Mental Model Mapping Method for Cybersecurity

Kaur Kullman[1], Laurin Buchanan[2], Anita Komlodi[3], Don Engel[3]

[1] Tallinn University of Technology, Tallinn EE, EU
[2] Secure Decisions, Northport NY, US
[3] University of Maryland, Baltimore County, Baltimore MD, US
m4c@coda.ee

Abstract. Visualizations can enhance the efficiency of Cyber Defense Analysts, Cyber Defense Incident Responders and Network Operations Specialists (Subject Matter Experts, SME) by providing contextual information for various cybersecurity-related datasets and data sources. We propose that customized, stereoscopic 3D visualizations, aligned with SMEs internalized representations of their data, may enhance their capability to understand the state of their systems in ways that flat displays with either text, 2D or 3D visualizations cannot afford. For these visualizations to be useful and efficient, we need to align these to SMEs internalized understanding of their data. In this paper we propose a method for interviewing SMEs to extract their implicit and explicit understanding of the data that they work with, to create useful, interactive, stereoscopically perceivable visualizations that would assist them with their tasks.

Keywords: Visualization design and evaluation methods, Cybersecurity, Data Visualization.

1 Introduction

Cybersecurity visualizations provide Cyber Defense Analysts[1], Cyber Defense Incident Responders[2] and Network Operations Specialists[3] (all three roles will collectively be referred to as Subject Matter Expert (SME) in this paper from here forward) with visual representation of alphanumeric data that would otherwise be difficult to comprehend due to its large volume. Such visualizations aim to efficiently support tasks including detecting, monitoring and mitigating cyberattacks in a timely and efficient manner. For more information about these and other cybersecurity related roles, see [1]. As noted in [2], cybersecurity-specific visualizations can be broadly classified into a) network analysis, b) malware analysis, c) threat analysis and situational awareness. Timely and efficient execution of tasks in each of these categories may require different types of visualizations addressed by a growing number of cybersecurity-specific visualization tools (for examples and descriptions of such see [3], [5] and [6]) as well as universal

[1] As designated PR-CDA-001 and bearing responsibilities for tasks identified in [18]
[2] As designated PR-CIR-001 and bearing responsibilities for tasks identified in [18]
[3] As designated OM-NET-001 and bearing responsibilities for tasks identified in [18]

software with visualization capabilities. These tools could be used to visualize data in myriad ways (for examples and descriptions of such see [7]) so that SMEs could explore their data visually and interactively (for interaction techniques see [8]). These are crucial qualities for SMEs, with emphasis on the importance of the low latency between SME's request for a change in visualization (change in applied filter, time window or other query parameters) and rendering of the visualized response from the system [9].

The challenge in creating meaningful visual tools for cybersecurity practitioners is in combining the expertise from specialists from the fields of data visualization and cybersecurity so that the resulting visualizations are effective and indeed useful for their intended users [10]. Further, creating visualizations useful for SMEs is not possible without an in-depth understanding of the tasks which the visualizations will support [11]. Hence, we describe here a multi-part, semi-structured interviewing method for extracting from an individual SME their internalized understanding of the dataset[4] that represents their protected environment, in order to create visualizations that align with their own understanding of that dataset and that will enhance the SMEs and their colleagues' ability to understand and work with that dataset.

The proposed interview method is rooted in the tradition of participatory design [12], a democratic form of design originating in Scandinavia. In participatory design all stakeholders are involved in the design by directly designing the user experience. Stakeholders are asked to not simply inform the design process but to contribute by actually designing interfaces and interactions.

2 Background

Although there are other design approaches for developing data visualizations [13], we identified the need for a cybersecurity specific method that would allow SMEs to create spatial three-dimensional layouts of visualized elements, referred to as data-shapes, that are specific to these SMEs datasets or data sources, in order to benefit from the novel capabilities of Virtual and Mixed Reality headsets that can provide users with stereoscopic perception of the data visualization environment.

We acknowledge that the efficiency of 3D data visualization has been subject to controversy (as thoroughly explained in [14]) and that the usability of visualizations overall are hindered by biological factors of the user (e.g. impaired color vision, impaired vison): these and other concerns were covered in an earlier papers of our project [15] and [4]. Despite that, for the users who can use and who do find 3D visualizations useful, we should provide methods they can use to create, and suitable technical tools to use useful visualization of their data. Other research [16] has previously shown that stereoscopically perceived, spatialized data visualizations may provide advantages for understanding and exploring the types of multidimensional (often partially deterministic) datasets and sources that SMEs work with.

