Reconnaissance Techniques and Industrial Control System Tactics Knowledge Graph

Eve Cohen[1], Elsa Deitz[1], Jordana Wilkes[1] and Thomas Heverin[2]
[1]The Baldwin School, Bryn Mawr, United States of America
[2]Girls Learn Cyber, Inc., Philadelphia, United States of America

hacker@girlslearncyber.com
thomas@girlslearncyber.com

Abstract: In the initial stages of industrial control system (ICS) penetration testing, pentesters conduct reconnaissance by using various tools including Nmap, Shodan, Maltego, Google, Google Hacking Database (GHDB), Recon-ng and more. Testers use various reconnaissance techniques (RTs) within the tools to directly access ICS devices. Many novice ICS-pentesters stop their reconnaissance work upon successfully accessing an ICS device. However, continuing to conduct reconnaissance after initial access can lead to pentesters finding even more information to find more ICS devices, ICS networks, and ways to make ICS exploitation more effective. Our research motivation stems from finding ways to explicitly model the continuation of using RTs once an ICS device is accessed. Knowledge graphs offer an approach for linking RTs together and creating chains of RTs. MITRE ATT&CK ICS provides a matrix of ICS adversarial behaviours. The matrix consists of main exploit tactics and techniques used to accomplish these tactics. Example techniques include ICS alarm suppression, blocking command messages, starting a device, and stopping services. ATT&CK ICS also provides ICS data sources that defenders use to detect the adversarial techniques. Application logs, files, logon sessions, network traffic, and operational databases represent some of the ICS data sources. We reasoned that if adversaries could find the ICS data sources and discover the ability to modify the data sources, then adversaries could cover their tracks to successfully carry out ICS tactics. For example, ICS attackers could modify log entries to hide the attacker's steps or ICS attackers could delete alarm notifications that showed that ICS attackers changed ICS settings. In this work in progress research, we used knowledge-graph modelling techniques to link together RTs with ICS data sources, the ability to modify the data sources, the ability to then cover tracks of ICS techniques, and the impact of techniques on accomplishing ICS tactics. We named the graph RT-ICS Graph. With knowledge graph queries and shortest-path algorithms run over the RT-ICS graph, we showed how RTs can explicitly lead to impacts on adversaries carrying out ICS tactics. The accomplishment of ICS tactics can cause severe damage or harm.

Keywords: Knowledge Graph, Reconnaissance, Industrial Control Systems

1. Introduction

MITRE ATT&CK Industrial Control System (ICS) (2022) models adversarial behaviours with a matrix of 12 ICS adversarial tactics and 79 techniques used to accomplish the tactics. Example ICS tactics include Execution, Persistence, Lateral Movement, Inhibit Response Function, and Impair Process Control. ICS Techniques include Activate Firmware Update-Mode, Alarm Suppression, Device Restart/Shutdown, Modify Program, and many more. ICS defenders use various data sources to detect ICS Techniques. We reasoned that if attackers could find and modify the data sources, then the attackers could cover the tracks for ICS techniques that are used to carry out ICS tactics. We based this conceptualization on many ICS reconnaissance tasks that we have completed in the real-world. Our preliminary research focused on using a knowledge graph to link the following: reconnaissance techniques (RTs) with ICS data sources, data sources with the ability to modify them, the ability to modify data sources with covering tracks for ICS techniques, and ICS techniques with ICS tactics. The motivation for our research stems from the fact that RTs rarely modelled explicitly even though reconnaissance is a key step in penetration testing.

2. Knowledge Graphs in Cybersecurity

Knowledge graphs have been used in the cybersecurity domain in various ways. For example, Noel et al. (2015) used a knowledge graph to predict the paths of attacks based on attack patterns and the resistance offered by defense technologies. Graphs have also been developed to conduct vulnerability assessments (Ye et al., 2019), security assessments (Zhang and Liu, 2020), and network security analytics (Noel, 2018).

