TAL TECH

DOCTORAL THESIS

Interactive Stereoscopically Perceivable Multidimensional Data Visualizations for Cybersecurity

Kaur Kullman

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY
TALLINN 2023

TALLINN UNIVERSITY OF TECHNOLOGY
DOCTORAL THESIS
10/2023

Interactive Stereoscopically Perceivable Multidimensional Data Visualizations for Cybersecurity

KAUR KULLMAN

TAL TECH PRESS

TALLINN UNIVERSITY OF TECHNOLOGY
Department of Software Science
Centre of Digital Forensics and Cyber Security
This dissertation was accepted for the defence of the degree 13/04/2023

Supervisor: Professor Olaf Manuel Maennel
School of Computer and Mathematical Sciences
The University of Adelaide
Adelaide, Australia

Co-supervisor: Professor Don Engel
Computer Science and Electrical Engineering
University of Maryland, Baltimore County
Baltimore, Maryland

Co-supervisor: Professor Stefan Sütterlin
Centre of Digital Forensics and Cyber Security
Tallinn University of Technology
Tallinn, Estonia

Opponents: Dr Alexander Kott
Chief Scientist
U.S. Army Research Laboratory, U.S. Army
Adelphi, Maryland

Dr Simon Su
Computer Scientist
National Institute of Standards and Technology
Gaithersburg, Maryland

Dr Matthew Sorell
Faculty of Sciences, Engineering and Technology
The University of Adelaide
Adelaide, Australia

Defence of the thesis: 25/04/2023, Tallinn

Declaration:
Hereby I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology has not been submitted for doctoral or equivalent academic degree.
Kaur Kullman

---
signature

Copyright: Kaur Kullman, 2023
ISSN 2585-6898 (publication)
ISBN 978-9949-83-966-7 (publication)
ISSN 2585-6901 (PDF)
ISBN 978-9949-83-967-4 (PDF)
Printed by Koopia Niini & Rauam

TALLINNA TEHNIKAÜLIKOOL
DOKTORITÖÖ
10/2023

Interaktiivsed, ruumiliselt tajutavad, mitmemõõtmelised andmekuvad küberturbele

KAUR KULLMAN

TAL TECH
KIRJASTUS

Contents

List of Publications

The list of author's publications, the foundation on which the thesis has been prepared:

I Kullman, K.; Cowley, J.; Ben-Asher, N. (2018). Enhancing Cyber Defense Situational Awareness Using 3D Visualizations. Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018: National Defense University, Washington DC, USA 8-9 March 2018. Ed. J. S. Hurley, J. Q. Chen. Academic Conferences and Publishing International Limited, 369−378. [1]

II Kullman, Kaur; Asher, Noam Ben; Sample, Char (2019). Operator Impressions of 3D Visualizations for Cybersecurity Analysts. Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019: University of Coimbra, Portugal, 4-5 July 2019. Ed. Cruz, Tiago; Simoe, Paulo. Reading, UK: ACPI, 257−266. [2]

III Kullman, Kaur; Ryan, Matt; Trossbach, Lee (2019). VR/MR Supporting the Future of Defensive Cyber Operations. 14th International-Federation-of-Automatic-Control (IFAC) Symposium on Analysis, Design, and Evaluation of Human Machine Systems (HMS), SEP 16-19, 2019, Tallinn, ESTONIA. Amsterdam: ELSEVIER, 181−186. (52). DOI: 10.1016/j.ifacol.2019.12.093 [3]

IV Kullman, Kaur; Buchanan, Laurin; Komlodi, Anita; Engel, Don; (2020). Mental Model Mapping Method for Cybersecurity. Lecture Notes in Computer Science, vol 12210. Ed. Moallem, Abbas;. Cham: Springer International Publishing, 458−470. DOI: 10.1007/978-3-030-50309-3_30 [4]

V Kullman, Kaur; Engel, Don; (2022). Interactive Stereoscopically Perceivable Multidimensional Data Visualizations for Cybersecurity. Journal of Defence & Security Technologies, Vol.4: Big Data Challenges – Situation Awareness and Decision Support. DOI: 10.46713/jdst.004.03 [5]

VI Kullman, Kaur; Engel, Don; (2022). User Interactions in Virtual Data Explorer. Augmented Cognition in Cyber Security, 24th International Conference on Human-Computer Interaction. DOI: 10.1007/978-3-031-05457-0_26 [6]

VII Varga, Margaret; Liggett, Kristen K.; Bivall, Petter; Lavigne, Valérie; Kullman, Kaur; Camossi, Elena; Ray, Cyril; Arkin, Ethem; Krilavičius, Tomas; Mandravickaitė, Justina; Winkelholz, Carsten; Träber-Burdin, Susan; Jayaram, Shivas; Panga, Marius; Acharya, Nikhil; (2022). NATO IST STO-141 Workgroup Final Report: Exploratory Visual Analytics. Science and Technology Organization of the North Atlantic Treaty Organization. DOI: 10.14339/STO-TR-IST-141 [7]

VIII Ask, Torvald F.; Kullman, Kaur; Sütterlin, Stefan; Knox, Benjamin J.; Engel, Don; Lugo, Ricardo G.; (2023). A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. Front. Big Data 6:1042783. DOI: 10.3389/fdata.2023.1042783 [8]

Author's Contribution to the Publications

Contribution to the papers in this thesis are:

I In I, I was the main author, designed the 3D data visualizations, developed the Virtual Reality software, prepared the figures, wrote the manuscript, and presented at the conference.

II In II, I was the main author, designed the study and its software components, conducted and transcribed the interviews, prepared the figures, wrote the manuscript, and presented at the conference.

III In III, I was the main author, gathered the sources, prepared the figures, wrote the manuscript, and presented at the conference.

IV In IV, I was the main author, gathered the team with necessary expertise for creating the M4C while spearheading its development, prepared the figures, wrote the manuscript, and presented at the conference.

V In V, I was the main author, gathered the sources, prepared the figures, and wrote the manuscript.

VI In VI, I was the main author, gathered the sources, prepared the figures, wrote the manuscript, and presented at the conference.

VII In VII, I was one of the authors of two chapters in the Final Report of NATO IST STO-141 workgroup: "Chapter 2: Human Factors Considerations for Visual Analytics" and "Chapter 7: Cyber Situation Awareness"

VIII In VIII, I was the second author, supplying the software and dataset for the study, preparing the scenario and tasks for the participants, executing the study with three other co-authors and writing the paper together with other co-authors.

Introduction

Cybersecurity has been defined in various wordings, but for the purpose of the thesis, this one will be used: “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.” [9].

To deliver that “availability, integrity, authentication, confidentiality, and nonrepudiation” of a to-be-protected system, the personnel responsible for such a task must maintain actionable situational awareness and situational understanding of said information system [10].

To grasp the complexities of that task, consider the definition of Information System as: “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information” and Cyber Incident as: “Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein.” [9].

The larger such a to-be-protected system (of systems) becomes the more vulnerabilities such a system may have, and the longer that system remains in use, the better the chances for those vulnerabilities to be discovered and (ab)used [11]. Therefore as functionalities are added to systems (of systems) that enable our information society to function and its existing components altered or such systems interconnected to each other, additional complexities may be introduced that, in combination, may yield such complex systems vulnerable in ways that even individual systems separately were not.

Hence, the personnel responsible for maintaining and protecting such (complex) systems must (in addition to other mitigations) monitor those systems for anomalous behaviours to timely detect and mitigate possible Cyber Incidents [12]. However, to identify such anomalous behaviours of (complex) systems, defenders first need to establish the baseline behaviour, either via human observations [13] or attempting to utilize machine learning methods on behavioural indicators gathered from that or similar system(s).

My research interest focuses on how to enhance operators’ capabilities: what current of future tools would best assist a defender, who has been tasked to learn the expected (baseline) behaviour of an information system (of systems) to identify anomalous behaviours affecting it. Further, given that the datasets which must be understood and monitored are usually large, inherently multidimensional, and given that a considerable part of human population is naturally better at reading visual than textual information [14], what visualization tools would be helpful, during sensemaking of such a dataset?

While visualizing complex systems’ network structures on a flat computer screen is helpful, the lack of stereoscopical perception of these visualizations hindered the usefulness of such visualizations (see: 2.1). As I was beginning this work, Virtual Reality (VR) headsets were coincidently making comeback on the consumer market and seemed to provide a possible platform for testing out stereoscopically perceivable multidimensional data visualizations rendered in VR (see: 2.3). As there were no 3D VR (nor Mixed Reality, MR) visualization tools publicly available at that time, I identified this as an interesting research area with possible benefits to cybersecurity practitioners, while also creating helpful tools for my cybersecurity peers.

1.1 Problem Statement

The quantity of logs, telemetry, and various other data that is collected from networked devices and devices that are running these networks is increasing steadily, if not exponentially due to our society's growing dependence on interconnected information technology [15]. This collected data is in turn instrumental for the protection of those interconnected devices that our society relies on. Cyber Defence Analysts, Cyber Defence Incident Responders and Network Operations Specialists (designated as PR-CDA-001, PR-CIR-001, OM-NET-001 respectively and bearing responsibilities for tasks identified in [16]), referred to as Subject Matter Experts (SME) from here onwards, are working in Security and Network Operations Centres (SOC/NOC), to maintain Cyber Defence Situational Awareness (CDSA) and Situational Understanding (CDSU) and thereby protect the interconnected systems, and our society.

More data does not in itself yield better information. To make sense of the collected data in a timely manner, i.e., to maintain actionable CDSA & CDSU, SMEs need to know well the system (of systems) they need to protect and be able to augment the expected (but everchanging) baseline of their (known) system with relevant (subset of) fresh data, to transform the combination of gathered information into actionable CDSE, that will then feed into timely CDSU: See Figure 1 Situational Awareness & Situational Understanding.

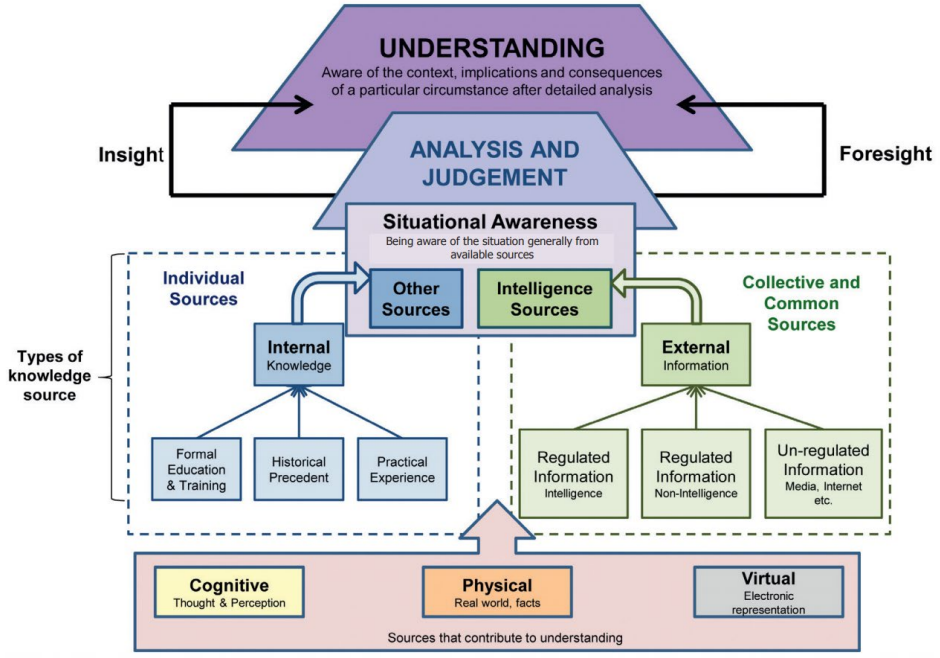


Figure 1 Situational Awareness & Situational Understanding [17]

To fulfil that task, SMEs usually combine the output from command line tools with dashboard visualizations, that allow them to interact (e.g., filter, drill, etc.) with the data depicted as charts and graphs on that dashboard. The dashboards that are deployed in a NOC/SOC usually provide an array of two-dimensional (2D) graphs and charts in addition to alphanumeric formats that summarize different types of data, such as system

logs, network traffic, threat feeds, and so on. However, because that data is often multidimensional, the entity responsible for designing a dashboard must solve the problem of how to translate multidimensional data (for example: the topology of an interconnected system) into 2D visualizations on flat screens [18].

If the mental models that SMEs have established internally to understand (to know the baseline and identify unexpected behaviours in) the protected systems, are relational and perceivable as spatial (or contain more than two data dimensions), then converting ingested data from textual inputs or flat 2D visualizations back to that perceivably spatial mental model, so that the SME could internalize the perceived data, will require some conversions and / or translations of the dimensionalities of the ingested data, hence adding to the mental workload of the SME. However, this dimensionality conversion should not be confused with interpreting 3D visualizations from flat screens (using shadows and other cues): while both conversions do render a measurable perceptual lag and often pile on to subjective mental workload, the underlying reasons for that lag are different [1].

Head Mounted Displays (HMD) with good enough resolution and interactive usability for providing SMEs with customized, stereoscopic 3D visualizations, may enhance SMEs capability to understand the state of their systems in ways that flat displays with either text, 2D, or 3D visualizations cannot afford, provided that the visualizations of their data is aligned with SMEs internalized representations of their data. In fact, for such visualizations to be useful, these must align with SMEs internalized understanding of their data [18]. Hence to reap the benefits of emerging technologies (in this case Virtual and Mixed Reality HMD-s) for CDSA, one must first address a few interdisciplinary problems (see: Research Questions below).

1.2 Research Questions

1. How to extract SMEs implicit and explicit understanding of the data that they work with?
2. How to create (based on findings from Research Question 1 [RQ1]) such useful, interactive, multi-dimensional visualizations that would assist SMEs with their tasks?
3. Acquire or develop software that would be capable of presenting SMEs with the visualizations created based on RQ2 findings: in stereoscopically perceivable (VR/MR) environments, enabling intuitive interactions with the visualizations, to allow experiments to disprove or verify the effectiveness of such visualizations.

The mapping of research questions to the particular publication and to the thesis chapter, where the question is explored and answered, is presented in Table 1:

Table 1 – Mapping of research questions and publications

Research Question	Publication	Chapter in Thesis
RQ1	II, IV, VII	3.2
RQ2	IV, VI	3.2
RQ3	I, II, III, V, VI, VII, VIII	3.1, 4.2

1.3 Research Methodology and Methods

Although data Visualization is a well-researched discipline [14], the subset dedicated to cybersecurity is a relatively new [19] and evolving rapidly with the industry, to accommodate the ever-changing needs of SMEs responsible for protecting their information systems [20]. Applied research methods are therefore usually qualitative rather than quantitative.

Although stereoscopically perceivable multidimensional data visualizations have become common for datasets which are either natively spatial (example: factory floor augmented with AR/MR to provide users with timely information on working equipment [21]) or natively geospatial (example: visualizing flooding effects on coastal areas [22]), during the past few years, natively non-spatial multidimensional datasets (example: network traffic, endpoint logs) visualized in 3D have attracted less attention from the research community, possibly due to a relatively high barrier of entry for users and researchers.

For the purposes of this research, multiple iterations of software were created to experiment with 3D data visualizations using various Virtual Reality (VR) and Mixed Reality (MR) headsets to evaluate the feasibility of such visualizations [1], and gather SMEs' feedback on stereoscopically perceivable data visualizations [2]. Such rapid prototyping was crucial for understanding the capabilities and limitations of the VR/MR technology that has evolved significantly since the beginning of this research (Oculus DK2 in 2014 vs Microsoft HoloLens 2 in 2022) and to gather SMEs feedback to data visualization prototypes [2] while following the design science research model.

1.4 Contribution

Prior to my research, there were no publicly available data visualization tools (RQ3) that would have enabled its users to create and use stereoscopically perceivable immersive and interactive 3D visualizations depicting non-(geo)spatial datasets as multidimensional shapes: existing tools (the likes of OpenGraphiti and V-Arc) were able to visualize force directed graphs, bar charts and the like.

There were no applicable method(s) detailing the process of creating such visualizations that would be rooted in Cybersecurity Subject Matter Experts (SMEs) mental models (such that would map to the visualized dataset), integrated into an analyst's existing working environment, while also support an analyst's existing problem-solving strategies (RQ1 & RQ2).

The software I created, Virtual Data Explorer (VDE), has been integrated into the Virtual Reality Data Analysis Environment (VRDAE) [3] and Mixed Reality Exploration Toolkit (MRET) [23]. These and other collaborative projects employing VDE for research have resulted in additional papers [24] [23], while commercial deployments are under way. VDE was instrumental in seeking answers for RQ3.

The Mental Model Mapping Method for Cybersecurity (M4C) addressing RQ1 & RQ2 was published in 2020 [4].

The overall contribution of this research is the development of the knowledge and practical approaches of how to visualize multidimensional non-(geo)spatial datasets in stereoscopically perceivable (artificial) environments in useful ways, how to design the three-dimensional layouts of such visualizations, but also the VDE software and its release as open source software.

1.5 Thesis Structure

This thesis is divided into 9 chapters. This introduction chapter provides a brief overview of the challenges that SMEs face while maintaining actionable CDSA, as well as the research questions and contribution of the thesis. Chapter 2 gives an overview of related work and background in VR/MR challenges and opportunities in the context of data visualization, challenges related to designing useful data visualizations for SMEs (either for flat screens or stereoscopically perceivable HMD visualizations), and current state of cybersecurity specific data visualization overall.

Chapter 3 focuses on human sciences side of the creation process of a (3D) data visualization, while Chapter 4 describes the high-level structure of VDE software components. In addition, this Chapter provides visual examples of VDE data visualizations and links to accompanying videos. Chapter 5 moves on to describing the novel Mental Model Mapping Method (M4C) created for designing stereoscopically perceivable (3D) data visualizations together with SMEs for their datasets.

Chapter 6 focuses on the applications of stereoscopically perceivable data visualizations in NOC/SOC settings, its use-cases, possible advantages, and disadvantages compared to conventional flat-screen data visualizations.

As the M4C research involves human subjects, Chapter 7 emphasizes the privacy and ethics aspects of such process and also confirms the ethical guidelines followed during this research. Chapter 8 acknowledges the limitations to this research. Chapter 9 concludes the work done and brings out the main findings of this research and outlines further work.

Abbreviations and Terms

AR	Augmented Reality Monoscopic view of information rendered on a tiny screen (usually) visible with only one eye for the user. Augmentation is not perceived relative to the real-world environment.
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CDSA	Cyber Defence Situational Awareness The perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. [25]
CDSU	Cyber Defence Situational Understanding Perception and interpretation of a particular (cybersecurity-related) situation in order to provide context, insight and foresight required for effective decision making.
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
CDX	Cyber Defence eXercise
Dataset	In the context of this thesis, “dataset” refers to a collection of individual data sources, e.g., network flow data, log files, PCAP, databases and other stores (Elasticsearch, Mongo, RDB-s,) used by an SME at a particular organization.
FPS	Frames Per Second Frames Per Second is the rate at which different frames (single pictures that together form a film or video game) appear on a screen.
HMD	Head Mounted Display
ISPMDV	Interactive Stereoscopically Perceivable Multidimensional Data Visualizations [5]
LS	NATO CCDCOE CDX Locked Shields (see: 4.6)
M4C	Mental Model Mapping Method for Cybersecurity [4]
MR	Mixed Reality Stereoscopically perceivable, interactive, computer-generated depiction or view of combined real-world and computer-generated elements.
MRET	Mixed Reality Exploration Toolkit [23]
NATO	North Atlantic Treaty Organization
NOC	Network Operations Centre
SME	Subject Matter Expert In the context of this thesis mostly used to refer to Cybersecurity SME-s.
SOC	Security Operations Centre
VDE	Virtual Data Explorer (see: 4.2)
VDEC	Virtual Data Explorer Client (see: 4.4)
VDES	Virtual Data Explorer Server (see: 4.3)
VR	Virtual Reality Stereoscopically perceivable, interactive, computer-generated depiction of a real or artificial world or activity.
VRDAE	Virtual Reality Data Analytics Environment [26]

Explanations of abbreviations used in the thesis – the table.

2 Related Works and Background

This chapter gives an overview of related work and background regarding current state of cybersecurity specific data visualization overall, challenges related to designing useful data visualizations for SMEs (either for flat screens or stereoscopically perceivable HMD visualizations), challenges and opportunities in the context of cybersecurity data visualization, and last but not least, possible benefits of using multidimensional (3D) and stereoscopically perceivable (VR/MR) data visualizations for cybersecurity.

2.1 Data Visualizations for Cybersecurity

Visualizations provide cybersecurity SMEs with visual representation of alphanumeric data that would otherwise be difficult to comprehend due to its large volume. Such visualizations aim to effectively support analysts tasks including detecting, monitoring and mitigating cyber-attacks in a timely and efficient manner [27]. Cybersecurity specific visualizations (see: 2.2) can be broadly classified into three main categories: 1) network analysis, 2) malware and threat analysis, and 3) 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 [19] as well as universal software with visualization capabilities like Tableau, MS Excel, R, Power BI, D3 libraries (d3.js) and a plethora of Python (with or without Jupyter Notebook) gadgets among many others. These tools could be used to visualize data in a myriad of ways [14] so that analysts could explore their datasets visually and interactively [28]. *Graphistry* is one recent example of a 2D force-directed graph visualization [29] with an interface that is easy to manage and responsive to queries on massive datasets. These are crucial qualities for cybersecurity analysts, with emphasis on the importance of the low latency between an analyst's request for a change in visualization (change in filter, time window, or other query parameters) and rendering of the visualized response from the system [30].

The usability of data visualizations for CND operations that have not been evaluated, may lead to low adoption rates by practitioners [31]. The challenge in creating useful visualization for cybersecurity practitioners is in aligning data visualization experts' knowledge with cybersecurity practitioners' needs and knowledge so, that the resulting visualizations would be useful for cybersecurity practitioners' tasks. A recent survey showed that 46% of 130 cybersecurity tools did not have any user-involvement in their evaluation phase [27].

To achieve higher visualization adoption rates, analysts should have the ability to intuitively and iteratively adjust the visualizations to suit with their changing needs [32]. Datasets used in cybersecurity operations are often multi-dimensional and analysts would either have to scale down the number of dimensions viewed at one time to be able to use 2D & 3D visualizations or combine multiple 2D visualizations displaying different dimensions of the same dataset in a single dashboard. This requires the designer to properly encode variables (dimensions) into shape, colour, size and other visual channels. The viewer must translate that shape into spatial perception and compare it to their internal understanding of the data in order to decode the meaning of the visualizations; a task that may be non-trivial [33]. There have been numerous attempts to employ 3D visualizations for cybersecurity data that are displayed on flat computer screens with varying degrees of success. Such visualizations sometimes use monocular depth cues [34] and object movement to convey the 3D shape of the

visualization; advantages and disadvantages of which were thoroughly discussed in [1]. VIDS [35] provides an interactive 3D environment for visualizing network and alert (or other) data in 3D shapes, whereby users can seamlessly switch styles and layouts to dynamically shape their data and easily adjust their viewpoint [36]. Real-time 3D visualization engine DAEDALUS-VIZ allows operators to grasp visually and in real-time an overview of alert circumstances, while providing highly flexible and tangible interactivity [37]. InetVis [38] allows the user to allocate source and destination IPv4 addresses to X and Z axis, while destination ports are being allocated to the Y axis on a 3D cube. To understand the shape of the cube and detect the positions on Z axis, user must manually change the viewpoint with a mouse. Shoki [39] allows the user to define what values are plotted on which axis, while the screen is divided to four squares, three of them showing each axis in 2D, while the fourth square displays the cube as a 3D object.

Due to the emergence of commodity VR devices, multiple data visualization tools have implemented support for VR headsets, that are capable of 6 degrees of freedom (6DOF) movement of the user's viewpoint, allowing the observer to perceive the depth of the visualization stereoscopically, avoiding the mental work needed to convert 2D images to 3D. OpenGraphiti [40] provides the ability to interact with customizable graphs, along with querying and filtering capabilities. While OpenGraphiti does not provide 3D VR interaction capacities, V-Arc [41] did enable the positioning of data in a predetermined layout; data selection; and color-coding amongst other capabilities. However, V-Arc was never released to the public.

To bridge the gap and enable users to visualize data as predetermined three-dimensional layouts that are be stereoscopically perceivable and interactive, I created the Virtual Data Explorer (VDE, see: 4). VDE enables a user to perceive the spatial layout of a dataset, for example the topology of a computer network, while the resulting visualization can be augmented with additional data, such as the count of TCP/UDP sessions between network nodes [1].

2.2 Purposes for Cybersecurity Visualizations

SMEs responsible for ensuring the security of networks and other assets utilize a wide array of computer network defence (CND) tools, such as Security Information & Event Management (SIEM) that allow data from various sources to be processed, providing alerts when appropriate. CND tools allow analysts to monitor, detect, investigate, and report incidents that occur in the network, as well as provide an overview of the network state. To provide analysts with such capabilities, CND tools depend on the ability to query, process, summarize and display large quantities of diverse data which have fast and unexpected dynamics [42]. Shneiderman [43] provided a taxonomy depicting 7 human-data interaction task levels:

1. Gaining Overview of the entire dataset,
2. Zoom on an item or subsets of items,
3. Filter non relevant items,
4. Get Details-on-Demand for an item or subset of items,
5. Relate between items or subset of items,
6. Keep History of actions and
7. Allow Extraction of subsets of items and query parameters.

Traditionally, cyber defenders have used command line tools and alphanumeric data displays to execute these seven tasks. With the need for faster and more accurate situational awareness of increasing data volume, many CND tools have integrated graphical user interface (GUI) and 2-dimensional (2D) data visualizations to expedite human information acquisition.

2.2.1 Exploratory Visualizations

An example of a visualization that may be useful for gaining an (initial) overview of an entire dataset or a subset thereof could be a force-directed 2D graph, of which an example is shown on Figure 2 below. These and many other illustrative visualizations in this thesis are rendered from the North Atlantic Treaty Organization's (NATO) Cooperative Cyber Defence Centre of Excellence (CCDCOE) Locked Shields (LS) Cyber Defence Exercise (CDX) datasets (the choice of those datasets, and details on its size and structure are discussed in: 4.6 Datasets used for Development and Testing).

Figure 2 below features force-directed graphs, generated with Moloch / Arkime from the metadata that was processed from packet capture collections (PCAPs), that were captured during (on the left) the NATO CCDCOE LS CDX in 2018 Partner Run (LS18PR) and (on the right) the NATO CCDCOE LS CDX in 2021 (LS21) (see: 4.6 for details on used datasets). Node/link weights are decided by the network connection session count between two hosts (nodes) that were observed during a ~5-minute period of the exercise.

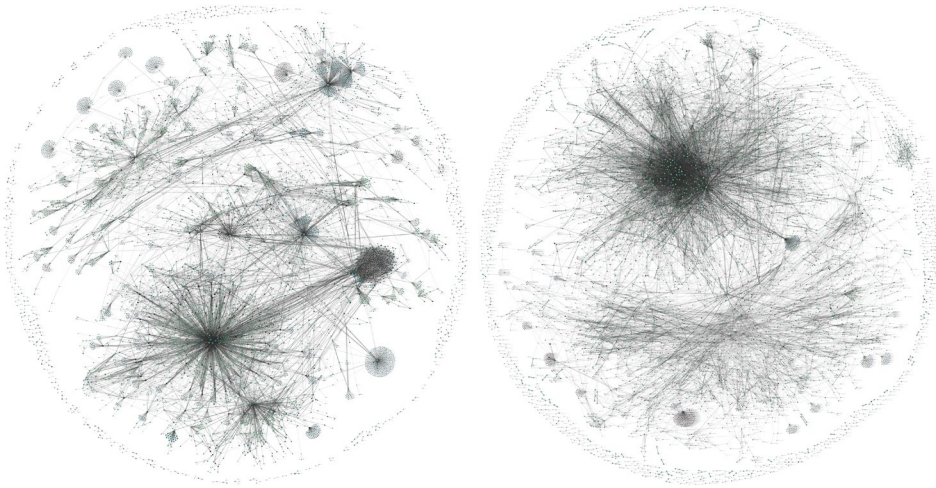


Figure 2 Network traffic (node/link weight calculated with session count) during a ~5-minute period, visualized with Moloch / Arkime. Left: LS18PR; Right: LS21.

Without prior knowledge of the intended or expected network topology, a user would need to use textual and visual tools in order to explore the dataset. Such an exploration would include discovery of the behaviours of the (groups of) networked devices (and their users). A force-directed graph may enhance Shneiderman's 1st, 2nd, 3rd and 5th task levels (see above) in such case.

For the Shneiderman's 4th task level the user would need to zoom in to the graph and hover its mouse cursor above a node or a link, to see detailed textual display with relevant information about that object.

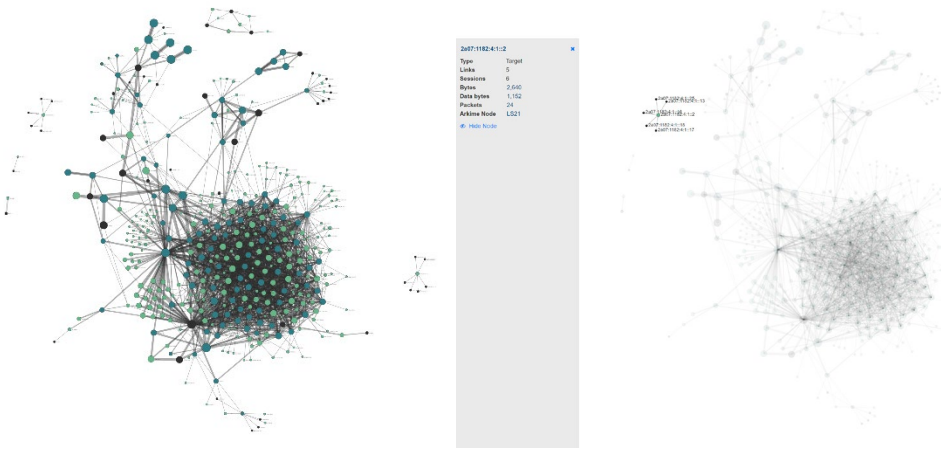


Figure 3 A Blue Team's networks' internal traffic visualized with Moloch / Arkime during a 1-hour period during the LS21 CDX. Left: force-directed graph; right: one node selected.

The user of such a visualization is expected to adjust the query of the to-be-visualized dataset, according to their exploration goals. In case of figuring out the topology of a Blue Team's networks during the LS, one might choose to query the dataset such that the results would include only nodes that should belong to an expected subgroup.

For the Figure 4 below, we'll apply the knowledge that, during an LS CDX, each Blue Team is responsible for defending entities that are using IP-addresses in a 10.x.0.0/16 netblock (amongst some other netblocks) and adjust the query to filter the network traffic based of this: resulting with an example for possible visualizations supporting Shneiderman task levels 2, 3, 4, and 5, by combining the "Zoom on an item or subsets of items" with "Get Details-on-Demand for an item or subset of items".

However, in case the user has already built an understanding of the dataset, and the force-directed graph re-calculates node positions on the fly (again for each time the user renders the graph), the positions of nodes and clusters visualized on a force-directed graph do not necessarily relate to an SMEs (previously built) understanding of the dataset. For example, in the case of exploring and making sense of a network's topology, an SME may have a network diagram depiction of the expected topology of that network, illustrating the expected relations of the networked devices. In Figure 4 (below), the nodes visible in Figure 3 are rearranged according to their expected positions as shown on the LS CDX BT network topology diagram shown in Figure 27 page 47.

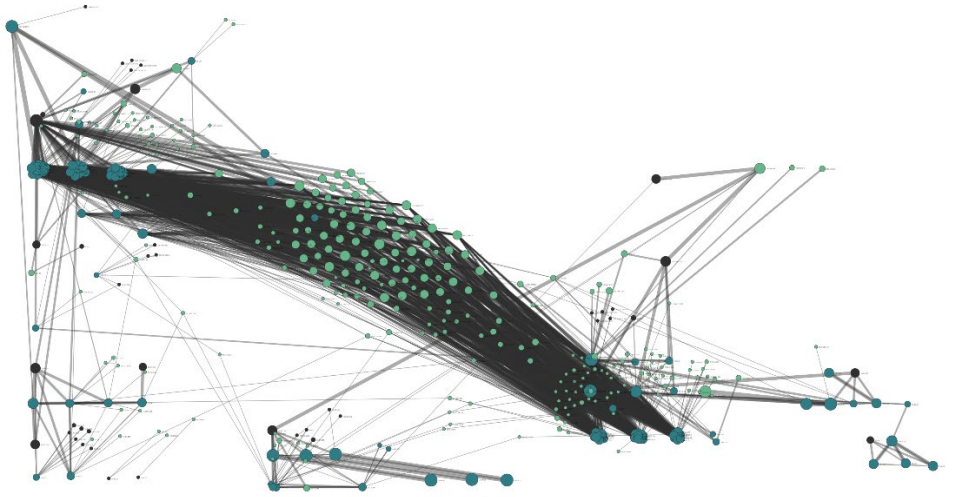


Figure 4 Same query as in Figure 3, but nodes that were expected to be active in that team's networks were allocated to their approximate positions per the LS CDX BT network diagram seen on Figure 27 on page 47.

On the rearranged graph, one can identify several groups of nodes that, while connecting to or being connected by that BT's devices, are not part of the expected BT infrastructure. Hence by combining the prior knowledge of the visual layout of the BT network topology diagram (Figure 27) and augmenting that with network session data (from a Moloch / Arkime instance) one can better identify the expected and unexpected entities that were active during the time window set for the query that's response was used for that graph.

Please see 2.3 for how to improve such pre-positioned topology visualizations with 3D visualizations.

2.2.2 Task-Specific Visualizations

In contrast to visualizations supporting exploration of a dataset, Figure 5, Figure 6 and Figure 7 provide an example of a task-specific visualization for identifying networked entity-entity relations to help finding anomalies amongst their behaviours [2]. These examples were created with Kibana, using the LS18PR dataset.

There the size of a sector on a radial diagram on Figure 5 and Figure 6 represents the count of observed network connection sessions (relative to the total nr of connections represented by this iteration of the visualization) that were observed between the source (outer ring) and destination (inner ring) entities. The colour of the session-count-block is randomly allocated to each node in that visualization to allow the observer to find that same node in that same radial.

Figure 5 Baseline relations of a computer network with about 100 devices.

Figure 6 Another network with same topology as in previous figure, but actively used.

Figure 7 Hovering mouse cursor over a sector of the visualization shown above would provide details of that sector.

Hao et al. [44] provided design requirements for creating ensembles of cybersecurity visualizations that should be used by SMEs in combination to address their tasks:

1. visualizations must "fit" an analyst's mental models,
2. visualizations must integrate into an analyst's working environment,
3. visualizations must be configurable by the analyst,
4. visualizations must be easily understandable to the analyst,
5. visualizations must scale to large data sources, and
6. visualizations must support an analyst's existing problem-solving strategies.

Once the SMEs for whom a visualization is created for learn to read those in the context of their tasks, they may find these visualizations to be crucial for their tasks going forward [46]. An example of such visualization, created with the 6 design requirements in mind are shown on Figure 8, where each destination IP:port combination forms a member in an ensemble, while the members of those ensembles are aligned on X and Y axises of the matrix, [44].

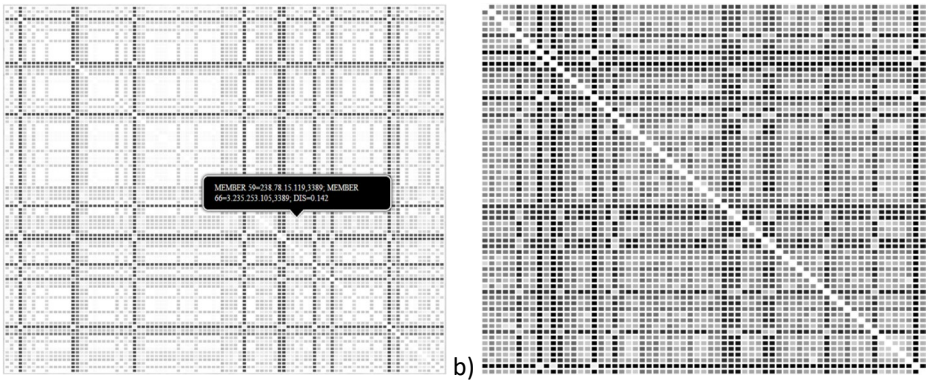


Figure 8 Abnormality matrix for comparing a a) 100-member alert ensemble and b) 60-member alert ensemble. [44]

These are but a small sample of data visualizations that may benefit cybersecurity use-cases. For further examples, please see VizSec conference papers [47].

The scale, heterogeneity, and complexity of cybersecurity datasets continue to pose challenges for visualization and interaction designers [48] despite the constant increase in computers' abilities to process and display more data on flat displays. This could be because visualization designers who get tasked with creating cybersecurity visualizations lack the understanding of the intended users (SMEs) tasks that rely on the to-be-visualized datasets. Yet, SMEs who are familiar with the technical aspect of network monitoring, incident response and other relevant tasks, do not necessarily have the expertise in data visualization (see: 2.3) and human perception (see: 4.1). Hence the designers of cybersecurity visualizations should have dual expertise and/or use a method that would allow them to combine their experience with the intended users' expertise (see: 3.2).

2.3 Stereoscopically Perceivable Multidimensional Data Visualizations

Keeping track of the changes of the various visualizations and their ensembles that often may be located in different applications and / or browser tabs, can be rather tolling for an SME. Also, visualizing multidimensional data on flat screens bears several limitations. First, the visualization that results after the dimensionality reduction methods have been applied, will likely differ from the mental representation that the analyst had acquired upon reviewing the same data in its numerical and textual representation. Additionally, contextual information may be removed in the reduction process, while still crucial for the understanding of the situation and for identifying relevant clues [45].

Utilizing stereoscopically perceivable multidimensional data visualizations may address some of the inherent limitations of flat displays, provided that the visualizations are aligned with the SMEs understanding of their datasets, either by design or alignment via training. Users' interactions in VR and MR may also be more intuitive if users are able to interact with the visualization in ways that humans manipulate objects in the physical world. This way the dexterity of human hand movement could be harnessed for intuitive interactions [49] and haptic feedback to further advance users interaction efficiency [50].

By providing a data visualization environment where minimalistic visual, audio, and haptic cues are informing the user of what is happening in that environment, the user can focus on the task. Furthermore, environmental cues should be perceptible and clear to avoid user confusion. Visualization should be functional and available utilities should

accurately convey their functions. Controls, navigation, interface, and all other interface conventions should be consistent. Users' cognitive and physical workload must be minimized. Human errors should be anticipated and prevented if possible. The environment should be flexible to allow customization for personal preferences, cultural differences, colour vision deficiency etc. [51]. An analyst may find it intuitive to use a 3D representation of cybersecurity network data that is aligned with the above guidelines as well as the analyst's internalized understanding of the data. Intuitive interfaces may enable the analysts to explore and understand their environment more efficiently.

To validate whether Interactive Stereoscopically Perceivable Multidimensional Data Visualizations (ISPMDV) [5] would be beneficial for SMEs, I had to either find existing tools (of which there were only a few in 2015 (see: 3.3)) or create one (either based on an existing one or anew), but also understand how to create such spatial layouts of data representations that would benefit the SMEs I wanted to help (see: 3.2 Mapping Mental Models), once it would be possible to present such visualizations in a stereoscopically perceivable and interactable form (see: 4 Virtual Data).

2.4 Geospatial and Natively Spatial Data

Providing users with accurate (spherical, topographical, etc.) representations of (a location of) a celestial body, has plethora of advantages for working with related datasets, compared to having the same location represented by a cartographical projection. Provided, of course, that the underlying topographical layers are accurate (enough) and its VR/MR representation intuitive to navigate and manipulate.

Google Earth VR being one of the first such of a tool available (publicly), got lots of attention after its release in 2016 [52]. US Army is routinely employing VR for soldier training and mission planning purposes as of 2022 [53], while US Air Force has been using VR for pilot training since the 1960s [54].

However, natively non-spatial data in VR/MR is (usually) still represented in its alphanumeric form, overlayed on the VR environment or with MR on physical world, rather than using graphical 3D representations of that data.

Augmented Reality (not Mixed Reality) has been extensively fielded and used for various purposes in manufacturing industry, but with rather limited functionality: the lack of stereoscopic rendering of such an augmentation restricts its usage to only providing its users with ability to access equipment documentation, video calls, etc. thas is displayed in users peripheral field of view (e.g. a tiny screen that user can focus on), while lacking the ability to show contextually relevant information next to (or seemingly attached to) the physical object in the real world that the information relates to.