[4] In the context of this paper, "dataset" refers to the collection of individual data sources, e.g., network flow data, log files, PCAP, databases and other stores (Elasticsearch, Mongo, RDBs,) used by an SME at a particular organization.

The Virtual Data Explorer (VDE) software that may be employed for visualizing cybersecurity specific datasets was covered in previous research [15] and [4]. For a data-shape or their constellations to be useful, the SME must be able to readily map data into a data-shape and choose visual encoding for its attributes so that the resulting visualization will enhance their understanding of that data. Only once an SME is intimate with the composition of the visualization and its relation to the underlying dataset or source can the SME use that visualization to extract information from it.

In this paper we describe a mental model mapping method that may be used to extract the necessary information for creating such data-shapes from SMEs while they're working with their actual data. To validate the usefulness of the new visualizations created with this method, it would be beneficial to involve at least three SMEs from the same group or company who are working with the same data so that the visualizations created with each participant could be evaluated at the end of the process with other members of the same group.

Visualization examples in this paper are showing NATO CCDCOE Locked Shields CDX networks traffic dataset [4], Figures feature screen captures from VDE Virtual Reality sessions.

2.1 Assumptions

The following assumptions underlie our work:

Assumption 1: Visualizations of different dimensions of network topology (functional, logical, geographic) using stereoscopically perceivable 3D can enhance an SME's understanding of their unique protected network environment if the visualizations are designed to match the individual SMEs mental model(s) of their environment's raw cyber data.

Assumption 2: It is possible to create data-shapes by interviewing SMEs in order to identify hierarchies of entities and entity[5] groups in their data that, when grouped by their functions, could be arranged into a 3D topology.

2.2 Hypotheses

We hypothesize that enriching the 3D data-shapes with additional contextual information that is derived from the queries that SMEs typically execute to find all relevant information to their data-focused tasks could be of benefit, specifically:

1. 3D data-shapes enriched with contextual information will provide significant insights more effectively in comparison with alphanumerical sources and/or 2D visualizations on flat screens.
2. 3D data-shapes enriched with contextual information will improve the efficiency of operators' workflow, e.g., seeking answers to their analytical questions.

[5] "Entity" refers to any atomic unit that the user could encounter in the data that's being investigated. In the context of this paper for example: a networked computer, IoT device, server, switch, but also a human actor (known user, malicious actor, administrator).

3 Process

The overarching goal of the SME interview process is to identify the properties that an SME seeks within the raw cyber data of their environment, i.e., their dataset, in order to obtain answers to the analytic questions for their work role. To do this, we must identify the relevant attributes of the data which enable the SME to form, verify, or disprove hypotheses about possible incidents or noteworthy events relevant to their work role. Based on the SME's role and specific inquiry goal, we determine the desired dimensions of data (entities, the relations of groups, subgroups, and sub-subgroups, etc.) to be visualized. We then consider which properties should be represented by which elements; an example of these dimensions and properties can be seen in Figure 1, where names of groups (e.g. "..Siemens Spectrum 5 power management..", "Substation equipment network") are visible above the "blades" of a data-shape, while names of subgroups (inside each group) (e.g. "Windows 10 workstations", "PLC-s", "Servers") are visible inside the "blades", above the entities of that subgroup. To better grasp the three-dimensionality of these shapes, see videos at https://coda.ee/M4C.

Fig. 1. Examining relationships and behavior of the entities of a group of groups.

This information is initially elicited through the first individual interviews with the SME group (Session 1 Interviews) by asking a series of specific questions designed to identify these groups and entities. In our example case, visualizing the functional topologies of computer networks, the entities are networked devices (server, laptop, fridge, gas turbine's controller, etc.) that can be classified into multiple, different groups (e.g., logical subnetwork, physical topology, geolocation, etc.). The relevant grouping (i.e., business functions, found vulnerabilities, etc.) depends on the goal of an SME's inquiry. If the visualization goal was different, for example, to visualize application logs, the initial interview questions should be adjusted accordingly.