Kurniawan et al. (2022) and Liu et al. (2022), analysed multiple knowledge-graph review studies (Ding, Liu, and Zhu, 2020 and Dong et al., 2020) and determined a key research need: the need to apply graphs to broad, practical issues that organizations face rather than applying graphs to specific network infrastructure instances. We aimed to address this need with preliminary research focused on linking RTs across ATT&CK ICS which is used broadly across all types of ICS networks rather than a particular ICS network. Also, previous cybersecurity

knowledge graph studies have not focused on linking RTs together; therefore, our research offers a novel approach.

3. Knowledge Graph Development and Structure

3.1 Knowledge Graph Development

In domain-focused knowledge graph development, it is critical to rely on domain expertise and reliable data sources (Sattar et al., 2020). The senior researcher of this work in progress paper has over 10 years of ICS cybersecurity experience. Also, all researchers on the team have conducted reconnaissance projects on ICS and successfully accessed ICS devices under bug bounty programs. ICS devices accessed included building automation systems, physical security systems, physical key boxes, and programmable logic controllers (PLCs). Additionally, the team has successfully submitted Google Hacking Database (GHDB) entries focused on ICS devices.

The knowledge graph developed for this research extended a reconnaissance graph called RT-Graph that modelled and linked together over 100 RTs (Deitz et al., 2023). However, RT-Graph contained zero links to ATT&CK ICS concepts. We linked RT-Graph to ATT&CK ICS concepts and named the combined graph "RT-ICS Graph." The foundation of RT-ICS Graph consists of an ontology. Ontologies are used to model domain concepts and relationships among the concepts. When ontologies are filled in with specific data, they turn into knowledge graphs (Kurniawan et al., 2022).

We approached the reconnaissance of ICS as a medium level adversary per the Sandia National Lab Generic Threat Matrix (Woodard, 2007). Table 1 shows the seven attributes from the Generic Threat Matrix used to evaluate threats and the application of the attributes to our ICS reconnaissance approach.

Table 1. Threat Level Attributes Used to Develop RT-ICS Graph.

General Threat Matrix Profile Attribute (Sandia National Lab)	Meaning of Attribute	RT-ICS Graph Approach
Intensity	How far a team is willing to go to achieve objectives; high intensity means the team will risk imprisonment or persecution to achieve goals	Low
Stealth	Level of effort in maintaining secrecy	Low
Time	Amount of time dedicated to reaching objective ranging from days to decades	Low
Technical Personnel	Number of people on the team ranging from individuals to hundreds of people	Low
Cyber Knowledge	Level of network and IT knowledge	Medium
Kinetic Knowledge	Level of ICS knowledge and physical operations knowledge	Medium
Access	Level of ability to place a team member with unlimited access on a device	High

According to the Generic Threat Matrix attributes, our ICS reconnaissance approach focused on using minimal intensity, stealth, time, and number of people to gain the highest level of access. Across various ICS reconnaissance projects, we have repeatedly been able to access ICS devices at the administrator level. We attempted to model our current knowledge in RT-ICS Graph.

3.2 Graph Structure

Ontology-based graphs contain five main entities: classes, objects, object properties, and data properties. Classes represent categories of objects, such as RTs or ICS Techniques or ICS Tactics. Objects are instantiations of classes. Object properties link specific objects together and data properties describe characteristics about the objects. Data properties describe objects. Figure 1 shows the main classes in RT-ICS Graph. ICS Techniques, ICS Tactics and ICS Data Source classes and their objects were drawn directly from ATT&CK ICS. We created the class ICS Ability class to represent the ability of adversaries in modifying data sources found during reconnaissance. Our previous research describes the Reconnaissance Tactic classes in more detail (Deitz et al, 2023).