In recent years Mixed Reality is being welcomed by various industries, medical use-cases being a poster child of such: preparing for a surgery using accurate (patient specific) 3D scans, rendered simultaneously for a group of doctors with synchronized MR headset provides numerous advantages [55]. However, the data visualized by such applications is still natively spatial: either scans of actual patient's body(parts), or normal body parts to practice on, etc.

In an industrial setting where alpha-numeric data representation is overlayed onto the physical world using a MR headset, the result is still inherently just a small step forward compared to having traditional physical displays on those same locations showing the data.

Due to such a plethora of “low-hanging-fruits” it is understandable, that for VR/MR advocates it makes sense to develop solutions for such (simpler) use-cases without investing into further studies on how to improve such visualizations to utilize more intuitive data representations for the benefits of the users of those systems.

2.4.1 Mixed Reality Exploration Toolkit

A great example of a tool that has been created to plan proof-of-concept physical solutions that are to-be-fielded in physical locations (e.g., in orbit), is NASA Mixed Reality Exploration Toolkit (MRET). Compared to its commercial or otherwise closed source counterparts (e.g., US ARL VRDAE [3]), MRET is publicly available for free and released as Open Source [23].

MRET provides users with a functionality to position precise and accurate models of (planned) tools onto their intended locations, relative to other components these tools are to be worked with. These intended locations may be on any (well mapped) celestial bodies, using accurate planetary positions at a set time, to assess accurate lighting of a location, possibility to establish communications, etc.

MRET’s native non-spatial data visualization capabilities were limited to conventional bar-, pie-, and other charts. VDE was included in MRET distribution in 2021 to enhance these capabilities further, and provide its users with more customizable data visualization tools, that could be combined with geospatial- and natively spatial visualization to enable natively non-spatial 3D data visualizations.

2.5 Non-Spatial Data

Contrary to natively spatial data, the creator of a visualization depicting natively non-spatial data (like software logs, network traffic) in a stereoscopically perceivable environment must decide the spatial layout for the datapoints found (or selected) from the to-be-visualized dataset.

Naïve approach would be to present it as a force-directed 3D graph, 3-axis bar/line/dot chart or even just textual labels augmented (in Mixed Reality) upon a physical object (in the Real Reality). OpenGraphiti (see: 4.4.1 Choosing the Platform) enabled me to experiment with exactly such graph visualizations derived from Locked Shields logs. However, these tests provided me with early realization that although force-directed graphs are great for exploring datasets with unknown topology (like social networks), such graphs are seldom helpful thereafter. Once the user has already learnt the internal relations or expected behaviour of (some of) the (groups of) entities that are active in that dataset: once the user becomes aware of the expected behaviour of some of these systems, predetermined spatial positioning of the visual representation of the (groups of) entities expected to be found in that dataset, becomes preferable.

Hence the approach taken with VDE is to provide its users with the ability to interact with data-shapes, that’s pre-determined layouts that are based on networked entities’ expected relations (e.g., computer network’s logical / functional topology), while allowing the user to augment such layouts with additional data (or information) queried from related datasets.

3 Method

Traditional approaches for cybersecurity visualizations have been either to provide SMEs with ready-to-use visualization components (combined into dashboards served as separate tools and views), or SMEs scripting ad-hoc case-specific visualizations because they need it to solve a problem at hand. Ad-hoc case-specific visualizations may be picked up later and could evolve into a tool (or a product) that may be helpful in solving other similar cases but may also be forgotten or be found to be unsuitable for any other use-case, except the one it was created for. On the other hand, ready-to-use visualization components (that are more than just time-sequence bar charts, etc.) are seldom useful for SMEs without a comprehensive training on the meaning (and underlying queries) of the visualizations (on dashboards).

Nevertheless, in case of most cybersecurity data visualizations, the SME using such a visualization needs to interrogate relevant (interesting) events in the dataset that the visualization was created for, while hunting [56] for anomalies or building a working-hypothesis of a suspected incident, and to understand the specifics of it. Such procedures usually involve alpha-numerical representations of the data, with 2D visualizations as occasional ad-hoc supporting tools.

While working as one of such SMEs, I identified the need to improve these common practices by using emerging technologies, the likes of MR and VR, that could expand SMEs toolsets and providing them with more intuitive visualization tools.

3.1 Design Science Research Methodology

Design science research methodology [57] was used to guide the research process:

1. identify the problem and motivation: see 1.1
2. define the objectives for a solution: see 1.2 and 1.3
3. design and develop method and software: see 3.2, 3.3 and [4]
4. demonstrate and evaluate the method and software: see Virtual Data and [2]
5. while communicating the findings to the community: see List of Publications.

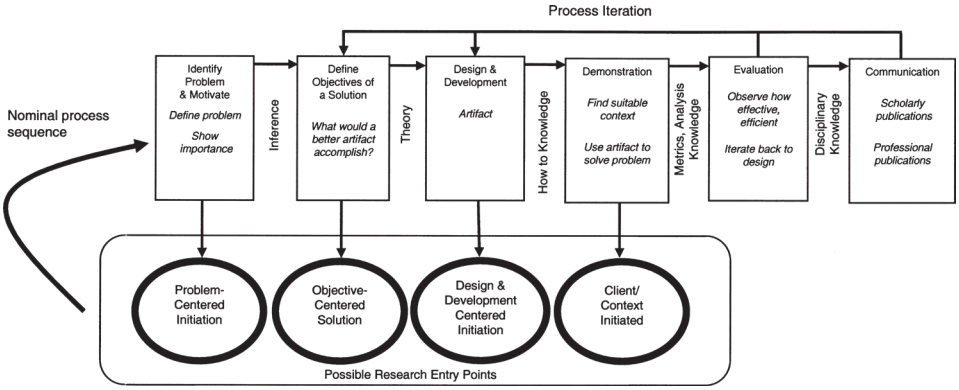


Figure 9 Design Science Research Methodology Process Model (from [57])

I chose to proceed in parallel with:

1. working on human sciences to choose or develop the interviewing method for deciding appropriate layouts for visualizations of (cybersecurity) datasets (see 3.2 below) and
2. create the software for enabling users to stereoscopically perceive and interact with data visualizations that could be created based on those interviews.

The latter got numerous iterations based on SMEs feedback and is now integrated in a few software distributions (see: 4.1), the former is proposed as the Mental Model Mapping Method for Cybersecurity in [4].

3.2 Mapping Mental Models

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 would be effective and indeed useful for their intended users [80]. Further, creating useful visualizations for SMEs is not possible without an in-depth understanding of the tasks which the visualizations would support [81]. Therefore, I identified the need for an interviewing method for extracting from an individual SME their internalized understanding of the dataset that they work with (e.g., logfiles of their protected environment), in order to create visualizations that align with their understanding of that dataset, and to design layouts for visualizing that dataset in a way, that would enhance the SMEs and their colleagues' ability to understand and work with that dataset: Mental Model Mapping Method for Cybersecurity [4] (M4C).

The proposed interview method is rooted in the tradition of participatory design [82], a democratic form of design originating from 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 designing interfaces and interactions.

The overarching goal of such SME interview process is to identify the properties that an SME seeks within their dataset, to obtain answers to the analytic questions for their work role. To do this, 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 must be identified. Based on the SME's role and specific inquiry goal, the desired dimensions of data (entities, the relations of groups, subgroups, and sub-subgroups, etc.) to be visualized can be determined. Then consider which properties should be represented by which elements (an example of these dimensions and properties can be seen on Figure 10), 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, please see videos at [83].

Information for creating the visualization is initially elicited through the first individual interviews with an SME group (Session 1 interviews), preferably with participants who do not suffer from aphantasia [84], by asking a series of specific questions designed to identify groups and entities (as described in the previous paragraph). An example case would be for visualizing the functional topologies of computer networks, where 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 would be different, for example, to visualize application logs, the initial interview questions should be adjusted accordingly.

Figure 10 Virtual Data Explorer's default Network Topology layout, one network group in focus on this screenshot. Layout is similar to the template shown in Figure 25 *below on page 45, although the dataset used for the visualization featured on the video where this screenshot was taken from, is from Locked Shields 2018 (see: 4.6 Datasets used for Development and Testing).*

Once all the first interviews have been completed, the layouts created during the interviews should be evaluated. All or some of the layouts can then be implemented using VDE: either by creating new configuration files or implementing necessary components in C#. 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 (or another visualization tool), 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

For proposed interview method and detailed description of Mental Model Mapping Method for Cybersecurity (M4C), please see 3.2. Note that due to the delays of more than a year for getting Internal Review Board exemption from involved parties for conducting interviews, and then the global pandemic shutting down the world in 2020, it was impossible to conduct interviews using M4C: its validation is left for further studies.

3.3 Tools for Testing the Hypotheses

To enable visualizing live data as predetermined three-dimensional layouts while it would be stereoscopically perceivable and interactable, I created the Virtual Data Explorer (see: 4 below). VDE enables a user to stereoscopically perceive spatial layout of a dataset using a Virtual or Mixed Reality headset: for example, the topology of a computer network, while the resulting visualization can be augmented with additional data, like TCP/UDP/ICMP session counts between network nodes [1]. Prior to having such a tool, it was not possible to evaluate the feasibility of such visualizations, as the viability and usability of three-dimensional visualizations can be adequately evaluated only in its stereoscopically perceivable forms.

As the pandemic made a larger-scale study with many participants impossible, VDE instead underwent a more iterative review process, drawing input from representative users and domain expertise. Once possible, a user study was conducted to validate the hypotheses [8] (see: 5).

4 Virtual Data Explorer

This chapter gives relevant background information on human visual system to contextualize the necessary considerations while debating the potential usefulness of, and the implementation of stereoscopically perceivable multidimensional data visualizations and then describes the high-level structure of Virtual Data Explorer (VDE) that provides the necessary capabilities as set of software components. In addition, this Chapter provides visual examples of VDE data visualizations, for accompanying videos please see: [83].

VDE allows its user to customize visualization layouts via two complimentary textual configuration files, that will be parsed by VDE Server (see: 4.3) and visualized by VDE Client (see: 4.4).

In its current form VDE is available as a part of NASA MRET open-source software [23].

4.1 Human Visual System

The human visual system has a finite amount of visual attention resources that are used to view and interpret the data presented on a computer screen [58]. Hence, the human visual system is one of the major bottlenecks of information flows between a computer system to a human analyst (refer the Communication–Human Information Processing (C–HIP) model for details [59]). Because of this bottleneck, the veracity and comprehensiveness of a human analyst's mental model about a network event is directly impacted by perceptual bottlenecks. A *mental model* is internal, cognitive representation of an environment based on the acquired information. Such models can provide ways to describe, explain, predict, and, sometimes, control the phenomena [60]; [61] and are built through direct perception of the environment. Hence, the design of a data visualization can impact the accuracy of the development and sustainment of an analyst's mental model [62].

Optimizing the codification of information can be used to reduce the chances of perceptual bottlenecks. Visual information can be efficiently augmented based on reasoning processes (see [63] for an overview on dual-coding and [64] for a review on working memory). Furthermore, information can be presented to the analyst in more than one sensory modality to maximize the amount of information perceived in a time epoch. In Human Computer Interaction research, codes are stimuli that represent the smallest unit of information communicated. For example, visual codes within a scatterplot are size, colour, shape, proximity, among others. These visual codes are relevant to 2D visualizations, but 'depth' may be an additional code in 3D environments that can be populated with additional data parameters and impact the interpretation of other codes like proximity. A group of codes representing a large amount of information can be configured to create a visual pattern, which can then be perceived rapidly. This visual pattern, according to Gestalt Psychology, is called *emergent features* [65] because the meta-data patterns emerge from the display of raw data. Meta-data patterns can form the basis of human mental models that analysts use when searching for expected patterns of malicious network behaviour as well as represent normal network behaviour. Gestalt laws of perception (e.g., Laws of Proximity, Closure [33]) characterize the natural ways humans perceive information groupings that the interface designer can capitalize on. Poor designs that violate the Gestalt laws of perception could force the analyst into controlled and deliberated processing that consumes attention resources [58].

Depth perception is facilitated with a set of monocular and/or binocular visual cues that could provide additional codes to depict network information. Monocular depth cues (i.e., light and shading, relative size, interposition, blur, texture gradient, and aerial perspective linear perspective) [34] allow for a 3D depiction in a 2D plane (i.e., a page or photograph or a flat computer display). These kinds of "3D in 2D" visualizations using monocular cueing were called "perspective views" [66] or "pseudo 3D" [67]. Binocular depth cues use stereopsis to present objects to the viewer that seem to 'pop out' from the visual scene. Visualizations with binocular depth cues are called "real 3D" [67]. Visual perception of natural 3D scenes is afforded by monocular and binocular depth cues working together [68].

Another 3D technique and design principle which can hamper perception in 3D visualization environments is to use perspective [69]. Upon entering a 3D environment, the analyst is perceiving the environment through the avatar's eyes or perceiving via a top-down view looking at an avatar that represents themselves. The terminology describing perspectives is non-standard and sometimes obtuse. Human factors research defines *allocentric* views [70], also called "through the window" [71] view, as one in which the observer is watching themselves through a viewpoint outside of the body. For example, an avatar representing a human has an allocentric view if the controller manipulates the avatar while observing its actions from behind. Allocentric is used interchangeably with *geocentric* or *exocentric* views [70] or *plan* views [69]. Plan views are allocentric perspectives in which the human is looking down from a higher altitude. Contrast this with *egocentric* views [70], also called *immersive* [71] or *inside perspective* [72], such that the controller is seeing the virtual environment through the eyes of the avatar. The type of perspective used for a particular task has been shown to lead to human perceptual and spatial memory errors [70].

The advantages and disadvantages of depicting data using 3D compared to flat 2D displays has been studied and debated for decades with no clear resolution. With the rise of more sophisticated augmented reality environments, modern visualization research has re-vamped. The advancement of computing provides some explanations to the discrepancies between recent and dated studies of human performance with 3D visualizations [73]. In some cases, 3D is advantageous because of a lower interpretive effort of perceived 3D information, given that the human visualization system has evolved to perceive the world stereoscopically as a three-dimensional environment [74]; [73]. Furthermore, 3D visualizations can potentially display more data using depth cueing compared to 2D displays. However, these benefits are couched in the type of work tasking required to complete with the visualization. Tasks such as altitude extraction, geospatial manoeuvring, and navigation improve with 3D displays [75] while, there are tasks and environments for which the 2D displays are more advantageous than 3D displays [76].

In sum, prior research indicates that while 3D visualizations in virtual reality environments afford more codes to use to depict data, the ways in which those codes are arranged using Gestalt's laws, emergent features and perspectives, determines how best to maximize the amount of data that could be perceived. Communication from the interface to the human analysis involves the clear mapping between a mental model of the data that is expected to be reviewed, and the manner the data is depicted in that visualization [33]. The 3D objects designed to represent data must fit the typical mental model building inherent in network defence job tasking. To my knowledge, no prior research has identified whether computer network defence analysts are re-visualizing

alphanumeric network data in spatial patterns in their minds. Furthermore, there's no clarity whether training an analyst to build their mental models on 3D representations of alphanumeric network data will be advantageous to performance. Although prior research has described basic Computer Network Defence (CND) operations and job tasking [77] [78], their findings are relatively generic to ascertain analyst mental models to build 3D visualizations from. Some preliminary research [79] has attempted to document analyst's mental models, but the granularity of the models was too coarse to guide the development of 3D visualizations.

4.2 Virtual Data Explorer

To be able to research the usefulness of interactive stereoscopically perceivable multidimensional data visualizations, I created software components that would facilitate that research, coupled with the M4C method (see: 3.2).

VDE allows its user to customize visualization layouts created with M4C using two textual configuration files (see 4.3.3 Server Configuration), that will be parsed by VDE Server (see: 4.3.4 Entity Templates) and visualized by VDE Client (see 4.4).

VDE functionality is decoupled to Server and Client components to pre-process the incoming data in a more powerful environment (than a wireless MR headset) before its visualized either in the VR or MR headset. VDE Server also acts as a multi-user relay to synchronize the visualizations (e.g., grabbed objects position in connected users' views) between connected user sessions.

4.3 Virtual Data Explorer Server

To accommodate timely processing of large query results (from the underlying dataset), the data-processing in VDE is separated into a Server component (VDES).

Thread-safe messaging is used extensively for asynchronous data processing, browser-based User Interface actions etc., but most importantly for keeping the Client component (VDEC) visualization in sync with (changes in) incoming data (ex: response to a Moloch/Arkime query).

4.3.1 Architecture

VDES has 7 main components:

1. Core is responsible for starting up the various VDES components, according to command line parameters and configuration file(s).
2. Webserver serving User Interface for monitoring and controlling VDES and connected VDE Clients' behaviour.
3. WebSocket server (SignalR) facilitating communication with the UI served by VDES Webserver and VDE Client sessions.
4. Browser Extension for enabling inter-tab communication in Chromium-based-browsers to monitor for query results in supported tools (for example Moloch/Arkime) and transfer these results to VDES via the SignalR WebSocket.
5. Entity Templates create from topology configurations, that are used while processing incoming data (see p6).
6. Data Processor that parses the incoming query response according to the currently active configuration.
7. Messenger component, relaying communications between VDES components and threads.

4.3.2 Choosing Language

C# was chosen for a variety of reasons, of which 4 are noteworthy:

1. Linq[1] query language for interrogating in-memory data structures is rugged and fast.
2. C# is a strong typed, memory-safe language, that encourages safe coding practices and (with appropriate tools) helps to avoid introducing vulnerabilities into the source code.
3. Compiled binaries can be tailored for various platforms (notably Windows, Linux, MacOS).
4. C# is also used for the VDE Client (see 4.2), as that's one of the scripting languages supported by Unity 3D.

4.3.3 Server Configuration

Data processor operating mode, server's IP address, port and other settings are read in from a JSON formatted configuration file, example provided in Figure 11.

Figure 11 VDES configuration example.

Setting "mode" chooses which Data Processor (see: 4.3.5) to use for processing the to-be ingested data.

Setting "layouts" lists additional files to read layout configuration(s) from; although these files are not processed by VDES, these settings are sent to connecting VDEC sessions.

Setting "networks" lists additional files to read data-shapes' topology configuration(s) from (in case the chosen Data Processor would need those), example show on Figure 12.

[1] https://docs.microsoft.com/en-us/dotnet/csharp/programming-guide/concepts/linq/

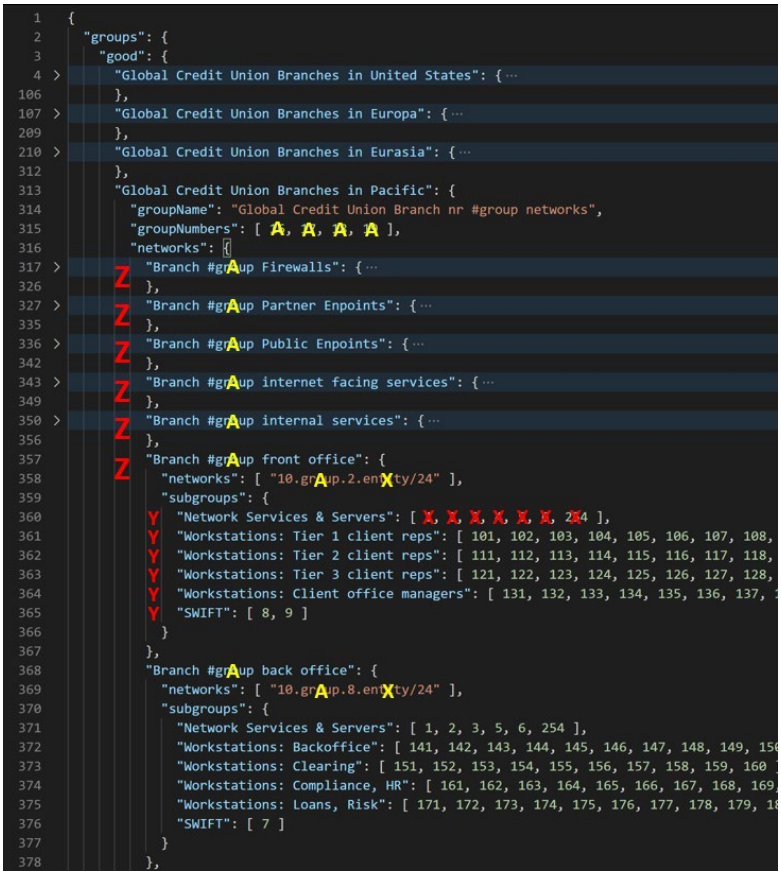


Figure 12 Configuration related to the visualization template shown on Figure 25 below on page 45. ***Red X, Y, Z*** *on this and Figure 25 indicate relations between 3D positioning of the visual of a representation of a datapoint and its definition in the configuration file.* ***Yellow A****-s on this figure point to syntax used to simplify the duplication of group templates (that can be tied to (expected) IP addresses found in the ingested data).* ***Yellow X*** *marks the relation between network CIDR template and individual entities belonging to subgroups (that are distinguished in by the last octet of its IP address).*

4.3.4 Entity Templates

During start-up, VDES creates internal templates of entities, that are expected to be found from ingested data. This behaviour speeds up data processing later.

For an example of a possible Data Template implementation, please see: Figure 13.

```
private void CreateTemplateEntitiesForNetwork(NetworkTemplateFromConfiguration current)
{
    bool report = true;
    int ready = 0;
    if (current.groupNumbers != null && current.groupNumbers.Count > 0)
    {
        report = false;
        int
            readies = 0,
            processed = 0;
        foreach (int groupNumber in current.groupNumbers)
        {
            System.Threading.ThreadPool.QueueUserWorkItem(input =>
            {
                CreateSubnetTemplates(
                    processed++,
                    entities.Create(
                        current.groupName.Replace("#group", groupNumber.ToString()),
                        current.localGroot,
                        VDE.Entity.Type.Group, groupNumber),
                    current,
                    ref readies,
                    groupNumber);
            });
        }
        while (current.groupNumbers.Count > readies)
        {
            Task.Delay(100);
        }
        ready = 1;
    }
    else
    {
        CreateSubnetTemplates(
            0,
            entities.Create(
                current.groupName,
                current.localGroot,
                VDE.Entity.Type.Group, 0),
            current,
            ref ready);
    }
    while (ready < 1)
    {
        Task.Delay(100);
    }
    current.processed = true;
    if (report)
    {
        log.Entry(current.groupName + " done.");
    }
}
```

Figure 13 Creating templates of expected entities and their groups.

4.3.5 Data Processor

Runtime VDES can have only one Data Processor running, determined by the “mode” setting in VDES configuration. The loading of Data Processor is implemented in such a way, as to allow loading add-on Data Processors from user-provided .DLL-s.

An example of a possible Data Processor implementation, please see: Figure 14.

```
async Task OperateMoloch(Schemas.Moloch response)
{
    int
        itemsProcessed = 0,
        nextCountUpdate = 0,
        items = response.IPCount.Count;

    data.entities.UpdateMaxCount(response.maxCount);

    foreach (KeyValuePair<IPAddress,int> node in response.IPCount)
    {
        VDE.Entity entity = null;
        Entity expectedEntity = networkConfig.CheckAddress(node.Key);

        if (expectedEntity != null)
        {
            VDE.Entity parent = VerifyAncestorsExistenceUpstream(expectedEntity);
            entity = data.entities.CreateOrGetExistingEntity(node.Key.ToString(), node.Value, parent, expectedEntity, VDE.Entity.Type.Node);

            entity.count = node.Value;

            entity.vectors = new int[4] {
                expectedEntity.theSubnetThatTheDeviceBelongsTo,
                expectedEntity.theSubnetSubgroupThatTheDeviceBelongsTo,
                expectedEntity.devicePositionInLogicalSubgroup,
                expectedEntity.groupNr,
            };
        }
        else
        {
            log.Entry("NO net found for: " + node.Key.ToString() + ", count: " + networkConfig.networks.Count);
            networkConfig.networks.FindIndex(net => net.CheckAddress(node.Key, out _, true));
            VDE.Entity parent = VerifyAncestorsExistenceUpstream(entities.unknownUnknown);
            entity = data.entities.CreateOrGetExistingEntity(node.Key.ToString(), node.Value, parent, null, VDE.Entity.Type.Node);

            entity.count = node.Value;
        }

        foreach (Schemas.SrcDstCount sdc in response.SrcDstCount.Where(sdc => sdc.src == node.Key.ToString()))
        {
            _ = Task.Run(() => data.relations.LinkEntities(sdc.src, sdc.dst, sdc.count));
        }

        data.queries.active.AdjustResponse(entity);

        data.entities.EnqueueEntityUpdate(entity);

        if (nextCountUpdate <= ++itemsProcessed)
        {
            nextCountUpdate = itemsProcessed + 100;
            data.messenger.Post(new Message() {
                progressStatus = Progress.Status.Update,
                floats = new List<float> { itemsProcessed, items },
                message = "Operating on the response from a Moloch",
                from = "Operators.IP.Operator"
            });
        }
    }
    data.messenger.Post(new Message()
    {
        progressStatus = Progress.Status.Update,
        floats = new List<float> { items, items },
        message = "Operating on the response from a Moloch",
        from = "Operators.IP.Operator"
    });
    await Task.Delay(1000);
}
```

Figure 14 Reference implementation for processing a response from Moloch / Arkime.

4.4 Virtual Data Explorer Client

Virtual Data Explorer Client (VDEC) is the component of VDE without which the ISPMDV related research would be impossible.

VDEC was created using Unity 3D, to facilitate deployment to various VR/MR HMD's. Over time this has proven to be a correct decision, as all relevant HMDs that have been released since 2015 (when I started with my research) have had Unity 3D support since early releases of their SDKs.

4.4.1 Choosing the Platform

I started my research while extending OpenGraphiti [40], that was the first (publicly available) 3D data visualization tool supporting Oculus Rift DK2 (being the first VR headset I managed to acquire for my research back then), but it lacked interactive capabilities (to handle user inputs from Leap Motion or Myo band) and worked exclusively on OSX. That turned out to be a dead end by 2016, when Oculus decided to not continue supporting OSX with their SDK. Additionally, the (lack of) performance and

the (lack of) memory querying abilities of Python (that was the data processing tool for OpenGraphiti) turned out to be a bottleneck while processing the data ingested from Bro [85] logs into a visualizable hierarchy.

As there were no other (publicly available) data visualization engine(s) existing then, such that would have supported VR (let alone MR) headsets for 3D data visualizations, I did not really have a choice but to build such a tool myself. At the time I was criticized for that decision for wasting my time as a mere "code monkey", but without such at tool there was no way to develop and test ISPMDV. In retrospect the decision to build VDE was the correct one and enabled everything that followed.

The choice of which platform to use for VDE development ended up being a decision between two game-engines, Unreal Engine and Unity 3D, as those two had good-enough graphics performance with VR (and limited MR) support, while also allowing the use of C++ or C# for extending the existing framework.

Finally, Unity 3D was chosen for VDE for it's (by then) aggressive development cycle (facilitating various VR and MR integration frameworks, that were being released by hardware manufacturers), it's use of C# as (one of) the scripting language (as opposed to C++ in Unreal Engine), and for the fact that the team I was going to work with at the US Army Research Lab was already using Unity 3D for their other VR projects.

4.4.2 Virtual or Mixed Reality

Although VDE was initially developed with Virtual Reality headsets (Oculus Rift DK2 and later with CV1 with Oculus Touch), its interaction components were always kept modular so that once mixed reality headsets such as the Meta 2, Magic Leap, and Hololens became available, their support could be integrated into the same codebase.

The underlying expectation for preferring MR to VR is the user's ability to combine stereoscopically perceivable data visualizations rendered by a MR headset with relevant textual information represented by other sources in the user's physical environment (SIEM, dashboard, or another tool), most likely from flat screens. This requirement was identified from early user feedback that trying to input text or define / refine data queries while in VR would be vastly inferior to the textual interfaces that users are already accustomed to operating while using conventional applications on a flat screen for data analysis. Hence, rather than spend time on inventing 3D data-entry solutions for VR, it was decided to focus on creating and improving stereoscopically perceivable data layouts and letting users use their existing tools to control the selection of data that is then fed to the visualization.

A major advantage provided by the VR environment, relative to MR, is that VR allows users to move (fly) around in a larger scale (overview) visualization of a dataset while becoming familiar with its layout(s) and/or while collaborating with others. However, once the user is familiar with the structure of their dataset, changing their position (by teleporting or flying in VR space) becomes less beneficial over time. Accordingly, as commodity MR devices became sufficiently performant, they were prioritized for development – first, the Meta 2, later followed by support for the Magic Leap and HoloLens.

4.4.3 Architecture

VDEC has 7 main components:

1. The core is responsible for starting up the various components.
2. WebSocket client (SignalR) facilitating communication with VDES to get appropriate configuration, the pre-processed data to be visualized and later updates to that visualization.
3. Layout class that can be extended to create dataset-specific layouts, if altering a configuration for an existing layout is not enough. Layout extensions can also be loaded runtime from user-provided DLL-s.
4. Input system that (as of 2022) allows users using Oculus (Rift & Quest), HTC Vive, Magic Leap, Meta 2 (deprecated), HoloLens 2 or Windows Mixed Reality headsets to interact with VDE visualizations using methods native to their devices, be it either hand-held controller based, or user's hand-, finger-, head-, gaze-inputs.
5. Entities: morph into groups or individual entities (depending on their designation), becoming groups of (groups of (groups of (…))) entities visualized by rectangles (or other shapes, as defined by the layout component).
6. Links: represent relations between visualized entities, say, observed network connections between two entities, observed during the time-window of the most recently received query response, that's result was processed by VDES.
7. Joints: are used to shape the layout autonomously: each group and each entity decides (based on Linq views), where should it be located amongst its siblings (in that same group) and adjusts its join-connections with nearest siblings accordingly. Joints (Unity's built-in components) can be defined to have desired lengths, strengths, dampening, etc., to allow the visual groups to be flexible enough, while adjusting their positions. VDE layouts are therefore relying on Unity 3D physics engine for the visualization layouts.

4.4.4 Simulator-Sickness

Another crucial property for in-VR data exploration environment is avoidance of users experiencing simulator sickness [86] while being "in" that VR environment. Various experiments have shown that applying certain limitations to a user's ability to move in the virtual environment – limit their view and other forms of constrained navigation – will limit confusion and help prevent simulator sickness while in VR. These lessons were learnt while developing VDE and adjusted later, as others reported success with same or other mitigations [87]. Amongst other things, but most importantly, if an immersed user can only move the viewpoint (e.g., its avatar) either forwards or backwards in the direction of user's gaze (or head-direction), the effects of simulator sickness can be minimized or avoided altogether [2]. This form of constrained navigation in VR is known as "the rudder movement" [87].

4.4.5 User Interface

In the early stages of VDE development on Unity 3D, efforts were made to either use existing VR-based menu systems (VRTK, later MRTK) or to design a native menu, such that would allow the user to control which visualization components are visible and/or interactive; to configure connection to VDE Server; to switch between layouts; and to exercise other control over the immersive environment. However, controlling VDE's server and client behaviour, including data selection and transfer, turned out to be more convenient when done in combination with the VDES web-based interface (see: Figure 15 and Figure 16 below) and with existing conventional tools on a flat screen. For

example, in case of cybersecurity related datasets, the data source could be a SIEM, log-correlation, netflow, or PCAP analysing environments. As an example, in the accompanying videos [83], Moloch/Arkime is used to select and feed data into VDE for visualization. Note that this is prone to change in the future, provided that hand and finger tracking of MR headsets becomes precise enough.

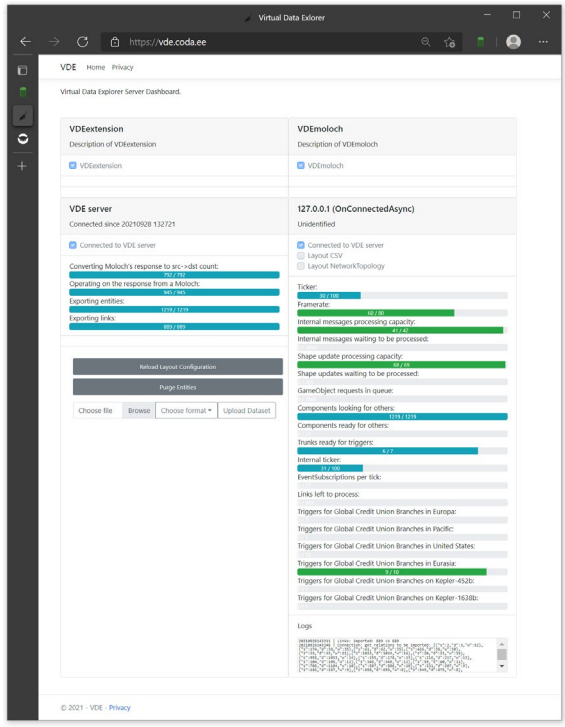


Figure 15 Screenshot of VDES UI providing status of the VDES backend (middle left), a connected VDEC status (mid-lower right) but also indicates the presence of the VDE Browser Extension and an open Moloch / Arkime tab to ingest data from.

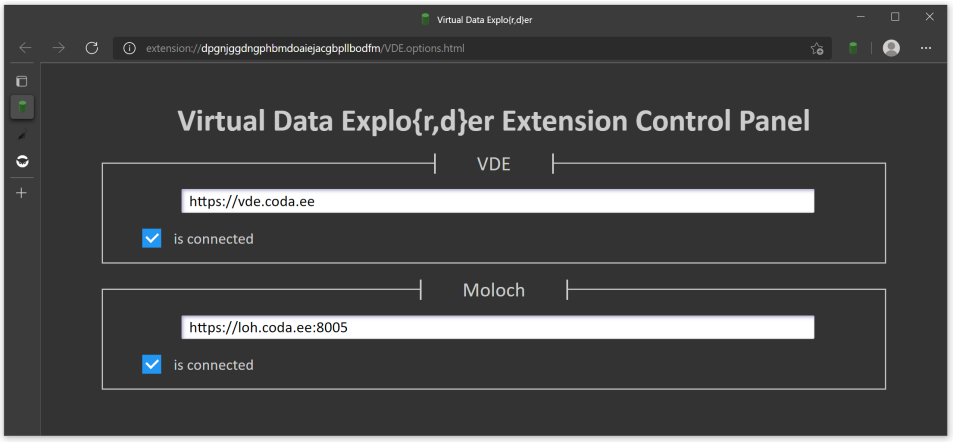


Figure 16 VDE Browser Extension facilitating communications between a data source (here: Moloch / Arkime) and VDES.

4.4.6 Head-Up Display

Contextual information is displayed on a head-up display (HUD) that is perceived to be positioned a few meters away from the user. The HUD smoothly follows the direction of user's head in order to remain in the user's field of view (see Figure 17). This virtual distance was chosen to allow a clear distinction between the HUD and the network itself, which is stereoscopically apparent as being nearer to the user.

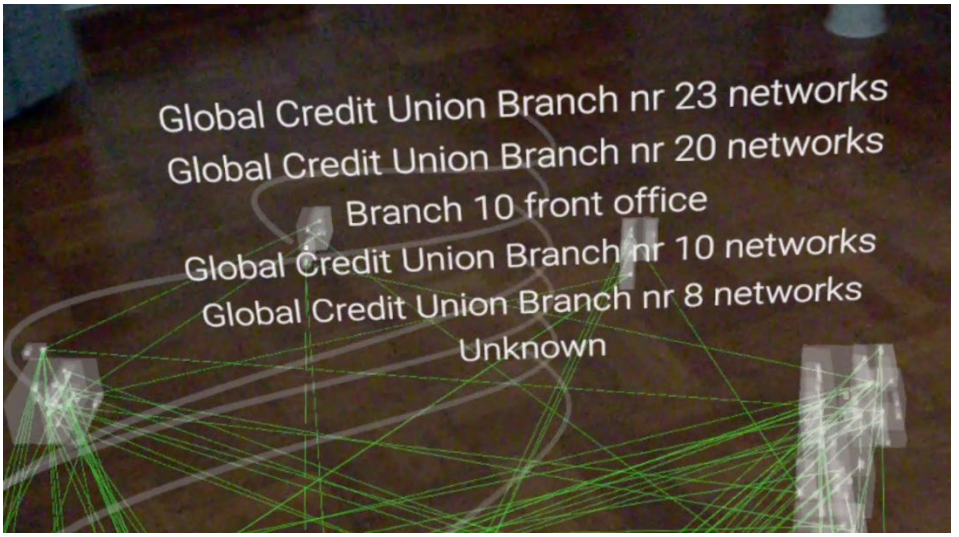


Figure 17 Head-Up Display showing labels of visualized groups that the user focuses on, retaining visual connections to those with Bezier´ curves. HUD is used also for other interaction and feedback purposes.

4.4.7 User Interactions

The ability to interact with the visualization, namely, to query detailed information about a visual representation of a datapoint (ex: semi-transparent cube for a node or line for a relation between two nodes) using input devices (ex: hand- and finger-tracking and input controllers) is imperative, and was one of the reasons to abandon the initial OpenGraphiti based work and start implementing VDE anew on Unity 3D. Only later, while gathering feedback from SMEs [2] were it confirmed to be also crucial for users' immersion in the VR data visualization to allow them to explore and build understanding of the visualized data while querying it intuitively [6].

Figure 18 MR view of Locked Shields 18 Partner Run network topology and network traffic using VDE; user is selecting a Blue Team's network with index finger. Screen capture from coda.ee/PhD

User's interactions with data-shapes are customized to each supported VR/MR headset's inputs. In case of Magic Leap, Meta 2 and HoloLens 2, it's user's tracked hands (see: Figure 18 above), specifically relevant fingers' joint's colliders that would be used to decide whether user is trying to grab something, point at a node or edge etc. In case of Oculus Rift / Quest it's the pseudo-hands that are rendered in the VR environment, based on hand-controllers' positions and touch detection (see: Figure 19 below).

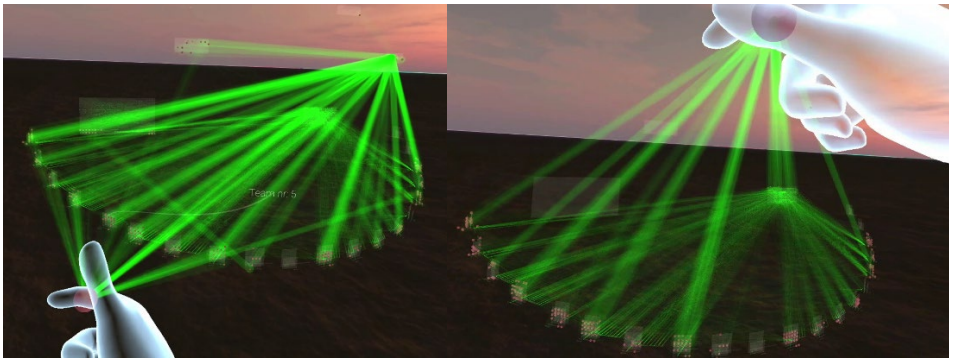


Figure 19 Screen capture from [83] illustrating user interactions while exploring a dataset with Oculus CV1 VR HMD. Edges originating from or terminating at the grabbed object are highlighted according to the strength of user's grip of the controller's "grip" sensor.

The VR system's input controllers are used to detect whether the user is trying to grab something, point at a node, or point at an edge. In case of MR and Oculus Quest, these interactions are based on the user's tracked hands (see: Figure 18), and in case of Oculus Touch, pseudo-hands (see: Figure 19) are used.

A user can:

1. point to select a visual representation of a data-object – a node (for example, a cube or a sphere) or an edge – with a "laser" or dominant hand's index finger of either the virtual rendering of the hand or users real hand tracking results (in case of Oculus Quest and MR headsets). Once selected, detailed information about the

selected object (node or edge) is shown on a line of text rendered next to user's hand, (Shneiderman Task Level 4).

2. grab (or pinch) nodes and move (or throw) these around to better perceive its relations by observing the edges that are originating or terminating in that node: humans perceive the terminal locations of moving lines better than that of static ones, (Shneiderman Task Levels 3, 5).
3. control data visualization layout's properties (shapes, curvature, etc.) with controller's analog sensors, (Shneiderman Task Levels 1, 5).
4. gesture with non-dominant hand to trigger various functionalities. For example: starfish – toggle the HUD; pinch both hands – scale the visualization; fist – toggle edges; etc.