Once all the first interviews have been completed, we evaluate the layouts created during the interviews (see 3.3). All or some of the layouts will be implemented using VDE (as described in [4]), either by creating new configuration files or implementing necessary components in C# (or with another visualization tool). Once done, the resulting data visualizations shall be tested with the data that the interviewed SMEs would be using it with (or an anonymized version of it), prior to a second round of SME interviews.

During Session 2 interviews, subjects are expected to use the custom visualizations with a VDE instance, that is rendering the data-shapes from actual data from the SME's environment to enable the SME to adequately evaluate the usefulness of the visualization.

3.1 Prescreening questionnaire

Participants should be pre-screened to verify their level of expertise and work roles to the participant pool. In our example case, SMEs working subject matter (e.g., computer network activity data) for at least a year with the specific dataset of their protected network environment (e.g., flow data, captured packets, Intrusion Detection System logs, logs of endpoints and servers, vulnerability scan reports, etc.,) may be invited to participate in the study.

3.2 Session 1 Interviews.

In the beginning of each session, the interviewer explains the purpose behind the knowledge elicitation and asks the SME for written permission to record audio and video during the session. The interviewer then conducts a semi-structured interview using guiding questions to learn the SME's understanding of the norms, behaviors, structure, context etc. of the available dataset (e.g., their computer network's topology, logfiles, etc.). In cases where the tasks or roles of the group being studied are different than described in this paper, the questions should be adjusted accordingly.

To gather actionable information from an interview, it is imperative that the interviewer quickly builds rapport with the SME to a level, that allows them to validate the level of subject matter competence of the interviewer [17]. If the interviewee, a seasoned SME, determines that the interviewer does not have a strong understanding of the related tasks, data, or concerns, they may choose to skip through the interview with minimal effort, rendering the efficiency and usefulness of the resulting visualization negligible.

Throughout the interview, equipment to support and capture the SME's participation in the design process must be available. Equipment could include a whiteboard, large sheets of paper with colored pens, LEGO sets, a computer with access to the datasets the SME could refer to, or other tools, that would help and encourage the SME to express their perception of the structure of the data in three-dimensional space. With LEGO sets, for example, they could lay out the structure of groups on the table and build them vertically, to a limit. With whiteboard SME could sketch the possible visualizations, while the interviewer may need to help with capturing its dimensionality.

The questions below are examples for how to enable the SME to think through their knowledge of the targeted data and lay out the groups. Not only should these questions be adjusted for the specifics of the role of the person and data source or data set, but also to the personality of the SME. The interviewer may need to adjust or rearrange the sequence of the questions based on the responsiveness of the SME.

Question 1: What are the primary everyday tasks that require you to use large data sources (datasets, data collections)?
The intent of this question is to build rapport with the SME, while finding out the specific role of the interviewee and the data that the interview should focus on. To help the SME articulate their tasks, a list of tasks from the Reference Spreadsheet for the NICE Framework [18] (respectively for PR-CDA-001, PR-CIR-001 and OM-NET-001 or others) could be shown to the interviewee. Depending on the tasks identified, interviewer could then choose which one(s) of the data source(s) relevant to the tasks to focus on.

Question 2: What groups of networked entities participate in your computer networks?
The intent of this question is to identify the nested groups of additional groups and entities (in the data source that was identified in Q1) that could be laid out spatially. If the interviewee can't name any such groups spontaneously, the interviewer may suggest the following examples:

1. Physical entities, e.g., users, administrators, guests, known external actors (including intruders).
2. Endpoints, e.g., user workstations and laptops.
3. Network infrastructure devices, e.g., switches, routers.
4. Virtual or physical networked services, e.g., Active Directory Domain Controller, a file server, databases, network security services (DLP, SIEM, traffic collectors, etc.), as well as physical computers running the virtualized containers, containing the offered services.
5. Special purpose equipment, e.g., physical access control, Industrial Control Systems.
6. External partners' services inside or outside the perimeter.
7. Unknown entities.