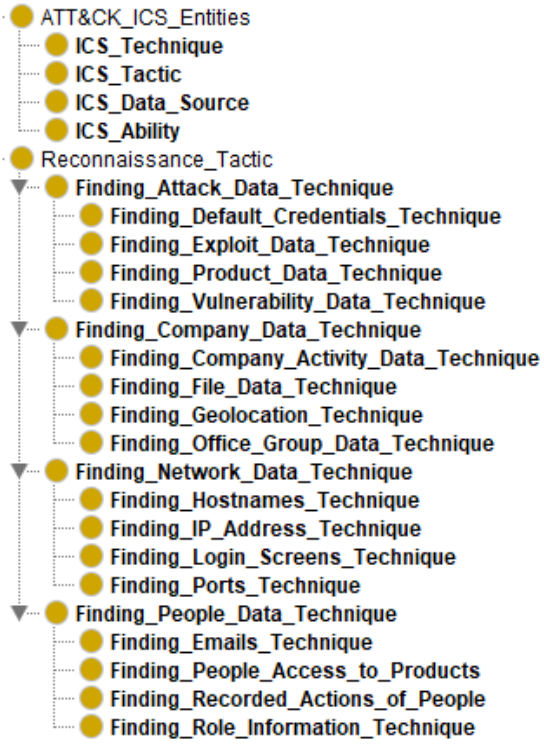

Figure 1. RT-ICS Graph Classes.

Each class is made up of objects which are instantiations of classes. Figure 2 shows objects contained within the ICS Data Source class. According to MITRE (2022), data sources "…represent the various subjects/topics of information that can be collected by sensors/logs. Data sources also include data components, which identify specific properties/values of a data source relevant to detecting a given ATT&CK technique or sub-technique."

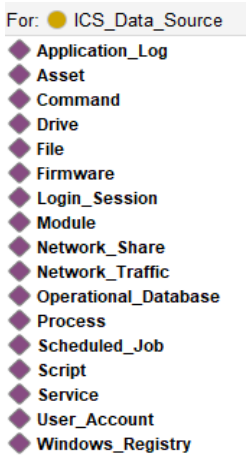

Figure 2. Objects Found in the ICS Data Source Class of RT-ICS Graph.

These data sources come from ATT&CK ICS and were further used to create objects in the ICS Ability class. For example, the data source called "Application Log" was used to create "Ability to Modify Application Log" in the ICS Ability class. This process was repeated for all 17 ICS data sources. The concept of "ability to modify" ICS data sources stems from the researchers' experience in ICS cybersecurity and in ICS reconnaissance projects.

RT-ICS Graph contains several object properties as shown in Table 2. Object properties link together objects. RT-ICS Graph object properties provide direction (one object points to another object) which makes RT-ICS a directed graph. Data properties describe objects. An example data property is ICS Tactic ID such as "T1592" for the ICS Tactic "Gather Victim Host Information." Other example data properties include ICS Technique ID, and Data Source ID all derived from ICS MITRE ATT&CK.

Table 2. Description of Object Properties in RT-ICS Graph.

Domain (Class)	Object Property	Range (Class)	Explanation
Reconnaissance Technique	*providesDataFor*	Reconnaissance Technique	One RT can provide data for another RT; this creates paths of RTs across the graph
Reconnaissance Technique	*findsDataSource*	Data Source	RTs can be used to find various ICS data sources once an ICS device is accessed
Data Source	*discoversAbility*	Ability	Once a data source is found, one can see if the data source can be modified
Ability	*coversTracksFor*	ICS Technique	Once the ability to modify a data source is confirmed, this ability can be used to cover the tracks for ICS techniques
ICS Technique	*accomplishesTactic*	ICS Tactic	ICS techniques are used to accomplish ICS tactics

Figure 3 shows the overall RT-ICS Graph visualized with Gephi, a graph visualization and statistical analysis tool. The Fruchterman-Reingold spatial-layout algorithm was used to produce they graph visual (Fruchterman and Reingold, 1991). Each node on the layout represents an object in RT-ICS Graph (specific instances of RTs, Data Sources, Abilities, ICS Techniques, and ICS Tactics). The arrows represent the object properties from Table 2 specified among specific RT-ICS Graph objects. The purpose of Figure 3 is to provide a representation of how all RT-ICS Graph objects are linked together. Future research shall describe the spatial layout in more detail.