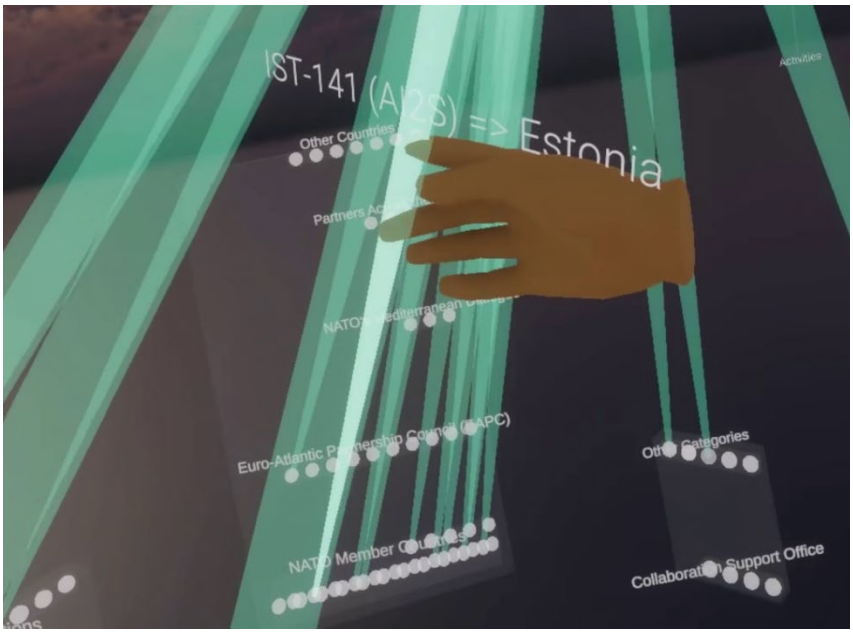


Figure 20 User touches an edge with the index finger of Oculus avatar's, to learn details about that edge.

In addition to active gestures and hand recognition, the user position and gaze (instead of just their head direction if available) are used to decide which visualization sub-groups to focus on, to enable textual labels, to hide enclosures, to enable update routines, colliders, etc. (Shneiderman Task Levels 2, 3, 4, 5, 7). Therefore, depending on user's direction and location amongst the visualization components and on the user's gaze (if eye-tracking is available), a visualization's details are either visible or hidden, and if visible, then either interactive or not.

The reasons for such a behaviour are threefold:

1. Exposing the user to too many visual representations of the data objects will overwhelm them, even if occlusion is not a concern.
2. Having too many active objects may overwhelm the GPU/CPU of a standalone MR/VR headset – or even a computer rendering into a VR headset – due to the computational costs of colliders, joints, or other physics. (see "Optimizations" section, below)
3. By adjusting their location (and gaze), the user can:
    a. Gain Overview of the entire dataset (Shneiderman Task Level 1),
    b. Zoom on an item or subsets of items (Shneiderman Task Level 2),
    c. Filter irrelevant items (Shneiderman Task Level 3),
    d. Get details-on-demand for an item or subset of items (Shneiderman Task Level 4),
    e. Relate between items or subsets of items. (Shneiderman Task Level 5).

Please see the accompanying videos [83], as although Figure 20, Figure 21 and Figure 22 try to convey that behaviour, understanding MR interactions from screenshots is a rather futile endeavour.

For descriptions of Shneiderman Task Levels referred above, please see "2.2 Purposes for Cybersecurity" on page 16.

4.4.8 Textual information

Text labels of nodes, edges, groups are a significant issue, as these are expensive to render due to their complex geometrical shapes and also risk the possible occlusion of objects which may fall behind them. Accordingly, text is shown in VDE only when necessary. Backgrounds are not used with text in order to reduce their occlusive footprint.

4.4.9 Optimizations

The basis for VDE: less is more.

Occlusion of visual representations of data objects is a significant problem for 3D data visualizations on flat screens. In VR/MR environments, occlusion is mitigated by stereoscopic perception of the visualizations of data objects and by parallax, but can still be problematic [88].

While occlusion in VR can be addressed by measures such as transparency, transparency adds significant overhead to the rendering process. To optimize occlusion-related issues, VDE strikes a balance between the necessity of transparency of visualized objects, while adjusting the number of components currently visible (textual labels, reducing the complexity of objects that are farther from the user's viewpoint, etc.) based on the current load (measured FPS); on objects' relative positions in user's gaze (in-view, not-in-view, behind the user); and on the user's virtual distance from these objects. This XR-centric approach to semantic zooming proves a natural user experience, visually akin to the semantic zooming techniques used in online maps which smoothly but dramatically change the extent of detail as a function of zoom level (showing only major highways or the smallest of roads, toggling the visibility of street names and point of interest markers).

Please see the accompanying videos [83], as although Figure 20, Figure 21 and Figure 22 try to convey that behaviour, understanding MR optimizations from screenshots is a rather futile endeavour.

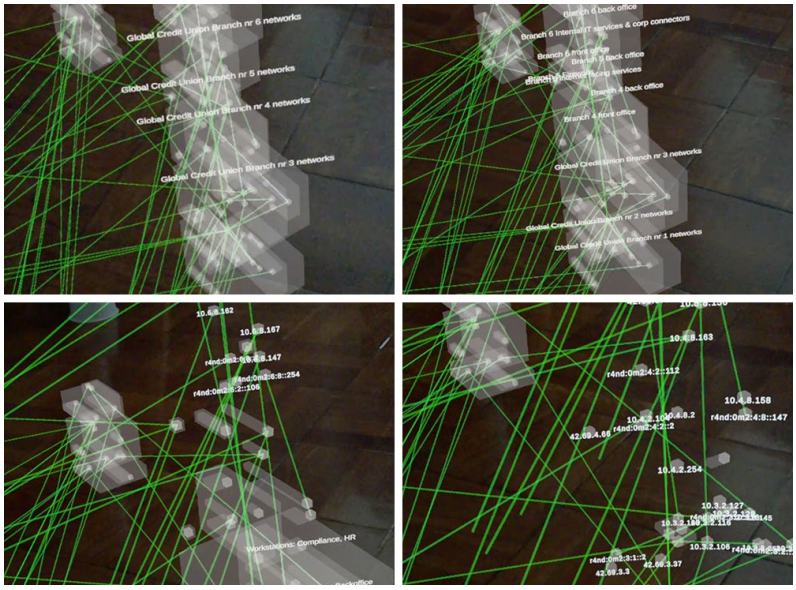


Figure 21 Once user moves closer to a part of the visualization that might be of interest, textual labels are shown for upper tier groups first, while the rectangular representations of these groups are disappeared as the user gets closer, to enable focusing on the subgroups inside, and then the nodes with their IP addresses as labels. To convey the changes in visualization as the user moves, screenshots are provided sequentially, from upper left to right. For comparison with Virtual Reality view, please see Figure 22.

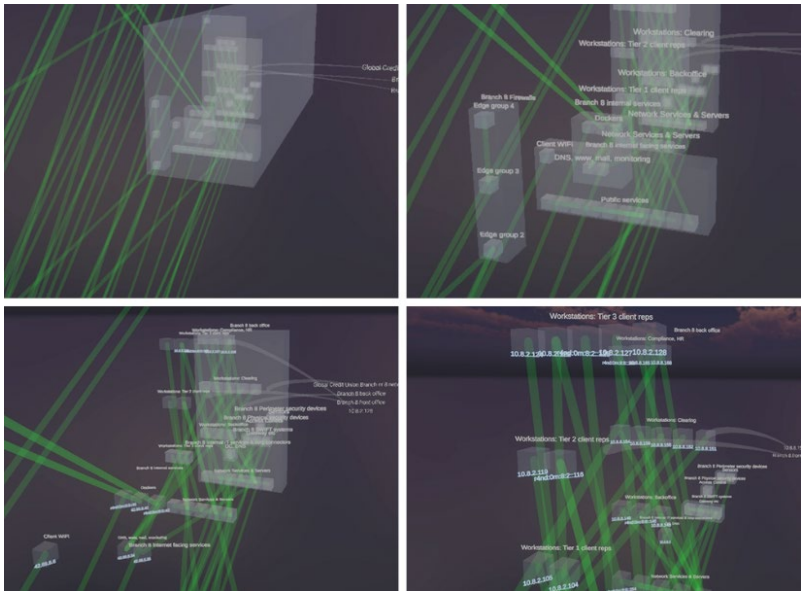


Figure 22 Once user moves closer to a part of the visualization that might be of interest, textual labels are shown for upper tier groups first, while the rectangular representations of these groups are disappeared as the user gets closer, to enable focusing on the subgroups inside, and then the nodes with their IP addresses as labels. To convey the changes in visualization as the user moves, screenshots are provided sequentially, from upper left to right. For comparison with Mixed Reality view, please see Figure 21.

Although colours and shapes of the visual representations of data objects can be used to convey information about their properties, user feedback has confirmed that these should be used sparsely. Therefore, in most VDE layouts, the nodes (representing data objects) are visualized as transparent off-white cubes or spheres, and the latter only in case if the available GPU is powerful enough. Displaying a cube versus a sphere may seem a trivial difference but considering the sizes of some of the datasets visualized (>10,000 nodes and >10,000 edges), these complexities add up quickly and take a significant toll.

4.5 Layouts

VDE has various data visualization layouts implemented, some of which are available in the open-source version of it (an example seen on Figure 23 below).

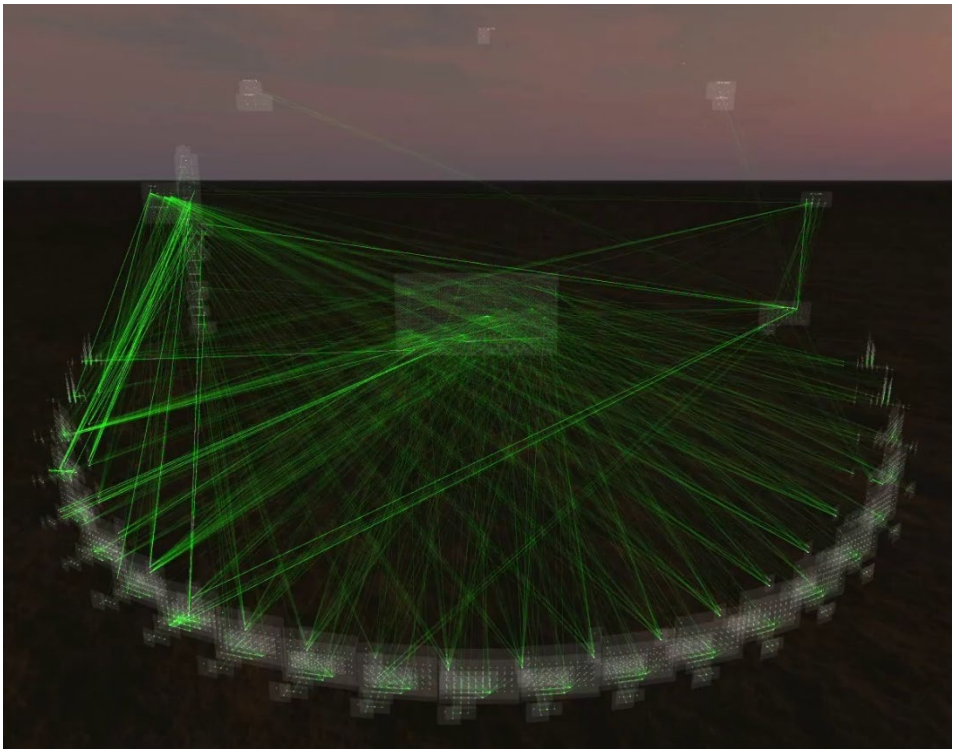


Figure 23 Overview of a layout visualizing Locked Shields CDX network topology augmented with network session counts (as edges) observed between networked nodes during a time window. Screenshot from VDE v1.

Primary challenges for designing visualization layouts are related to deciding how to position the entities (and their groups) found in a dataset into a three-dimensional space (see: 3.2).

Secondary challenges are the technical ones and relate to how to align the entities relative to each other so, that the visualization could be updated on-the-fly, without hindering VR or MR HMD FPS, while not confusing the user, and retaining the visualization in such a way that would not disturb the user from “reading” it. And, how to transform from one layout to another so, that the observer could retain the mental model and the internalized understanding of the visualized data through visual changes.

4.5.1 VDEC Layout Configuration

To accommodate to the specifics of different headsets' capabilities and user preferences, the layout of the visualization that VDEC populates based on the ingested data can be customized by tuning the layout configuration (see: Figure 24).

```
"name": "default",
"settings": {
  "defaultScale": 0.1,
  "defaultLineWidth": 0.01,
  "defaultLineWidthMultiplier": 61.5,
  "nodeSize": 0.5,
  "nodeOffset": 0.755,
  "edgeWidth": 0.02,
  "edgeCollidersEnabled": 1,
  "adjustToFPS": 1,
  "targetFPS": 69,
  "groupShapeAlpha": 0.1,
  "groupShapeMargin": 0.5,
  "groupShapePadding": 2,
  "maxColorForFirstXnodes": 50,
  "maxColorForFirstXedges": 50,
  "commonDataShapeWidth": 6,
  "mataShapeSize": 100,
  "maxNodesInShape": 2345,
  "minNodesInRow": 10,
  "dataShapeDistanceFromSINET": 100,
  "enlargeNodeSizeAccordingToCameraDistanceBy": 20,
  "showLables": 1,
  "showLabelsMaxDepth": 1,
  "showLabelsMinDepth": 2,
  "groupLabelVisibleSinceDistanceFromCamera": 8,
  "nodeLabelVisibleSinceDistanceFromCamera": 1.9,

  "HUDPositionX": -9,
  "HUDPositionY": 0,
  "HUDPositionZ": 20,
  "HUDPositionX": -9,
  "HUDPositionY": 0,
  "HUDPositionZ": 20,
  "notificationPositionX": 30,
  "notificationPositionY": -1,
  "notificationPositionZ": -5,
  "notificationOffset": 2,
  "notificationConnectorWidth": 0.15,
  "notificationConnectorPositions": 40,
  "showNotificationsOnDashboard": 0,
  "timeToGazeFocus": 4,
  "timeToGazeFocusOut": 5,

  "grabOffsetFromHandX": 0.03,
  "grabOffsetFromHandY": 0.01,
  "grabOffsetFromHandZ": -0.02
},
"rigidJoints": {
  "MemberMember": {
    "RigidBodyMass": 1,
    "RigidBodyDrag": 9,
    "JointMinDistance": 0.05,
    "JointMaxDistance": 0.05,
    "JointMixnDistance": 1,
    "JointMaxxDistance": 1,
    "JointSpringStrength": 1000,
    "JointDamper": 0,
    "JointTolerance": 0.2,
    "JointBreakForce": 9999999,
    "JointBreakTorque": 9999999,
    "ShouldCollideWithJointBody": 1
  },
```

Figure 24 Layout configuration for specifying how VDEC should position groups.

However, note that the rules for spatial positioning and grouping of the visual representations of ingested data is decoupled from the layout configuration, as these address two distinct tasks:

1. Layout configuration contains settings relevant to spatial positioning of groups (of groups (of groups)) of entities, their relative distances, text sizes, HUD positioning, labels visibility, and the like, while
2. Topology configuration allows the user (or designer of the visualization) to define rules for VDE, based on which the visual representations of (expected) entities found from the ingested data should be grouped and positioned.

VDEC expects VDES to provide it with the layout configuration upon connection, while the topology configuration will be used by VDES when processing the ingested data before sending the resulting groups (of groups (of groups)) of entities to connected VDEC-s.

For an example on how the positions of visual representations of data objects are decided for individual entities in a groups (of groups (of groups)) of entities, please see Figure 10 on page 26, accompanied with Figure 25 below. The intent of such configurability is to allow the users and / or visualization designers to configure the (relative) positions of entity visualizations via a configuration file, to maintain the expected visual topology of the visualization layout over time and over varying queries of that same dataset.

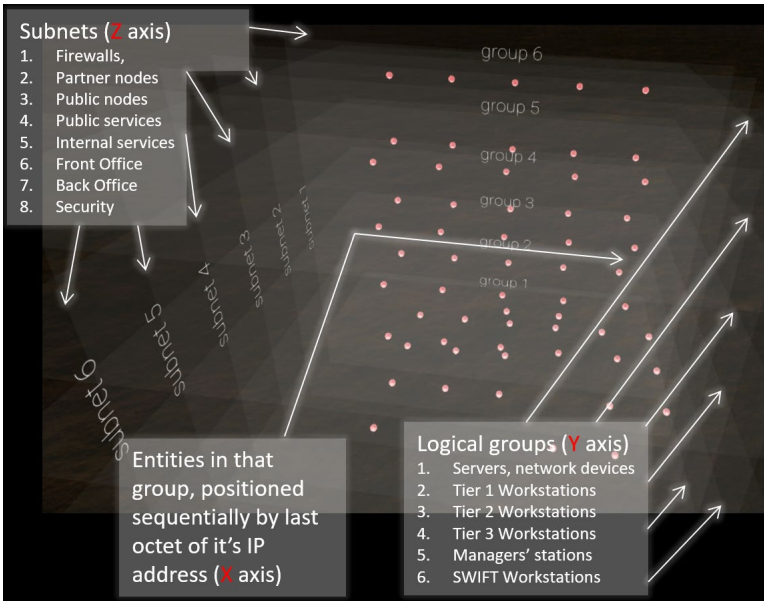


Figure 25 Explanatory schematics for a subgroup's layout in VDE Network Topology layout: similar layout populated with data is shown on Figure 10 *on page 26. This screenshot is an excerpt from my MAVRIC 2020 presentation (see: coda.ee/MAVRIC).*

The resulting visual representations of groups (of groups (of groups)) will be arranged relative to other groups based on the C# implementation of that layout and its configuration. An example of such a constellation of groups can be seen on Figure 26, where each transparent cube contains a topology visualization, containing subgroups arranged as explained on Figure 25.

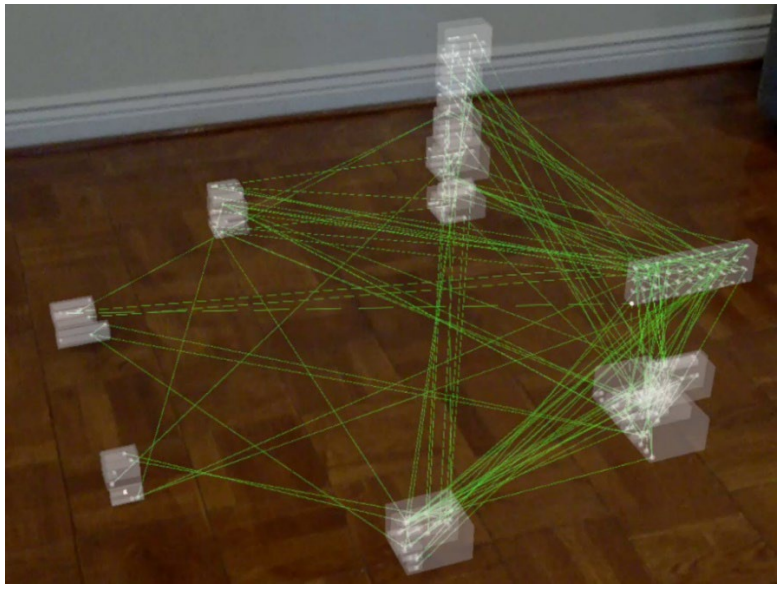


Figure 26 Overview of a layout visualizing a network topology. Screenshot from VDE v2, running on Magic Leap MR headset.

4.6 Datasets used for Development and Testing

Although there are some public, reasonably large cybersecurity related datasets like VAST [89] and [90], these do not represent the complexities (and messiness) of such real-world datasets that need to be dissected, understood and monitored for CDSA by SMEs [91]. Therefore, for creating and testing VDE, while also creating and testing its visualization layouts, I had to use large and complex enough datasets, that I was familiar with. An additional requirement for choosing the dataset was, that the visualizations created using that dataset would be publishable.

I was lucky enough to be entrusted with the NATO CCDCOE Locked Shields (LS) Cyber Defence Exercises' full packet captures (PCAP files from years 2015, 2016, 2017, 2018, 2019, 2021 and 2022 that were used during various stages of VDE development), while also having intimate knowledge of that exercise inner workings: I've been participating as a Red Team member since 2010, witnessed the environment expanding to satisfy growing demands, learnt its topology and expected behaviours. Hence most of my published papers used visualizations featuring LS datasets (or a mock-up dataset made for visualization capabilities' demonstration purposes), as other datasets for which' VDE has been used for, are not publishable.

LS PCAP files contain network traffic captured from the Game Network during the 2 days of exercise. That traffic consists of up to 26 defensive teams' (Blue Teams, BT) networks (each of which contains more than 100 nodes), an offensive (Red Team, RT), infrastructure support (Green Team), situational awareness (Yellow Team) and the managing team (White Team) nodes and traffic: totalling at more than 4000 active virtual machines engaged at a time, with about 2500 (documented) attacks executed by the Red Team against all Blue Teams combined. As both, the full IPv4 and IPv6 address space is usable for the game (with some exceptions), the expected network topology (a complicated system) blends with known unknown and unknown unknown (complex systems), resulting in a nice and messy environment that is well suited for my research purposes.

For reference, an abstraction of the expected topology of a network that one Blue Team (out of 26) may have been expected to protect during an LS exercise is shown on Figure 27.

VDE has also been used to visualize non-cybersecurity related datasets, an example of such being the IST-141 Interactive Exploration of NATO Panels' Activities [7].

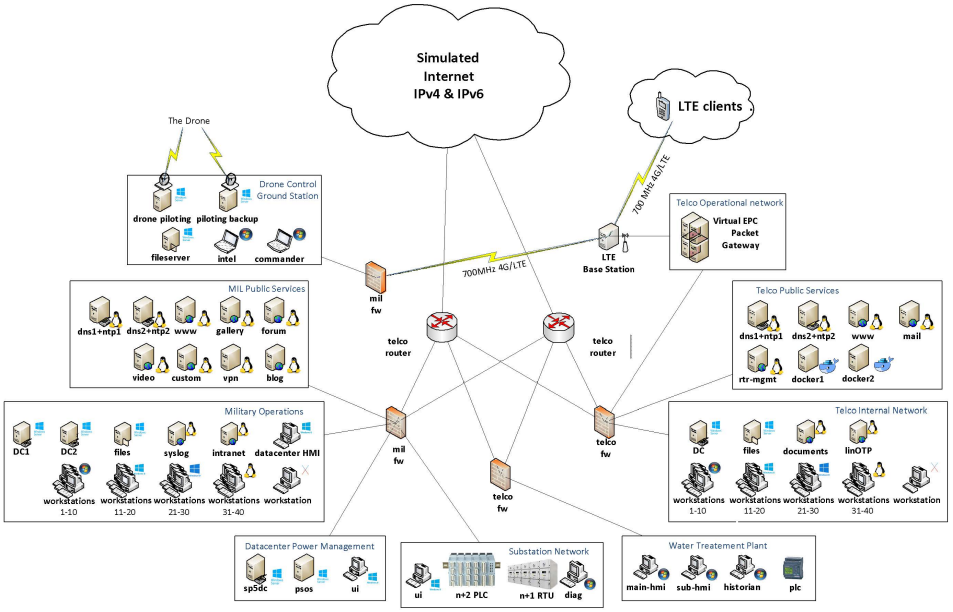


Figure 27 Simplified network topology diagram of a Blue Team's networked assets during a Locked Shields Cyber Defence Exercise

5 Feedback and User study

User feedback to VDE has been very positive. A study [2] that captured cybersecurity analysts' impressions of a network topology presented as a stereoscopically-perceivable 3D structure found, that overall, the impressions towards stereoscopically-perceivable 3D data visualizations were highly favourable. Multiple participants acknowledged that such 3D visualizations of network topology could assist in their understanding of the networks they use daily. Participants expressed a wish to integrate such visualization capabilities in their workflow. Prior experience with 3D displays had no influence on user preferences, while participants with prior gaming experience adjusted quickly to the Oculus Touch motion controllers, suggesting that the relevant dexterity and muscle memory for gaming console controller usage helps users adjusting from those controllers to handling input devices for VR experiences.

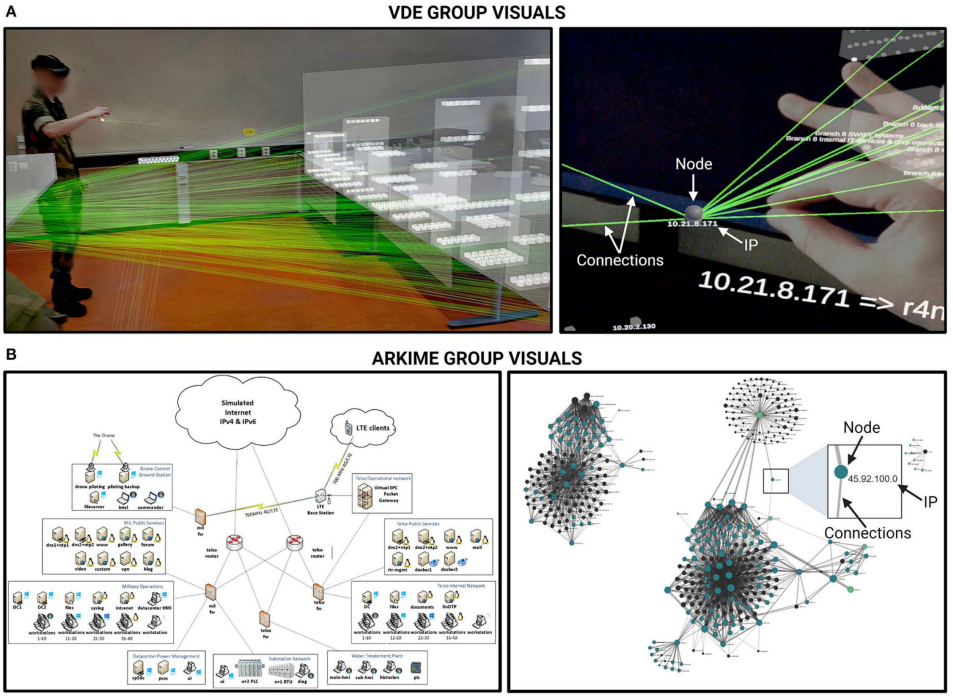


Figure 28 Overview of the visualization tools used in each condition. [8]

A) The Virtual Data Explorer (VDE) representation of the network topology. The first image in the panel (left-hand side) depicts an overview of the network layout used in the present study. The second image (right-hand side) is a representative close-up (taken from [6]). White arrows have been superimposed on the image on the right to indicate node/hosts, edges that represent connections between nodes, and the host IP address. (B) Images depicting the 2D network topology as shown in the Arkime condition. The first image in the panel depicts an approximation of the 2D representation of network topology as shown in the paper schematics. The second image depicts a graph representation of the network topology as shown in the Arkime software, where dots are hosts and edges are the connections between them. Participants could zoom in, select nodes to see exclusive connections, session number, and so on.

In the dyadic cyber team communication and cyber situational awareness study [8], we compared how visual representation of network topology and traffic as ISPMDV (see: Figure 28.a) vs. 2D visualizations (see: Figure 28.b) affected team performance in a sample of cyber cadets (N = 22) cooperating in dyads. Performance outcomes included network topology recognition, cyber situational awareness, confidence in judgements, experienced communication demands, observed verbal communication, and forced choice decision-making. The study utilized network data from the NATO CCDCOE 2022 Locked Shields cyber defence exercise (see: 4.6) and the Virtual Data Explorer software (see: 4.2).

We found that participant dyads using the VDE ISPMDV had better cyber situational awareness compared to the participant dyads that relied only on flat screen (2D) visualizations and textual information. The ISPMDV group was generally more confident in their judgments except when performing worse than the 2D group on the topology recognition task (which by design favoured the dyads that used flat screen and textual information only). Participants in the 3D mixed reality group experienced less communication demands and performed more verbal communication aimed at establishing a shared mental model and less communications discussing task resolution. Better communication was associated with better cyber situational awareness.

A collaborative, Mixed Reality representation of a network topology and network attack provided better CDSA compared to using flat screen or printed, 2D topology schematics and graph representation in the packet capture software Arkime.

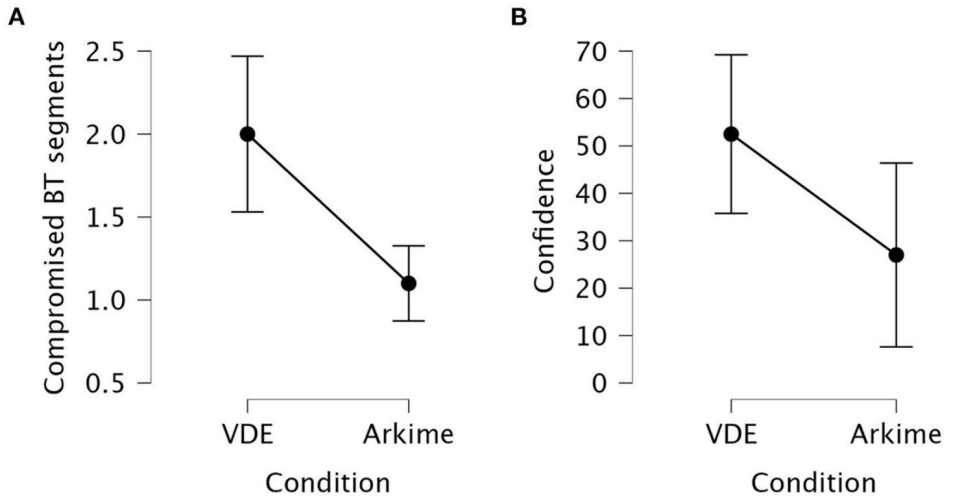


Figure 29 Interval plots for the differences in identifying compromised Blue Team systems. [8]

(A) Identified compromised Blue Team systems.

(B) Confidence in having identified compromised Blue Team segments. Whiskers are 95% confidence intervals.

The most apparent difference was in the detection of the top five Red Team hosts targeting Blue Team systems. The traffic associated with the identified Red Team hosts in the Mixed Reality condition differed in the tens of thousands. This is remarkable,

as participants in the ISPMDV condition could only use edge brightness as a cue for traffic while participants in the Arkime condition could see the actual session number statistics.

Observed and self-reported communication was better for dyads in the ISPMDV condition and was associated with their CSA. This may suggest that the VDE has neuroergonomic benefits when SOC team analysts need to communicate for shared CSA. Although participants in the ISPMDV condition had higher CSA, we were not able to measure its effect on decision-making. This could be due to cohort effects such as training or the modest sample size. See Figure 29 on page 49.

Finally, the experimental tasks and preliminary nature of the study does not reflect SOC tasks with sufficient realism. Thus, to truly assess the potential effects of VDE on communication for shared CSA, the study should be repeated in a naturalistic setting with a larger and more diverse sample.

As such, ours was the first study comparing the efficiency of ISPMDV and flat screen visualizations of network topology on dyadic cyber team communication and cyber situational awareness. Using ISPMDV resulted in better situational awareness and team communication. The experiment should be repeated in a larger and more diverse sample to determine its potential effect on decision-making.

6 Results and Findings

The overall contribution of my research is the development of the knowledge and practical approaches of how to visualize multidimensional non-(geo)spatial datasets in stereoscopically perceivable (artificial) environments in useful ways, how to design the three-dimensional layouts of such visualizations, but also the Virtual Data Explorer software and its release as Open-Source Software [23].

I chose to approach Research Questions (see: 1.2) in parallel: develop the necessary software for ISPMDV (RQ3), while figuring out the human side of the problem – how to decide such visualizations' layouts (RQ1, RQ2).

To enable users to visualize data as predetermined three-dimensional layouts while it would be stereoscopically perceivable and interactable (RQ3), I created the Virtual Data Explorer (VDE, see: chapter 4). VDE enables a user to perceive the spatial layout of a dataset, for example the topology of a computer network, while the resulting visualization can be augmented with additional data, like network session counts between network nodes.

Before SMEs could be provided with useful data visualization tools for their tasks, their needs had to be understood: together with my co-authors I created the Mental Model Mapping Method for Cybersecurity (see: 3.2), that enables one to design data visualizations (RQ2) together with SMEs using a participatory method (RQ1): components of these visualizations would be arranged as a set of objects in stereoscopically perceivable artificial environment (either Virtual or Mixed Reality) – referred to as data-shapes.

Useful visualizations for SMEs can be created with the combination of employing M4C and using VDE for data visualization. Although larger scale user studies were hindered by covid-19, user feedback [2] and ongoing studies have confirmed the advantages of M4C and VDE.

Amongst many findings during my research that guided the outcome, the most important one is the realization of the importance of providing users with intuitive interaction capabilities to explore and query the visualized data, while (also) being able to control the visualized dataset using contemporary on-screen toolset that they've learnt to rely on (see: 4.4.7).

I will be continuing my research, investigating 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 to oncoming team members. It is possible that this would speed up the onboarding of new team members by assisting them in learning the functional topology and the behaviour of entities that are present in their datasets, for example, the logs from various devices in the protected computer networks.

Most importantly however, I'm curious to find out, how to quantify the level of improvement of how much more beneficial, more useful would an ISPMDV be for the users, with whom these visualizations are created, compared to contemporary alphanumeric and 2D visualization tools. The user study (see: 5) was a first step in that regard.

7 Conclusion

The quantity of logs, telemetry and various other data collected from networked devices and devices that are running computer networks is increasing steadily, if not exponentially due to our society's growing dependence on interconnected information technology [15].

More data does not in itself yield better information. To make sense of the collected data in a timely manner, to maintain actionable CDSE & CDSU, SMEs need to know well the system (of systems) they need to protect and be able to augment the expected (but everchanging) baseline of their (known) system with relevant (subset of) fresh data, to transform the combination of gathered information into actionable CDSE, that will then feed into timely CDSU.

7.1 Novelty

Prior to my research, there were no publicly available data visualization tools (RQ3) that would have enabled its users to create and use stereoscopically perceivable immersive and interactive 3D visualizations depicting non-(geo)spatial datasets as multidimensional shapes: existing tools (the likes of OpenGraphiti and V-Arc) were able to visualize force directed graphs, bar charts and the like.

There were no applicable method(s) detailing the process of creating such visualizations that would be rooted in Cybersecurity Subject Matter Experts (SMEs) mental models (such that would map to the visualized dataset), integrated into an analyst's existing working environment, while also support an analyst's existing problem-solving strategies (RQ1 & RQ2).

I identified that there was a need for structured evaluation of visualizations that are created based on an analyst's internalized understanding of a dataset. Preliminary work also demonstrated that through purposeful interaction with SMEs it is possible to identify the core concepts of their mental models for relevant datasets, and to create matching data-shapes for those.

To address that, the Mental Model Mapping Method for Cybersecurity (M4C, see: 3.2) addressing RQ1 & RQ2 was published in 2020 [4]. This paper describes the theory and a method that can be used to develop a 3D visualization of network topology and overlay it with relevant data. The selection of attributes of data-shapes and their display layout aims to capture cybersecurity analysts' mental models, to enable the analysts to better understand their respective datasets.

M4C 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.

Currently available Virtual and Mixed Reality (VR/MR) technology can provide users with interactive stereoscopically perceivable multidimensional data visualizations (ISPMDV) that can be used to better understand complex data structures and datasets. M4C demonstrates that through tight interaction with SMEs it is possible to identify core concepts in their mental models and transform these into data-shapes that these same SMEs can then use with VR/MR equipment for their tasks. Further research is needed to find out, how generalizable are such data-shapes, compared over different types of networks, cyber operations, analyst past training and other individual differences.

However, the benefits of harnessing human visual perception for CDSA/CDSU can provide a much-needed advantage to these SMEs.

The software I created, Virtual Data Explorer (VDE, see: 4.2), has been integrated into the Virtual Reality Data Analysis Environment (VRDAE) [3] and Mixed Reality Exploration Toolkit (MRET) [23]. These and other collaborative projects employing VDE for research have resulted in additional papers [24] [23], while commercial deployments are under way. VDE was instrumental in seeking answers for RQ3.

Immersive visualizations of large and dynamic node-link diagrams require careful consideration for visual comprehensibility and computational performance. While many forms of node-link visualization idioms are well-studied in the form of 2D flat screen visualizations, the opportunities and constraints presented by VR and MR environments are distinct.

Optimizing VR/MR user interactions for VDE presented the design challenge of providing an interface that intuitively offers an informative presentation of the node-link network both at a high-level "overview" zoom level and at a very zoomed-in "detail" view, with well-chosen levels of semantic zoom available along the continuum between these extremes. Constrained navigation further optimizes the user experience, limiting confusion and motion sickness. Dynamic highlighting, through the selection and controller-based movement of individual notes, enhances the users' understanding of the data.

7.2 Relevance

User feedback to VDE has been very positive. A study [2] that captured cybersecurity analysts' impressions of a network topology presented as a stereoscopically-perceivable 3D structure found, that overall, the impressions towards stereoscopically-perceivable 3D data visualizations were highly favourable. Multiple participants acknowledged that such 3D visualizations of network topology could assist in their understanding of the networks they use daily. Participants expressed a wish to integrate such visualization capabilities in their workflow. Prior experience with 3D displays had no influence on user preferences, while participants with prior gaming experience adjusted quickly to the Oculus Touch motion controllers, suggesting that the relevant dexterity and muscle memory for gaming console controller usage helps users adjusting from those controllers to handling input devices for VR experiences.

In our latest study [8] we found that participant dyads using the VDE ISPMDV had better cyber situational awareness compared to the participant dyads that relied only on flat screen (2D) visualizations and textual information. The ISPMDV group was generally more confident in their judgments except when performing worse than the 2D group on the topology recognition task (which by design favoured the dyads that used flat screen and textual information only). Participants in the 3D mixed reality group experienced less communication demands and performed more verbal communication aimed at establishing a shared mental model and less communications discussing task resolution. Better communication was associated with better cyber situational awareness.

As the scientific and engineering community continues to adopt VR and MR for their work, it is likely that there will be an ongoing acceleration in the development of open-source VR/MR tools for related tasks. Some of the needs of specific technical communities will vary as a function of their data and problem spaces, requiring visualization of various forms of spatial (voxel, point cloud, mesh) and non-spatial data (such as the node link diagrams supported by VDE). However, most R&D use cases will

also share many requirements, such as the ability to securely share a VR/MR environment in real time with other VR/MR users; the ability to support a wide range of VR/MR hardware with the same software; and the ability to load or stream large datasets. NASA MRET is an example on that regard on how to address these problems and provide a free open source solution for it [23].

While SPMDVs for intrinsically (geo)spatial data have received substantial publicity, the creation, presentation, and usability research of SPMDVs and ISPMDVs designed to show non-spatial data has attracted less attention. I encourage cybersecurity professionals and researchers to use emerging technologies (e.g., VR/MR) to explore novel ways for visualizing datasets relevant to their problems and tasks.

List of Figures

References

[1] 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.

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

[3] 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.

[4] K. Kullman, L. Buchanan, A. Komlodi and D. Engel, "Mental Model Mapping Method for Cybersecurity," in *HCI for Cybersecurity, Privacy and Trust*, Tallinn, 2020.

[5] K. Kullman and D. Engel, "Interactive Stereoscopically Perceivable Multidimensional Data Visualizations for Cybersecurity," *Journal of Defence & Security Technologies,* vol. 4, no. 3, pp. 37-52, 2022.

[6] K. Kullman and D. Engel, "User Interactions in Virtual Data Explorer," in *International Conference on Human-Computer Interaction*, 2022.

[7] M. Varga, K. K. Liggett, P. Bivall, V. Lavigne, K. Kullman, E. Camossi, C. Ray, E. Arkin, T. Krilavičius, J. Mandravickaitė, C. Winkelholz, S. Träber-Burdin, S. Jayaram, M. Panga and Achary, "Exploratory Visual Analytics," North Atlantic Treaty Organization, 2022.

[8] T. F. Ask, K. Kullman, S. Sütterlin, B. J. Knox, D. Engel and R. G. Lugo, "A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness," *Frontiers in Big Data,* vol. 6, pp. 1-21, 2023.

[9] The White House, "National Security Presidential Directive / NSPD-54," 08 01 2008. [Online]. Available: https://irp.fas.org/offdocs/nspd/nspd-54.pdf.

[10] J. Yen, R. F. Erbacher, C. Zhong and P. Liu, "Cognitive Process," in *Cyber Defense and Situational Awareness*, Springer, 2014, pp. 119-144.

[11] P. Kapur, V. Yadavali and A. Shrivastava, "A Comparative Study of Vulnerability Discovery Modeling and Software Reliability Growth Modeling," in *1st International conference on futuristic trend in computational analysis and knowledge management (ABLAZE 2015)*, Greater Noida, 2015.

[12] C. Gonzalez, N. Ben-Asher, A. Oltramari and C. Lebiere, "Cognition and Technology," in *Cyber Defense and Situational Awareness*, Springer, 2014, pp. 93-115.

[13] S.-Y. Ji, B.-K. Jeong and D. H. Jeong, "Evaluating visualization approaches to detect abnormal activities in network traffic data," *International Journal of Information Security,* pp. 331-345, 2021.