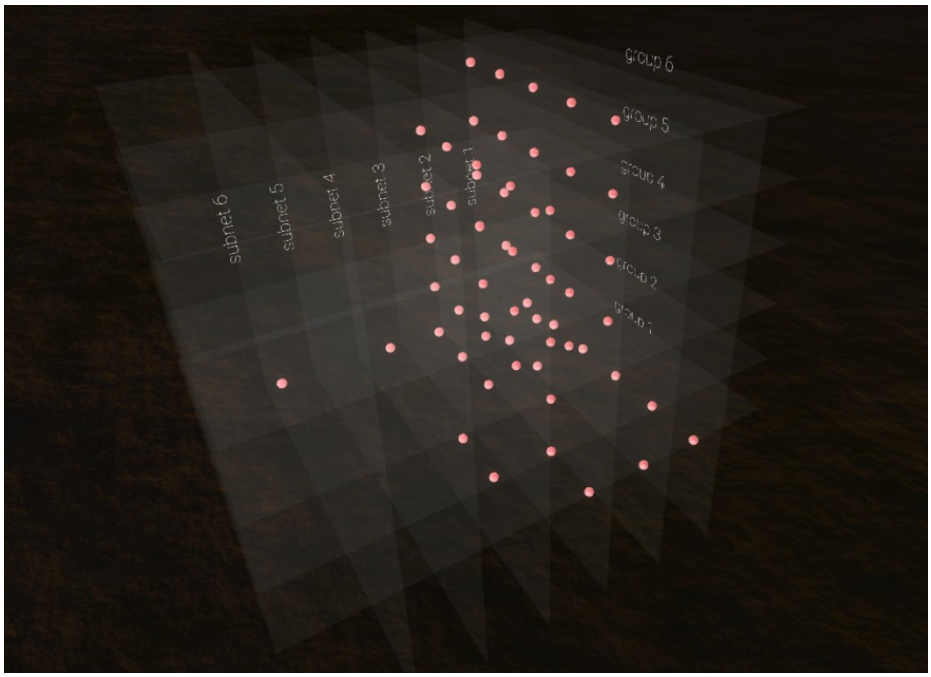

Fig. 2. Closeup of an example of triples arranged in a cube shape.

Question 3: What subgroups [and further subgroups] could there be within those groups?
The intent of this question is to help the interviewee to consider different ways of thinking about the dimensions of data and choose the better candidates to be represented by the three axes in a 3D visualization, and the relative positioning of these groups.

See Figure 2, where entities' positions on XYZ axes are determined by:

Z) the group this entity belongs to (a subnet).

Y) subgroup (a functional group in that subnet: servers, networks devices, workstations).

X) entity's sequential (arbitrary) position in in that subgroup (for example the last octet of its IP address).

Question 4: How would you decide to which group an entity belongs, based on its behavior?
The intent of this question is to understand how to build the decision process for the VDE (or other visualization interface) that determines where and how to show each entity in the visualization.

Question 5: While working on task X (identified in Q1), what data source do you investigate first (second, third, etc.), and what would you be looking for in that data?

1. What questions are you asking while building a query to find relevant data in that data source?
2. What clauses would you use to build a query on that data source to acquire relevant information for this question?
3. How do you determine if the result returned by the query contains benign information or if it requires further investigation from the same or other data sources?
4. What other data sources do you consult to validate if the data is an anomaly or indicator you found is interesting or benign?
5. If you've identified a recurring identifier, how do you implement its automatic detection for the future?
6. Repeat {1 - 5} for other data sources relevant for the interviewee.

Question 6: Please group the most relevant query conditions (or categories of indicators) that you use in your tasks to group the found entities into groups of three. This question elicits triples that will then be aligned on 3 axes to create 3D data-shapes. Examples of potential triple groupings are shown in Table 1, while Figures 1 and 2 show a 3D data-shape for an individual triple. Multiple related triples can be presented in constellations of data-shapes, as shown in Figures 3 and 4.

The intent of this question is to find the queries that should be run to gather data for rendering the visualization of groups identified in Question 3.

Table 1. Examples for mapping identified groups to 3D axes (triples).

axis	Example 1 (see Fig. 2)	Example 2 (combination of addressing components)	Example 3 (functional topology of groups of entities in an organization)	Example 3 (private address space)
Z	entity group	subnet (e.g., 10.0.x.0/8)	Organizational group (marketing, admin, HR, etc.) the entity is part of	10.x.0.0/8
Y	entity subgroup	last octet of entity's IP address	Team within larger Org. group (accounts payable / receivable) the entity is part of	10.0.x.0/8
X	inter-subgroup sequence	active ingress / egress port nr	Sequential position in the team (team manager or staff; HQ or satellite office)	10.0.0.x/8

Question 7: Please arrange triples (see examples in Table 1) into a relational structure on the whiteboard.
The intent of this question is to encourage the SME to reimagine (and redraw if needed) the groups and their arrangement into subgroups so that instead of just 3x3 relations, triples would be positioned spatially into a stereoscopically perceivable constellation

data-shape (see Figure 3), adding additional dimensions for potential additional data encoding.