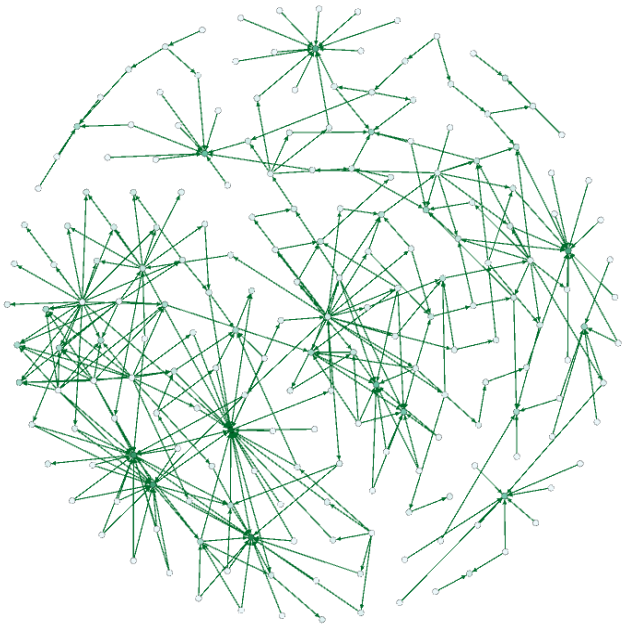

Figure 3. Graph Visualization of RT-ICS Graph Using the Fruchterman-Reingold Spatial-Layout Algorithm in Gephi.

4. Graph Queries and Shortest-Path Algorithm Analyses

4.1 SPARQL for Graph Queries

SPARQL, a recursive acronym for SPARQL Protocol and Resource Description Framework (RDF) Query Language, represents a common query language used to query knowledge graphs (World Wide Web Consortium, 2008). SPARQL holds many similarities with Structured Query Language (SQL). For example, SPARQL uses similar query expressions such as: SELECT, FROM, WHERE, UNION, GROUP, HAVING and more. SPARQL results can provide insights about data and about the connections among data within graphs.

4.2 SPARQL Queries for Preliminary Insights

We developed SPARQL queries to examine how RTs can be used by adversaries once on an ICS device and how these RTs can lead to impacts on ICS Tactics. Across various ICS reconnaissance projects, we have discovered the

ability to modify, upload or download firmware. We developled a SPARQL query focusing on the potential implications of discovering this ability. The SPARQL syntax is as follows:

```
Select    ?ReconTechnique ?DataSource ?Ability ?ICS_Technique ?ICS_Tactic

          WHERE          {?ReconTechnique recon:findsDataSource ?DataSource .
          FILTER (?DataSource = recon:Firmware) .
          ?DataSource recon:discoversAbility          ?Ability .
          ?Ability recon:coversTracksFor ?ICS_Technique .
          FILTER (?ICS_Technique = recon:Module_Firmware)
          ?ICS_Technique recon:accomplishesTactic ?ICS_Tactic . }

ORDER BY ?ICS_Tactic
```

Figure 4 shows the results for the above SPARQL query focused on ICS firmware and shows the ultimate impact on ICS Tactics if adversaries find they can modify the firmware.

ReconTechnique	DataSource	Ability	ICS_Technique	ICS_Tactic
Device_search_for_ability_to_download_files	Firmware	Ability_to_modify_firmware	Module_Firmware	ICS_Impair_Process_Control_Tactic
Device_search_for_files	Firmware	Ability_to_modify_firmware	Module_Firmware	ICS_Impair_Process_Control_Tactic
Device_search_for_ability_to_upload_files	Firmware	Ability_to_modify_firmware	Module_Firmware	ICS_Impair_Process_Control_Tactic
Device_search_for_ability_to_download_files	Firmware	Ability_to_modify_firmware	Module_Firmware	ICS_Persistence_Tactic
Device_search_for_files	Firmware	Ability_to_modify_firmware	Module_Firmware	ICS_Persistence_Tactic
Device_search_for_ability_to_upload_files	Firmware	Ability_to_modify_firmware	Module_Firmware	ICS_Persistence_Tactic

Figure 4. Results of Firmware-Focused SPARQL Query to Show Links from RTs to ICS Tactics in RT-ICS Graph.

One goal of this preliminary research was to show the value of conducting ICS reconaissance tasks even after gaining access to an ICS device. Based on the senior reseacher's 10 years of teaching experience, many novices in reconnaissance stop their tasks once they gain initial access to an ICS device. Novices often lack the insight about the value of continuing to do reconnaissance at this stage; they often miss out on how further reconnaissance can find other critical information to help accomplish ICS tactics. The results of the above query show that RTs can lead to impacts on ICS Tactics that adversaries use to exploit ICS. The above query only focused on firmware. Another example is shown in Figure 5 which is focused on finding the Application Log data source via various RTs and the ability to modify it in terms of user activities.