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

[15] S. Kaisler, F. Armour, A. J. Espinosa and W. Money, “Big Data: Issues and Challenges Moving Forward,” in *2014 47th Hawaii International Conference on System Sciences*, Wailea, 2014.

[16] 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].

[17] T. Lovering, “Odin's Ravens,” *The Three Swords,* no. 27, pp. 50-52, 11 2014.

[18] C. G. Healey, L. Hao and S. E. Hutchinson, “Visualizations and Analysts,” in *Cyber Defense and Situational Awareness*, Springer, 2014, pp. 145-165.

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

[20] M. Varga, C. Winkelholz and S. Träber-Burdin, “The Application of Visual Analytics to Cyber Security,” NATO, 2017.

[21] F. Ababsa, “Augmented Reality Application in Manufacturing Industry: Maintenance and Non-destructive Testing (NDT) Use Cases,” in *7th International Conference on Augmented Reality, Virtual Reality, and Computer Graphics*, Lecce, 2020.

[22] S. Skolnik, “Using Virtual Reality to Visualize Disasters, Climate, and Extreme Weather Impacts,” in *MAVRIC*, College Park, 2020.

[23] National Aeronautics and Space Administration, “Mixed Reality Exploration Toolkit,” 2020. [Online]. Available: https://github.com/nasa/Mixed-Reality-Exploration-Toolkit. [Accessed 06 08 2022].

[24] University of Texas at San Antonio (UTSA), “TBD (Britta Munsinger),” 2021.

[25] M. R. Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal,” *The Journal of the Human Factors and Ergonomics Society,* vol. 37, no. 1, pp. 32-64, 1995.

[26] U.S. ARL, *SEEING THE CYBERTHREAT,* Aberdeen Proving Ground, Maryland: U.S. Army Research Laboratory, 2018.

[27] 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.

[28] M. O. Ward, G. Grinstein and D. Keim, Interactive Data Visualization: Foundations, Techniques, and Applications, Second Edition, A K Peters/CRC Press , 2015.

[29] L. Meyerovich and P. Tomasello, “Display Relationships Between Data,” *IQT Quarterly,* vol. 7, no. 4, 2016.

[30] 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.

[31] D. M. Best, A. Endert and D. Kidwell, “7 Key Challenges for Visualization in Cyber Network Defens,” in *In Proceedings of the Eleventh Workshop on Visualization for Cyber Security*, 2014.

[32] A. Kirk, Data Visualisation, A Handbook for Data Driven Design, Sage, 2016, p. 223.

[33] W. H. Ehrenstein, L. Spillmann and V. Sarris, "Gestalt Issues in Modern Neuroscience," in *Axiomathes*, Springer, 2003, pp. 433-458.

[34] P. Lebreton, A. Raake, M. Barkowsky and P. Le Callet, "Evaluating Depth Perception of 3D Stereoscopic Videos," *IEEE Journal of Selected Topics in Signal Processing,* vol. 6, no. 6, 2012.

[35] G. Shearer and J. Edwards, "Vids: Version 2.0 Alpha Visualization Engine," US Army Research Laboratory, Adelphi, 2018.

[36] T. J. Gaw, *3D Information Visualization of Network Security Event,* Munice, Indiana: Ball State University, 2014.

[37] D. Inoue, K. Suzuki, M. Suzuki, M. Eto and K. Nakao, "DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System," in *VizSec*, 2012.

[38] J.-P. van Riel and B. Irwin, "InetVis, a Visual Tool for Network Telescope Traffic Analysis," in *AFRIGRAPH 2006*, Cape Town, 2006.

[39] S. P. Berry, "The Shoki Packet Hustler," [Online]. Available: http://shoki.sourceforge.net/.

[40] T. Reuille, S. Hawthorne, A. Hay, S. Matsusaki and C. Ye, "OpenDNS Data Visualization Framework," 2015. [Online]. Available: http://www.opengraphiti.com/.

[41] K. Maddix, "Big Data VR Challenge – Winners!," 2015. [Online]. Available: http://www.mastersofpie.com/big-data-vr-challenge-winners/.

[42] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Computers in Human Behavior,* vol. 48, pp. 51-61, 2015.

[43] B. Shneiderman, "The eyes have it: a task by data type taxonomy for information visualizations," in *Proceedings 1996 IEEE Symposium on Visual Languages*, Boulder, CO, USA, USA, 1996.

[44] L. Hao, C. G. Healey and S. E. Hutchinson, "Ensemble Visualization For Cyber Situation Awareness of Network Security Data," in *IEEE SYMPOSIUM ON VISUALIZATION FOR CYBER SECURITY (VIZSEC)*, 2015.

[45] P. Rajivan, E. Konstantinidis, N. Ben-Asher and C. Gonzalez, "Categorization of Events in Security Scenarios: The Role of Context and Heuristics," *Human Factors and Ergonomics Society Annual Meeting,* vol. 60, no. 1, pp. 274-278, 2016.

[46] D. A. Fisher, "BubbleUp: Supporting DevOps With Data Visualization," *IEEE Computer Graphics and Applications,* vol. 41, no. 1, pp. 99-105, 2021.

[47] VizSec, 2004-2021. [Online]. Available: https://vizsec.dbvis.de/.

[48] K. Reda, A. Febretti, A. Knoll, J. Aurisano, J. Leigh, A. Johnson, M. E. Papka and M. Hereld, "Visualizing large, heterogeneous data in hybrid-reality environments," *IEEE Computer Graphics and Applications,* vol. 33, no. 4, pp. 38-48, 2013.

[49] P. Gershon, R. L. Klatzky and R. Lee, "Handedness in a virtual haptic environment: Assessments from kinematic behavior and modeling," *Acta Psychologica,* pp. 37-42, 2014.

[50] P. Gershon, R. L. Klatzky, H. p. Palani and N. A. Giudice, “Visual, Tangible, and Touch-Screen: Comparison of Platforms for Displaying Simple Graphics,” *Assistive technology: the official journal of RESNA,* vol. 28, no. 1, pp. 1-6, 2016.

[51] C. Hodent, The Gamer’s Brain; How Neuroscience and UX Can Impact Video Game Design, CRC Press, 2018, pp. 221,222.

[52] M. Podwal, “Google Earth VR — Bringing the whole wide world to virtual reality,” 16 11 2016. [Online]. Available: https://blog.google/products/google-ar-vr/google-earth-vr-bringing-whole-wide-world-virtual-reality/.

[53] U.S. Army DEVCOM ARL Public Affairs, “Army leverages virtual reality to understand network influence,” 23 06 2021. [Online]. Available: https://www.army.mil/article/247165.

[54] Voices of VR, “50 years of VR with Tom Furness: The Super Cockpit, Virtual Retinal Display, HIT Lab, & Virtual World Society,” 17 11 2015. [Online]. Available: https://voicesofvr.com/245-50-years-of-vr-with-tom-furness-the-super-cockpit-virtual-retinal-display-hit-lab-virtual-world-society/. [Accessed 08 2022].

[55] S. Daley, “9 Companies Using VR and Augmented Reality to Improve Surgery,” 7 5 2022. [Online]. Available: https://builtin.com/healthcare-technology/augmented-virtual-reality-surgery. [Accessed 6 8 2022].

[56] S. Taschler, “What is Proactive Threat Hunting?,” 18 02 2021. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/threat-hunting/.

[57] K. Peffers, T. Tuunanen, M. A. Rothenberger and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research,” *Journal of Management Information Systems,* vol. 24, no. 3, pp. 45-77, 2007.

[58] W. Schneider, S. T. Dumais and R. N. Shiffrin, “Automatic and Control Processing and Attention,” University of Illinois, Illinois, 1982.

[59] D. M. Dejoy, K. R. Laughery and M. S. Wogalter, “Organizing theoretical framework: a consolidated communication-human information processing (C-HIP) model. Warnings and risk communication,” 1999, pp. 15-23.

[60] D. Gentner and A. Stevens, Mental Models (Cognitive Science Series), Lawrence Erlbaum Associates, 1983.

[61] P. N. Johnson-Laird, Mental Models, Cambridge University Press, 1983.

[62] D. Paradice and R. A. Davis, DSS and Multiple Perspectives of Complex Problems, 2008.

[63] A. Paivio, “Dual Coding Theory: Retrospect And Current Status,” *Canadian Journal of Psychology/Revue canadienne de psychologie,* vol. 45, no. 3, pp. 255-287, 1991.

[64] A. Baddeley, “Working Memory: Theories, Models, and Controversies,” *Annual Review of Psychology,* vol. 63, pp. 1-29, 2012.

[65] A. Treisman and R. Paterson, “Emergent features, attention, and object perception,” *Journal of Experimental Psychology: Human Perception and Performance,* vol. 10(1), no. 12, 1984.

[66] S. R. Ellis, M. W. Mcgreevy and R. J. Hitchcock, “Perspective traffic display format and airline pilot traffic avoidance,” *Human Factors,* vol. 29, pp. 371-382, 1987.

[67] M. Lange, T. Dang and M. Cooper, “Interactive resolution of conflicts in a 3d stereoscopic environment for air traffic control,” in *Research, Innovation and Vision for the Future, 2006 International Conference on*, Ho Chi Minh City, Vietnam, Vietnam, 2006.

[68] K. Lee and S. Lee, “3D Perception Based Quality Pooling: Stereopsis, Binocular Rivalry, and Binocular Suppression,” *IEEE Journal of Selected Topics in Signal Processing ,* vol. 9, no. 3, pp. 533-545, 2015.

[69] D. C. Foyle, A. D. Andre and B. L. Hooey, “Situation Awareness in an Augmented Reality Cockpit: Design, Viewpoints and Cognitive Glue,” Las Vegas, 2005.

[70] R. L. Klatzky, J. M. Loomis, A. C. Beall, S. S. Chance and R. G. Golledge, “Spatial Updating of Self-Position and Orientation during Real, Imagined, and Virtual Locomotion,” Sage Publications, Inc., 1998.

[71] M. A. Brown, “Displays for Air Traffic Control: 2D, 3D and VR - A Preliminary Investigation,” Queen Mary & Westfield College, London, 1994.

[72] D. J. Bryant and B. Tversky, “Mental Representations of Perspective and Spatial Relations from Diagrams and Models,” *Journal of Experimental Psychology Learning Memory and Cognition,* vol. 25, no. 1, pp. 137-156, 1999.

[73] H. S. Smallman, M. St. John, H. M. Oonk and M. B. Cowen, “Information availability in 2D and 3D displays,” *IEEE Computer Graphics and Applications,* vol. 21, no. 5, pp. 51-57, 2001.

[74] M. T. Dennehy, D. W. Nesbitt and R. A. Sumey, “Real-Time Three-Dimensional Graphics Display for Antiair Warfare Command and Control,” *Johns Hopkins APL Technical Digest,* vol. 15, no. 2, pp. 110-119, 1994.

[75] M. S. Burnett and W. Barfield, “Perspective versus plan view air traffic control (ATC) displays - Survey and empirical results,” in *International Symposium on Aviation Psychology, 6th*, Columbus, 1991.

[76] M. St. John, M. B. Cowen, H. S. Smallman and H. M. Oonk, “The Use of 2D and 3D Displays for Shape-Understanding versus Relative-Position Tasks,” *Human Factors,* vol. Spring, pp. 79-98, 2001.

[77] A. D‘Amico, L. Buchanan, D. Kirkpatrick and P. Walczak, “Cyber Operator Perspectives on Security Visualization,” in *Advances in Human Factors in Cybersecurity*, Springer, 2016, pp. 69-81.

[78] A. D’Amico, K. Whitley, D. Tesone, B. O’Brien and E. Roth, “Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts,” in *Proceedings of the HFES 49th Annual Meeting*, 2005.

[79] S. J. Perl and R. O. Young, “A Cognitive Study of Incident Handling Expertise,” Berlin, 2015.

[80] 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.

[81] 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.

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

[83] K. Kullman, "Virtual Data Explorer," 2022. [Online]. Available: https://coda.ee/tees.

[84] R. Keogh and J. Pearson, "The blind mind: No sensory visual imagery in aphantasia," *Cortex,* vol. 105, pp. 53-60, 2017.

[85] The Bro Project, [Online]. Available: https://www.bro.org/.

[86] D. M. Johnson, "Introduction to and Review of Simulator Sickness Research," U.S. Army Research Institute, Fort Rucker, 2005.

[87] C. Pruett, "Lessons from the frontlines modern VR design patterns," 09 06 2017. [Online]. Available: https://developer.oculus.com/blog/lessons-from-the-frontlines-modern-vr-design-patterns/.

[88] N. Elmqvist and P. Tsigas, "A Taxonomy of 3D Occlusion Management for Visualization," *IEEE Transactions on Visualization and Computer Graphics,* vol. 14, no. 5, pp. 1095-1109, 2008.

[89] Visual Analytics Benchmark Repository, "VAST Challenge 2011, MC2 - Computer Networking Operations," University of Maryland, [Online]. Available: http://visualdata.wustl.edu/varepository/VAST%20Challenge%202011/challenges/MC2%20-%20Computer%20Networking%20Operations/.

[90] Visual Analytics Benchmark Repository, "VAST Challenge 2013, MC3 - Big Marketing," University of Maryland, 2013. [Online]. Available: http://visualdata.wustl.edu/varepository/VAST%20Challenge%202013/challenges/MC3%20-%20Big%20Marketing/.

[91] M. E. Halisdemir, H. Karacan, M. Pihelgas, T. Lepik and S. Cho, "Data Quality Problem in AI-Based Network Intrusion Detection Systems Studies and a Solution Proposal," in *14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*, Tallinn, 2022.

[92] J. Bertin, Graphics and Craphic Information Processing, Berlin: Walter de Gruiter, 1981.

[93] S. A. a. L. Shih, "Towards and Interactive Learning Approch in Cybersecurity Education.," in *Proceedings of the 2015 Information Security Curruculum Development Conference*, New York, 2015.

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

[95] P. J. Schoenwaelder, M. Burgess, O. Festor, G. Martinez Perez, R. Stadler and B. Stiller, "Key research challenges in network management," *IEEE Communications Magazine,* vol. 45, no. 10, p. 104–110, 2007.

[96] A. Kabil, T. Duval, N. Cuppens, G. L. Comte, Y. Halgand and C. Ponchel, "Why should we use 3D Collaborative Virtual Environments for Cyber Security?," in *VR International Workshop on Collaborative Virtual Environments (3DCVE)*, Reutlingen, 2018.

[97] A. Kabil, T. Duval and N. Cuppens, “Alert Characterization by Non-expert Users in a Cybersecurity Virtual Environment - A Usability Study,” in *Augmented Reality, Virtual Reality, and Computer Graphics. AVR 2020. Lecture Notes in Computer Science*, 2020.

[98] 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.

[99] A. Batch and N. Elmqvist, “The Interactive Visualization Gap in Initial Exploratory Data Analysis,” *IEEE Transactions on Visualization and Computer Graphics,* vol. 24, no. 1, pp. 278-287, 2018.

Acknowledgements

For all the hints, ideas, help, and mentoring, I wholeheartedly thank you: Olaf Manuel Maennel, Alexander Kott, Don Engel, Jennifer A. Cowley, Lee C. Trossbach, Matthew Ryan, Stefan Sütterlin, Noam-Ben Asher, Char Sample, Laurin Buchanan, Anita Komlodi, Jaan Priisalu, Hillar Aarelaid, Toomas Vaks.

This research was partly supported by the Army Research Laboratory under Cooperative Agreement Number W911NF-17-2-0083 and in conjunction with the CCDC Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center. 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.

This research was partly supported by National Aeronautics and Space Administration under award number 80GSFC21M0002.

Abstract

Interactive Stereoscopically Perceivable Multidimensional Data Visualizations for Cybersecurity

The personnel responsible for maintaining and protecting complex systems must monitor those systems for anomalous behaviours to timely detect and mitigate possible security incidents. To identify such anomalous behaviours of complex systems, defenders first need to establish the baseline behaviour, either via human observations or attempting to utilize machine learning methods on behavioural indicators gathered from that or similar system(s).

My PhD research interest focused on the former: what tools would assist a defender, who has been tasked to learn the expected (baseline) behaviour of an information system (of systems) to then identify anomalous behaviours affecting it, using that or other tools in the future. Further, as datasets that must be understood and monitored are usually large, inherently multidimensional, and considerable part of human population is naturally better at reading visual than textual information, what visualization tools would be helpful, during sensemaking of such a dataset?

While visualizing complex systems' network structures on a flat computer screen is helpful, the lack of stereoscopical perception of these visualizations hindered the usefulness of such visualizations. Virtual Reality (VR) headsets were coincidently making comeback on consumer market and seemed to provide a possible platform for testing out stereoscopically perceivable multidimensional data visualizations rendered in VR. As there were no 3D VR (nor Mixed Reality, MR) visualization tools publicly available at that time, I identified this as an interesting research area with possible benefits to cybersecurity practitioners, while also creating helpful tools for my cybersecurity peers.

As the visualization possibilities are fundamentally different in stereoscopically perceivable environments, compared to textual or flat-screen visualization, there was a need for structured evaluation of visualizations that are created based on an analyst's internalized understanding of a dataset. Preliminary work also demonstrated that through purposeful interaction with Subject Matter Experts (SMEs) it is possible to identify the core concepts of their mental models for relevant datasets, and to create matching data-shapes for those.

To address that, I created Mental Model Mapping Method for Cybersecurity (M4C), that can be used to develop a 3D visualizations of network topology, to then overlay that with relevant data. The selection of attributes of data-shapes and their display layout aim to capture cybersecurity analysts' mental models, to enable the analysts to better understand their respective datasets. M4C 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.

Currently available Virtual and Mixed Reality (VR/MR) technology can provide users with interactive stereoscopically perceivable multidimensional data visualizations (ISPMDV) that can be used to better understand complex data structures and datasets. M4C demonstrates that through tight interaction with SMEs it is possible to identify core concepts in their mental models and transform these into data-shapes that these same SMEs can then use with VR/MR equipment for their tasks. Further research is needed to

find out, how generalizable are such data-shapes, compared over different types of networks, cyber operations, analyst past training and other individual differences. However, the benefits of harnessing human visual perception for CDSA/CDSU can provide a much-needed advantage to these SMEs.

Immersive visualizations of large and dynamic node-link diagrams require careful consideration for visual comprehensibility and computational performance. While many forms of node-link visualization idioms are well-studied in the form of 2D flat screen visualizations, the opportunities and constraints presented by VR and MR environments are distinct.

Optimizing VR/MR user interactions for VDE presented the design challenge of providing an interface that intuitively offers an informative presentation of the node-link network both at a high-level "overview" zoom level and at a close, zoomed-in "detail" view, with well-chosen levels of semantic zoom available along the continuum between these extremes. Constrained navigation further optimizes the user experience, limiting confusion and motion sickness. Dynamic highlighting, through the selection and controller-based movement of individual notes, enhances the users' understanding of the data.

User feedback to VDE has been very positive. A study that captured cybersecurity analysts' impressions of a network topology presented as an interactive stereoscopically perceivable multidimensional structure found, that overall, the impressions towards interactive stereoscopically perceivable multidimensional data visualizations (ISPMDV) were highly favourable. Multiple participants acknowledged that such 3D visualizations of network topology could assist in their understanding of the networks they use daily. Participants expressed a wish to integrate such visualization capabilities in their workflow. Prior experience with 3D displays had no influence on user preferences, while participants with prior gaming experience adjusted quickly to the Oculus Touch motion controllers, suggesting that the relevant dexterity and muscle memory for gaming console controller usage helps users adjusting from those controllers to handling input devices for VR experiences.

As the scientific and engineering community continues to adopt VR and MR for their work, it is likely that there will be an ongoing acceleration in the development of open-source VR/MR tools for this broad community. Some of the needs of specific technical communities will vary as a function of their data and problem spaces, requiring visualization of various forms of spatial (voxel, point cloud, mesh) and non-spatial data (such as the node link diagrams supported by VDE).

While SPMDVs for intrinsically (geo)spatial data have received substantial publicity, the creation, presentation, and usability research of SPMDVs and ISPMDVs designed to show non-spatial data has attracted less attention. I encourage cybersecurity professionals and researchers to use emerging technologies (e.g., VR/MR) to explore novel ways for visualizing datasets relevant to their problems and tasks.

I will be continuing my research, investigating 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 to oncoming team members. It is possible that this would speed up the onboarding of new team members by assisting them in learning the functional topology and the behaviour of entities that

are present in their datasets, for example, the logs from various devices in the protected computer networks.

Most importantly however, I'm curious to find out, how to quantify the level of improvement of how much more beneficial, more useful an ISPMDV would be for the users, with whom these visualizations are created, compared to contemporary alphanumeric and 2D visualization tools.

Lühikokkuvõte

Interaktiivsed, ruumiliselt tajutavad, mitmemõõtelised andmekuvad küberturbele

Võimalike turvaintsidentide aegsaks tuvastamiseks ja leidude mitigeerimiseks peavad keerukate süsteemide kaitsjad neid süsteeme järjepidevalt seirama: tuvastama anomaaliad, eristama valepositiivsed, delegeerima leiud pädevale kolleegile, kes intsidendi lahendamise eest hoolitseks. Ühe keeruka süsteemi kaitsmise eelduseks on selle kaitsjate hea arusaam sellest süsteemist, selle komponentidest, nende omavahelistest ja välistest seostest, komponentide ootuspärasest käitumisest, süsteemi kasutajate harjumustest jm – süsteemi mentaalne mudel. Mõistagi on seda probleemi, küberrünnete tuvastamist ja mitigeerimist püütud lahendada masinõppe abil, kuid aktiivsed ründajad on tavaliselt siiski inimesed, kes oma käitumist vastavalt sihtmärgile korrigeerivad: kui kaitsja on hästi-õppind masin, tuleb selle vastu kasutada ka sobivat taktikat. Seega isegi juhul, kui hästi-õppind masinad süsteemi seiramisel ja kaitsmisel abiks on, peavad turvaseirajad mõistma, miks too masin just nii aga mitte naa otsustas: kaitsjad peavad süsteemi tervikuna mõistma, omama süsteemile vastavat mentaalmudelit isegi juhul, kui õpetatud masinad seirel abiks on.

Oma doktoritöös keskendun inimesele: mis vahendid aitavad kaitsjail alul tundma õppida ning seejärel mõista kaitstavat süsteemi (ja selle alamsüsteeme), tundmaks ära anomaaliaid, vaenulikke või mitte? Andmehulgad, mida kaitsjad süsteemi turvaseireks hoomama peavad, on suured ja reeglina mitmemõõtelised: nende kuvamine lamedal ekraanil on võimalik, kuid teksti abil kuvatu mõistmine üsna kohmakas – visuaalse teabe hoomamine on inimestele loomulikum kui sama teabe tekstilisest või numbrilisest vormist dekodeerimine, lisaks on me visuaalne taju evolutsiooni käigus kohandunud ruumilisele keskkonnale, mitte lamedale meediumile, nagu paber või ekraan. Sellest lähtudes: millised andmete visualiseerimise vahendid aitaksid keerukate süsteemide kaitsjail tõhusamalt mõista andmehulki, mida peavad oma ülesannete täitmiseks jälgima?

Kuigi keerukate süsteemide topoloogia visualiseerimine kahemõõtmelise kujutisena lamedal ekraanil võib süsteemi mõistmisel kasuks tulla, on rohkema kui kolme mõõtme samaaegne visualiseerimine lamedal ekraanil kohmakas selle hoomamatu ruumilisuse tõttu: kuvatu ruumilisus pole paberilt ega lamedalt ekraanilt lihtsasti tajutav. Üks mu uurimistöö tõukureist oli virtuaalreaalsuse taas-tulemine eelmise kümnendi keskel: Oculus DK2 oli piisavalt võimekas proovimaks, kas stereoskoopiliselt tajutavate ruumiliste andmekujutiste abil oleks võimalik teavet masinalt inimesele edastada efektiivsemalt ja selgemalt kui muude tol hetkel olemas olnud vahendite abil. Kuna virtuaal- ega liitreaalsuses andmekuva võimekust pakkuvaid lahendusi tollal (avalikult saadaval) polnud, tuvastasin selle kui huvitava uurimisvaldkonnana, mille lahendamisest võiks kasu olla küberjulgeoleku praktikuile, mu (toonastele) kolleegidele.

Kuna stereoskoopiliselt tajutavate ruumiliste kujundite abil andmete visualiseerimise võimalused on lamedal ekraanil võimalikuga võrreldes täiesti erinevad, ei saanud ma lähtuda vaid olemasolevaist teadustöist: pidin alustama kaugemalt. Uurisin alustuseks, kuidas luua andmekuva, mis vastaks just selle kasutaja arusaamale andmestikust, mida ta mõista püüab: kuidas kaardistada see mentaalmudel, mida kasutaja mingi andmestiku (või süsteemi) mõistmiseks pruugib? Eeltöö käigus selgus ka, et andmestike kasutajaid eesmärgipäraselt intervjueerides on võimalik kaardistada nende mentaalmudelid ning

leitu põhjal luua mentaalmudeleile vastavad andmekujundid, mis andmestiku mõistmisele kaasa aitavad.

Lõin mentaalmudeli kaardistamise meetodi (M4C), mida saab kasutada näiteks kasutaja mentaalmudelile vastava, arvutivõrgu topoloogiat kujutava ruumilise andmekuva loomiseks, mille kaudu kasutaja andmestikuga intuitiivselt suhelda saab. Loodud andmekuvad peavad olema kasulikud intervjueeritule ja võivad olla kasulikud tema kolleegidele. Lisaks võivad sellised andmekuvad olla abiks meeskonna uutele liikmetele, kel andmestikule või süsteemile vastav mentaalmudel alles puudub – nemad saavad kuvatu põhjal luua oma mentaalmudeli, mis vanemate kolleegide mentaalmudelitega sarnane ning võimaldab süsteemi mõistmise paremat ühtlustamist meeskonna sees.

Kuigi M4C abil võib luua ka nö tavalisi, kahemõõtmelisi ja tekstilisi kuvasid, saab sellega disainida uudseid, ruumilisi andmekuvasid, mis võimaldavad kasutajal hoomata oluliselt rohkem teavet juhul, kui need kuvad on stereoskoopiliselt tajutavad. Õnneks on aastal 2023 saada olevad seadmed, mille abil virtuaal- ja liitreaalsust kasutada saab, juba piisavalt võimekad, et M4C abil loodud ruumilisi andmekuvasid kasutajasõbralikult pruukida. Kas sellise metoodika abil saab luua andmekuvasid ka teistsuguste kui arvutisüsteemidega seotud andmehulkade, andmestike, andmekogude mõistmiseks, on edasiste uurimistööde teema.

Ruumiliste andmekuvade vaatlemisest liitreaalsuses on kasu, kuid veel kasulikum on, kui kasutaja kuvatuga suhelda saab, näiteks pärides kuvatut katsudes või sellele lähenedes mõne leiu kohta lisateavet või muutes kuvatu aluseks olevat päringut. Näiteks saab kasutaja asukohast ja silmade fookusest sõltuvalt otsustada, kui detailset teavet parasjagu fookuses oleva objekti kohta kuvada, milliseid komponente näidata, millistele objektidele kuvada lisaks nimed või sildid, jmt. Omaette huvitav probleem on „merehaigus“ (*motion sickness*) virtuaalreaalsuses: selle vältimiseks peab kasutaja liikumisvabadust küll pisut piirama, kuid tulemuseks on kokkuvõttes oluliselt parem kasutajakogemus.

Uurimistöö hüpoteeside valideerimiseks kirjutasin tarkvara, Virtual Data Explorer (VDE), mis koondab endas aastate jooksul kogutud teadmuse. VDE võimaldab M4C abil loodud andmekuvasid esitada nii virtuaal- kui liitreaalsuses, keskkonnas kus kasutaja saab ruumilist andmekuva kogeda stereoskoopiliselt ning kuvatud teabega ka suhelda.

Kasutajate tagasiside VDE-le on olnud väga positiivne. Uuring, mis kogus küberturbe praktikute muljeid VDE abil kuvatud interaktiivsele, ruumiliselt tajutavale arvutivõrgu topoloogia andmekuvale tõdes, et üldiselt olid muljed *interactive stereoscopically perceivable multidimensional data visualizations* (ISPMDV) suhtes väga soodsad. Osalejad nentisid, et sellised võrgutopoloogia andmekuvad võivad aidata neil mõista neid süsteeme, mida nad igapäevaselt kasutatavad ja kaitsma peavad. Varasem kogemus liit-ega virtuaalreaalsusega ei mõjutanud kasutaja eelistusi, samas kui varasem kogemus arvutimängudega aitas osalejail kiiremini kohaneda kasutatud Oculus Touch sisendseadmetega. Uuring, kus osalenud paaride soorituste tulemuslikkust kahemõõtmeliste ja tekstiliste andmetega töötades võrdlesime paaridega, kes arvutivõrgu topoloogiat VDE abil hoomasid, tuvastas märkimisväärse eelise neil, kes kasutasid just ruumilist andmekuva.

Erinevate valdkondade vajadused sõltuvad nende andmete eripäradest: näiteks geograafiliste või juba loomupäraselt ruumiliste asjade (konstrueeritav lennuk, lahingusimulatsioon, atmosfäärinähtused, jm) kuvamiseks on kommertsiaalseid ja vabavaralisi vahendeid juba praegu ohtralt (visualiseerides asju vokselikogumikena,

punktipilvedena, jm) kuid loomupäraselt mitteruumiliste süsteemide ruumiliseks hoomamiseks loodud kujundite visualiseerimist võimaldavaid lahendusi (mis poleks vaid *force-directed* graafid) peale VDE ega mõne muu vahendi pole. Potentsiaali aga, nagu mu uurimistöö tulemusel selgub, on küll. Seetõttu julgustan küberturbe praktikuid ja teisi katsetama liit- ja virtuaalreaalsuse võimalusi, proovimaks uudseid meetodeid oma ülesannetega seotud süsteemide visualiseerimiseks.

Doktoritöö kaitsmise järel jätkan uuringutega: selgust vajab näiteks, kas kogenud ekspertide intervjuude põhjal koostatud andmekuvad on täpsemad, üksikasjalikumad ja andmestiku mõistmiseks sobivamad kui samade andmestike jaoks vähemkogenud spetsialistide poolt loodud andmekuvad. Teisalt on oluline mõista, kui tõhusad on ruumilised andmekuvad meeskonnaga liituvate liikmete koolitamisel: võimalik, et nende abil saab edastada süsteemide funktsionaalse topoloogia ja sellega seotud komponentide käitumist hõlmavaid mentaalmudeleid tõhusamalt kui seni pruugitavate, tavapäraste meetoditega. Aga ka, kuidas mõõta ruumiliste andmekuvade tõhusust ja võrrelda seda tavapäraste, lameekraanil või paberil esitatavate andmekuvade tõhususega: kui ISPMDV on tõhusam, siis millistes valdkondades, milliste ülesannete lahendamisel, kellele ja kui, siis kui palju tõhusam?

Appendix 1

Publication I

Kullman, K.; Cowley, J.; Ben-Asher, N. (2018). Enhancing Cyber Defense Situational Awareness Using 3D Visualizations. Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018: National Defense University, Washington DC, USA 8-9 March 2018. Ed. J. S. Hurley, J. Q. Chen. Academic Conferences and Publishing International Limited, 369−378.

Enhancing Cyber Defense Situational Awareness Using 3D Visualizations

Kaur Kullman[1, 2], Jennifer Cowley[1] and Noam Ben-Asher[1]
[1]Computational and Information Sciences, US Army Research Laboratory, Adelphi, USA
[2]Tallinn University of Technology, Tallinn, Estonia
kaur@ieee.org
jennifer.a.cowley.civ@mail.mil
noam@noamba.com

Abstract: The human visual system is generally more adept at inferring meaning from graphical objects and natural scene elements than reading alphanumeric characters. Graphical objects like charts and graphs in cybersecurity dashboards often lack the requisite numbers of features to depict behaviors of complex network data. For example, bar charts afford few features to encode a panoply of parameters in network data. Furthermore, dashboard visualizations seldom support the transition of human work from situation awareness building to requisite responses during intrusion detection events. This research effort aims to identify how graphical objects (also referred as data-shapes) depicted in Virtual Reality tools, developed in accordance with an analyst's mental model of an intrusion detection event, can enhance analyst's situation awareness. We demonstrate the proposed approach using Locked Shields 16 CDX network traffic. Implications of this study and future case study are discussed.

Keywords: visualization, decisionmaking, mental model, analysts, virtual reality, cybersecurity

1. Introduction

The quantity of information collected by network monitoring tools has increased steadily in parallel to the society's growing dependence on information technology (Kaisler, et al., 2014). The use of monitoring tools to maintain Cyber Defense Situational Awareness (CDSA) is a prominent task among cybersecurity analysts who work in a Security Operations Center (SOC) or Network Operations Center (NOC). One way to potentially mitigate the increasing workload of the cybersecurity analyst is to visualize the network architecture and types of data traversing through it. Typical dashboard charts and graphs (e.g., line charts, node diagrams, etc.) could overlay this architecture. However, visualizing data acquired from a wide range of sources on charts and graphs in isolation may stymie the rapid acquisition of information about changing network behaviors because: (i) graphs and charts have limited scalability for networks complexity and size, (ii) commonly user graphs/charts often fail to account for the highly dynamic nature of the cyber environment, and (iii) detection of threats demand the ability to notice and highlight small anomalies that tend to disappear when visualizing large volumes of data (Schoenwaelder, et al., 2007). What is needed is a set of new types of graphs and charts, called visualizations herein, which flex with the changing parameter space while pictorially representing of dynamic, evolving network behavior. The purpose is to expedite analyst's situation awareness by designing a visualization that reflects the analyst's mental model of the network environment.

Anecdotally, the common NOC/SOC analyst's workstation often includes command line tools juxtaposed to dashboard tools; some dashboards allow the user to interact (e.g., filter, drill, etc.) with the data depicted in the chart or graph. Dashboards usually provide an array of two-dimensional (2D) graphs and charts that summarize different types of network data. Network data has a high-parameter space and is often multidimensional, leaving the dashboard designer to fit multidimensional network data into 2D visualizations. If NOC/SOC analysts have multidimensional mental models network behaviors, then some conversions of 2D may occur. This conversion renders a measurable perceptual lag and often augments subjective mental workload. The goal of this study is to design a visualization aligned with analyst's mental model of the network environment, which facilitates a faster and more accurate detection of network behavioral change (Kandel, et al., 2012). Our approach is to utilize a virtual environment to create new 3D visualizations with the capacity to encode a panoply of data parameters into depth, spatial and temporal cues.

In this study, we describe the development of a 3-dimensional (3D) visualization technique for CDSA. First, we describe the technique and application architecture. Then, we demonstrate how it can be used by network operators to obtain and maintain CDSA using data from the Locked Shields 2016 cyber defense exercise as an

example. Finally, we discuss the integration of this visualization with a virtual reality, interactive environment as well as plans for future evaluation.

2. Human visual perception

The human visual system has a finite amount of visual attention resources used to view the data presented on a computer screen (Schneider, Dumais, & Shiffrin, 1982). Hence, the human visual system is one of the major bottlenecks of information flows between a computer system to a human analyst (refer the Communication–Human Information Processing (C–HIP) model for details (Dejoy, et al., 1999)). Because of this bottleneck, the veracity and comprehensiveness of a human analyst's mental model about a network event is directly impacted by perceptual bottlenecks. A *mental model* is internal, cognitive representation of the environment based on the acquired information. Then, these models can provide ways to describe, explain, predict, and, sometimes, control the phenomena (Gentner & Stevens, 1983); (Johnson-Laird, 1983) and they are built through direct perception of the environment. Hence, the design of data visualizations can impact the accuracy of an analyst's mental model development and sustainment (Paradice & Davis, 2008).

Coding information can be used to reduce the chances of perceptual bottlenecks. Visual information can be efficiently augmented in reasoning processes based (See (Paivio, 1991) for an overview on dual-coding and (Baddeley, 2012) for a review on working memory). Furthermore, information can be presented to the analyst in more than one sensory modality to maximize the amount of information perceived in a time epoch. In Human Computer Interaction research, codes are stimuli that represent the smallest unit of information communicated. For example, visual codes within a scatterplot are size, color, shape, proximity, among others. These visual codes are relevant to 2D visualizations but 'depth' may be an additional code in 3D environments that can be populated with additional data parameters and impact the interpretation of other codes like proximity. A group of codes representing a large amount of information can be configured to create a visual pattern, which can then be perceived rapidly. This visual pattern, according to Gestalt Psychology, is called *emergent features* (Treisman & Paterson, 1984) because the meta-data patterns emerge from the display of raw data. Meta-data patterns can form the basis of human mental models that analysts use when searching for expected patterns of malicious network behavior as well as represent normal network behavior. Gestalt laws of perception (e.g., Laws of Proximity, Closure) (Ehrenstein, et al., 2003) characterize the natural ways humans perceive information groupings that the interface designer can capitalize on. Poor designs that violate the Gestalt laws of perception could force the analyst into controlled and deliberated processing that consumes attention resources (Schneider, et al., 1982).

Depth perception is facilitated with a set of monocular and/or binocular visual cues that could provide additional codes to depict network information. Monocular depth cues (i.e., light and shading, relative size, interposition, blur, texture gradient, and aerial perspective linear perspective) (Lebreton, et al., 2012) allow for a 3D depiction in a 2D plane (i.e., a page or photograph). These kinds of "3D in 2D" visualizations using monocular cueing were called "perspective views" (Ellis, et al., 1987) or "pseudo 3D" (Lange, et al., 2006). Binocular depth cues use stereopsis to present objects to the viewer that seem to 'pop out' from the visual scene. Visualizations with binocular depth cues are called "real 3D" (Lange, et al., 2006). Visual perception of natural 3D scenes is afforded by monocular and binocular depth cues working together (Lee & Lee, 2015).

Perspective (Foyle, et al., 2005) is another 3D technique and design principle which can hamper perception in 3D visualization environments. Upon entering a 3D environment, the analyst is perceiving the environment through the avatar's eyes or perceiving via a top-down view looking at an avatar that represents themselves. The terminology describing perspectives is non-standard and sometimes obtuse. Human factors research defines *allocentric* views (Klatzky, et al., 1998), also called "through the window" (Brown, 1994) view, as one in which the observer is watching themselves through a viewpoint outside of the body. For example, an avatar representing a human has an allocentric view if the controller manipulates the avatar by watching it from behind. Allocentric is used interchangeably with *geocentric* or *exocentric* views (Klatzky, et al., 1998) or *plan* views (Foyle, et al., 2005). Plan views are allocentric perspectives in which the human is looking down from a higher altitude. Contrast this with *egocentric* views (Klatzky, et al., 1998), also called *immersive* (Brown, 1994) or *inside perspective* (Bryant & Tversky, 1999), such that the controller is seeing the virtual environment through the eyes of the avatar. The type of perspective used for a particular task has been shown to lead to human perceptual and spatial memory errors (Klatzky et al., 1998).

The advantages and disadvantages of depicting data using 3D compared to 2D displays has been studied and debated for decades with no clear resolution. With the rise of more sophisticated augmented reality environments, modern visualization research has re-vamped. The advancement of computing provides some explanations to the discrepancies between recent and dated studies of human performance with 3D visualizations (Smallman, et al., 2001). In some cases, 3D is advantageous because of a lower interpretive effort of perceived 3D information, given the human visualization system is designed to see in 3D (Dennehy, et al., 1994); (Smallman, et al., 2001). Furthermore, 3D visualizations potentially can display more codes with depth cueing compared to 2D displays. However, these benefits are couched in the type of work tasking required to complete with the visualization. Tasks such as altitude extraction, geo-spatial maneuvering, and navigation improve with 3D displays (Burnett & Barfield, 1991) while, there are tasks and environments for which the 2D displays are more advantageous than 3D displays (see (St. John, et al., 2001).

In sum, prior research indicates that while 3D visualizations in virtual reality environments afford more codes to use to depict data, the ways in which those codes are arranged using Gestalt's laws, emergent features and perspectives, determines how best to maximize the amount of data perceived. Communication from the interface to the human analysis involves the clear mapping between a mental model of the data that is expected to be reviewed, and the manner the data is depicted in the visualization (Ehrenstein, et al., 2003). The 3D objects we design must fit the typical mental model building inherent in network defense job tasking. To our knowledge, no prior research has identified whether computer network defense analysts are re-visualizing alphanumeric network data in geospatial patterns in their minds. Furthermore, we have no clarity whether training an analyst to build their mental models on 3D representations of alphanumeric network data will be advantageous to performance. These are assumptions we are exploring in our research. Although prior research has described basic Computer Network Defense (CND) operations and job tasking (D'Amico, et al., 2016) (D'Amico, et al., 2005), their findings are relatively generic to ascertain analyst mental models to build 3D visualizations from. Some preliminary research (Perl & Young, 2015) has attempted to document analyst's mental models, but the granularity of the models was too coarse to guide the development of 3D visualizations.