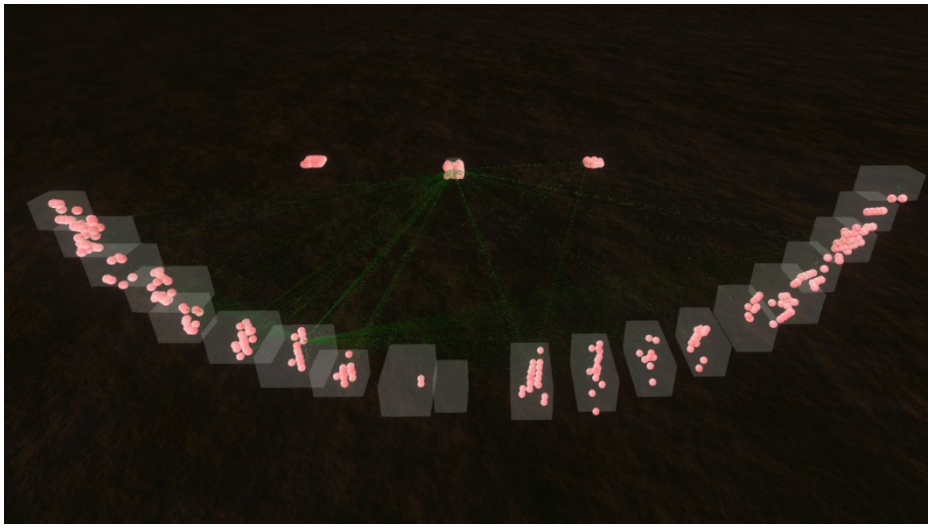

Fig. 3. Overview of a set of groups of groups of entities arranged into a constellation.

At this stage the interview should be ripe for in-depth discussion about the findings and possible enhancements of the sketches of visualizations that were created by the SME and the interviewer to make sure there is enough details for its implementation.

Based on the sketches created during the interview by the interviewer and SME, they will select one or more layouts as potential designs to be implemented in VDE (or other) software for further evaluation. Once the SME's understanding of their dataset has been documented, the interviewer will explain further steps (e.g., timeline of implementation, further testing with her / his data, if necessary).

3.3 Implementation of Data Visualization

After conducting Session 1 interviews, the data-shapes identified during those interviews will be evaluated by the conductor of the study with the following criteria:

1. The proposed visualization differs from existing 2D or 3D data-shapes that either the SMEs referred to, or which are previously known to authors (for example, Figures 1 - 4). If the visualization layouts are easily customizable to the needs of the SME and with the available data, that shall be done.
2. The data-shape can be rendered functional using the data that the SME referred to during their Interview Session 1.