ReconTechnique	DataSource	Ability	ICS_Technique	ICS_Tactic
Device_search_for_ability_to_upload_files	Application_Log	Ability_to_modify_application_log	User_Execution	ICS_Execution_Tactic
Device_search_for_alarm_status	Application_Log	Ability_to_modify_application_log	User_Execution	ICS_Execution_Tactic
Device_search_for_user_activities_log	Application_Log	Ability_to_modify_application_log	User_Execution	ICS_Execution_Tactic
Device_search_for_ability_to_download_files	Application_Log	Ability_to_modify_application_log	User_Execution	ICS_Execution_Tactic

Figure 5. Results of Application Log SPARQL Query to Show Links from RTs to ICS Tactics in RT-ICS Graph.

In our ICS reconnaissance work, we have found many application logs that track user activities and user accounts. We have found the ability to modify user activities and even the ability to create new users on ICS devices. Figure 6 shows this ability for an Allen-Bradley PLC that we discovered under a bug bounty program. It also shows that we have the ability to create news users with administrator privileges.

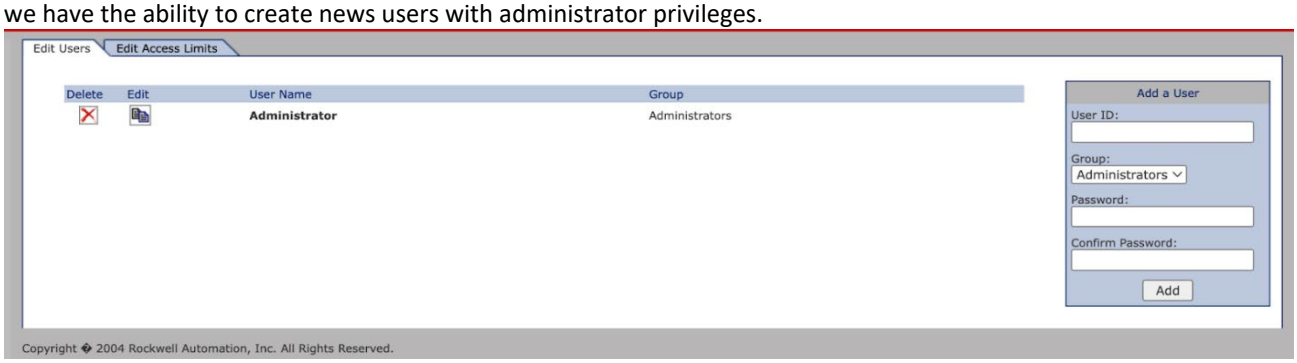

Figure 6. Ability to Modify User Accounts on a PLC.

4.3 Shortest Path Algorithm Analyses

We used Gephi to conduct shortest path analyses from initial RTs to ICS Tactics using the Dijkstra (2022) shortest-path algorithm. For example, we explored various paths from RTs used to scan a hostname with Nmap, a network mapping and port scanning tool, all the way to reaching the ICS Execution Tactic. The ICS Execution Tactic focuses on an adversary running code or manipulating "…system functions, parameters and data in an unauthorized way" severely impacting ICS (MITRE, 2023). Figure 7 shows the shortest path algorithim result. Once the ICS device is accessed via a chain of RTs, starting with a Nmap Quick Scan through a Google search for default credentials to get onto the device, the search for ICS object rules (such as rules for various PLCs) can lead to finding an operational database. If adveraries can modify the operational database, then they can cover their tracks for changing operating modes (an ICS technique) that helps accomplish the ICS Execution Tactic. This is one example of many shortest-path analyses that we ran.