Based on discussions with subject matter experts, we hypothesize that akin to self-morphing graph structures often used to make sense of new datasets, the relations in data that cybersecurity analysts are after with their mental models to distill information, are more related to distinct data-shapes that arise while working with the datasets that analysts are using to solve the task at hand. While analyzing different datasets during incident response or other tasks. To verify this hypothesis a 3D environment and data-shapes was created, that and can be observed and manipulated by analysts using devices providing them stereoscopic view of those shapes.

3. Virtual data explorer

Initially, the OpenGraphiti (Reuille, et al., 2015) (http://www.opengraphiti.com/) platform was used to develop 3D visualizations, but due to lack of compatibility with motion controllers (i.e., input devices) Thus we used Unity 3D game engine to create a dedicated environment called Virtual Data Explorer (VDE, https://coda.ee/vde) which allow for motion controllers to interact as input devices for Oculus Touch controllers (Unity 3D, 2017) or the Microsoft Mixed Reality headset with their appropriate controllers (Microsoft, 2017). VDE is currently an academic prototype platform for building 3D data-shapes for data visualizations. The VDE affords 3D data visualizations by exporting rendered stereoscopic images to a Virtual, Augmented or Mixed Reality Head Mounted Display (HMD) to create an illusion for the user of immersion to virtual space, containing data-shapes consisting of the data that the user wishes to analyze. Technically a HMD is a set of screens; each screen rendering one of the pair of stereoscopic image per eye to provide vision for binocular depth cueing.

The type of data (network traffic, sessions and flows, but also application logs and process memory usage logs among others) we visualize can be static (logs, forensic evidence) or live-wire data. In the case of a live ingest, the characteristics of the data would be dynamic, however, our current prototype described herein is based off a static repository, as the added complexity of live ingest was not deemed necessary for initial testing of the usability of proposed 3D data-shapes. Note that VDE does not constrain the data-shape development to one type of environment; ingested data could be visualized as data-shapes in virtual-, mixed-, or augmented reality environments. The added benefit of using VR/AR is that 3D visualizations afford ample visual real estate to depict high-parameter (but originally non-spatial) data, allowing perception of numerous variables for each unit of observation. Each parameter can be encoded into visual codes like size, shape, color, and depth (Ware & Franck,

1996). For example, the perceived distance between observer and an object in the 3D virtual environment could represent a continuous value like total bandwidth usage, or number of bytes transmitted per unit of time.

Although using stereoscopic vision and motion cues to encode data have been found useful (Ware & Franck, 1996), it can be challenging to provide analysts with such technical capability that will make good use of humans' natural abilities. Unless analysts can immerse in and manipulate with the data-visualization environment intuitively, it may not be helpful in accomplishing their tasks; in addition, it is assumed that users must be able to use such environment without fatigue and simulator sickness (Kolasinski, 1995; Johnson, 2005), or as it's sometimes referred to – cybersickness.

Prior to current generation Graphics Processing Units (GPU), slow processing power created rendering lags that yielded visually mismatched orienting cues in the environment – this mismatch often led to user nausea. With the intensive development of the Interactive Entertainment Industry that has driven the market need, consumer grade GPU-s have become powerful enough to provide users with non-nauseating VR experiences, while being affordable enough to be used for our purposes. Recent GPUs with current generation HMDs significantly reduce the occurrence of visual lag, therefore reducing the chances of users' nausea.

There are also other factors that could cause unpleasant user experiences in VR. To minimize these effects, we've implemented a few methods in our environment to avoid such experiences. For example, while the user navigates the 3D space in avatar-less first-person perspective, we restrict the range of head movement during motion such that the user can only move in a linear direction towards the point of gaze, or away from it, sometimes referred to as "rudder head movement" (Unity 3D, 2017). The user of course has freedom to observe 360 degrees of the visual field (Kemeny, et al., 2017), only her movements are restricted to back-and-forth directions.

This approach allows us to immerse the user rather conveniently into the VDE environment, where she can, with hand and head gestures, roam around in 3D space to view the 3D data-shapes' visualizations from multiple vantage points, grab and interact with the visualization, experience, manipulate, and explore the data presentations that are dynamically created and adjusted to build situation awareness (in case of NOC/SOC analysts). Akin to self-morphing graphs (as implemented for example in OpenGraphiti (Reuille, et al., 2015)), VDE allows us to examine whether presenting data in 3D data-shapes and enabling interaction with its components could help analysts detect changes in network traffic (this method could also be extended to application logs and process' memory usage, for example). Furthermore, VDE allows us to evaluate whether deliberately structured visual data-shapes that are observed with stereoscopic HMD could enhance CDSA.

For the purposes of this study, we define:

- Dataset – values (e.g. IP addresses, their relations, connections, sessions etc.) collected from sensors, log files and network traffic monitors
- Data-object – one instance from dataset, that may be a key-value pair, set of values related to an event that caused a log-line or alert to be logged
- Data-shape – a specific form of data visualization, where pixels (that in collections represent nodes, connections etc.) are arranged so, that in the resulting visual data representation of the data-objects, visual objects are positioned according to their logical topology so, that the resulting 3D structure would relate to a specific task for which the NOC/SOC analyst is responsible for, and would be using that data-shape for (e.g. relate to hers mental model of the problem/hypothesis/situation)
- VDE scene – combined set of data-shapes, a meta-shape, that consists of spatially positioned data-shapes, that in combination enable to user to view relations between different data-shapes' nodes.

3.1 Data preparation

The ingested network traffic data used to demonstrate the 3D visualization was not live-wire data but a collection of data from the 2016 Locked Shields Cyber Defense Exercise (LS16) (NATO CCDCOE, 2016) (see https://ccdcoe.org/locked-shields-2016.html). This is an international cyber defense exercises with more than 550 participants from 26 nations. Participants were assigned roles in various teams, while most of them were

arranged into 20 defensive teams (Blue Teams) and one adversarial team (Red Team). In this exercise, the Blue Teams' goal was to maintain the availability and security of their networks during two days of the exercise.

Locked Shields' dataset was selected as it is relatively well documented, reasonably large (~20TB of PCAP files), has ground truth (what and when did Red Team members do) and there are 20 comparable networks that start out as identical but change as respective Blue Teams adjust them. IPv6 visualization was chosen for first VDE data-shape, as Blue Teams' ability to monitor and secure their IPv6 addresses was a relevant topic during this exercise.

A valuable advantage of LS16 dataset to researchers is the availability of knowledge about the network topology (of the Blue Teams' assets) and ground truth of Red Team actions – e.g., what and when did the Red Team members do during their attacks, and also the Blue Teams responses to adversarial activities (at least to some degree).

To prepare that dataset (IPv6 network traffic information) for 3D visualization, the packets captured (into PCAP files) during LS16 exercise were parsed with Bro IDS (https://www.bro.org) to get textual log files describing network connections between nodes (servers, workstations, network devices in Blue Teams' networks, and elsewhere in the "game network") that were observed in captured traffic. Textual log files were then queried with SpectX (SpectX, 2017) (https://www.spectx.com) to count the connections between devices to describe relations of nodes by coloring the edges (connections) between nodes according to the number of times those nodes were observed communicating – from transparent green to opaque green to red.

Based thet data, VDE would then generate a virtual environment, with LS16 data visualization in it. For our first concept design we chose to visualize a network topology where the nodes (white spheres) represent devices like computer desktops, servers, switches or routers, and the edges (lines connecting spheres) represent the network traffic between those devices. VDE positions nodes according to their logical topology in their respective networks, visualized as data-shapes that are generated per every Blue Team. Such environment enables the user to immersively explore the data-shapes, its components using VR equipment. An example of a user exploring VDE environment composed of data-shapes visualizing LS16 Blue Teams' networks can be seen in a brief video released with this article (https://coda.ee/iccws).

3.2 Data-Shapes for visualizing logical topology of networked entities

When the user first enters the VDE, the viewer can look down at a ~30 degree angle at the scene that is positioned at such a distance, as to fit in the view. The floor of the VDE environment (in VR) is a dark patterned desert that continues until it meets a horizon line that delineates floor and skyline. The background environment is chosen such, that it would be unobtrusive to the viewer's task, while providing horizon for spatial orientation. Visualized data-shapes are floating well above the floor and a little below the horizon line, to ease its components' visibility (brighter objects against darker background).

Contrary to self-organizing graphs which are useful for initial examination of unknown datasets, our goal is to provide analysts with (the ability to create) data-shapes that would help them better comprehend datasets that are depicted as structures they can learn to know well over time. We propose creating data-shapes where networked entities (e.g. computers) are positioned according to their logical topology (e.g. computer or server groups and not only physical or functional topology) so, that the resulting 3D structure(s) would relate to a SOC/NOC analyst's task, which in this LS16 example would be to detect prohibited connections between Blue Team's network devices. Data-shapes as such are nothing new (Hurter, 2016), but few have tried to use stereoscopically perceivable 3D data-shapes for computer security (Payer & Trossbach, 2015).

One could consider following as prerequisite knowledge to the creation of the LS16 VDE scene, containing set of proposed data-shapes:

- Understand the principles of how does a computer network function; specifically, how such network is set up for Locked Shields exercise;
- Understand of the logical grouping of networked entities and their topology during Locked Shields; also understand networks (virtual entities) and this game's stakeholders' (physical entities) goals, e.g. Red vs Blue, but also Green, Yellow, White teams' functions;

- Understanding the expected behavior of the above actors and how it should reflect on network data
- Search for indicators, validate, visualize and act.

To create data-shapes for other datasets, a different set of knowledge is required, but can be acquired by mapping the mental models of the analysts who will be using these data-shapes.

To test the usefulness of using 3D data-shapes when encoding non-spatial data, networked entities were spatially positioned, considering their position in network topology, and more importantly, entities' affiliation to logical groups (by functionality (e.g. SCADA components), purpose (e.g. DMZ servers), risk exposure, OS etc.). This results in custom 3D data-shapes, that could be combined to a meta-shape (a VDE scene) representing larger whole of the LS network(s) that are of interest in our scenario. A meta-shape, VDE scene depicted in Figure 2 is the overall view of the percept the LS16 network traffic visualization makes from a distance.

As we have three axises available to encode data (we are not using time in this visualization scenario), we chose to use two of those to encode parts of network topology (subnet number (third octet in case of LS16) and entity's IP addresses' last octet or position in its subgroup) while the third axis binds to the functional or logical group of that entity. Using the common X, Y, Z referencing: within a data shape shown in Figure 1, the Y axis is the group number, the X axis is the subnet number (the team number) and the Z axis has no relevant values other than the IP addresses within a particular range cluster together (i.e., the IP addresses' last octet or position in its subgroup) along the Z-axis. A group number is assigned to a type of 6 functions the nodes or network devices perform. These groups are:

- 1. DMZ servers for email, WWW, DNS, NTP, and others
- 2. Office network with Domain Controller and workstations
- 3. Lab network for research and development
- 4. Control network for drone operators
- 5. Secure devices
- 6. Incident Command System (ICS) systems as the high level objective of the Red Team attacks

Groups contain nodes in their respective subnets, grouped vertically according to their logical positions in their functional groups (subnets). For example, Windows, Linux, OSX workstations are positioned onto separate layers to distinguish them visually in subnets 2 and 3, while Windows, Linux and other servers, networks devices, etc. are kept on the lowest group to distinguish intra-group traffic from inter-group traffic.

For example, to find suspicious connections inside a LS16 Blue Team's network, entities were first positioned according to their subnet and then by their functional groups—servers, network devices, workstations (distinguished further by their type (Windows, Linux, OSX)), and SCADA components among others (see Figure 1). The third dimension is entity's sequential position inside of its subgroup (often the last octet of its IP address). Because the designated functions (and therefore behavior) of the entities in same functional group should be similar, it is beneficial for the analyst to have them close together, while still being spatially distinguishable to quickly diagnose which group and which member to focus on.

At the start of the exercise, there were 20 functionally identical Blue Teams' networks, whose entities should have been communicating identically, but as the exercise advanced, the Blue Teams' networks' behavior (in this case, entities' activity and relative connections / edges) deteriorated from each other's. Each Blue Team's network had 68 preconfigured nodes, and the teams could add two virtual machines per their specifications.

Entities that fell outside of the known functional groups were positioned to three cube-shaped matrixes: i) entities with public IP addresses (simulated in-game internet); ii) entities that had IP addresses in Blue Teams' internal address ranges, but which were not preconfigured prior to game; and iii) entities that had IP addresses in Blue Teams' internal address ranges, were not preconfigured before the game, and did not follow the Locked Shields' addressing logic (for example, those that had letters in IPv6 address). Before positioning entities to those groups, these were sorted by their IP address.

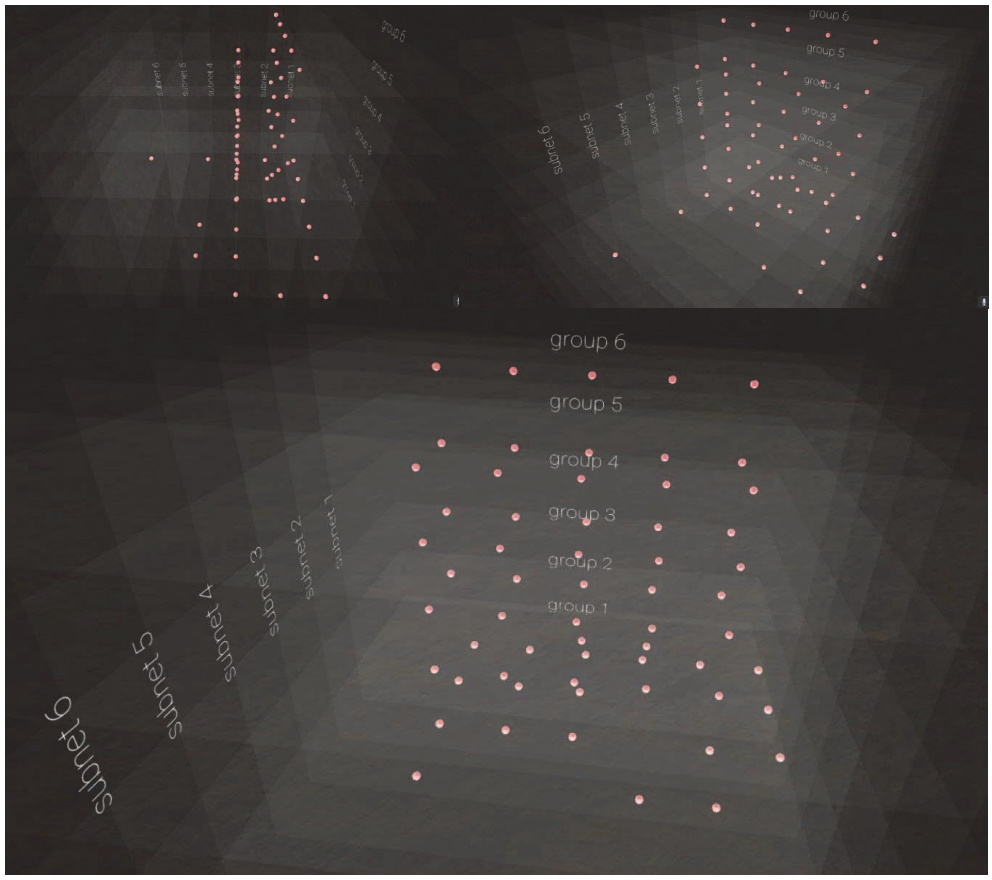


Figure 1: Viewing same data-shape from three different angles

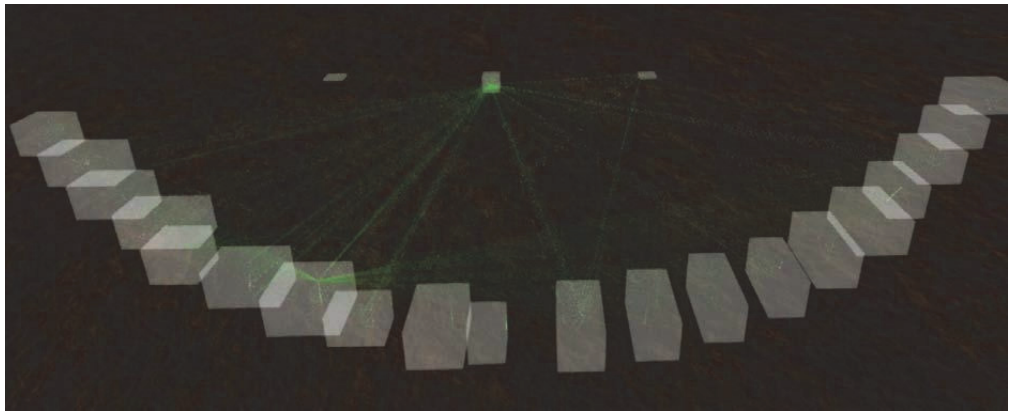


Figure 2: The analyst's initial view of the meta-shape of the Locked Shield dataset in the VDE

Teams' networks curved around three shapes containing external and/or potentially interesting hosts. All data-shapes contain the Blue Teams' systems with the same (or similar) layout as seen in Figure 1. From this broad view, an analyst who knows the logical positioning and internal functions of the Blue Team's networks' groups, subgroups and nodes may find anomalies to investigate further, which in this visualization scenario are connections (green edges) between different Blue Teams' systems. For example, the connections (green edges) originating from a host in the 7th team's network (7th data-shape from left) to other Blue Teams' systems should

not be happening. In addition, connections from the 11th team's network (11th cube from left) to hosts that were named unconventionally (so that they appear to be in the 11th team's IPv6 address range) should be examined by taking a closer look at the visualization (selecting specific host that seems to be trying to blend in and exploring it's relations) or continuing exploration in textual logs. For a better understanding of this process, please see the videos (https://coda.ee/iccws).

Data-shapes were then spatially positioned to a meta-shape (as shown in Figure 2) to allow the user to take advantage of stereoscopic viewing and the sense of binocular depth that it provides. Several layouts were considered to minimize possible edge clutter and enable convenient distinguishability of intra- and extra-network connections.

Edges connecting the nodes were then added to the data-shapes, as prepared using the process described in subsection 3.1. From the initial vantage point user can distinguish edges that connect one Blue Teams' node(s) to those of other Blue Teams' internal nodes (mostly horizontal edges as opposed to vertical ones); on the other hand the edges connecting Blue Teams' internal nodes with entities in either of the three matrixes have different implications. Would an NOC/SOC operator have to evaluate a network from this view, she would want to see only i) Blue Team's first subnet (e.g. DMZ) nodes connecting to legitimate services located in "game internet" and ii) Blue Team's internal hosts communicating only to that same Blue Team's hosts. All other edges might need further examination.

3.3 Detecting abnormalities in traffic

In Figure 2, the vertical and diagonal lines that connect one node with multiple nodes in other Blue Teams' networks indicate a possible abnormality that should be investigated. Is it possible that the highlighted behaviors represent a compromised node in the Blue Team's network, which is used by a Red Team member to scan other Blue Teams' systems to find those that have not been correctly firewalled? Is it possible that some devices or tasks (e.g., network scans) were misconfigured, e.g., SYN packets were found in the traffic but not ACK or RST, meaning that the host did scan but could not connect to those hosts?

One could argue that this kind of anomalous behavior would be blocked by the network devices' ACL rules, a myriad of "cybersecurity appliances" endorsed by cyber-insurance providers, or at least detected by conventional "cyber-devices" (e.g., IDS/IPS and firewalls). We argue, that while systems that help NOC/SOC personnel to protect their networks are a necessity, our adversaries will always find functionalities (weaknesses) in those systems that enable them to bypass those protections. Therefore NOC/SOC analysts will need to be able to creatively approach their datasets to find their adversaries attacks in novel ways, and we need to provide analysts with appropriate tools for those tasks. One such tool could be a system (ex. VDE) that would provide analysts' with environment where, using the same, similar, or improved structured data views to visualize familiar but dynamic datasets, the analyst could have different views of relevant datasets to find anomalies, which could be missed otherwise, would they rely on 2D and textual tools only.

4. Discussion and conclusion

This paper describes the theory and methodology used to develop a 3D visualization of network data. The selection of attributes, data-shapes and display aims to capture cybersecurity analysts' mental models enable the analysts to better understand their respective datasets. Following the development of the visualization, we are planning to conduct controlled validation study with experienced cybersecurity analysts and vulnerability analysts. We will be using a mixed method that begins with a set of qualitative task analyses while the participant is using the new visualization tool moving to quantitative behavioral studies. Our dependent measures are situation awareness content and accuracy, speed of SA acquisition, mental model accuracy.

We argue that there is a need for structured evaluation of visualizations that are comparable with the analyst's mental model. Current technology is capable of delivering the basic 3D visualization needs and this preliminary work demonstrates that through tight interaction with SMEs it is possible to identify core concepts in their mental models and transform them into Data-shapes. Further research is needed on how general are the Data-shapes over different types of networks, cyber operations, analyst past training and other individual differences. However, the benefits of harnessing human superior visual-perception to cyber detection can provide a much needed advantage to cyber defenders.

Acknowledgements

For all the hints, ideas and mentoring, authors thank Alexander Kott, Jaan Priisalu, Olaf Manuel Maennel and Lee Trossbach. This research was partly supported by the Army Research Laboratory under Cooperative Agreement Number W911NF-13-2-0045 (ARL Cyber Security CRA) and under Cooperative Agreement Number W911NF-16-2-0113 and 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.

References

Baddeley, A., 2012. Working Memory: Theories, Models, and Controversies. *Annual Review of Psychology,* Volume 63, pp. 1-29.

Brown, M. A., 1994. *Displays for Air Traffic Control: 2D, 3D and VR - A Preliminary Investigation,* London: Queen Mary & Westfield College.

Bryant, D. J. & Tversky, B., 1999. Mental Representations of Perspective and Spatial Relations from Diagrams and Models. *Journal of Experimental Psychology Learning Memory and Cognition,* 25(1), pp. 137-156.

Burnett, M. S. & Barfield, W., 1991. *Perspective versus plan view air traffic control (ATC) displays - Survey and empirical results.* Columbus, s.n.

D'Amico, A., Buchanan, L., Kirkpatrick, D. & Walczak, P., 2016. Cyber Operator Perspectives on Security Visualization. In: *Advances in Human Factors in Cybersecurity.* s.l.:Springer, pp. 69-81.

D'Amico, A. et al., 2005. *Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts.* s.l., s.n.

Dejoy, D. M., Laughery, K. R. & Wogalter, M. S., 1999. Organizing theoretical framework: a consolidated communication-human information processing (C-HIP) model. Warnings and risk communication. In: s.l.:s.n., pp. 15-23.

Dennehy, M. T., Nesbitt, D. W. & Sumey, R. A., 1994. Real-Time Three-Dimensional Graphics Display for Antiair Warfare Command and Control. *Johns Hopkins APL Technical Digest,* 15(2), pp. 110-119.

Ehrenstein, W. H., Spillmann, L. & Sarris, V., 2003. Gestalt Issues in Modern Neuroscience. In: *Axiomathes.* s.l.:Springer, pp. 433-458.

Ellis, S. R., Mcgreevy, M. W. & Hitchcock, R. J., 1987. Perspective traffic display format and airline pilot traffic avoidance. *Human Factors,* Volume 29, pp. 371-382.

Feltovich, P. J., Prietula, M. J. & Ericsson, K. A., 2006. Studies of expertise from psychological perspectives. In: *The Cambridge handbook of expertise and expert performance.* Cambridge: Cambridge University Press, pp. 41-67.

Foyle, D. C., Andre, A. D. & Hooey, B. L., 2005. *Situation Awareness in an Augmented Reality Cockpit: Design, Viewpoints and Cognitive Glue.* Las Vegas, Proceedings of the 11th International Conference on Human Computer Interaction.

Gentner, D. & Stevens, A., 1983. *Mental Models (Cognitive Science Series).* s.l.:Lawrence Erlbaum Associates.

Hurter, C., 2016. *Image-Based Visualization: Interactive Multidimensional Data Exploration.* s.l.:Morgan & Claypool.

Johnson, D. M., 2005. *Introduction to and Review of Simulator Sickness Research,* Arlington: U.S. Army Research Institute for the Behavioral and Social Sciences.

Johnson-Laird, P. N., 1983. *Mental Models.* s.l.:Cambridge University Press.

Kaisler, S., Armour, F., Espinosa, A. J. & Money, W., 2014. *Big Data: Issues and Challenges Moving Forward.* Wailea, s.n.

Kandel, S., Paepcke, A., Hellerstein, J. M. & Heer, J., 2012. Enterprise data analysis and visualization: An interview stud. *IEEE Transactions on Visualization and Computer Graphics,* 18(12), pp. 2917-2926.

Kemeny, A., George, P. & Mérienne, F., 2017. New VR Navigation Techniques to Reduce Cybersickness. *Electronic Imaging, The Engineering Reality of Virtual Reality,* pp. 48-53.

Klatzky, R. L. et al., 1998. *Spatial Updating of Self-Position and Orientation during Real, Imagined, and Virtual Locomotion,* s.l.: Sage Publications, Inc..

Kolasinski, E. M., 1995. *Simulator Sickness in Virtual Environments,* Alexandria: United States Army Research Institute.

Lange, M., Dang, T. & Cooper, M., 2006. *Interactive resolution of conflicts in a 3d stereoscopic environment for air traffic control.* Ho Chi Minh City, Vietnam, Vietnam, s.n.

Lebreton, P., Raake, A., Barkowsky, M. & Le Callet, P., 2012. Evaluating Depth Perception of 3D Stereoscopic Videos. *IEEE Journal of Selected Topics in Signal Processing,* 6(6).

Lee, K. & Lee, S., 2015. 3D Perception Based Quality Pooling: Stereopsis, Binocular Rivalry, and Binocular Suppression. *IEEE Journal of Selected Topics in Signal Processing ,* 9(3), pp. 533-545.

Microsoft, 2017. *Windows Dev Center, Motion controllers.* [Online] Available at: https://developer.microsoft.com/en-us/windows/mixed-reality/motion_controllers

NATO CCDCOE, 2016. *Locked Shields 2016.* [Online] Available at: https://ccdcoe.org/locked-shields-2016.html

Paivio, A., 1991. Dual Coding Theory: Retrospect And Current Status. *Canadian Journal of Psychology/Revue canadienne de psychologie,* 45(3), pp. 255-287.

Paradice, D. & Davis, R. A., 2008. *DSS and Multiple Perspectives of Complex Problems.* s.l.:s.n.

Payer, G. & Trossbach, L., 2015. The Application of Virtual Reality for Cyber Information Visualization and Investigation. In: *Evolution of Cyber Technologies and Operations to 2035.* s.l.:Springer, Cham, pp. 71-90.

Perl, S. J. & Young, R. O., 2015. *A Cognitive Study of Incident Handling Expertise.* Berlin, 27th Annual FIRST Conference.

Reda, K. et al., 2013. Visualizing large, heterogeneous data in hybrid-reality environments. *IEEE Computer Graphics and Applications,* 33(4), pp. 38-48.

Reuille, T. et al., 2015. *OpenDNS Data Visualization Framework.* [Online] Available at: http://www.opengraphiti.com/

Schneider, W., Dumais, S. T. & Shiffrin, R. N., 1982. *Automatic and Control Processing and Attention,* Illinois: University of Illinois.

Schoenwaelder, P. J. et al., 2007. Key research challenges in network management. *IEEE Communications Magazine,* 45(10), p. 104–110.

Smallman, H. S., St. John, M., Oonk, H. M. & Cowen, M. B., 2001. Information availability in 2D and 3D displays. *IEEE Computer Graphics and Applications,* 21(5), pp. 51-57.

SpectX, 2017. *Inertia in Processing Machine Generated Data.* [Online] Available at: https://www.spectx.com/articles/processing-machine-generated-data

St. John, M., Cowen, M. B., Smallman, H. S. & Oonk, H. M., 2001. The Use of 2D and 3D Displays for Shape-Understanding versus Relative-Position Tasks. *Human Factors,* Volume Spring, pp. 79-98.

The Bro Project, n.d. [Online] Available at: https://www.bro.org/

Treisman, A. & Paterson, R., 1984. Emergent features, attention, and object perception. *Journal of Experimental Psychology: Human Perception and Performance,* 10(1)(12).

Unity 3D, 2017. *Unity 3D Manual, Input for Oculus, Oculus Touch Controllers.* [Online] Available at: https://docs.unity3d.com/Manual/OculusControllers.html

Unity 3D, 2017. *Vision 2017 - Lessons from Oculus: Overcoming VR Roadblocks.* [Online] Available at: https://youtu.be/swA8cm8r4iw?t=9m42s

Ware, C. & Franck, G., 1996. Evaluating stereo and motion cues for visualizing information nets in three dimensions. *ACM Transactions on Graphics,* March.15(2).

Wickens, C. D. & Hollands, J. G., 2000. *Engineering psychology and human performance.* Upper Saddle River: Prentice Hall.

Young, I., 2008. *Mental Models: Aligning Design Strategy with Human Behavior.* s.l.:Rosenfeld Media.

Appendix 2

Publication II

Kullman, Kaur; Asher, Noam Ben; Sample, Char (2019). Operator Impressions of 3D Visualizations for Cybersecurity Analysts. Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019: University of Coimbra, Portugal, 4-5 July 2019. Ed. Cruz, Tiago; Simoe, Paulo. Reading, UK: ACPI, 257−266.

Operator Impressions of 3D Visualizations for Cybersecurity Analysts

Kaur Kullman[1], Noam Ben Asher[2] and Char Sample[3]
[1]TalTech University, Tallinn, Estonia
[2]ORAU, Oak Ridge TN, USA
[3]ICF Inc. Columbia, USA
kaur@ieee.org

Abstract: Cybersecurity analysts ingest and process significant amounts of data from diverse sources in order to acquire network situation awareness. Visualizations can enhance the efficiency of analysts' workflow by providing contextual information, various sets of cybersecurity related data, information regarding alerts, among others. However, textual displays and 2D visualizations have limited capabilities in displaying complex, dynamic and multidimensional information. There have been many attempts to visualize data in 3D, while being displayed on 2D displays, but success has been limited. We propose that customized, stereoscopically perceivable 3D visualizations aligned with analysts' internal representations of network topology, may enhance their capability to understand their networks' state in ways that 2D displays cannot afford. These 3D visualizations may also provide a path for users who are trained and comfortable with textual and 2D representations of data to assess visualization methods that may be suitably aligned to implicit knowledge of their networks. Thus, the premise of custom data-visualizations forms the foundation for this study. Herein, we report on findings from a comparative, qualitative, within-subjects usability analysis between 2D and 3D representations of the same network traffic dataset. Study participants (analysts) provided information on: 1.) ability to create an initial understanding of the network, 2.) ease of finding task-relevant information in the representation, and 3.) overall usability. Results indicated that interviewees indicated a preference for 3D visualizations over the 2D alternatives and we discuss possible explanations for this preference.

Keywords: visualization, cybersecurity, decision-making, data visualization, virtual reality

1. Introduction

Cyber is the newest domain of war (Lynn, 2010), endowed with unique sensory characteristics that differentiate this warfare environment from kinetic-physical warfare (Gonzalez, Ben-Asher, Oltramari, & Lebiere, 2014). Cyber security analysts who are responsible for ensuring the security of networks and other assets, utilize a wide array of computer network defense (CND) tools, such as Security Information & Event Management (SIEM) that allow data from various sources to be processed and alerted on. CND tools allow analysts to monitor, detect, investigate and report incidents that occur in the network, as well as provide an overview of the network state. To provide analysts with such capabilities, CND tools depend on the ability to query, process, summarize and display large quantities of diverse data which have fast and unexpected dynamics (Ben-Asher & Gonzalez, 2015). Shneiderman (Shneiderman, 1996) provided a taxonomy depicting 7 human-data interaction task levels: 1.) gaining *Overview* of the entire dataset, 2.) *Zoom* on an item or subsets of items, 3.) *Filter* non relevant items, 4.) get *Details-on-Demand* for an item or subset of items, 5.) *Relate* between items or subset of items, 6.) keep *History* of actions and 7.) allow *Extraction* of subsets of items and query parameters. Traditionally, cyber defenders have used command line tools and alphanumeric data displays to execute these seven tasks. With the need for faster and more accurate situational awareness of increasing data volume, many CND products have integrated graphical user interface (GUI) and 2-dimensional (2D) data visualizations to expedite human information acquisition.

Visualizing multidimensional data on 2D screens bears several limitations. First, the resulting visualization after the dimensionality reduction methods have been applied will likely differ from the mental representation that the analyst had acquired upon reviewing the same data in numerical and textual data. Contextual information will likely be removed in the reduction process that could be crucial to the understanding of the situation and to identify relevant clues (Rajivan, Konstantinidis, Ben-Asher, & Gonzalez, 2016). Also, three dimensional visualizations may address some of the inherent limitations of 2D displays by aligning with the analysts' internal representation of their datasets, if the analyst naturally thinks about data in three dimensions. Users' interactions in VR (Virtual Reality) and XR (Mixed Reality) may also be more intuitive if users are expected to interact with the visualization in ways that humans manipulate objects in the physical world. This way we could harness the dexterity of human hand movement for interactions (Gershon, Klatzky, & Lee, 2014) if the tools used are capable enough, using haptic feedback to further advance users interaction efficiency (Gershon, Klatzky, Palani, & Giudice, 2016).

However, the scale, heterogeneity, and complexity of cybersecurity datasets continue to pose challenges for visualization and interaction designers (Reda, et al., 2013) despite the constant increase in computers' abilities to process and display more data on 2D displays. This could be because visualization designers lack an understanding of cybersecurity operations and network infrastructure to create an effective visualization for cybersecurity analysts. Yet, cybersecurity analysts who are familiar with the technical aspect of network monitoring do not have expertise in data visualization and human perception. The visualization designer might need to have dual expertise.

By providing a data visualization environment where minimalistic visual, audio and haptic cues are informing the user of what is happening in that environment, we allow the user to focus on the task. Furthermore environmental cues should be perceptible and clear to avoid user confusion. Visualization should be functional and available utilities should accurately convey their functions. Controls, navigation, interface, and all other interface conventions should be consistent. Users cognitive and physical workload must be minimized. Human errors should be anticipated and prevented if possible. The environment should be flexible to allow customization for personal preferences, cultural differences, color vision deficiency etc. (Hodent, 2018). We hypothesize that the analyst may find it intuitive to use a 3D representation of cybersecurity network data that is aligned with the above guidelines as well as the analyst's internalized understanding of the data. Intuitive interfaces may enable the analysts to explore and understand their environment more efficiently.

2. Visualization for cyber defense

Cybersecurity visualizations provide analysts with visual representation of alphanumeric data that would otherwise be difficult to comprehend due to its large volume. Such visualizations aim to effectively support analyst's tasks including detecting, monitoring and mitigating cyber attacks in a timely and efficient manner (Sethi & Wills, 2017). Cybersecurity specific visualizations can be broadly classified into three main categories: 1.) network analysis, 2.) malware and 3.) threat analysis, and situational awareness (Sethi & Wills, 2017). 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 (Marty, 2008) as well as universal software with visualization capabilities like Tableau, MS Excel, R, Python, and D3 libraries (d3.js) among others. These tools could be used to visualize data in myriad of ways (Munzner, 2014) so that analysts could explore their datasets visually and interactively (Ward, Grinstein, & Keim, 2015). *Graphistry* is one recent example of a 2D force-directed graph visualization (Meyerovich & Tomasello, 2016) whose interface is easy to manage and visualization and is responsive to queries on massive datasets. These are crucial qualities for cybersecurity analysts, with emphasis on the importance of the low-latency between analyst's request for a change in visualization (change in filter, time window or other query parameters) and rendering of the visualized response from the system (Wu, Xu, Chang, Hellerstein, & Wu, 2018).

The usability of data visualizations for CND operations that have not been evaluated, may lead to low adoption rates by practitioners (Best, Endert, & Kidwell, 2014). The challenge in creating useful visualization for cybersecurity practitioners is in aligning data visualization experts' knowledge with cybersecurity analysts' needs and knowledge so, that the resulting visualizations would be useful for work tasking. A recent survey showed that 46% of 130 tools did not have any user-involvement in the evaluation phase (Sethi & Wills, 2017).

To achieve higher visualization adoption rates, analysts should have the ability to intuitively and iteratively adjust the visualizations to suit with their changing needs (Kirk, 2016). Datasets used in cybersecurity operations are often multi-dimensional and analysts would either have to scale down the number of dimensions viewed at one time to be able to use 2D & 3D visualizations, or combine multiple 2D visualizations displaying different dimensions of the same dataset in a single dashboard. This requires the designer to properly encode variables (dimensions) into shapes, colors, sizes among others. The viewer has to translate that shape into spatial perception and compare it to her internal understanding of the data, to decode the meaning of the visualizations; a task that may be non-trivial (Ehrenstein, Spillmann, & Sarris, 2003). There have been numerous attempts to employ 3D visualizations for cybersecurity data that are displayed on 2D computer screens with varying degrees of success. Such visualizations sometimes use monocular depth cues (Lebreton, Raake, Barkowsky, & Le Callet, 2012) and object movement to convey the 3D shape of the visualization; advantages and disadvantages of which were thoroughly discussed in our previous paper (Kullman, Cowley, & Ben-Asher, 2018). VIDS (Shearer & Edwards, 2018) provides an interactive 3D environment for visualizing network and alert (or other) data in 3D shapes, whereby users can seamlessly switch styles and layouts to dynamically shape their data and easily adjust their viewpoint (Gaw, 2014). Real-time 3D visualization engine DAEDALUS-VIZ allows

operators to grasp visually and in real-time an overview of alert circumstances, while providing highly flexible and tangible interactivity (Inoue, Suzuki, Suzuki, Eto, & Nakao, 2012). InetVis (van Riel & Irwin, 2006) allows the user to allocate source and destination IPv4 addresses to X and Z axis, while destination ports are being allocated to the Y axis on a 3D cube. To understand the shape of the cube and detect the positions on Z axis, user must manually change the viewpoint with mouse. Shoki (Berry, n.d.) allows the user to define what values are plotted on which axis, while the screen is divided to four squares, three of them showing each axis in 2D, while the fourth square displays the cube as a 3D object.

Due to the emergence of commodity VR devices, multiple data visualization tools have implemented support for VR headsets, that are capable of 6 degrees of freedom (6DOF) movement of the user's viewpoint, allowing the observer to perceive the depth of the visualization stereoscopically, avoiding the mental work needed to convert 2D images to 3D. OpenGraphiti (Reuille, Hawthorne, Hay, Matsusaki, & Ye, 2015) enables provides customizable graphs, along with querying and filtering capabilities. However, OpenGraphiti does not provide 3D VR interaction capacities. However, V-Arc (Maddix, 2015) enables the positioning of data in a predetermined layout, data selection and color-coding amongst other capabilities. Virtual Data Explorer (VDE) is a VR tool that allows users to collaborate while investigating 3D data visualizations, to find anomalies in a variety of cybersecurity-related datasets (U.S. ARL, 2018). For our research herein, we used VDE (see 3.4), because it enables the user to perceive the spatial layout of the topology based on observed network traffic, while the resulting visualization can be augmented with additional data, like TCP/UDP session counts between network nodes (Kullman, Cowley, & Ben-Asher, 2018). Due to the 6DOF of Oculus Rift VR headset (OVR) used for this study, VDE also allows us to test the usefulness of stereoscopically perceived depth-cues (contrary to monocular depth-cues on flat screens) for encoding data.

3. Method

To understand whether stereoscopically-perceivable 3D data-shapes representing a complex computer network's topology is usable, we conducted semi-structured interviews with 10 subject matter experts working as cybersecurity analysts (as suggested in (Ward, Grinstein, & Keim, 2015)). Included in the usability assessment, we asked analysts about whether network behavior is understandable, helpful and useful for cybersecurity analysts' tasks.

3.1 Participants

Ten cybersecurity analysts (Mean age = 36.5yr., 20% females) were interviewed in a semi-structured format. All participants work as cyber security practitioners, having 2 months to 10 years of experience in the field (Mean = 4.5 years). Participation was voluntary and these volunteers were not compensated for their time.