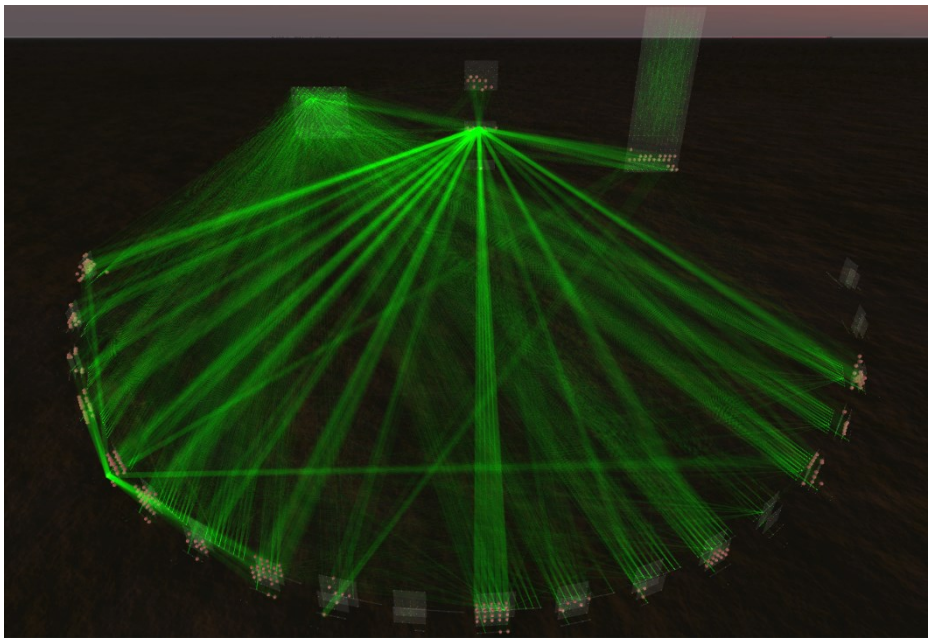

Fig. 4. Overview of a constellation of groups, where subgroups of entities can be distinguished afar, and examined in detail when user zooms in (moves closer with the VR headset).

Layouts that meet the evaluation criteria are implemented with chosen software. In case the VDE is used, the visualization layouts are either created via new configuration files, or by implementing the necessary new components with C# and Unity 3D.

Once all the data-shapes identified during the Session 1 interviews have been implemented in the visualization software, and each SME's visualization has been reviewed with the data sources specified by the SME and found to support the analytical goals provided by the interviewee that it was designed with, Session 2 interviews will be scheduled.

3.4 Interview Session 2

The goal of these interviews is for each SME to evaluate the usefulness of the visualization(s) developed based on their interview and other visualizations that were created for their colleagues for the same data and / or role. At the start of the interview, the SME will be reminded about the findings from the Session 1 interview and asked for permission to record the audio and video during the current session. When each visualization is introduced, the interviewer will thoroughly explain the logic of the visualization process to the SME, to make sure they fully understand what is being visualized and why, and ensure the SME knows how to use the visualization with their data and interpret its results.

The SME will then be asked to answer some task-related questions while using each of the visualizations: for example, can the visualization enable the SME to identify

whether (a) *a suspicious host* has initiated a connection targeting an entity that is currently (b) *vulnerable* and/or the physical or functional provenance of the targeted entity is (c) *part of the protected network* at the (d) *time* when this behavior was observed. Afterwards, the SME will be asked to provide feedback on the visualizations. This feedback will be subjective measures of mental workload and usability, measured using standard survey instruments, respectively the Modified Cooper-Harper (MCH) [19] Scale and the System Usability Scale (SUS) [20]. MCH uses a decision tree to elicit mental workload; the SME simply follows the decision tree, answering questions regarding the task and system in order to elicit an appropriate workload rating. In the SUS, participants are asked to respond to 10 standard statements about usability with a Likert scale that ranges from "Strongly Agree" to "Strongly Disagree". The SUS can be used on small sample sizes with reliable results, effectively differentiating between usable and unusable visualizations. Once done, the SME is asked, using open ended questions to provide overall feedback on the visualizations used, as well on the process of the interviews.

4 Conclusion

The mental model mapping method described in this paper could be used to create data visualizations with SMEs that would be beneficial for them and their immediate peers' purposes. Visualizations that originate from the same SME group could be evaluated by peers from that same group, preferably with the same dataset or using the same original data sources.

The participatory design method described in this paper focuses on creating 3D visualizations for Virtual Data Explorer. With appropriate changes, it may be also applicable for developing 2D visualizations for cybersecurity.

Our follow-up study will describe the results of applying this interviewing method, including an overview of the results of Session 1 interviews, descriptive visualizations of the data-shapes created during the study, lessons learnt from applying the interviewing method and overview of SME feedback on the visualizations used during Interview Session 2.

Later studies could investigate whether data-shapes created based on interviews with experienced SMEs are more accurate and detailed than the data-shapes for the same data that were created during interviews with less experienced SMEs. Another area ripe for research is evaluating what impact these 3D data-shapes developed based on experienced users' interview might have in teaching the (functional, physical, logical) topology of a protected network environment. It is possible that this would speed up the onboarding of new team members by assisting them in learning the functional topology and the behavior of entities that are present in their datasets, for example, the logs from various devices in the protected computer networks.

Further evaluation of the qualitative differences between the 3D visualizations created with SMEs could be done with a follow up study, where the control group's members are not granted access to these 3D visualizations, while experimental group will be taught to use the 3D visualizations created during the study.