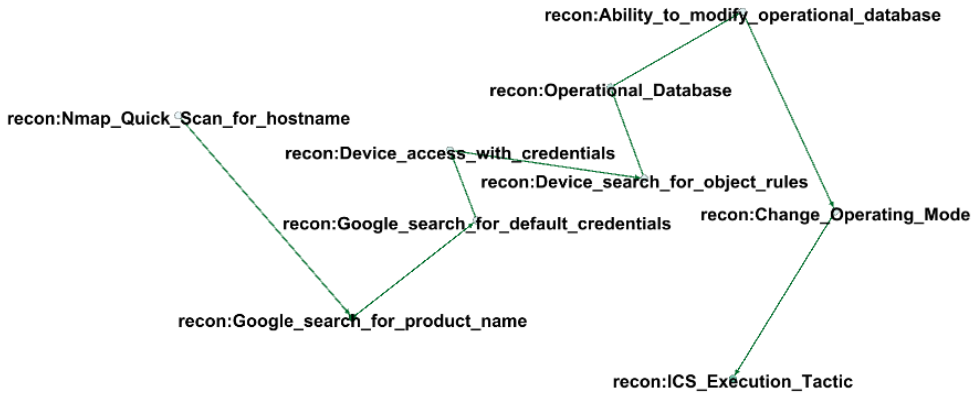

Figure 7. Shortest Path Algorithm Results from Nmap Quick Scan to ICS Execution Tactic in RT-ICS Graph.

Figure 8 shows the shortest path algorithm results starting from an Nmap Intense scan all the way through to the ICS Inhibit Response Function.

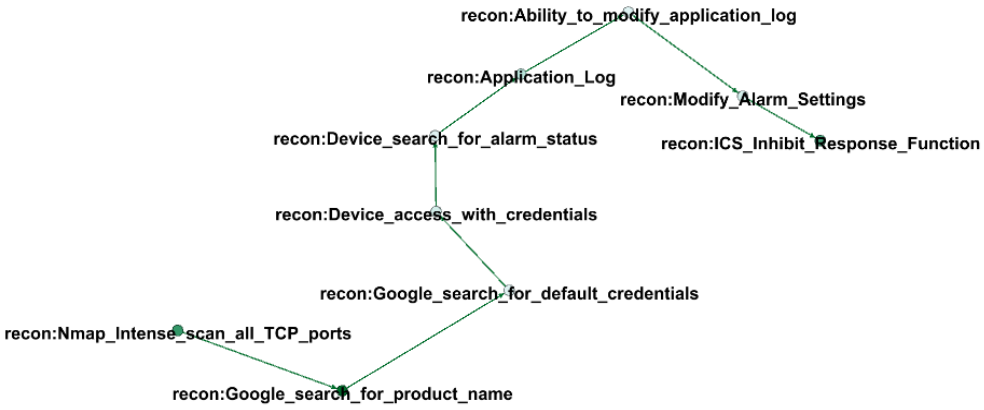

Figure 8. Shortest Path Algorithm Results from Nmap Intense Scan to ICS Inhibit Response Function.

Once an ICS device is accessed, adversaries can search for application logs and the ability to change the logs which then allows the adversaries to cover their tracks for modifying alarms. By modifying alarms, adversaries can better achieve their objective of Inhibiting Response Function. Figure 9 shows the results of bug-bounty reconnaissance work for finding alarm statuses at a university facilities' ICS. Though we did not take actions, one can see that the alarms can be acknowledged and cleared. When adversaries acknowledge and clear alarms, they can distort the awareness of ICS defenders. This can result in adversaries gaining access to ICS systems without being detected and can result in ICS defenders and maintainers lacking awareness of ICS parameters moving towards danger (such as temperatures getting to high, flooding happening, ICS devices overheating) and more.

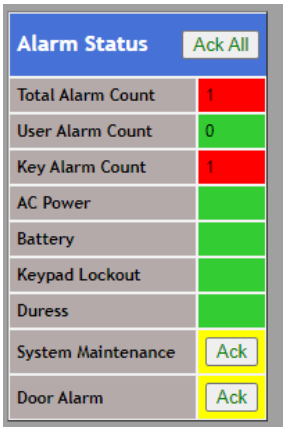

Figure 9. Display Showing the Capability of Modifying ICS Alarms.