3.2 Materials

The network traffic data used during the interviews was part of the NATO CCDCOE CDX Locked Shields 2018 (LS18) "Partner Run" (LS18PR) dataset. This dataset includes 23 defensive teams' (Blue Teams, BT) networks, an offensive (Red Team, RT), infrastructure support (Green Team), situational awareness (Yellow Team) and the managing team (White Team) nodes and traffic. During LS18 exercise the network included more than 4000 virtual machines, with about 2500 attacks executed by the Red Team against all Blue Teams combined. LS18PR function was to test Read Team' and infrastructure' readiness. Distinct of the main event, LS18 that ran for 2 days (2x7 hours), LS18PR ran for 7 hours, during which only few Blue Team networks were attacked and defended, while the rest of the networks were running as usual. Hence LS18PR dataset provides the ability to observe networks in their "normal" as well as "under attack" and "compromised" states during the same time.

The time-window for the network sessions used in the visualizations shown to the participants was set to 40-minute periods. For data preparation, Moloch (https://molo.ch/) was used to process the LS18PR packet data (PCAP). The resulting data and metadata was stored in an Elasticsearch server to allow dynamic querying. Kibana (https://www.elastic.co/products/kibana) was used to generate dynamic and interactive 2D visualizations based on the data stored in Elasticsearch server. VDE queried the Elasticsearch server for session counts between entities and presented the information using Oculus Rift (https://www.oculus.com/rift/) VR headset (OVR) while an Oculus Touch controller (OTC) was used to interact with the VDE. The controller allowed users to move around the virtual space (by changing their viewpoint), select different groups of objects (e.g. connections from/to a Blue Team), grab a network node to alter its position (and better perceive the destinations of the connections that this node had) and query additional information about the node (e.g. it's IP addresses).

3.3 Procedure

Upon arrival to the interview, participants were asked about their cybersecurity expertise, experience with 2D and 3D visualizations, as well as gaming preferences. Gaming preferences were discussed to build the rapport and understand interviewee's level of experience in cybersecurity. Below is a list of the basic questions asked in this introduction portion of the procedure. Participants provided open ended answers that were documented by the experimenter.

- What are your favorite console / computer games?
- Have you used Moloch and / or Kibana before?
- Have you experienced Virtual, Augmented or Mixed Reality before?
- Do you have formal education on IT and / or cybersecurity?
- What area do you specialize in cybersecurity?
- How long have you been working on your current specialty; on cybersecurity?

Then, participants received a short briefing about the purpose of the study and an overview of the dataset. They were shown a printed diagram (see Figure 1) illustrating the network topology of a single blue team network. Based on the diagram, participants were asked to consider, what (textual and visual) tools they would prefer to use to learn that network's topology to acquire situational awareness.

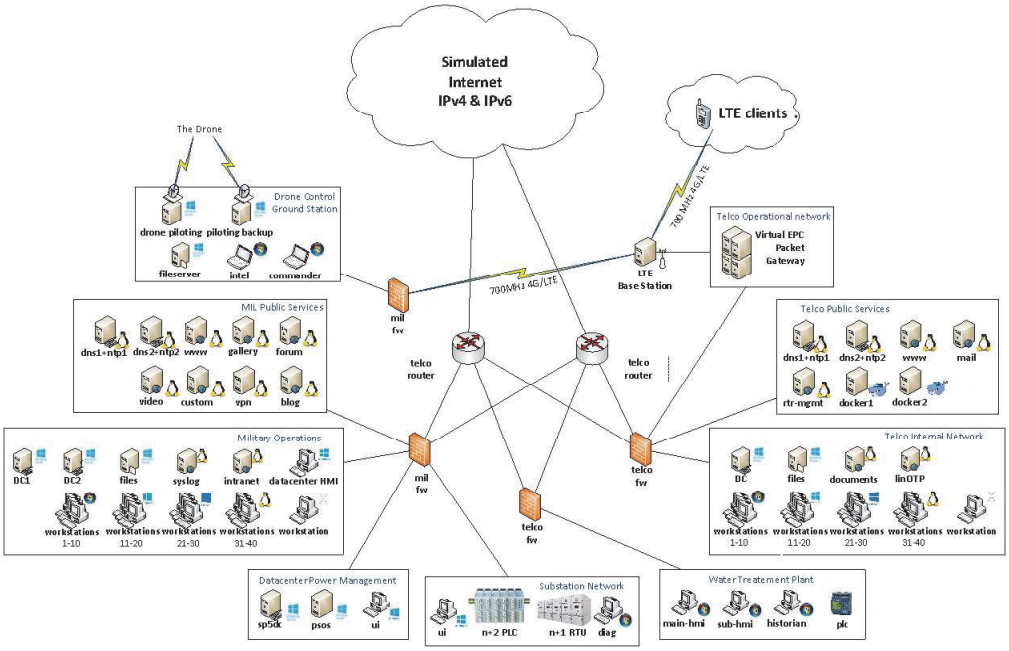


Figure 1: Simplified network topology diagram for traffic used in this study

Following, the experimenter presented a 2D visualization of session counts between the different entities in the Blue Team's network as radial figures (Figure 2 using Kibana). As seen in Figure 2a and Figure 2b there is a difference of an actively attacked and maintained network (on the left) compared to another one with exactly the same topology and active services, while unmaintained and not attacked network (on the right).

Size of a sector on Figure 2 represents the count of observed sessions. The radial diagram also indicated how many connections were initiated between the source and the inner ring, how many of those connections were targeted at the one represented in the outer ring, etc. The color of the session-count-block is randomly allocated to each node in that Blue Team network and does not have any relation to other networks. However, the color allocated to each node does allow the observer to find that same node in that same radial. The other sectors belonging to that same node are also highlighted by a mouse-over, which displays a popup detailing the IP addresses of source and its destination nodes and their session counts (see Figure 3).

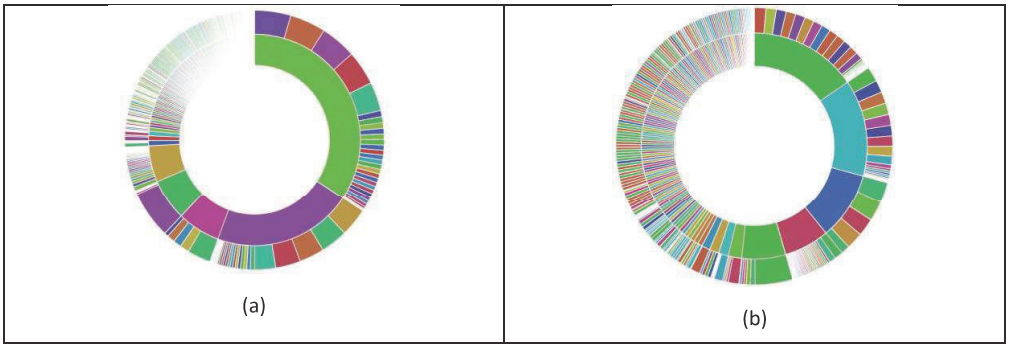


Figure 2: Radial 2D diagrams visualizing activeness of Blue Teams' internal nodes. Inner ring contains source addresses of the entities present in that Blue Team's network while the outer ring contains destination addresses of that same Blue Team's entities, with network connection sessions to that source address during a time-window

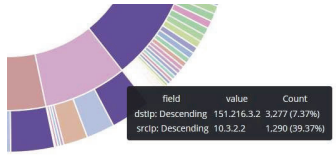


Figure 3: Mouse-over example for selected data-point displayed in a popup window, with source IP address and observed session count (srcIp) and destination IP address with its respective session count (destIp)

Participants were also shown a 2D visualization of a force directed graph (using Moloch) to provide another example of graphical representation of relations between networked entities (Figure 4).

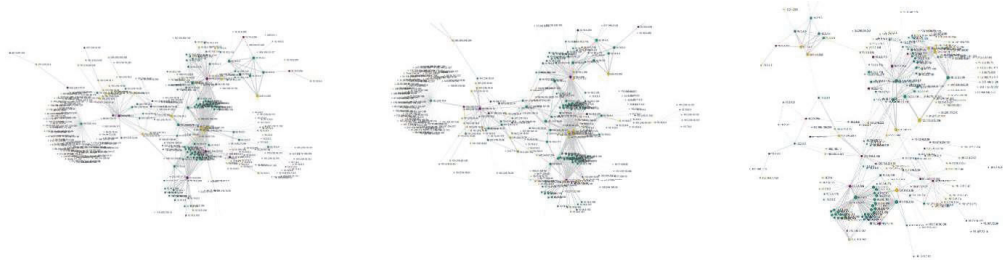


Figure 4: Network connections observed in the two unused BT (a) and (b) networks compared to a BT (c) networks that were actively engaged during LS18PR. Traffic observed during a set period of time is applied as pull strength of the edges between nodes, while nodes represent the hosts initiating and/or receiving connections, visualized on a 2D graph

Following the review of various 2D visualizations, participants were introduced to the VDE and the reasoning behind the spatial positioning of network elements in a 3D space. During this step, LS18PR networks were first shown as 3D shapes on a 2D display and once participants felt comfortable with their understanding of the 3D visualization as shown in VDE, they were fitted with an Oculus Rift VR Headset and Touch Controller. Participants were encouraged to explore the 3D display by changing their viewpoint while using VDE so that they could observe Blue Team networks from close distance (Figure 5) and would be able to read explanatory texts, reach out to grab the nodes, move those around, highlight nodes' features, select edges' groups and so on. After participants had familiarized themselves with the VDE environment and it's 6DOF "rudder head movement" (Pruett, 2017), they were asked to evaluate if and how such network topology visualization and its augmentation with additional data (e.g. network session counts) would relate to the 2D visualizations (Figures 2, 3, 4) and the print-out topology (Figure 1) shown to them before. Once the participant gained an understanding of a blue team's network, she/he was guided to adjust the viewpoint in VR so that all the LS18PR network components

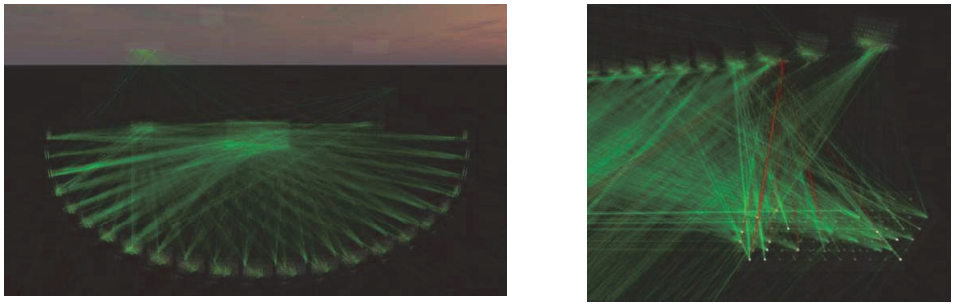
would be in the field of view. Then, the participant was asked to provide feedback and critique regarding the usability of VDE, subjective ease of stereoscopical perception of the 3D data shapes and her/his ability to acquire situation awareness with such tool.

3.4 Virtual data explorer

Virtual Data Explorer (VDE) was developed with the Unity 3D game engine to present users with stereoscopically perceivable data visualizations in VR and XR.

Figure 5: VDE 3D display of network topology and traffic focusing on a single Blue Team network topology ("Zoom" on "Details-on-Demand", per (Shneiderman, 1996)). Additional videos of VDE can be found: https://coda.ee/vde

The VDE uses a predefined topology description (configuration) for the visualized network. Data-shapes were spatially positioned into a meta-shape (viewed from different angles as shown in Figure 6) to allow the user to take advantage of stereoscopic viewing that VR provides. Multiple layouts were considered to minimize possible edge clutter and enable convenient distinguishability of intra- and extra-network connections and nodes' relations. These 3D shapes are easily understandable in stereoscopically-perceivable VR headsets, while often cluttered and unusable on a 2D screen or on a printed paper.



(a) (b)

Figure 6: 3D display of LS18PR network topology and network traffic using VDE: (a) overall view of the meta-shape ("Overview"); (b), RT group ("Zoom") with some added connections and selected ("Filtered") edges colored red ("Relations", per (Shneiderman, 1996)

VDE allows the spatial topology of the network to be augmented with additional data. For this study, the visualization was enriched with network session counts so, that the most popular connection (represented as a green line (edge) between the nodes that were observed connecting) was fully visible, while the least popular connection was almost transparent. User could add additional sessions using VDE menu system in VR, in which

case the added edges were colored red until a next set of edges was added. Additional information about VDE design decisions can be found in our previous paper (Kullman, Cowley, & Ben-Asher, 2018).

4. Results

Participants were asked for impressions on the technology, ideas or suggestions for modifications, should such a tool be made available for their tasking. All participants had used 2D visualizations, 6 had used Kibana, and 4 out had experienced VR prior to this study. Seven interviewees self-rated themselves as 'experienced' in playing computer games. All participants used command line interfaces or GUIs for tasks like querying NetFlow data, inspect captured packets, review incidents in SIEM, explore various configuration files of the routing and perimeter devices etc. Seven used Kibana and / or Excel for simple 2D visualization. All participants agreed that although printed or electronically provided 2D diagrams of the network topology would be helpful, topologies provided are usually outdated. Overall, there emerged a common process that analysts would have used to build their understanding of a network's topology. First, analysts would build an understanding of what is "normal" in that specific environment and then find the behaviors that would need further investigation. In order to execute that process, the analysts begins by building filters on available data to exclude the findings that are deemed "normal" and continue fine-tuning that filter, while the analyst learns that network's behavior and builds her/his internalized understanding of that datasets expected demeanor.

To the questions "How would you build the understanding of a network? How would you map the network topology?" participants responded with: "Textual logs from SIEM [or similar]";"Textual tools"; "flow in Kibana, xflow, tcpdump". "Whatever tools that are available. Textual mostly, if some visualization is available, then that too." To the question "How would you establish expectations regarding normal behaviors of the different entities in the network?" participants responded with: "I just read the logs [..]. Look in packets."; "Check Ingress/egress points, what services are allowed through firewall, what VLANs&VPNs are in use."; "filter logs, what type of systems are in these networks from SIEM. Use different filters and queries in Kibana."; "Work through documentation, dive in, see configuration."; "flow data, who's talking to each other, as opposed to heading outside; I've used to bar graphs [..while trying to identify..] what IP's are being hit, what hosts are endangered a lot in traffic. Usually I would likely see just textual lists of IP addresses, ports etc."; "Look at netflows, do a graph chart. Use excel, build bar graphs [and so on]"; "Use a sensor that sees all the traffic in this network, build a BPF to exclude things (ICMP, TCP, UDP) [from tcpdump] to see what's left, what falls out, what ports and protocols, [..], to find what stands out, what weird ports are in use."

Once in the VDE VR environment, users had some trouble getting comfortable with the "rudder head movement" to roam around in the VR environment. Few participants found the rudder head movement intuitive to use. Learning to use this tool usually took between one to two minutes. Most problematic was the vertical movement. To execute vertical movement, users had to look straight up or straight down and move backwards or forwards to change their vertical viewpoint. However, one participant commented, "[moving around in this environment] is very natural to me". Only two participants reported feeling dizzy or having any simulator sickness/motion sickness symptoms during or after the session. The precision of depth perception or the predicting the physical distance of each virtual object from the self was highly variable. Most of the participants managed to grab and hold visualized entities easily, while others struggled. Further tuning of haptic and visual feedback is needed to improve interaction with 3D data representations.

Once the participants were comfortable with adjusting their position and viewpoint in the VR environment, all were able to observe the data-shapes and understand its relation to the network's textual and 2D visualizations they had seen moments before. Most participants stated that once the logical structure of the shapes positioned in VR had been understood, the topology of these networks became much clearer. Participants also understood the underling relations between 3D visualization and the textual / 2D representation they had seen previously:

> *[P1]: "Does this [3D visualization] map back to the topology you saw on the paper before? I think so, I mean I'd have to figure out where things are, but... [yes]";*
>
> *[P6]: "It is not how I thought about, but... [...] I think it would definitely be helpful, but it would take some re-learning, [e.g.] how to think visually. When you learn networking, then you're kind of trying to build this in your brain already. But then getting used to seeing this and not having to build your own picture. Like, training brain to think visually not only textually.";*

> *[P4]: "So this is what you showed [me] before on the network diagram [on paper]? [...] Yes, I like this. This is different than looking graphs on your computer screen. [...] I take it you'd prefer this to the regular [tools]? Yes, definitely.";*

Participants could "see" where "things" are in the network, helping them spatially perceive and understand the structure and topology of this computer network and networked entities' (nodes) positions and logical grouping inside that network ("Overview", as per (Shneiderman, 1996) taxonomy):

> *[P1]: "This agrees with me particular. I like visual. I always kind of visualize things, in a way like this. And this particularly agrees with me. That's very easy for me to understand.";*
>
> *[P6]: "If you now look at this network diagram [printed on paper], does this looks familiar? It is familiar, but very flat. Would you prefer 3d? Well, of course. This 2D looks like... why are we still using this.. it seems so.. like.. limited.";*
>
> *[P2]: "For our team this is a great representation of what we could use. This is a good representation of a network that would work for us. A way to visualize this and interact with.";*

Participants admitted that they perceived the traffic "going" between nodes, referring to the edges representing the count of sessions observed between these two nodes ("Relations" of groups, subgroups and nodes, as per the taxonomy):

> *[P1]: "They are clearly grouped, and I can see exactly where everything is going [which node has been connecting to what other nodes]."*
>
> *[P4]: "This would help a lot. You can see the traffic leaving networks and so..."*
>
> *[P5]: "This makes a lot of sense to me. I really like the visualization. I can see.. there's the first firewall, DMZ.. I can kind of understand how the network is built..."*
>
> *[P2]: "This is useful... and this seems very utilizable. Useful in terms of what's reaching out to what. There's definitely usefulness in this for what we do here. [..] This makes much sense for what we do here in terms of usefulness and utility..."*

Participants recognized the advantages of using such visualizations could provide to transfer knowledge about specific networks from senior analysts to trainees:

> *[P6]: "Since I've been here for 4 years, I've trained about 80 people. I think if we'd have something like that from the start, it would change their whole perception of how to [think of networks] and jump start [their ability to work the networks]. […] I think a lot of analysts would have different views, that would depend on their knowledge base and artistic side also. [..] When you're using tool like this, when you build your network diagrams, you would like to have same setup, that way [when] you're looking at them on a pdf, you'd have the same layout."*

Participants suggested capabilities (see correlation with taxonomy, described in Introduction and (Shneiderman, 1996)), that they would like to have at their disposal:

> *[P9]: "This is awesome! [..] As an analyst I would want to see [in addition to the visualization] what's happening, the [textual] details. [..] It is cool; you could definitely do a lot with it. [..] This is one of the coolest things I've ever seen. But I do need [additional, textual] information. As an analyst, I could definitely use this. [..] I could probably play with this all day.";*
>
> *[P1]: "[It] would be nice to control how far apart they [nodes, groups] are. Would be easier to navigate between them. [..] [option to] change the icon of the node to something that would indicate the function of the entity. I would prefer to use colors for grouping the entities.";*
>
> *[P3]: "Color-code the layers in the network. Any host that is associated [has had sessions] with those should also be color accordingly. 6DOF movement should be available.";*
>
> *[P6]: "Lines should have arrows showing the direction of the sessions.";*

5. Conclusion

This study captured cybersecurity analysts' impressions of a network topology presented as a stereoscopically-perceivable 3D structure. Overall, the impressions towards stereoscopically-perceivable 3D data visualizations were highly favorable. Multiple participants acknowledged that such 3D visualizations of network topology could assist in their understanding of the networks they use daily. Participants expressed a wish to integrate such visualization capabilities in their workflow. Prior experience with 3D displays had no influence on user

preferences, while participants with prior gaming experience adjusted quickly to the Oculus Touch motion controllers, suggesting that the relevant dexterity and muscle memory for gaming console controller usage helps users adjusting from those controllers to handling input devices for VR experiences. Further research is needed to understand what specific 3D data shapes would be useful and for which datasets (e.g. computer network topology) to create additional 3D visualization suitable for analysts' preferences and test the usefulness of those visualizations. Follow-up studies should evaluate operator performance in 3D environments.

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-13-2-0045 (ARL Cyber Security CRA) and under Cooperative Agreement Number W911NF-16-2-0113 and 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.

Results

Arthur, K. W., Booth, K. S., & Ware, C. (1995, 7). Evaluating 3D Task Performance for Fish Tank Virtual Worlds. ACM Transactions on Information Systems, 11(3), 239-265. doi:10.1145/159161.155359

Aukstakalnis, S. (2017). Practical Augmented Reality. Addison-Wesley.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51-61.

Berry, S. P. (n.d.). The Shoki Packet Hustler. Retrieved from http://shoki.sourceforge.net/

Best, D. M., Endert, A., & Kidwell, D. (2014). 7 Key Challenges for Visualization in Cyber Network Defens. In Proceedings of the Eleventh Workshop on Visualization for Cyber Security (pp. 33-40). ACM.

Burnett, M. S., & Barfield, W. (1991). Perspective versus plan view air traffic control (ATC) displays - Survey and empirical results. International Symposium on Aviation Psychology, 6th. Columbus. Retrieved from http://adsabs.harvard.edu/abs/1991STIA...9244967B

Dennehy, M. T., Nesbitt, D. W., & Sumey, R. A. (1994). Real-Time Three-Dimensional Graphics Display for Antiair Warfare Command and Control. Johns Hopkins APL Technical Digest, 15(2), 110-119.

Ehrenstein, W. H., Spillmann, L., & Sarris, V. (2003). Gestalt Issues in Modern Neuroscience. In Axiomathes (pp. 433-458). Springer.

Gaw, T. J. (2014, 4). 3D Information Visualization of Network Security Event. Munice, Indiana, USA: Ball State University. Retrieved from https://pdfs.semanticscholar.org/f3fa/c8a059369b96202a70ceb19828c07444dc42.pdf

Gazzaniga, M. S., Ivry, R. B., & Mangun, G. R. (2013). Cognitive Neuroscience: The Biology of the Mind, 4th Edition. W. W. Norton & Company.

Gershon, P., Klatzky, R. L., & Lee, R. (2014). Handedness in a virtual haptic environment: Assessments from kinematic behavior and modeling. Acta Psychologica, 37-42.

Gershon, P., Klatzky, R. L., Palani, H., & Giudice, N. A. (2016). Visual, Tangible, and Touch-Screen: Comparison of Platforms for Displaying Simple Graphics. Assistive technology: the official journal of RESNA, 28(1), 1-6. doi:10.1080/10400435.2015.1054566

Gonzalez, C., Ben-Asher, N., Oltramari, A., & Lebiere, C. (2014). Cognition and technology. In Cyber defense and situational awareness, 93-117.

Hodent, C. (2018). The Gamer's Brain; How Neuroscience and UX Can Impact Video Game Design. CRC Press.

Hurter, C. (2016). Image-Based Visualization: Interactive Multidimensional Data Exploration. (N. Elmqvist, & D. Ebert, Eds.) Morgan & Claypool.

Inoue, D., Suzuki, K., Suzuki, M., Eto, M., & Nakao, K. (2012). DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System. VizSec (pp. 72-79). ACM.

Kirk, A. (2016). Data Visualisation, A Handbook for Data Driven Design. Sage.

Kullman, K., Cowley, J. A., & Ben-Asher, N. (2018). Enhancing Cyber Defense Situational Awareness Using 3D Visualizations. Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018: National Defense University, Washington DC, USA 8-9 March 2018 (p. 369–378). Washington DC: Academic Conferences and Publishing International Limited.

Lebreton, P., Raake, A., Barkowsky, M., & Le Callet, P. (2012). Evaluating Depth Perception of 3D Stereoscopic Videos. IEEE Journal of Selected Topics in Signal Processing, 6(6). Retrieved from http://ieeexplore.ieee.org/document/6269042/

Lynn, W. J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. Foreign Affairs, 89(5), 97-108. Retrieved from https://city.rl.talis.com/items/71ACA705-9A0A-8C2B-EAD3-5FF314AAC847.html

Maddix, K. (2015). Big Data VR Challenge – Winners! Retrieved from Masters of Pie: http://www.mastersofpie.com/big-data-vr-challenge-winners/

Marty, R. (2008). Applied Security Visualization.

Meyerovich, L., & Tomasello, P. (2016). Display Relationships Between Data. IQT Quarterly, 7(4).

Munzner, T. (2014). Visualization Analysis & Design. A K Peters/CRC Press.

Payer, G., & Trossbach, L. (2015). The Application of Virtual Reality for Cyber Information Visualization and Investigation. In M. Blowers, Evolution of Cyber Technologies and Operations to 2035 (Vol. 63, pp. 71-90). Springer. doi:10.1007/978-3-319-23585-1_6

Pruett, C. (2017, 05 17). Vision 2017 - Lessons from Oculus: Overcoming VR Roadblocks. Retrieved from https://youtu.be/swA8cm8r4iw?t=9m42s

Rajivan, P., Konstantinidis, E., Ben-Asher, N., & Gonzalez, C. (2016). Categorization of Events in Security Scenarios: The Role of Context and Heuristics. Human Factors and Ergonomics Society Annual Meeting, 60(1), 274-278.

Reda, K., Febretti, A., Knoll, A., Aurisano, J., Leigh, J., Johnson, A., . . . Hereld, M. (2013). Visualizing large, heterogeneous data in hybrid-reality environments. IEEE Computer Graphics and Applications, 33(4), 38-48.

Reuille, T., Hawthorne, S., Hay, A., Matsusaki, S., & Ye, C. (2015). OpenDNS Data Visualization Framework. Retrieved from OpenGraphiti: http://www.opengraphiti.com/

Schneider, W., Dumais, S. T., & Shiffrin, R. N. (1982). Automatic and Control Processing and Attention. Illinois: University of Illinois. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a115078.pdf

Sethi, A., & Wills, G. (2017). Expert-interviews led analysis of EEVi — A model for effective visualization in cyber-security. IEEE Symposium on Visualization for Cyber Security (pp. 1-8). Phoenix, AZ, USA: IEEE.

Shearer, G., & Edwards, J. (2018). Vids: Version 2.0 Alpha Visualization Engine. Adelphi: US Army Research Laboratory.

Shneiderman, B. (1996). The eyes have it: a task by data type taxonomy for information visualizations. Proceedings 1996 IEEE Symposium on Visual Languages. Boulder, CO, USA, USA: IEEE. doi:10.1109/VL.1996.545307

Smallman, H. S., St. John, M., Oonk, H. M., & Cowen, M. B. (2001). Information availability in 2D and 3D displays. IEEE Computer Graphics and Applications, 21(5), 51-57. Retrieved from http://journals.sagepub.com/doi/pdf/10.1518/001872001775992534

St. John, M., Cowen, M. B., Smallman, H. S., & Oonk, H. M. (2001). The Use of 2D and 3D Displays for Shape-Understanding versus Relative-Position Tasks. Human Factors, Spring, 79-98. Retrieved from http://journals.sagepub.com/doi/pdf/10.1518/001872001775992534

U.S. ARL. (2018, 02 12). SEEING THE CYBERTHREAT. Aberdeen Proving Ground, Maryland, USA: U.S. Army Research Laboratory. Retrieved from https://dodstem.us/sites/default/files/lab-narratives/Seeing-the-Cyberthreat_0.pdf

van Riel, J.-P., & Irwin, B. (2006). InetVis, a Visual Tool for Network Telescope Traffic Analysis. AFRIGRAPH 2006. Cape Town: Association for Computing Machinery, Inc.

Ward, M. O., Grinstein, G., & Keim, D. (2015). Interactive Data Visualization: Foundations, Techniques, and Applications, Second Edition. A K Peters/CRC Press .

Ware, C., & Franck, G. (1996, 4). Evaluating Stereo and Motion Cues for Visualizing Information Nets in Three Dimensions. ACMTransactions on Graphics, 15(2), 121-140. doi:10.1145/234972.234975

Wu, Y., Xu, L., Chang, R., Hellerstein, J. M., & Wu, E. (2018). Making Sense of Asynchrony in Interactive Data. JOURNAL OF LATEX CLASS FILES, 14(8).

Appendix 3

Publication III

Kullman, Kaur; Ryan, Matt; Trossbach, Lee (2019). VR/MR Supporting the Future of Defensive Cyber Operations. 14th International-Federation-of-Automatic-Control (IFAC) Symposium on Analysis, Design, and Evaluation of Human Machine Systems (HMS), SEP 16-19, 2019, Tallinn, ESTONIA. Amsterdam: ELSEVIER, 181−186. (52). DOI: 10.1016/j.ifacol.2019.12.093

Preprints, 14th IFAC Symposium on
Analysis Design and Evaluation of Human Machine Systems
Tallinn, Estonia, Sept. 16-19, 2019

VR/MR Supporting the Future of Defensive Cyber Operations

Kaur Kullman*,
Matt Ryan, Lee Trossbach****

**US Army Research Laboratory, Adelphi, Maryland, USA.*
***C5ISR Center CSSP, Army Futures Command, Adelphi, Maryland, USA*

Abstract: US Army C5ISR Center Cyber Security Service Provider (CSSP) is a 24/7 Defensive Cyber Operations (DCO) organization that defends US Department of Defense and US Army networks from hostile cyber activity, as well as develops technologies and capabilities for use by DCO operators within the DoD. In recent years, C5ISR Center CSSP has been researching various advanced data visualization concepts and strategies to enhance the speed and efficiency of cybersecurity analyst's workflow. To achieve these goals Virtual and Mixed Reality (VR/MR) tools have been employed to investigate, whether these mediums would enable useful remote collaboration of DCO operators and whether stereoscopically perceivable 3D data visualizations would enable DCO operators to gain improved hindsight into their datasets. We'll be giving overview of the capabilities being developed as aligned to our research and operational requirements, our expected outcomes of using VR/MR in training and operational cyber environments and our planned path to accomplish these goals.

Keywords: Virtual and Augmented Reality; Decision Support Systems; Human – Computer Interaction.

INTRODUCTION

To protect an information system, analysts need to have actionable situational awareness of that system. To have actionable situational awareness, analysts ingest and process significant amounts of data from diverse sources to extract relevant information. Adding data visualizations tools to precise alphanumeric displays can improve the efficiency of cybersecurity analysts' workflow by providing them with a wider context to the data they need to understand, while extracting information from it. However, alphanumeric displays and 2D visualizations have limited capabilities for displaying complex, dynamic and multidimensional information. There have been many attempts to visualize multidimensional data in 3D, while being displayed on flat displays, albeit with limited success.

To provide cybersecurity analysts working at C5ISR CSSP with useful tools that would allow them to harness the potential of stereoscopically perceivable Virtual and Mixed Reality (look for definitions of Stereoscopy, also Virtual, Mixed and other Realities in (Unity 3D, n.d.)) environments and visualizations, C5ISR is building Virtual Reality Data Analysis Environment (VRDAE), which will provide analysts with a collaborative environment and a variety of 3D data visualization tools, including one that can provide a representation of the network, complete with the computers, routers, switches and communication lines between them all (Payer & Trossbach, The Application Of Virtual Reality for Cyber Information Visualization and Investigation, 2015). VRDAE is in its early stages of being tested by CSSP cybersecurity analysts and researchers. The project has been underway since early 2017 and a fully functioning prototype is just starting to come out of the lab (US Army Research Laboratory, 2018).

VRDAE environment will enable analysts to use various data visualization tools collaboratively, two of which are currently being developed by C5ISR and US Army Research Laboratory (ARL): Visual Intrusion Detection System (VIDS) (Shearer & Edwards, 2018) and Virtual Data Explorer (VDE) (Kullman, Cowley, & Ben-Asher, Enhancing Cyber Defense Situational Awareness Using 3D Visualizations, 2018).

APPROACH

Cybersecurity analysts ingest and process significant amounts of data from diverse sources to acquire situational awareness of the environment they must protect. Visualizations provide analysts with visual representation of alphanumeric data that would otherwise be difficult to comprehend due to its large volume. Such visualizations aim to effectively support analyst's tasks including detecting, monitoring and mitigating cyber-attacks in a timely and efficient manner (Sethi & Wills, 2017). Cybersecurity specific visualizations can be broadly classified into three main categories: 1) network analysis, 2) malware analysis, 3) threat analysis and situational awareness (Sethi & Wills, 2017). Timely and efficient execution of tasks in each of these categories may require different types of visualizations. Herein we focus on visualizations that would benefit analysts in 1st and 3rd category.

Security Operations Centers (or equivalent) provide limited visualization capabilities both in the physical and logical sense. The physical space available to install display devices on analyst's workspace is usually very limited (a few UHD monitors), while universally placed larger screens can be obstructed or otherwise difficult to purposefully employ from analysts' viewpoint. Therefore, analysts must allocate all necessary applications into a few logical stacks on their screens, limiting their ability to leverage their full field of view and creating inefficient workflows.

Copyright © 2019 IFAC

While most of the analytical work is done independently using their own screens and in their heads, analysts often need to share their findings and consult with their colleagues or superiors. Hence the necessity to have a standardized VR environment (VRDAE) for (data) visualization, where collaboration would be possible, no matter the physical location of the participants of a session.

Stereoscopically perceivable 3D data visualizations are being developed in parallel with VRDAE, as their development doesn't depend on the specifics of the VR/MR environment where these visualizations will be used in, once ready, provided these components will be compatible with each other then. Hence the VIDS and VDE projects are being developed using the Unity 3D game engine, as is VRDAE. Which specific VR/MR technologies will be used once the software and visualization methods are ready, can therefore be chosen or adjusted in future, as deemed necessary.

TOOLS IN DEVELOPMENT

3.1 Virtual Reality Data Analysis Environment

VRDAE provides analysts with a collaborative environment and a variety of 3D visualization tools. Oculus Rift headsets are used to immerse the user in stereoscopically perceivable virtual environment and Oculus Touch controllers are used to capture user's hand gestures to allow her to manipulate and sift through the data projected into the virtual space; for example to maneuver around the visual representation of a computer network, zoom in to individual nodes and machines. Traffic anomalies are represented as colored lines between machines, and nodes that are under attack or being investigated are surrounded by a red bubble.

User interaction with, and user experience in the virtual environment is of keen interest. For example, the system tracks user's head movement, so is a text bubble with more detailed information pops up when an analyst looks at a component of interest and fixes her gaze on it. And if she needs another set of eyes on the problem, she can invite another analyst into her virtual space. That person might be in the next room or in a base across the country – he'll slide on a VR headset to join her (US Army Research Laboratory, 2018).

VRDAE will function as an operating environment for other tools (for network and data visualization, but also for others), abstracting user interaction and collaboration. Hence VRDAE's focus being more on user interaction, user experience and user interface design.

3.2 Visual Intrusion Detection System

The VIDS project is aimed at addressing open questions in designing and testing logical layouts of computer network features into a 3D visualization. VIDS allows a high degree of flexibility for users to organize data into any number of available layouts, while allowing users to transition between these layout states without reloading the underlying data nor recalculating the visualization.

Another significant goal of VIDS is to research, how can analysts best interact with data inside a 3D visualization environment. Specifically, VIDS seeks to investigate what interactions are feasible and, through the mechanism of analyst feedback, what interaction mechanisms are desirable, including functions such as filtering data, sorting data, moving objects, and changing visual styles.

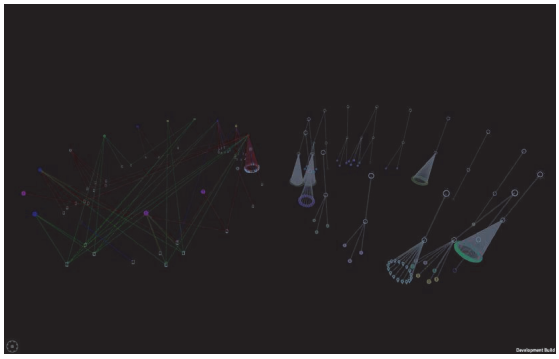


Fig. 1. Vids: Hierarchical representation of alerts in 2 different formats.

By providing a platform to investigate these questions, VIDS is intended as a foundation for several areas of further research. From a basic research perspective, VIDS can be used as a platform for evaluating what metrics of visualization utility are useful to the analyst or Warfighter. VIDS can also be used to evaluate what cyber symbology and iconography is most effective for conveying meaning to analysts and decision makers. Additionally, as a tool, VIDS can be used as it is for visualizing a variety of data or it may be tailored in the future to specific visualization tasks according to operational needs.

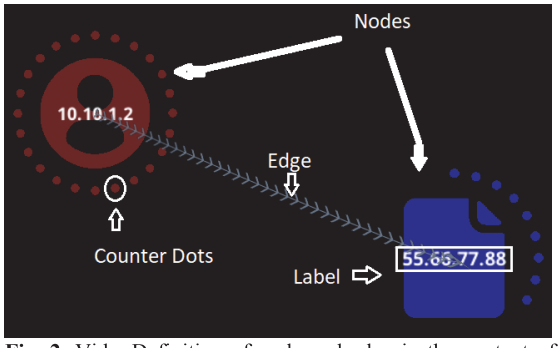


Fig. 2. Vids: Definition of node and edge in the context of Vids, and some labelled key features.

The "Vids" alpha version provides a variety of data views, currently 8 different major types, some with additional subtypes. These are presented to the user as a set of selectable layouts that dictate how data are arranged within the virtual 3-D environment. Each data view has parameters that can be

adjusted by the end user. Such parameters include algorithmic details, such as the desired radius of a randomly arranged sphere layout or the repulsion versus attraction coefficient of a force-directed graph layout, and feature selection details, such as which data features should be plotted on the x, y, and z axes, or which features should be used to form groups of nodes.

The Vids project aims to demonstrate a new direction in 3D interactive visualization for the Army. Faced with ever-increasing data volumes, new solutions are needed to maintain network situational understanding. Visualizations are one way to enable the Warfighter or network defender to process, and most importantly, understand, a larger volume of data. By using a modern game development platform, Vids allows streamlined development, strong portability across operating systems and platforms, and a variety of 3D, VR, and AR display options. In summary, Vids is intended as a first step to bridge the gap between network and security visualizations as they currently exist and the envisioned future where visualizations act as a ubiquitous and crucial aid to operations in cyberspace. (Shearer & Edwards, 2018)

3.3 Virtual Data Explorer

Virtual Data Explorer (VDE) was developed to present users with stereoscopically perceivable data visualizations in VR and MR environments. For example, to visualize the functional topology of a set of computer networks and their members, VDE uses a configuration describing the relations and group-memberships of (some of) the expected entities and groups.

In the context of VDE:

- Dataset – values (e.g. IP addresses, their relations, connections, sessions etc.) collected from sensors, log files, network traffic monitors or other sources;
- Data-object – one instance from a dataset, that may be a key-value pair, set of values related to an event that caused a logline or alert to be logged, etc.;
- Data-shape – a specific form of data visualization, where visual representations of nodes, connections etc. are arranged and positioned according to their logical or functional topology so, that the resulting visual representations of these data-objects would be helpful for a seasoned analysts while working with the dataset, that this data-shape was created for, or has deemed to suit well by a competent analyst. Data-shapes for same dataset but different tasks may differ;
- Meta-shape – combined set of data-shapes that consists of spatially positioned data-shapes, that in combination enable to user to view relations between different data-shapes' and nodes therein.

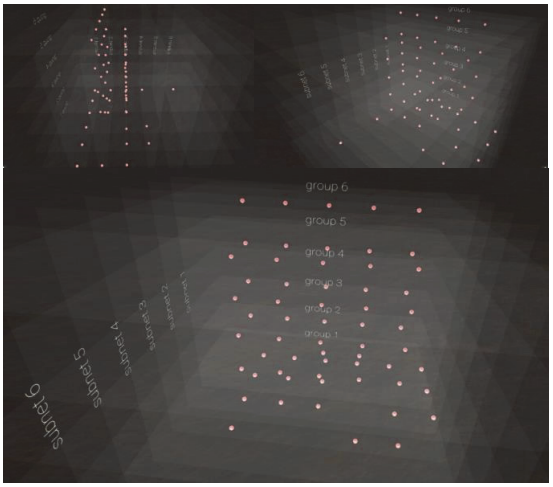


Fig 3. Viewing same data-shape from three different angles. Reddish spheres are nodes that were present in a sample used to generate a Blue Team's networks data-shape.

Data-shapes as such are nothing new (Hurter, 2016), but few have tried to use stereoscopically perceivable 3D data-shapes for computer security (Payer & Trossbach, The Application of Virtual Reality for Cyber Information Visualization and Investigation, 2015), while enabling the user to intuitively and / or with a common query language to manipulate the visualization to better understand the underlying dataset.

Fig. 4. VDE: VR display of a Blue Team's network topology and behavior rendered from NATO CCDCOE Locked Shields 2018 Partner Run dataset.

In VDE data-shapes are spatially positioned into a meta-shape (viewed from different angles as shown in Figures 5, 6, 7, 8) to allow the user to take advantage of stereoscopic viewing that VR and MR provide. Multiple layouts were considered to minimize possible edge clutter and enable convenient distinguishability of intra- and extra-network connections and nodes' relations. These 3D shapes are easily understandable while stereoscopically perceived in VR/MR headsets, but often cluttered and unusable on a flat screen or when printed on a paper.

