changes in its decision making process. Alternatively, one can argue that subject 1 was simply pursuing a different objective with a different sophistication level that required d toggling between different intrusion chain stages. This analysis can provide further insight into the decision making process of the adversarial team members.

IV. Conclusion

This paper provides a framework for analysis of of adversarial movement across the cyber intrusion chain through meas of network theory and algorithms. Despite existing limitations

Subject	Backgrounds and Skill Sets	No. of Stages
S1	Linux, Sniffing	7
S2	Metasploit	9
S3	Programmable Logic Controller (PLC) Programming, Minimal Linux, Strategy Planning	3
S4	Project Supervisory Control and Data Acquisition (SCADA), Metasploit, Several Capture The Flag (CTF)	4
S5	Cyber Security Compliance, Management, Minimal Industrial Control Systems (ICS), Networking, Switching Configurations	3
S6	Cyber security, Distributed Control Systems (DCS) Networks, Networking, ICS Pen Testing, Metasploit	4
S7	Critical Manufacturing, Systems Engineering, Programming PLC, Minimal Linux	4
S8	Threat Advisories/Warnings, Broad Cyber Security Knowledge	5
S9	PLC Connectivity, Remote iOS	5
S10	Network Engineering	4

TABLE I. RED TEAM MEMBER BACKGROUND AND EXPERTISE AND THE NUMBER OF DIFFERENT INTRUSION STAGES PERFORMED BY EACH SUBJECT

Subject	Maximum Path Length	Edge density
S1	6	0.083
S2	5	0.0833
S3	2	0.25
S4	3	0.15
S5	3	0.107
S6	2	0.091
S7	4	0.211
S8	3	0.1302
S9	2	0.169
S10	3	0.1141

TABLE II. THE STRUCTURAL CHARACTERISTICS OF THE TOPOLOGICAL GRAPH ORDERING OF EACH SUBJECT

to the analysis provided in this work with regards to generalizability of the analysis to real cyber attacks as well as the limited case study data, this paper aims to lay the groundwork for further similar analysis using data science methodology. Moreover, the case study used in this paper is one of the most well-established Red Team/Blue Team exercises (RTBTE) in the United States. Having stated these facts, we provide a number of conclusions based on our analysis of the case study.

1) There is little association between the breadth of the of the team member's skill set and the patterns in their adversarial movement: The expertise and background knowledge of the subjects does not necessarily display a high level of association with the patterns of their adversarial movement. These patterns include but are not limited to linearity of the movement or multiple back-and-forth movements, focused on small number of stages or frequent changes from one stage to another, etc. This means that subjects with similar set of skills did not necessarily take similar paths during their adversarial movement. However, we cannot make the same conclusion about the depth of the members'skill set as the information related to that matter was not available in the dataset.

2) Common adversarial movements are not linear: By observing the structural characteristics of the topological networks related to the adversarial movements of each subject we can conclude that most graphs contained edges back-and-forth between stages which indicates the fact that the subjects move from one intrusion chain stage back to the one they performed previously. This can be due to their failure in advancing through the kill chain, differences between the objectives, or the fact that the subjects are involved in more than one intrusion chain. While the adversarial kill chain model in Figure 1 provides a basic set of sequential stages, it does not capture the fact that subjects may take non-linear paths and progress through the different stages in a non-sequential manner. As mentioned previously, there are several possible explanations for the patterns of subjects'movements.

3) The adversarial movements of the Red team is not homogeneous throughout the exercise: By comparing the information provided in Table 2 and Figure 4 we can conclude that despite some similarities, the pattern of adversarial movement is not homogeneous among the team members. This means that the overall decision making of the Red team throughout the case study was rather individual than based on a centralized process.

While this paper analyses a single case study, it offers a unique mixed-methods approach that sheds light on the complexity of adversarial movement. We hope this research starts a dialog on group adversarial dynamics and how individual adversaries may exhibit different movement trajectories and properties within the group. Future research could use empirical data to delve further into adversarial dynamics and movement.

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] DELL 2015. *Advanced Persistent Threats: Understand the Threat.* http://www.secureworks.com/cyber-threat-intelligence/advanced-persistent-threat/understand-the-threat/. Accessed: 2015-06-10.

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

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

[5] RSA (RSA Division of EMC). (2012). *Stalking the Kill Chain.* http://www.emc.com/collateral/hardware/solution-overview/h11154-stalking-the-kill-chain-so.pdf. Accessed: 2012.

[6] Joshua D Guzman et al. "An analytical comparison of social network measures". In: *IEEE Transactions on Computational Social Systems* 1.1 (2014), pp. 35–45.

[7] Alan D Kalvin and Yaakov L Varol. “On the generation of all topological sortings”. In: *Journal of Algorithms* 4.2 (1983), pp. 150–162.

[8] Donald Ervin Knuth. *The art of computer programming*. Vol. 3. Pearson Education, 1997.

[9] Jens Krause, DP Croft, and Richard James. “Social network theory in the behavioural sciences: potential applications”. In: *Behavioral Ecology and Sociobiology* 62.1 (2007), pp. 15–27.

[10] Niels Lohmann. “Correcting deadlocking service choreographies using a simulation-based graph edit distance”. In: *BPM*. Vol. 8. Springer. 2008, pp. 132–147.

[11] Aunshul Rege et al. “A temporal assessment of cyber intrusion chains using multidisciplinary frameworks and methodologies”. In: *Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2017 International Conference On*. IEEE. 2017, pp. 1–7.

[12] Kaspar Riesen. “Structural pattern recognition with graph edit distance”. In: *Advances in Computer Vision and Pattern Recognition, Cham* (2015).