5. Conclusion and Future Work

In our work in progress research, we modelled ICS data sources, the ability to modify the data sources, ICS techniques, and ICS tactics used by adversaries to exploit ICS. We connected these ICS concepts to RT-Graph which models over 100 RTs used across various tools including Nmap, Shodan, GHDB, Recon-ng and more. We explored how SPARQL queries can show the value for adversaries in continuing to conduct reconnaissance once an ICS device is accessed. We also explored how shortest path algorithms can show the direct links between initial RTs (such as an Nmap Quick scan) all the way through to ICS Tactics (such as ICS Execution). One limitation within this work in progress research is showing direct impacts on targets. Another limitation is that the modelling does not differentiate between successful execution of steps and when there is not successful execution. Rather, the current modelling only shows potential for successful execution. Future work will focus on adding more RTs to the RT-ICS Graph, conducting more shortest path analyses, and running statistical algorithms over the graph. Finally, ICS experts will examine RT-ICS Graph to provide feedback and improvements on the concepts modelled.

References

Dijkstra, E. W. (2022) "A Note on Two Problems in Connexion with Graphs" In *Edsger Wybe Dijkstra: His Life, Work, and Legacy* (pp. 287-290).

Ding Z., Liu K., Liu B., and Zhu, X. (2020) "Survey of Cyber Security Knowledge Graph*", Journal of Huazhong University of Science and Technology,* Vol 49, No. 7, pp 79-91.

Dong, C., Jiang, B., Lu, Z., Liu, B., Li, N. and Ma, P. (2020) "Knowledge Graph for Cyberspace Security Intelligence: A Survey", *Journal of Cyber Security* Vol 5, pp 56–76.

Fruchterman, T. M. J. and Reingold, E. M. (1991) "Graph Drawing by Force-Directed Placement", *Software: Practice and Experience*, Vol 21, No. 11, pp 1129-1164.

Deitz, E., Cohen, E., Wilkes, J., and Heverin, T. (2023) "Development and Analysis of a Reconnaissance-Technique Knowledge Graph", *18th International Conference on Cyber Warfare and Security*.

Kurniawan, K., Ekelhart, A., Kiesling, E., Quirchmayr, G., and Tjoa, A. M. (2022) "KRYSTAL: Knowledge Graph-Based Framework for Tactical Attack Discovery in Audit Data" *Computers & Security*, Vol 121.

Liu, K., Wang, F., Ding, Z., Liang, S., Yu, Z., and Zhou, Y. (2022) "Recent Progress of Using Knowledge Graph for Cybersecurity", *Electronics*, Vol 11*,* No. 15.

MITRE (2022) "MITRE ATT&CK ICS", viewed January 1, 2023 < https://attack.mitre.org/matrices/ics/>

MITRE (2022) "MITRE ATT&CK Data Sources", viewed January 31, 2023 < https://attack.mitre.org/datasources/>

Noel, S., Harley, E., Tam, K. H., and Gyor, G. (2015) "Big-Data Architecture for Cyber Attack Graphs: Representing Security Relationships in NoSQL Graph Databases", *IEEE Symposium on Technologies for Homeland Security*.

Noel S. (2018) "A Review of Graph Approaches to Network Security Analytics", In *From Database to Cyber Security*, pp 300-323.

Sattar, A., Surin, E. S. M., Ahmad, M. N., Ahmad, M., & Mahmood, A. K. (2020) "Comparative Analysis of Methodologies for Domain Ontology Development: A Systematic Review." *International Journal of Advanced Computer Science and Applications*, Vol 11, No. 5., pp 98-108

Woodard, L., Veitch, C. K., Thomas, S. R., & Duggan, D. P. (2007). *Categorizing threat: building and using a generic threat matrix* (No. SAND2007-5791). Sandia National Laboratories (SNL), Albuquerque, NM, and Livermore, CA (United States).

World Wide Web Consortium (2008). "SPARQL Query Language for RDF", viewed January 1, 2023 <https://www.w3.org/TR/rdf-sparql-query/>

Ye, Z.W., Guo, Y.B., Li, T. and Ju, A.K. (2019) "Extended Attack Graph Generation Method Based on Knowledge Graph", *Computer Science*, Vol 46, No. 12, pp 165-173.

Zhang, K. and Liu, J. (2020) "Review on the Application of Knowledge Graph in Cyber Security Assessment" *IOP Conference Series: Materials Science and Engineering*, Vol. 768.