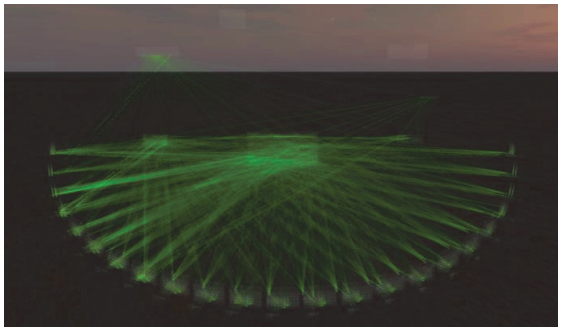


Fig. 5. VDE: VR view of Locked Shields 18 Partner Run network topology and network traffic using VDE; displaying an overall view of the meta-shape – a data-shape consisting of multiple data-shapes. Detailed description of this layout is found in (Kullman, Cowley, & Ben-Asher, Enhancing Cyber Defense Situational Awareness Using 3D Visualizations, 2018).

For our recent user study, a computer networks' topology visualization was enriched with network session counts (as edges) so, that the most popular connection was fully visible, while the edge representing the least popular connection was almost transparent. Session counts were represented as green lines (edges) between nodes that were observed communicating. During a VDE session, a user could adjust the filter to expose additional sessions (edges) using VDE menu system in VR, in which case the added edges were colored red until a next set of edges was added; select (filter) whole groups' connections (by pointing at those with a controller); select and disposition nodes by grabbing them with her hand (controller) etc.

When the user first starts a VDE session and enters the VR or MR scene, she looks at a scene that is positioned at such a distance, that the meta-shape depicting the network would fit in the view, while being visible slightly below the horizon (see Fig 5). The floor of the VDE environment (in VR) is a dark patterned desert that continues until it meets a horizon line that delineates floor and skyline. The background environment is chosen such, that it would be unobtrusive to the viewer's task, while providing horizon for spatial orientation. Visualized data-shapes are floating well above the floor and a little below the horizon line, to ease its components' visibility (brighter objects against darker background).

Contrary to self-organizing graphs which are useful for initial examination of unknown datasets, VDE's goal is to provide analysts with (the ability to create) data-shapes that would help them better comprehend datasets that are depicted as structures they can learn to know well over time. We propose creating data-shapes where networked entities (e.g. computers) are positioned according to their logical (but not necessarily their physical) topology so, that the resulting 3D structure(s) would relate to a cybersecurity analyst's task.

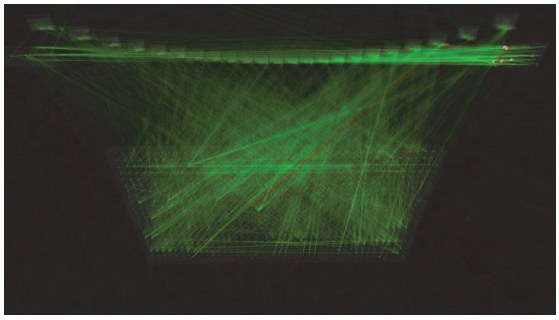


Fig 6. VDE: VR view of Locked Shields 18 Partner Run network topology and network traffic using VDE; view from the other side of the meta-shape, where the data-shape consisting of unknown entities is in foreground (lower side of this screenshot), while Blue Teams' networks (see close-up on Fig 4) are positioned father (on the upper side of this screenshot). Some edges and entities have been selected and are rendered red instead of the default green.

Prerequisite knowledge to create a VDE scene, containing a set of proposed data-shapes for depicting a computer networks functional topology would be to:

a) Understand the principles of how does a computer network function; specifically, how is such a network set up in the environment, that the author of this visualizations needs to protect;

b) Understand of the logical grouping of networked entities and their topology but also networked entities and stakeholders' goals (e.g. corporate, employees, external {friendly, neutral, malicious} actors, etc.);

c) Understanding the expected behavior of the above actors and how it should and would reflect on network data;

d) What indicators to look for, how to validate the findings, how act with that combined knowhow.

Data-shapes for other datasets could be created by mapping appropriately the mental models of these analysts, who have the experience of working with those datasets.

In case of the example shown on the figures, the task was to understand and explore a computer networks' topology, internal relations and behaviors during a cybersecurity exercise (NATO CCDCOE Locked Shields).

To test the usefulness of using stereoscopically perceivable 3D data-shapes for encoding non-spatial data, networked entities that were found present in NATO CCDCOE Locked Shields exercise' network traffic were spatially positioned, according to their positions in that networks functional topology, and more importantly, entities' affiliation with logical groups present in LS networks. Logical groups could be distinguished by their members' functionality (e.g. SCADA components), purpose (e.g. DMZ servers), risk exposure, OS etc. (see Fig 4). This resulted in custom 3D data-shapes, that were combined to a meta-shape (a VDE scene) representing larger whole of the

LS network(s). A meta-shape depicted on Figures 5, 6, 7, 8 are displaying an overall view of the percept that the LS network traffic visualization makes from a distance.

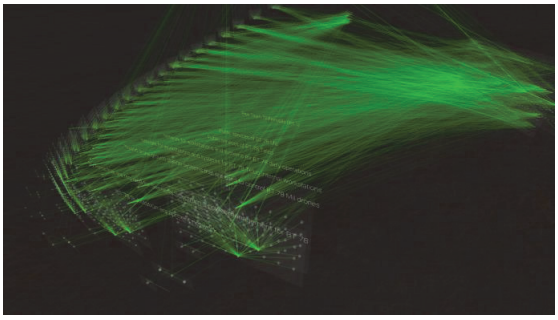


Fig 7. VR view of Locked Shields 18 Partner Run network topology and network traffic using VDE; view from the side of the meta-shape, where the data-shape consisting of unknown entities are seen on the right side, while Blue Teams' networks are curving from the upper center, to the center left, to the lower center of the screenshot.

As we have three axises available to encode data, we chose to use two of those axises to encode entities position in LS networks functional topology (subnet number) and entity's IP addresses' last octet or position in its subgroup while the third axis binds to the functional or logical group of that entity.

Using the common X, Y, Z referencing, nodes are positioned into a data-shape as seen on Fig 3 by:

X. This node's position inside a group;
Y. The group this node belongs to;
Z. The subnet this node belongs to.

Groups contain nodes in their respective subnets, grouped into horizontal groups according to their positions in their functional groups (subnets). For example, Windows, Linux, OSX workstations are positioned onto separate layers to distinguish them visually in subnets 2 and 3, while Windows, Linux and other servers, networks devices, etc. are kept on the lowest group to distinguish intra-group traffic from inter-group traffic.

For example, to expose (possibly) interesting connections inside a network that a Blue Team had to protect, it's entities were first positioned according to their subnet and then by their functional groups – servers, network devices, workstations (distinguished further by their type (Windows, Linux, OSX)), and SCADA components among others (see Figure 1). The third dimension is entity's sequential position inside of its subgroup (often the last octet of its IP address). Because the designated functions (and therefore behavior) of the entities in same functional group should be similar, it is beneficial for the analyst to have them close together, while still being spatially distinguishable to quickly diagnose which group and which member to focus on.

At the start of the exercise, there were 20 functionally identical Blue Teams' networks, whose entities should have been communicating identically, but as the exercise advanced, the Blue Teams' networks' behavior (in this case, entities' activity and relative connections / edges) deteriorated from each other's. Each Blue Team's network had 68 preconfigured nodes, and the teams could add two virtual machines per their specifications.

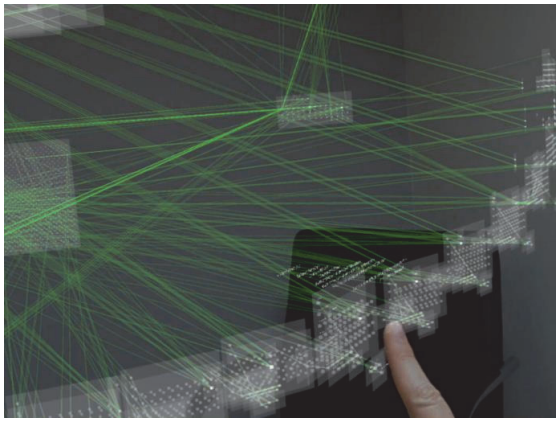


Fig 8. MR view of Locked Shields 18 Partner Run network topology and network traffic using VDE; user is selecting a Blue Team's network with index finger).

To validate the usefulness of such visualizations, a study was recently conducted (Kullman, Ben-Asher, & Sample, Operator Impressions of 3D Visualizations for Cybersecurity Analysts, 2019) to capture cybersecurity analysts' impressions of a network topology presented as a stereoscopically perceivable 3D data-shape.

Overall, the impressions towards stereoscopically-perceivable 3D data visualizations were highly favorable. Multiple participants acknowledged that such 3D visualizations of network topology could assist in their understanding of the networks they use daily. Participants expressed a wish to integrate such visualization capabilities in their workflow. Prior experience with 3D displays had no influence on user preferences, while participants with prior gaming experience adjusted quickly to the Oculus Touch motion controllers, suggesting that the relevant dexterity and muscle memory for gaming console controller usage helps users adjusting from those controllers to handling input devices for VR experiences.

Results of this study show, that customized, stereoscopically perceivable 3D data visualizations aligned with seasoned analysts' internal representations of a dataset may enhance their and other analysts' capability in having actionable situational awareness of that dataset in ways that textual information and 2D nor 3D visualizations on flat displays cannot afford (Kullman, Ben-Asher, & Sample, Operator Impressions of 3D Visualizations for Cybersecurity Analysts, 2019).

Overall, the impressions towards stereoscopically perceivable 3D data visualizations were highly favorable. Multiple participants acknowledged that such 3D visualizations of network topology could assist in their understanding of the networks they use daily.

Please see videos of the layouts at: https://coda.ee/IFACHMS

RESULTS AND DISCUSSION

We argue that there is a need for structured evaluation of visualizations that are created based on an analyst's internalized understanding of a dataset. Current technology is good enough for stereoscopically perceivable (3D) data visualizations; preliminary work also demonstrates that through purposeful interaction with subject matter experts it is possible to identify the core concepts of their mental models for relevant datasets, and to create matching data-shapes for those.

Further research is needed to understand, how generalizable are the data-shapes over different types of networks, cyber operations, analyst past training and other individual differences. However, the benefits of harnessing human visual-perception for cybersecurity can provide that much needed advantage to cyber defenders.

Further research is needed to understand what specific 3D data shapes would be useful, and for which datasets (e.g. other than computer network topology) should we create additional 3D visualizations for, that would be helpful for analysts' tasks and would enable us to test the usefulness of those visualizations in working environments.

Follow-up studies should also evaluate operator performance in 3D environments, be it then for collaboration, situational awareness, data analysis or other cybersecurity related task.

ACKNOWLEDGEMENTS

VRDAE team Barry Byrd, Alexander Rieschick.

VIDS team Joshua Edwards, Gregory Shearer.

For all the hints, ideas and mentoring, authors thank Alexander Kott, Jennifer Cowley, Jaan Priisalu and Olaf Manuel Maennel.

This research was partly supported by the Army Research Laboratory under Cooperative Agreement Number (CA) W911NF-16-2-0008. 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.

REFERENCES

Hurter, C. (2016). *Image-Based Visualization: Interactive Multidimensional Data Exploration.* (N. Elmqvist, & D. Ebert, Eds.) Morgan & Claypool.

Kullman, K., Ben-Asher, N., & Sample, C. (2019). Operator Impressions of 3D Visualizations for Cybersecurity Analysts. *18th European Conference on Cyber Warfare and Security.* Coimbra, Portugal.

Kullman, K., Cowley, J. A., & Ben-Asher, N. (2018). Enhancing Cyber Defense Situational Awareness Using 3D Visualizations. *Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018: National Defense University, Washington DC, USA 8-9 March 2018* (p. 369−378). Washington DC: Academic Conferences and Publishing International Limited.

Payer, G., & Trossbach, L. (2015). The Application of Virtual Reality for Cyber Information Visualization and Investigation. In *Evolution of Cyber Technologies and Operations to 2035* (Vol. 63, pp. 71-90). Springer, Cham. doi:10.1007/978-3-319-23585-1_6

Payer, G., & Trossbach, L. (2015, 12 28). The Application Of Virtual Reality for Cyber Information Visualization and Investigation. *Evolution of Cyber Technologies and Operations to 2035*. Springer. Retrieved from https://books.google.com/books?id=NYlNCwAAQBAJ

Sethi, A., & Wills, G. (2017). Expert-interviews led analysis of EEVi — A model for effective visualization in cyber-security. *IEEE Symposium on Visualization for Cyber Security* (pp. 1-8). Phoenix, AZ, USA: IEEE.

Shearer, G., & Edwards, J. (2018). *Vids: Version 2.0 Alpha Visualization Engine.* Adelphi: US Army Research Laboratory. Retrieved from https://www.arl.army.mil/arlreports/2018/ARL-CR-0827.pdf

Unity 3D. (n.d.). *What is AR, VR, MR, XR, 360?* (Unity 3D) Retrieved 06 2019, from https://unity3d.com/what-is-xr-glossary

US Army Research Laboratory. (2018). Seeing The Cyberthreat. *DoD Lab Narrative, Seeing the Cyberthreat*.

Appendix 4

Publication IV

Kullman, Kaur; Buchanan, Laurin; Komlodi, Anita; Engel, Don; (2020). Mental Model Mapping Method for Cybersecurity. Lecture Notes in Computer Science, vol 12210. Ed. Moallem, Abbas;. Cham: Springer International Publishing, 458–470. DOI: 10.1007/978-3-030-50309-3_30

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.

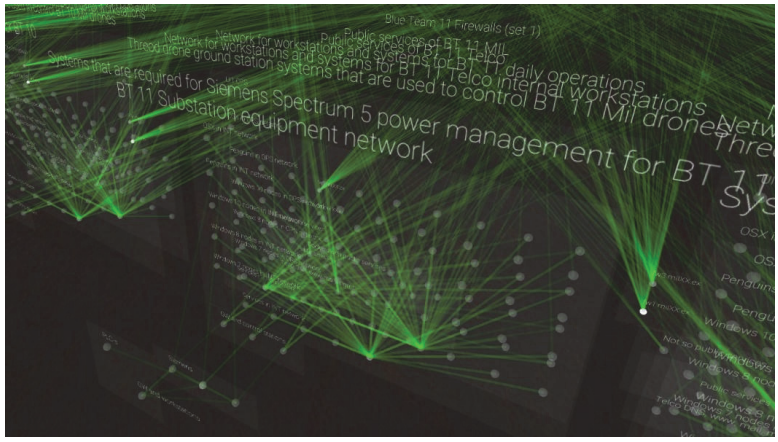


Fig. 1. Examining relationships and behavior of the entities of a group of groups.

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.

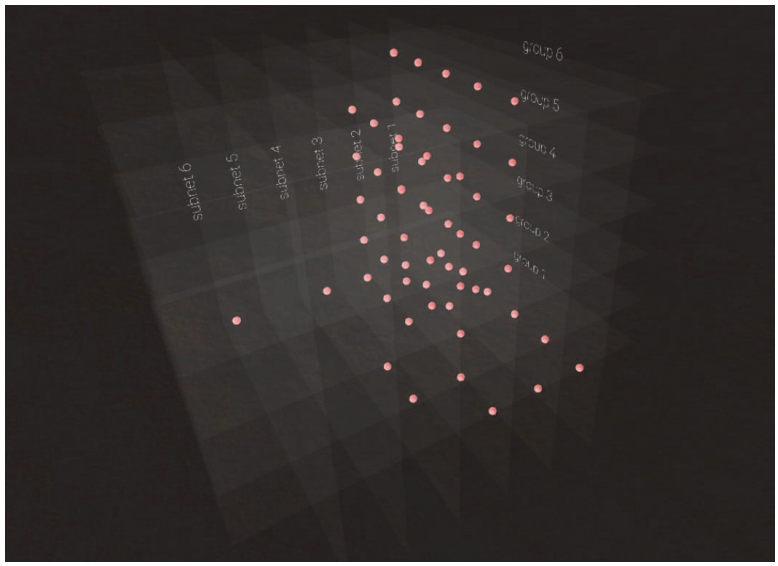


Fig. 2. Closeup of an example of triples arranged in a cube shape.

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.

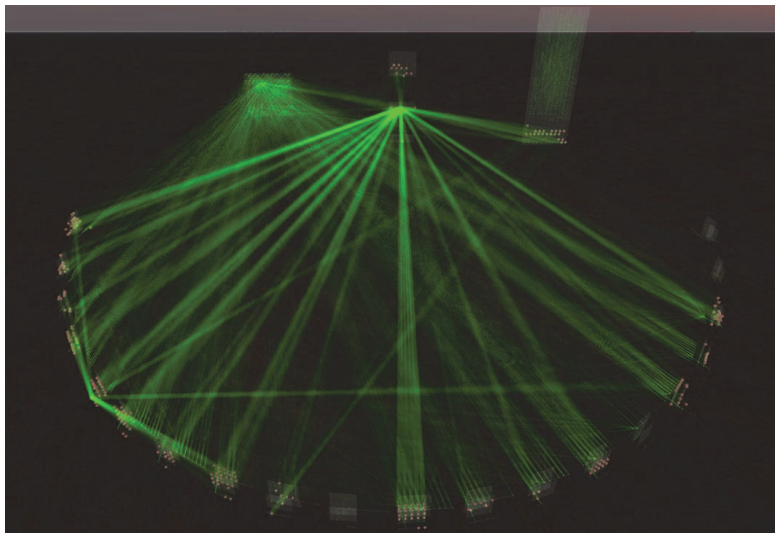


Fig. 4. Overview of a constellation of groups, where subgroups of entities can be distinguished afar, and examined in detail when user zooms in (moves closer with the VR headset).

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 and in conjunction with the CCDC Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center. 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.

Appendix 5

Publication V

Kullman, Kaur; Engel, Don; (2022). Interactive Stereoscopically Perceivable Multidimensional Data Visualizations for Cybersecurity. Journal of Defence & Security Technologies, Vol.4: Big Data Challenges – Situation Awareness and Decision Support. DOI: 10.46713/jdst.004.03

JDST., vol. 4, no. 3, p37-p52, 2021
https://doi.org/10.46713/jdst.004.03

www.jdst.eu, e-ISSN 2534-9813

Research Article

Interactive Stereoscopically Perceivable Multidimensional Data Visualizations for Cybersecurity

Kaur Kullman [a], ***Don Engel*** [a]

[a] *University of Maryland, Baltimore County, 1000 Hilltop Circle, Baltimore, MD 21250, US*
https://csst.umbc.edu

ABSTRACT

Interactive Data Visualizations (IDV) can be useful for cybersecurity subject matter experts (CSMEs) while they are exploring new data or investigating familiar datasets for anomalies, correlating events, etc. For an IDV to be useful to a CSME, interaction with that visualization should be simple and intuitive (free of additional mental tasks) and the visualization's layout must map to a CSME's understanding. While CSMEs may learn to interpret visualizations created by others, they should be encouraged to visualize their datasets in ways that best reflect their own ways of thinking. Developing their own visual schemes makes optimal use of both the data analysis tools and human visual cognition.

In this article, we focus on a currently available interactive stereoscopically perceivable multidimensional data visualization solution, as such tools could provide CSMEs with better perception of their data compared to interpreting IDV on flat media (whether visualized as 2D or 3D structures).

ARTICLE INFO

RECEIVED: 09 Oct 2021
REVISED: 10 Nov 2021
ACCEPTED: 30 Nov 2021
ONLINE: 12 DEC 2021

KEYWORDS

Stereoscopically Perceivable, Immersive, Data Visualization, Interactive Data Visualization, Cybersecurity, Virtual Reality, Augmented Reality, Mixed Reality, Interactive Stereoscopically Perceivable Multidimensional Data Visualization

Creative Commons BY-NC-SA 4.0

✉ Corresponding Author: E-mail: jdst@coda.ee

I. Overview

As commercially available virtual [1], augmented [2] and mixed reality [3] (VR, AR, MR; collectively "xR") devices have become significantly more performant over the last decade, there has been a commensurate growth in interest in using these tools for three-dimensional data visualizations. Most of this interest has been in (geo)spatial data visualization [4] [5] [6], i.e., the visualization of imaginary, proposed, or real physical environments with overlayed textual information [6] [7]. Researchers and practitioners have focused less on how to represent non-(geo)spatial data using stereoscopically perceivable multidimensional data visualizations (SPMDV).

As with all other types of interactive data visualizations (IDV), interactive SPMDV (ISPMDV) should be created with or by subject matter experts (SMEs) in order to ensure that these creations will indeed serve their intended audience well [8]. To enable cybersecurity SMEs (CSMEs) to create useful stereoscopically perceivable IDVs (SPIDVs), these CSMEs need (at least):

1) An easy-to-follow method identifying what to visualize.
2) Easy-to-configure tools for creating the visualizations proposed in (1).
3) Tools which enable ingesting data from its source (e.g., SIEM, log correlation) into the visualization created in (2).

Although (2) and (3) may be combined into one tool, the objectives of (2) and (3) are distinct; (2) focuses on data visualization (in an xR headset), while (3) deals with "translating" ingested data from its source to a preferred format that would be suitable for (2).

In this paper we will give an overview of such a method and combined tool.

II. What to Visualize and How

ISPMDV can be considered an "add-on" to SPMDV, which in turn derives from multidimensional data visualizations (MDV). While MDV on flat screens is a well-researched topic [9] [10] [11] [12], SPMDV has received broader public attention only gradually during the past ten years [13] [14] [5] [15], with the emergence of VR and MR headsets that are good enough to have enabled researchers [16] [17] [18] and practitioners [19] [20] [21] to explore their capabilities for data visualization.

Being fundamentally spatial in nature, geospatial data visualization [4] and graphs [19] have relatively straightforward implementations in SPMDV. Given that cybersecurity data is not intrinsically spatial, then for which CSME tasks would SPMDV visualizations be useful? Or rather, what kind of SPMDVs and ISPMDVs would best suit the CSME tasks, and how might these be designed? CSMEs rely on large datasets, so it stands to reason that the full use of a third dimension afforded by xR will be useful in making more data visually discernable without relying on cluttering cues like shading, occlusion, and perspective (as is needed for MDV on flat screens). Model Mapping Method for Cybersecurity (M4C) [8] is one method

that can be used to design SPMDV while enabling the CSMEs to serve as both the designers and consumers of their own visualizations. In M4C, visualizations of networked entities (e.g., computers) are positioned according to their logical (but not necessarily their physical) topology, with the resulting 3D structure(s) matching a CSME's understanding of a network's expected topology. While other methods exist [22] [23], the essence of M4C is to extract the understanding of a dataset that CSMEs use for their tasks. That extracted understanding is then used in the process of creating such an SPMDV or ISPMDV for these CSMEs, that would enable them to further explore their dataset in ways that are aligned to their internalized understanding of that dataset.

It is important to note that these visualizations cannot be created independently of the CSMEs who would be using these visualizations for their tasks. An ISPMDV may look like a fancy scene pulled from science fiction to third parties, but it must be useful for its users; otherwise, these visualizations are not worth the cost of electricity that is needed to power the equipment that is running them. For verifying effectiveness, metrics established for the evaluation of ISPMDV should be used [24].

To explain the idea of creating data-specific 3D layouts further, let's take a simplistic computer network topology and lay it out onto a three-dimensional data-shape based on the IP addresses that are used by the entities in that network.

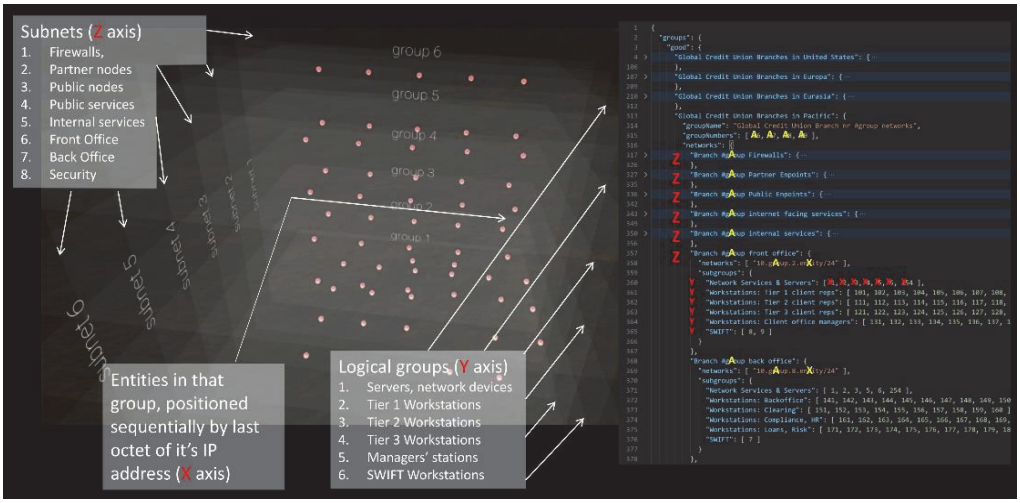


Figure 1. Networked entities arranged in a cube shape based on their functional topology; respective configuration of such data-shape shown on the right (from [25]).

A demo (mock-up) dataset consisting of an imaginary credit union's corporate and branch networks traffic (and its logical topology) is distributed with Virtual Data Explorer (VDE) [26]. We will discuss VDE in more detail in the next section, but for now, we focus on how a CSME would define a 3D layout of a dataset using VDE.

The left side of Figure 1 depicts a simplified version of the three-dimensional structure of that imaginary credit union's branch network (data-shape), with the

reddish spheres marking entities on the network. On the right side of Figure 1 is the snippet from the configuration file which VDE uses to map ingested data (in this case, observed and filtered network traffic) to spatial structures. From this vantage point, we can use the common XYZ axes to describe the Figure 1 data-shape, but it doesn't make much sense to stick with the XYZ thinking in complex constellations.

In the configuration example on the right of Figure 1:

1) the red letters Y and Z refer to the spatial positions of entities in that group in the data-shape, respectively, on the Y and Z axes,
2) the red X refers to the sequential position (on the X axis inside that group (Y)) of an entity with a matching IP address,
3) the yellow 'A's refer to group numbers (in this example, matching with the second octet of entity's IP address) and
4) yellow 'X's refer to the IP-address' last octets.

Note that the "networks" descriptor in the configuration (line 358), contains two variables – "group" and "entity". Subgroup members are mapped to the "entity" part of it (the last octet of the IP address in this case, yellow or red X), while the "group" number (line 315) refers to both the branch number (lines 317, 327, 336, etc.) and the second octet of an entity's IP address template (line 358).

Determining which subgroup contains a given entity, and determining which parameter(s) serve as the basis for this decision, is completely up to the CSME author of the visualization. This grouping is up to their perception, based on their understanding of the dataset. In this example case, these are the business functions of involved devices and their groups.

Such data-shapes representing groups of entities can then be positioned into constellations according to the CSME's understanding of the dataset that is being visualized. For example, the prerequisite knowledge needed from a CSME to create such a constellation containing a set of proposed data-shapes for depicting a computer networks functional topology would be to:

a) Understand the principles of how a computer network functions; specifically, how is such a network set up in the environment that the author of this visualization (the CSME) needs to understand.

b) Understanding the logical grouping of networked entities and their topology, but also networked entities and stakeholders' goals (e.g., corporate, employees, external {friendly, neutral, malicious} actors, etc.).

c) Understanding the expected behavior of the above actors and how it might be reflected in network data.

d) What indicators to look for, how to validate the findings, how to act with that combined knowledge.

Please refer to [8] for further information on how to design such data-shapes with CSMEs for CSMEs.

III. ISPMDV Examples

Although there are use cases for SPMDVs without user interaction, the implementation of even simple interactions can significantly accelerate a user's familiarization with visualized data. More importantly, the ability for the user to interact, select, and alter the selection of visualized (or augmented) data via queries greatly enhances the CSME's ability to learn to interpret the visualization.

It has been shown that first-time users tend to intuitively reach out to the data representations, as if to verify the existence of these artificial objects hanging in front of them [27]. Haptic feedback (using controllers), auditory cues, and realistic shaders further enhance users' immersion in an ISPMDV environment.

To create and customize ISPMDVs for CSMEs with CSMEs, Virtual Data Explorer (VDE) software was created with US Army Research Lab support [27]. VDE has three components:

1) A backend, which interprets the configurations of your network topology (json) and maps the ingested data according to that config into groups (of groups (of groups (of groups))) of entities.
2) A browser plugin, which helps in feeding the data from a Moloch, SIEM or custom log correlation tool as appropriate (say, after running a query), via a WebSocket to the VDE backend.
3) A headset (Magic Leap, Oculus, MS Mixed Reality, HTC Vive, HoloLens 2), which gets the set of groups from the backend and positions these for the viewer according to the selected layout configuration (json).

Unity 3D is used to create the software responsible for the ISPMDV in the headsets, C# is used for the backend, and JavaScript is used for the browser plugin.

Due to the medium on which you are reading this paper being flat (a screen or a physical piece of paper), it is impossible to convey here the "spatialness" of ISPMDV with figures. The next-best option to observing ISPMDV examples directly in xR are first-person videos of users interacting with an ISPMDV; for these, please visit coda.ee/JDST. Below are a few screenshots from video captures of VR and MR sessions, where the user either explores or interacts with an ISPMDV.

A. NATO CCDCOE CDX Locked Shields

To test the utility of ISPMDV when encoding non-spatial data, networked entities that were found to be present in NATO CCDCOE Locked Shields Cyber Defence eXercise (LS) [28] network traffic were spatially positioned as semi-transparent spheres, according to entities' positions in that (Blue Team's) network's functional topology, and, more importantly, entities' affiliation with logical groups present in LS networks. Logical groups could be distinguished by their members' functionality (e.g., SCADA components), purpose (e.g., DMZ servers), risk exposure, operating system, etc. (see Figure 2). This resulted in custom 3D data-shapes that were combined into a constellation (a VDE layout) representing a larger whole of the LS network(s). Constellations shown in Figures 3-5 depict LS network traffic with

VDE (in VR or MR), while Figures 6 and 7 use a slightly more primitive approach with OpenGraphiti (in VR).

LS traffic was chosen for testing purposes due to the complexity of its network and because the first author, having been involved with LS since 2010, has a deep understanding of that network's topology and its components' expected behavior.

Network topology (positions of groups of groups of groups of nodes), displayed as spheres and cubes, is overlayed with network traffic, visualized as lines (edges) rendered as connecting the nodes that were observed to have initiated or received network connections (sessions) during a time window. Which edges are visible, their opacity, and their coloring depend on the results of the underlying query that was executed once the user defined the time window and other query parameters (e.g. ASN, IP range, ports used, and amount of data transferred).

Figure 2: VR view of Locked Shields 18 Partner Run, focus on 11th Blue Team's networks (refer to config example, from line 313 onward, in Figure 1): subnets' labels are visible above the blades ("Blue Team 11 Firewalls," "Threod drone ground station …," etc.), that contain groups of entities ("OSX in INT network," "Services in INT network," etc.), that, in turn, contain spheres representing individual entities (IP address) of that group.

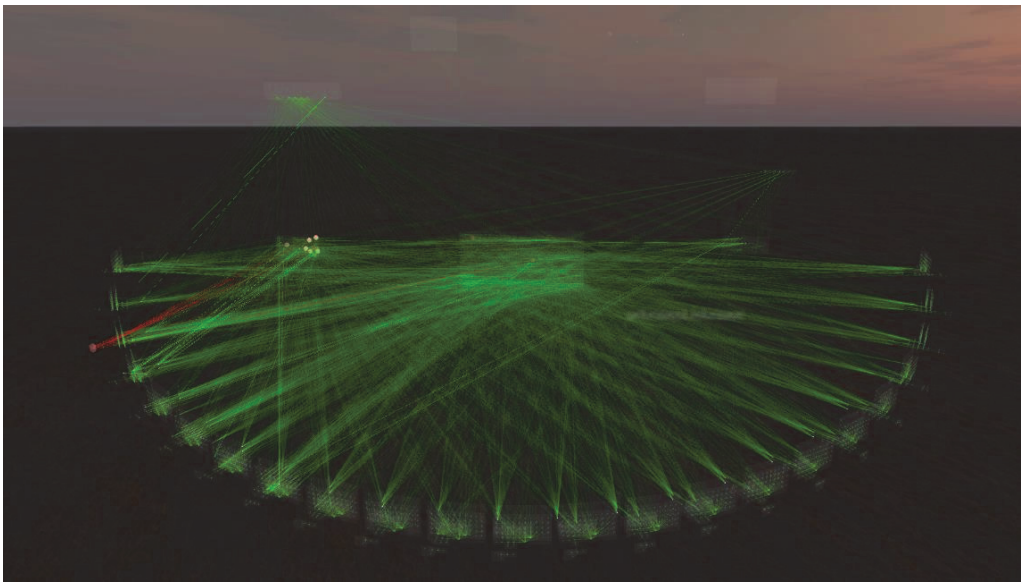


Figure 3: VR view of Locked Shields 18 Partner Run network topology and network traffic using VDE, displaying an overall view of the meta-shape: a data-shape consisting of multiple data-shapes. Red edges represent selected connections between Blue Team 3 device and Red Team nodes. A detailed description of this layout can be found in [21].

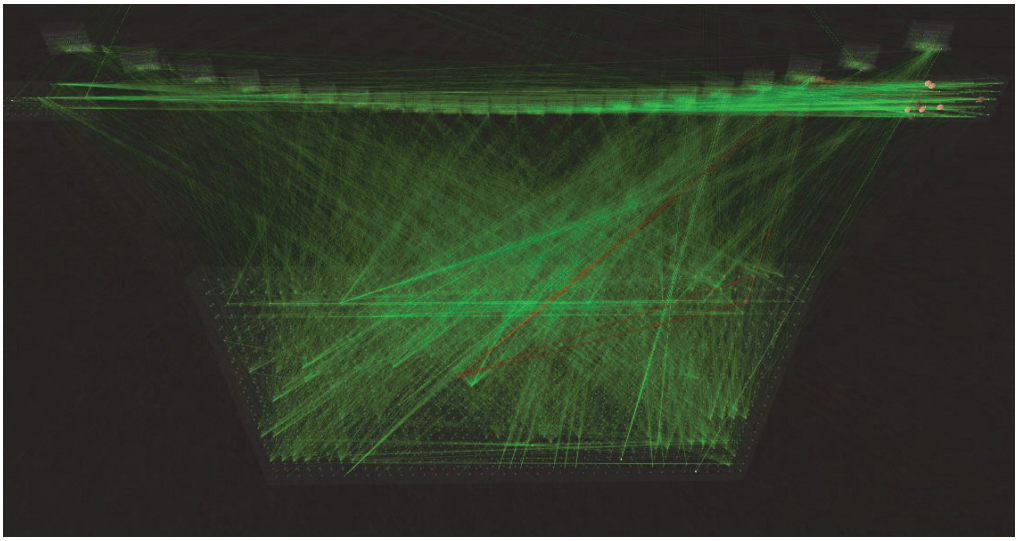


Figure 4: VR view of Locked Shields 18 Partner Run network topology and network traffic using VDE, shown from the other side of the meta-shape, where the data-shape consisting of unknown entities is in foreground (lower side of this screenshot), while Blue Teams' networks are positioned farther away (on the upper side of this screenshot). Some edges and entities have been selected and are rendered red instead of the default green [21].

Two distinct datasets are combined in such an ISPMDV: a logical topology of the entities that are expected to be active in the network (i.e., the positions of nodes representing those entities) and the observed network traffic.

Feedback from analysts on the ISPMDV shown in Figures 2-4 is covered in [27]. Overall, the impressions of stereoscopically perceivable 3D data visualizations were highly favorable, with multiple participants acknowledging that such 3D visualizations of network topology could assist in their understanding of the networks they use daily. Study participants expressed a wish to integrate such visualization capabilities in their workflow. Videos of VR and MR sessions with VDE, as well as some prior conference presentations featuring that tool, are available at coda.ee/JDST.

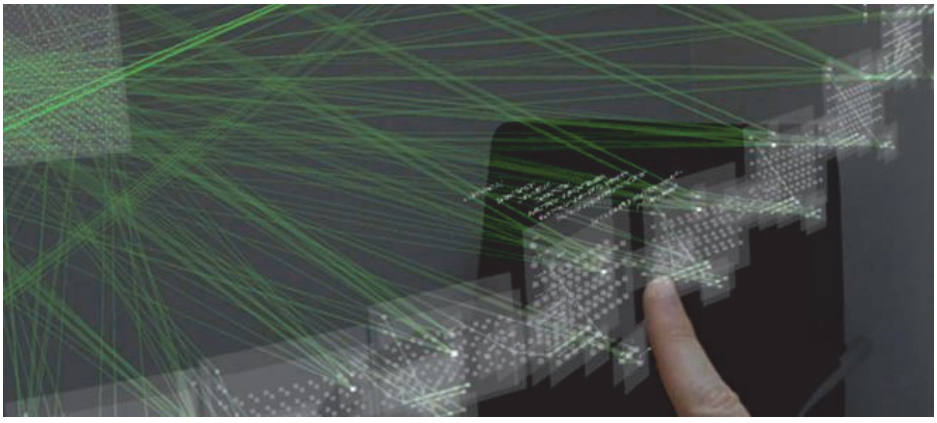


Figure 5: MR view of Locked Shields 18 Partner Run network topology and network traffic using VDE. A user's index finger is selecting a Blue Team's network [21].

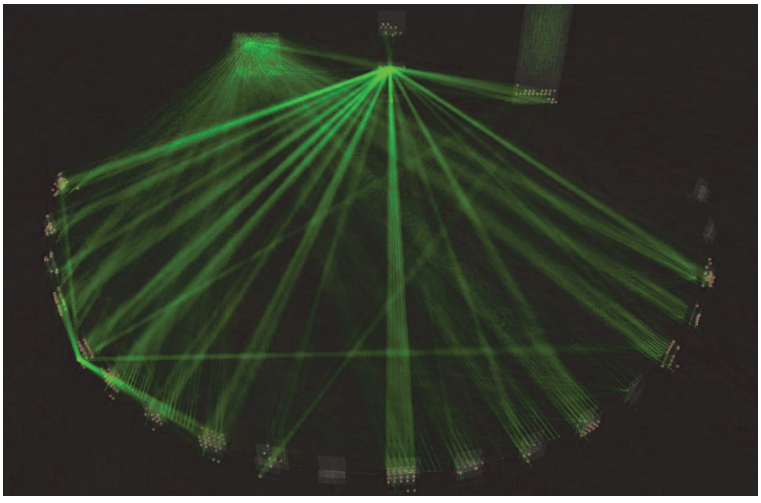


Figure 6: VR view of Locked Shields 16 network topology and traffic using VDE. Notice the slightly different constellation layout compared to Figures 2 - 5 [29]**.**

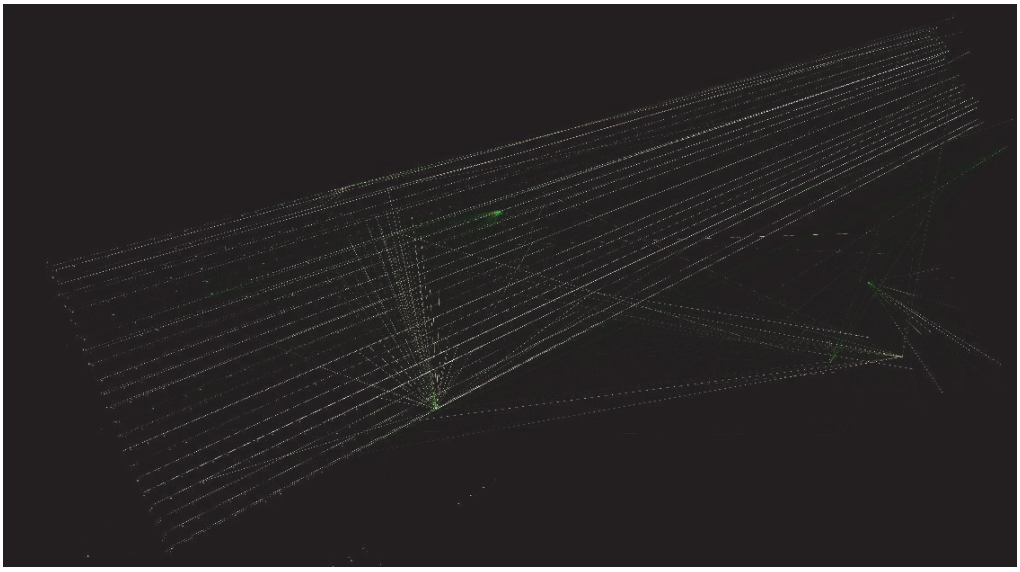


Figure 7: VR view of Locked Shields 16 network topology and traffic using OpenGraphiti. Blue Teams' networks are aligned onto "blades" consisting of subnets, while nodes are positioned on a line sequentially, according to their last octet.