5 Acknowledgements

For all the hints, ideas and mentoring, authors thank Jennifer A. Cowley, Alexander Kott, Lee C. Trossbach, Jaan Priisalu, Olaf Manuel Maennel. This research was partly supported by the Army Research Laboratory under Cooperative Agreement Number W911NF-17-2-0083. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

6 References

[1] NIST, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800-181)," NIST, Gaithersburg, 2017.

[2] A. Sethi and G. Wills, "Expert-interviews led analysis of EEVi — A model for effective visualization in cyber-security," in *IEEE Symposium on Visualization for Cyber Security*, Phoenix, AZ, USA, 2017.

[3] R. Marty, Applied Security Visualization, 2008.

[4] K. Kullman, N. B. Asher and C. Sample, "Operator Impressions of 3D Visualizations for Cybersecurity Analysts," in *ECCWS 2019 18th European Conference on Cyber Warfare and Security*, Coimbra, 2019.

[5] K. Kullman, M. Ryan and L. Trossbach, "VR/MR Supporting the Future of Defensive Cyber Operations," in *The 14th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine Systems*, Tallinn, 2019.

[6] G. Shearer and J. Edwards, "Vids Cyber Defense Visualization Project," US Army Research Laboratory, Adelphi, 2020.

[7] T. Munzner, Visualization Analysis & Design, A K Peters/CRC Press, 2014, p. 428.

[8] M. O. Ward, G. Grinstein and D. Keim, "Interaction Techniques," in *Interactive Data Visualization: Foundations, Techniques, and Applications, Second Edition*, A K Peters/CRC Press, 2015, pp. 387-406.

[9] Y. Wu, L. Xu, R. Chang, J. M. Hellerstein and E. Wu, "Making Sense of Asynchrony in Interactive Data," *JOURNAL OF LATEX CLASS FILES,* vol. 14, no. 8, 2018.

[10] S. Mckenna, D. Staheli and M. Meyer, "Unlocking user-centered design methods for building cyber security visualizations," in *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Chicago, IL, 2015.

[11] L. Buchanan, A. D'Amico and D. Kirkpatrick, "Mixed method approach to identify analytic questions to be visualized for military cyber incident handlers," in *IEEE Symposium on Visualization for Cyber Security (VizSec)*, Baltimore, MD, 2016.

[12] J. Simonsen and T. Robertson, Routledge International Handbook of Participatory Design, Routledge, 2012.

[13] K. Marriott, J. Chen, M. Hlawatsch, T. Itoh, M. A. Nacenta, G. Reina and W. Stuerzliger, "Just 5 Questions: Toward a Design Framework for Immersive Analytics," in *Immersive Analytics*, Cham, Springer, 2018, pp. 259-288.

[14] K. Marriott, J. Chen, M. Hlawatsch, T. Itoh, M. A. Nacenta, G. Reina and W. Stuerzlinger, "3D for Information Visualization," in *Immersive Analytics*, Cham, Springer, 2018, pp. 25-55.

[15] K. Kullman, J. Cowley and N. Ben-Asher, "Enhancing Cyber Defense Situational Awareness Using 3D Visualizations," in *13th International Conference on Cyber Warfare and Security*, Washington, DC, 2018.

[16] W. Stuerzlinger, T. Dwyer, S. Drucker, C. Görg, C. North and G. Scheuermann, "Immersive Human-Centered Computational Analytics," in *Immersive Analytics*, Cham, Springer, 2018, pp. 139-163.

[17] G. Klein and D. G. MacGregor, "Knowledge Elicitation of Recognition-Primed Decision Making," US Army Systems Research Laboratory, Alexandria, Virginia, 1988.

[18] NIST, Applied Cybersecurity Division, National Initiative for Cybersecurity Education (NICE), "Reference Spreadsheet for the NICE Framework, NIST SP 800-181," 18 01 2018. [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center/current. [Accessed 01 2020].

[19] P. W. Jordan, B. Thomas, I. L. McClelland and B. Weerdmeester, "Modified Cooper-Harper (MCH) Scale," in *Usability Evaluation In Industry*, CRC Press, 1996, pp. 189-194.

[20] B. Donmez, A. S. Brzezinski, H. Graham and M. L. Cummings, "Modified Cooper Harper Scales for Assessing Unmanned Vehicle Displays," MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 2008.