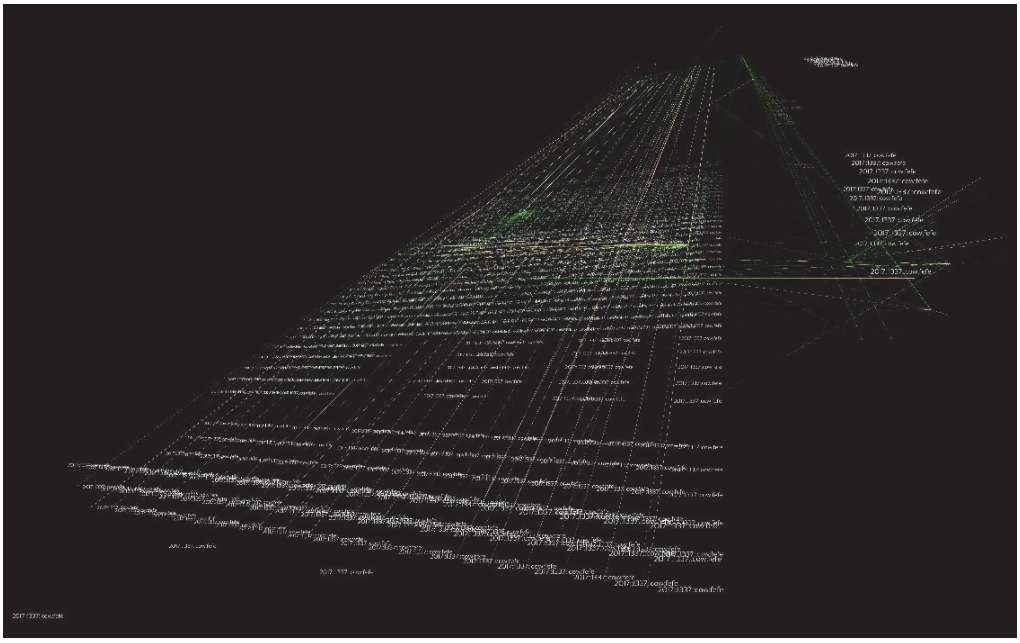


Figure 8: VR view of Locked Shields 16 network topology and traffic using OpenGraphiti. Such layouts are simple to create from network traffic and are useful for initial exploration

of a dataset's topology (after or together with graphs), but are too messy for spotting more subtle anomalies.

B. VDE Demo Dataset

The lack of a public dataset containing the traffic of a computer network with sufficiently complex topology motivated the creation of a mock-up dataset of an imaginary credit union (CU) to showcase a possible network topology ISPMDV, which was then modeled in VDE. This mock-up CU dataset features a financial institution with operations on multiple continents and countries, with multiple branches in each of those, where the branches have standardized, but distinctly populated, internal networks.

Figures 9-14 are screenshots from a VDE v2 VR session, exploring the ISPMDV of the mock-up CU dataset. Video of this exploration was presented at MAVRIC 2020 [25], a VDE v2 demo build is available to experience it in VR [26] and VDE is also included in the NASA MRET open source toolset [6].

In this ISPMDV, subnets of branch networks are grouped to cubes (see internals of that data-shape in Figure 11) which are then stacked vertically based on the organizational group to which that branch belongs (e.g., country, continent). The vertical branch groups are then positioned on a ⅔ circle (Figure 10), with groups containing public services facing the center or the circle. In the center of the ISPMDV are three other groups:

a) known entities (corporate net, partners, etc.),
b) known threats (IP addresses from threat feeds, prior compromises, etc.),
c) unknown IPs.

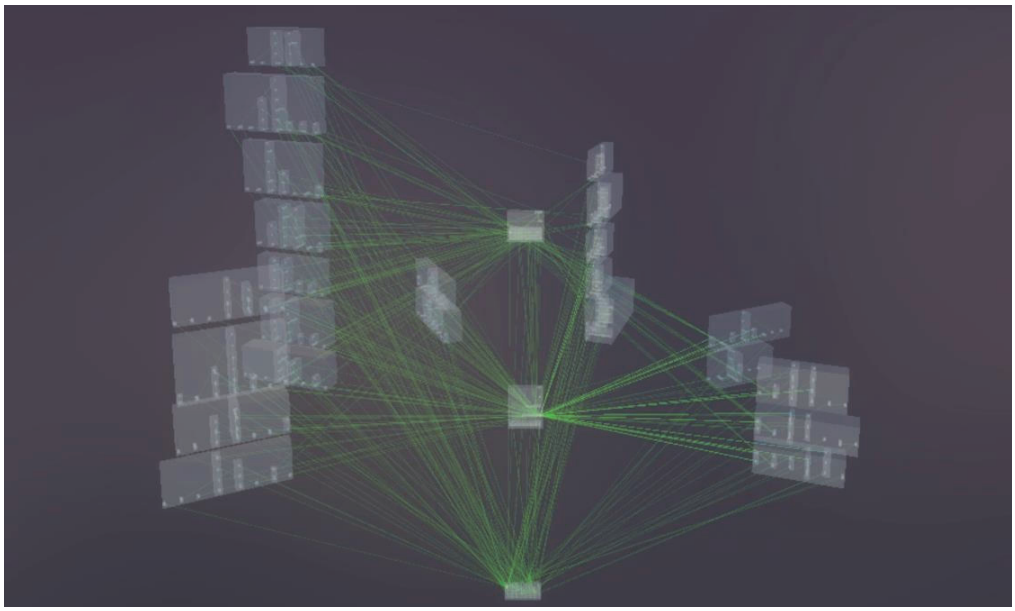


Figure 9: VDE VR sessions of exploring an imaginary CU network's ISPMDV, arranged as a constellation of data-shapes representing the functional topology of that network, overlaid with network traffic.

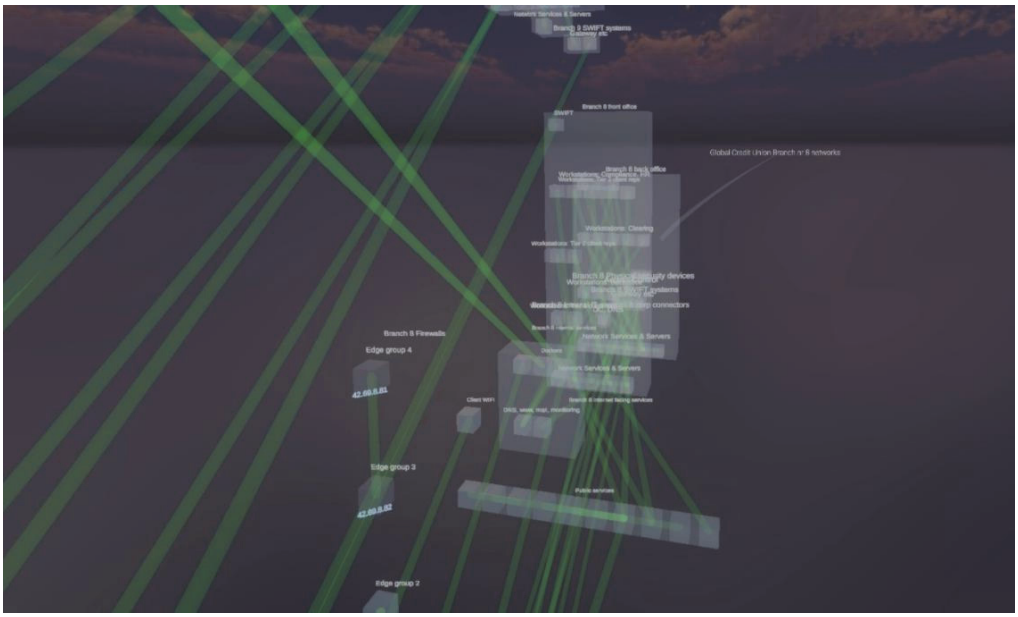


Figure 10: When the user moves the viewpoint closer to one of the data-shapes representing a CU branch network, the outer (cube) shell disappears, while labels of internal groups are activated. Labels of nodes (transparent cubes) are activated only once the user is close enough and are kept facing the user for readability.

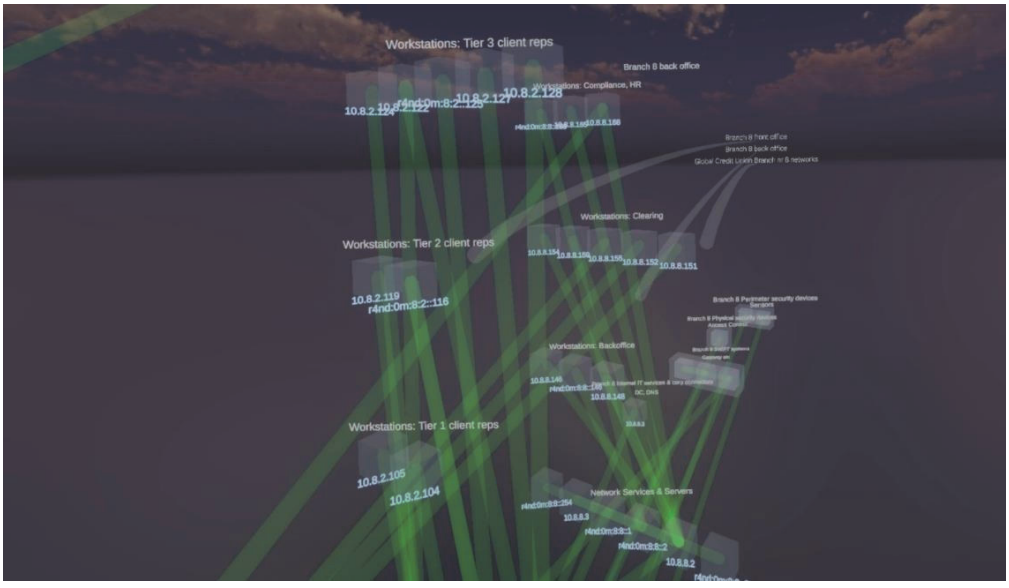


Figure 11: Although subgroup outer shells disappear once the user is close enough (to reduce visual clutter and let the user to focus on individual entities / nodes), subgroups labels (e.g., "Workstations: Backoffice") are kept visible above those, and groups labels (e.g., "Branch 8 front office") are activated based on the direction of the user's gaze.

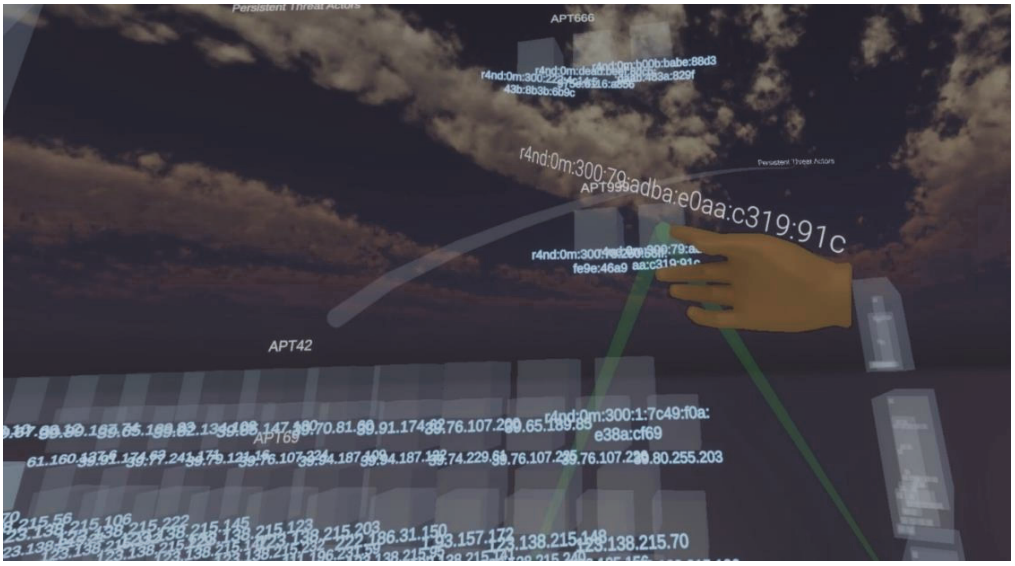


Figure 12: The user can select nodes either (1) from afar, with a pointer or (2) by touching them with their virtual index finger (rendered based on inputs from a VR controller). The selected node's name (in this case, the IP address) is displayed next to the VR hand. The node's incoming and outgoing edges are kept visible while other edges are disabled.

Figure 13: Edges (representing an observed network session) are highlighted when touched, with the corresponding source and destination nodes' names appearing above the user's hand. A single line of text is attached to the hand, avoiding the clutter which a head-up display would have caused. User studies have shown this to be an intuitive feature of the interface.

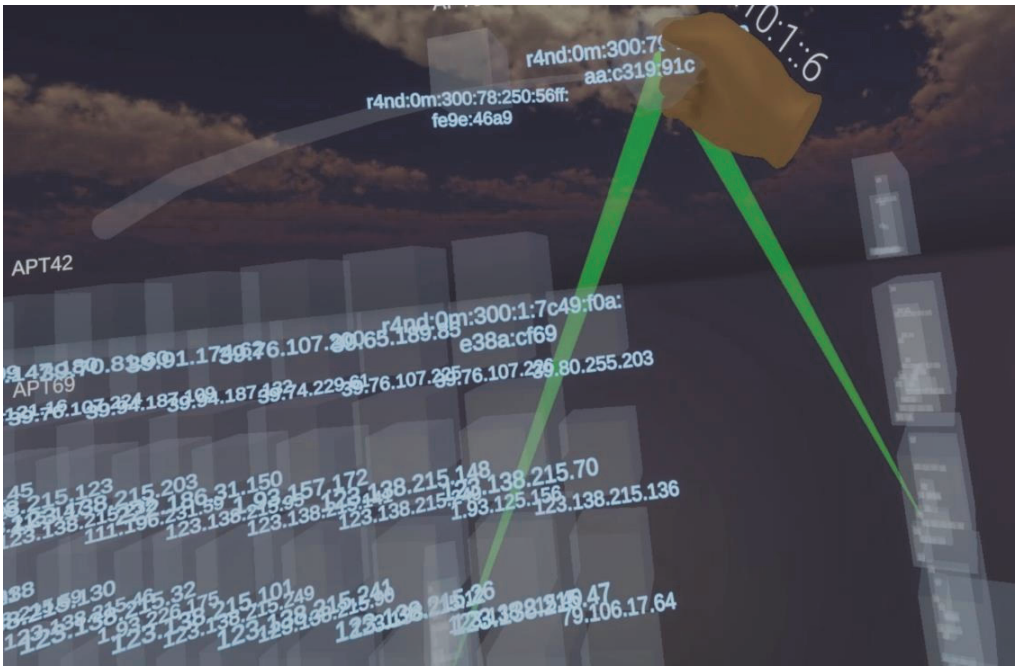


Figure 14: The user can grab a node and move it around, to better perceive the location of the targets and sources of its connections (i.e., terminal points of the edges are easier to spot this way).

The demo build of VDE containing the ISPMDV shown on Figures 9-14 could be used for further studies of user interaction. Together with the VDE server component, VDE can be used to visualize data ingested from SIEM, log correlation, or other data sources' APIs. Please feel free to reach out to the authors to discuss academic research collaboration.

VI. Conclusions

While SPMDVs for intrinsically spatial data have received substantial publicity, the creation, presentation, and usability research of SPMDVs and ISPMDVs designed to show non-spatial data has attracted less attention. In this paper, we explored three distinct ISPMDV examples, all rendered with VDE, with each being used to visualize computer network traffic and topology.

We encourage cybersecurity professionals and researchers to use emerging technologies (e.g., xR HMDs) to explore novel ways for visualizing datasets relevant

to their problems and tasks. The examples provided in this paper are just modest illustrations of what is already possible with existing tools (see [26] [16] [20] [19] [6] and others) and should be used for inspiration.

Appropriate methods (e.g., [8], [24]) should be used when creating ISPMDVs to ensure the utility of the resulting visualization for the CSMEs who would be using them.

ACKNOWLEDGEMENTS

The authors thank Alexander Kott, Jennifer A. Cowley, Lee C. Trossbach, Matthew C. Ryan, Jaan Priisalu, and Olaf Manuel Maennel for their ideas and guidance. This research was partly supported by the Army Research Laboratory under Cooperative Agreement Number W911NF-17-2-0083 and in conjunction with the CCDC Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.

REFERENCES

[1] Unity Technologies, "Definition of: Virtual Reality (VR)," [Online]. Available: https://unity3d.com/what-is-xr-glossary#paragraph70. [Accessed 2021].

[2] Unity Technologies, "Definition of: Augmented Reality (AR)," [Online]. Available: https://unity3d.com/what-is-xr-glossary#paragraph12. [Accessed 2021].

[3] Unity Technologies, "Definition of: Mixed Reality (MR)," [Online]. Available: https://unity3d.com/what-is-xr-glossary#paragraph42. [Accessed 2021].

[4] S. Skolnik, "Using Virtual Reality to Visualize Disasters, Climate, and Extreme Weather Impacts Shayna Skolnik," in MAVRIC, College Park, 2020.

[5] C. Hurter, Image-Based Visualization: Interactive Multidimensional Data Exploration, N. Elmqvist and D. Ebert, Eds., Morgan & Claypool, 2016.

[6] National Aeronautics and Space Administration, "Collaborative Mixed-Reality Engineering Tool (MRET)," [Online]. Available: https://techport.nasa.gov/view/95677. [Accessed 2021].

[7] A. Kabil, T. Duval and N. Cuppens, "Alert Characterization by Non-expert Users in a Cybersecurity Virtual Environment: A Usability Study," in International Conference on Augmented Reality, Virtual Reality and Computer Graphics, Lecture Notes in Computer Science, 2020.

[8] K. Kullman, L. Buchanan, A. Komlodi and D. Engel, "Mental Model Mapping Method for Cybersecurity," in 22nd International Conference On Human-Computer Interaction, Copenhagen, 2020.

[9] C. Ware and G. Franck, "Evaluating Stereo and Motion Cues for Visualizing Information Nets in Three Dimensions," ACM Transactions on Graphics, vol. 15, no. 2, pp. 121-140, 4 1996.

[10] J.-P. van Riel and B. Irwin, "InetVis, a Visual Tool for Network Telescope Traffic Analysis," in AFRIGRAPH 2006, Cape Town, 2006.

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

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

[13] H. S. Smallman, M. St. John, H. M. Oonk and M. B. Cowen, "Information availability in 2D and 3D displays," IEEE Computer Graphics and Applications, vol. 21, no. 5, pp. 51-57, 2001.

[14] M. Teräs and S. Raghunathan, "Big Data Visualisation in Immersive Virtual Reality Environments: Embodied Phenomenological Perspectives to Interaction," ICTACT Journal on Soft Computing, vol. 05, no. 04, pp. 1009-1015, 2015.

[15] A. Kabil, T. Duval, N. Cuppens, G. L. Comte, Y. Halgand and C. Ponchel, "Why should we use 3D Collaborative Virtual Environments for Cyber Security?," in IEEE Fourth VR International Workshop on Collaborative Virtual Environments, Reutlingen, 2018.

[16] M. Cordeil, A. Cunningham, B. Bach, C. Hurter, B. H. Thomas, K. Marriott and T. Dwyer, "IATK: An Immersive Analytics Toolkit," in IEEE Conference on Virtual Reality and 3D User Interfaces (VR), Osaka, 2019.

[17] A. Batch, A. Cunningham, M. Cordeil, N. Elmqvist, T. Dwyer, B. H. Thomas and K. Marriott, "There Is No Spoon: Evaluating Performance, Space Use, and Presence with Expert Domain Users in Immersive Analytics," IEEE Transactions on Visualization and Computer Graphics, vol. 26, no. 1, pp. 536 - 546, 2020.

[18] S. Beitzel, J. Dykstra, P. Toliver and J. Youzwak, "Exploring 3D Cybersecurity Visualization with the Microsoft HoloLens," in International Conference on Applied Human Factors and Ergonomics, 2017, 2017.

[19] T. Reuille, S. Hawthorne, A. Hay, S. Matsusaki and C. Ye, "OpenDNS Data Visualization Framework," 2015. [Online]. Available: http://www.opengraphiti.com/.

[20] 3Data, "Advanced Analytics for SecOps," 3Data, [Online]. Available: https://3data.io/solutions-cybersecurity/. [Accessed 01 2021].

[21] M. Ryan, K. Kullman and L. Trossbach, "VR/MR Supporting the Future of Defensive Cyber Operations," in NATO Computer Aided Analysis, Exercise, Experimentation Forum., Paris, 2019.

[22] Y. Seong, J. Nuamah and S. Yi, "Guidelines for Cybersecurity Visualization Design," in IDEAS 2020, Seoul, South Korea, 2020.

[23] C. Zhong, A. Alnusair, B. Sayger, A. Troxell and J. Yao, "AOH-Map: A Mind Mapping System for Supporting Collaborative Cyber Security Analysis," in 2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), Las Vegas, 2019.

[24] D. J. Clark and B. P. Turnbull, "Experiment Design for Complex Immersive Visualisation," in Conference: Military Communications and Information Systems Conference (MilCIS) 2020, Canberra, 2020.

[25] K. Kullman, "Creating Useful 3D Data Visualizations for Cybersecurity," in MAVRIC, College Park, MD, 2020.

[26] K. Kullman, "Virtual Data Explorer," Cognitive Data OÜ, [Online]. Available: https://coda.ee/getvde.

[27] 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.

[28] The NATO Cooperative Cyber Defence Centre of Excellence, "Locked Shields Cyber Defence eXercise," [Online]. Available: https://ccdcoe.org/exercises/locked-shields/.

[29] 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.

Appendix 6

Publication VI

Kullman, Kaur; Engel, Don; (2022). User Interactions in Virtual Data Explorer. Augmented Cognition in Cyber Security, 24th International Conference on Human-Computer Interaction. DOI: 10.1007/978-3-031-05457-0_26

User Interactions in Virtual Data Explorer

Kaur Kullman[1,2(✉)] and Don Engel[1]

[1] University of Maryland, Baltimore County, Baltimore, MD 21250, USA
donengel@umbc.edu
[2] Tallinn University of Technology, 12616 Tallinn, Estonia
hcii@coda.ee

Abstract. Cybersecurity practitioners face the challenge of monitoring complex and large datasets. These could be visualized as time-varying node-link graphs, but would still have complex topologies and very high rates of change in the attributes of their links (representing network activity). It is natural, then, that the needs of the cybersecurity domain have driven many innovations in 2D visualization and related computer-assisted decision making. Here, we discuss the lessons learned while implementing user interactions for Virtual Data Explorer (VDE), a novel system for immersive visualization (both in Mixed and Virtual Reality) of complex time-varying graphs. VDE can be used with any dataset to render its topological layout and overlay that with time-varying graph; VDE was inspired by the needs of cybersecurity professionals engaged in computer network defense (CND).

Immersive data visualization using VDE enables intuitive semantic zooming, where the semantic zoom levels are determined by the spatial position of the headset, the spatial position of handheld controllers, and user interactions (UIa) with those controllers. This spatially driven semantic zooming is quite different from most other network visualizations which have been attempted with time-varying graphs of the sort needed for CND, presenting a broad design space to be evaluated for overall user experience (UX) optimization. In this paper, we discuss these design choices, as informed by CND experts, with a particular focus on network topology abstraction with graph visualization, semantic zooming on increasing levels of network detail, and semantic zooming to show increasing levels of detail with textual labels.

Keywords: User interactions · Virtual reality · Mixed reality · Network visualization · Topology visualization · Data visualization · Cybersecurity

The material is based upon work supported by NASA under award number 80GSFC21M0002.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
D. D. Schmorrow and C. M. Fidopiastis (Eds.): HCII 2022, LNAI 13310, pp. 333–347, 2022.
https://doi.org/10.1007/978-3-031-05457-0_26

1 Introduction

This work follows a large volume of prior research done on 3D user interactions [3,6,10,24], immersive analytics [1,4,5,18] and the combination of the two [9,17,21,23]. Although the task-specific layout of an immersive data visualization is arguably the most important aspect determining its utility [15], non-intrusive and intuitive user interfaces (UI) and overall user experiences (UX) are also important in determining the usability and utility of an immersive data visualization. In this paper, we report on the applicability of various user interaction (UIa) methods for immersive analytics of node-link diagrams.

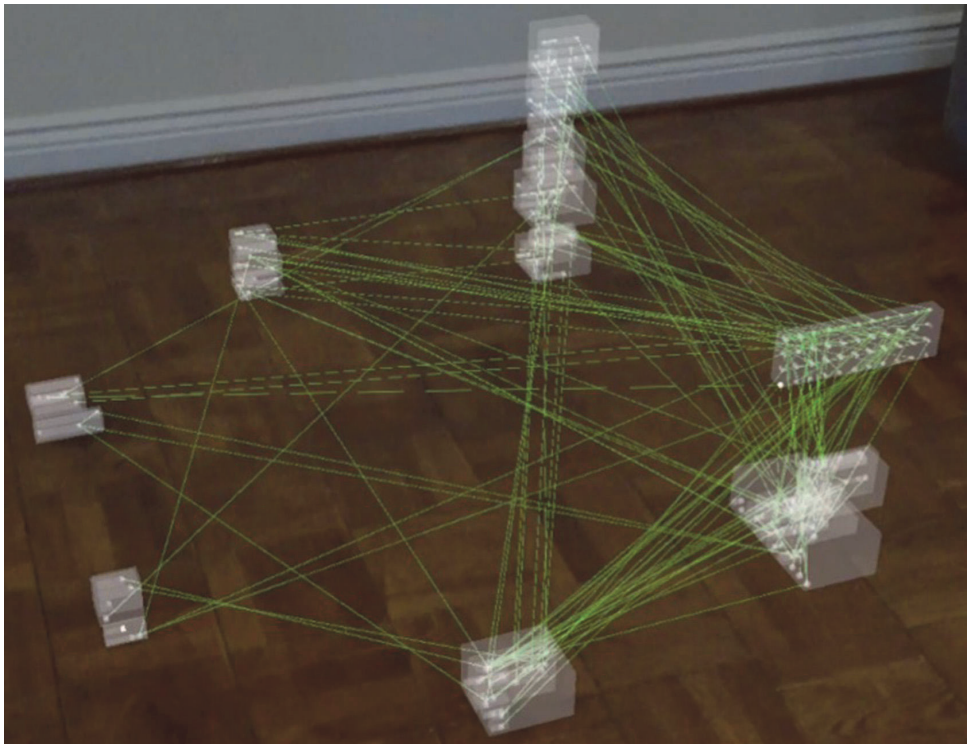


Fig. 1. A computer network's topology visualized with VDE, using a Mixed Reality headset.

Work on Virtual Data Explorer (VDE, Fig. 1) started in 2015, initially as a fork of OpenGraphiti and then rebuilt from scratch as a Unity 3D project [14]. One of the factors that motivated the transfer away from OpenGraphiti at the time was its lack of support for user interactions in virtual reality, which became a particularly significant omission when Oculus Touch controllers were released in late 2016 which enabled sufficiently precise user interactions to be implemented with Unity 3D. User feedback solicited from early VDE users motivated various alterations and additions to the interactions implemented for virtual and mixed reality in VDE.

2 Objective

Encoding information into depth cues while visualizing data has been avoided in the past for a good reason: on a flat screen, it's not helpful [19]. Nevertheless, recent studies have confirmed [23] that with equipment that provides the user with stereoscopic perception and parallax, three-dimensional shapes can be useful in providing users with insight into the visualized dataset [12]. Additionally, researchers have found that test subjects managed to gather data and to understand the cyber situation presented to them only after few sessions with great performance scores, even if the task seemed difficult to them on the first try [8].

The motivating factors for creating VDE were the challenges that cyber defense analysts, cyber defense incident responders, network operations specialists, and related professionals face while analyzing the datasets relevant to their tasks. Such datasets are often multidimensional but not intrinsically spatial. Consequently, analysts must either scale down the number of dimensions visible at a time for encoding into a 2D or 3D visualization, or they must combine multiple visualizations displaying different dimensions of that dataset into a dashboard. The inspiration for VDE was the hope that immersive visualization would enable the 3D encoding of data in ways better aligned to subject matter experts' (SMEs') natural understanding of their datasets' relational layout, better reflecting their mental models of the multilevel hierarchical relationships of groups of entities expected to be present in a dataset and the dynamic interactions between these entities [13].

Therefore, the target audience for the visualizations created with VDE are the SMEs responsible for ensuring the security of networks and other assets. SMEs utilize a wide array of Computer Network Defense (CND) tools, such as Security Information & Event Management (SIEM) systems which allow data from various sources to be processed and for alerts to be handled [15]. CND tools allow analysts to monitor, detect, investigate, and report incidents that occur in the network, as well as provide an overview of the network state. To provide analysts with such capabilities, CND tools depend on the ability to query, process, summarize and display large quantities of diverse data which have fast and unexpected dynamics [2]. These tools can be thought of along the lines of the seven human-data interaction task levels defined by Shneiderman [22]:

1. Gaining an overview of the entire dataset,
2. Zooming in on an item or subsets of items,
3. Filtering out irrelevant items,
4. Getting details-on-demand for an item or subset of items,
5. Relating between items or subset of items,
6. Keeping a history of actions, and
7. Allowing extraction of subsets of items and query parameters.

These task levels have been taken into account while developing VDE and most have been addressed with its capabilities. When appropriate, Shneiderman's task levels are referred to by their sequential number later in this paper.

3 Virtual Data Explorer

VDE enables a user to stereoscopically perceive a spatial layout of a dataset in a VR or MR environment (e.g., the topology of a computer network), while the resulting visualization can be augmented with additional data, like TCP/UDP/ICMP session counts between network nodes [16]. VDE allows its users to customize visualization layouts via two complimentary text configuration files that are parsed by the VDE Server and the VDE Client.

To accommodate timely processing of large query results, data-processing in VDE is separated into a server component (VDES). Thread-safe messaging is used extensively - most importantly, to keep the Client (VDEC) visualization in sync with (changes in) incoming data, but also for asynchronous data processing, for handling browser-based user interface actions, and in support of various other features.

A more detailed description of VDE is available at [11].

3.1 Simulator Sickness

Various experiments have shown that applying certain limitations to a user's ability to move in the virtual environment - limit their view and other forms of constrained navigation - will limit confusion and help prevent simulator sickness while in VR [7]. These lessons were learned while developing VDE and adjusted later, as others reported success with the same or similar mitigation efforts [20]. Most importantly, if an immersed user can only move the viewpoint (e.g., its avatar) either forwards or backwards in the direction of user's gaze (or head-direction), the effects of simulator sickness can be minimized or avoided altogether [12]. This form of constrained navigation in VR is known as "the rudder movement" [20].

3.2 Virtual or Mixed Reality

Although VDE was initially developed with Virtual Reality headsets (Oculus Rift DK2 and later CV1 with Oculus Touch), its interaction components were always kept modular so that once mixed reality headsets such as the Meta 2, Magic Leap, and Hololens became available, their support could be integrated into the same codebase.

The underlying expectation for preferring MR to VR is the user's ability to combine stereoscopically perceivable data visualizations rendered by a MR headset with relevant textual information represented by other sources in the user's physical environment (SIEM, dashboard, or another tool), most likely from flat screens. This requirement was identified from early user feedback that

trying to input text or define/refine data queries while in VR would be vastly inferior to the textual interfaces that users are already accustomed to operating while using conventional applications on a flat screen for data analysis. Hence, rather than spend time on inventing 3D data-entry solutions for VR, it was decided to focus on creating and improving stereoscopically perceivable data layouts and letting users use their existing tools to control the selection of data that is then fed to the visualization.

A major advantage provided by the VR environment, relative to MR, is that VR allows users to move (fly) around in a larger scale (overview) visualization of a dataset while becoming familiar with its layout(s) and/or while collaborating with others. However, once the user is familiar with the structure of their dataset, changing their position (by teleporting or flying in VR space) becomes less beneficial over time. Accordingly, as commodity MR devices became sufficiently performant, they were prioritized for development - first, the Meta 2, later followed by support for the Magic Leap and HoloLens.

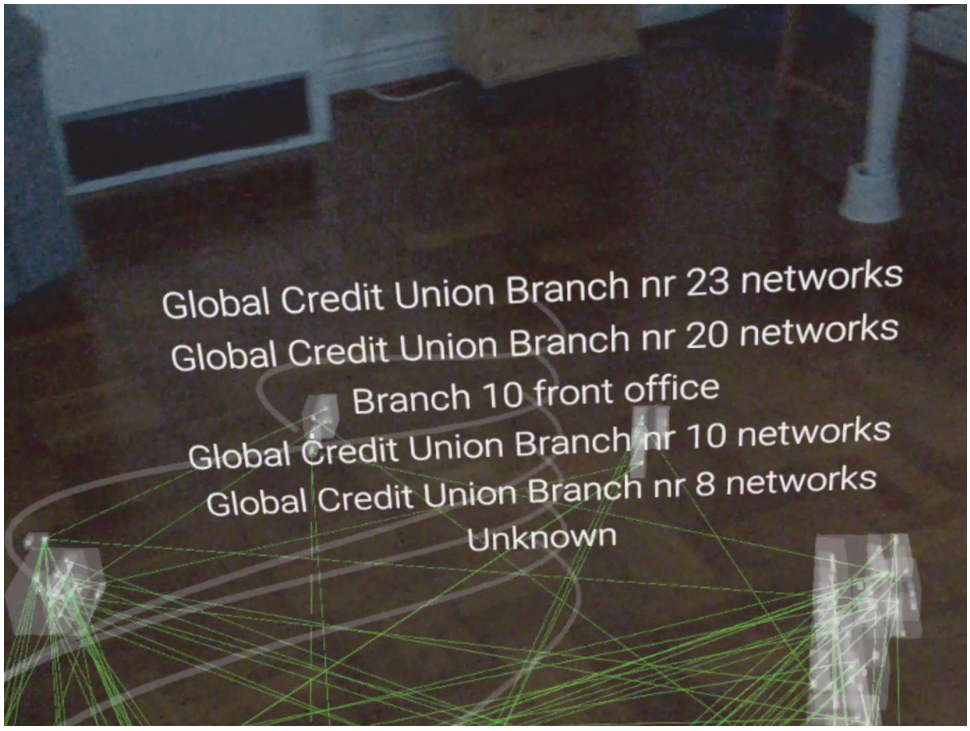


Fig. 2. Head-Up Display showing labels of visualized groups that the user focuses on, retaining visual connections to those with Bézier curves. HUD is used also for other interaction and feedback purposes.

3.3 User Interface

In the early stages of VDE development on Unity 3D, efforts were made to either use existing VR-based menu systems (VRTK, later MRTK) or to design a native menu, such that would allow the user to control which visualization components are visible and/or interactive; to configure connection to VDE Server; to switch between layouts; and to exercise other control over the immersive environment. However, controlling VDE's server and client behavior, including data selection and transfer, turned out to be more convenient when done in combination with the VDES web-based interface and with existing conventional tools on a flat screen. For example, in case of cybersecurity related datasets, the data source could be a SIEM, log-correlation, netflow, or PCAP analyzing environments.

3.4 Head-Up Display

Contextual information is displayed on a head-up display (HUD) that is perceived to be positioned a few meters away from the user in MR and about 30m in VR. The HUD smoothly follows the direction of user's head in order to remain in the user's field of view (see Fig. 2). This virtual distance was chosen to allow a clear distinction between the HUD and the network itself, which is stereoscopically apparent as being nearer to the user.

3.5 User Interactions

The ability to interact with the visualization, namely, to query information about a visual representation of a datapoint (ex: semi-transparent cube for a node or line for a relation between two nodes) using input devices (ex: hand- and finger-tracking, input controllers) is imperative. While gathering feedback from SMEs [12], this querying capability was found to be crucial for the users' immersion in the VR data visualization to allow them to explore and to build their understanding of the visualized data.

The MR or VR system's available input methods are used to detect whether the user is trying to grab something, point at a node, or point at an edge. In case of MR headsets, these interactions are based on the user's tracked hands (see: Fig. 3 and Fig. 4), and in case of VR headsets, pseudo-hands (see: Fig. 5 Fig. 6) are rendered based on hand-held input controllers.

A user can:

1. point to select a visual representation of a data-object - a node (for example, a cube or a sphere) or an edge - with a "laser" or dominant hand's index finger of either the virtual rendering of the hand or users real hand tracking results (in case of MR headsets). Once selected, detailed information about the selected object (node or edge) is shown on a line of text rendered next to user's hand, (Shneiderman Task Level 4).
2. grab (or pinch) nodes and move (or throw) these around to better perceive its relations by observing the edges that are originating or terminating in that node: humans perceive the terminal locations of moving lines better than that of static ones, (Shneiderman Task Levels 3, 5).

3. control data visualization layout's properties (shapes, curvature, etc.) with controller's analog sensors, (Shneiderman Task Levels 1, 5).
4. gesture with non-dominant hand to trigger various functionalities. For example: starfish - toggle the HUD; pinch both hands - scale the visualization; fist - toggle edges; etc.

In addition to active gestures and hand recognition, the user's position and gaze (instead of just their head direction) are used if available to decide which

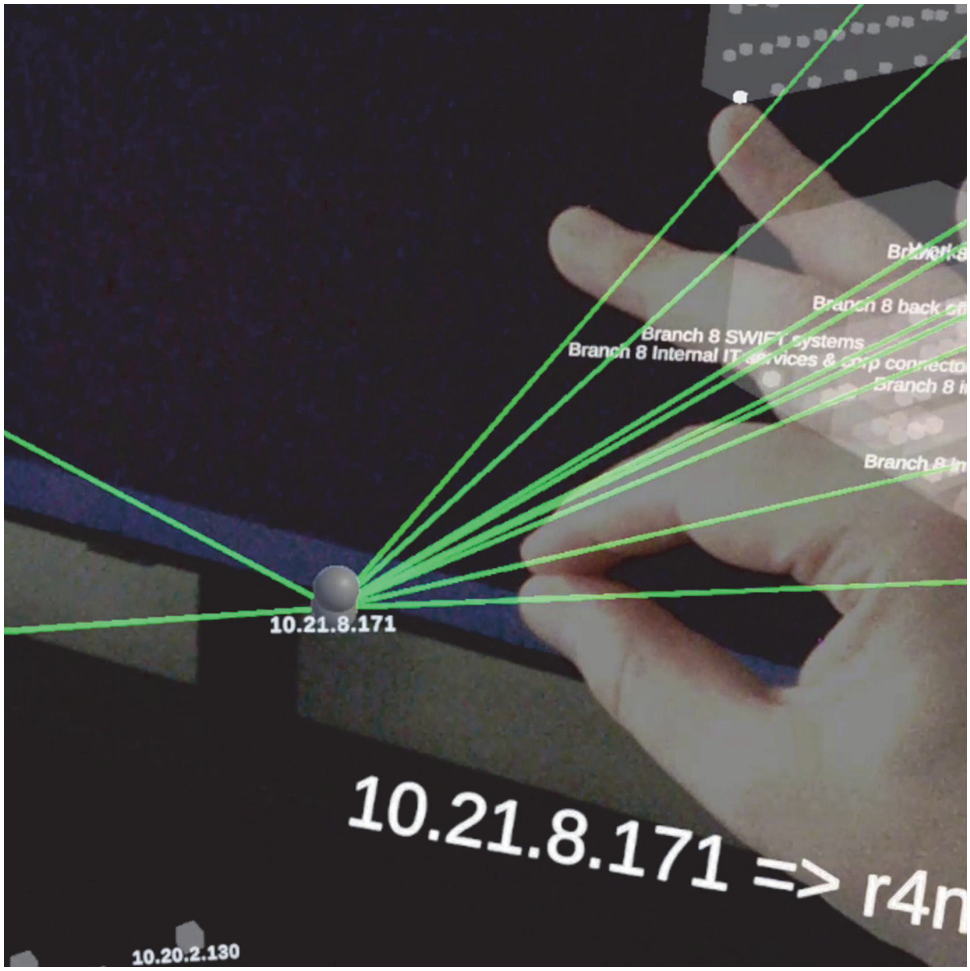


Fig. 3. In an MR environment, the user pinches a node, that is sized accordingly, to move that around and explore its relations. Notice the two gray spheres indicating the location, where the MR device (Magic Leap) perceives the tips of user's thumb and index finger to be: due to the device' lack of precision, these helper-markers are used to guide the user. Note that the distortion is further aggravated by to the way the device records the video and overlays the augmentation onto it. For comparison with Virtual Reality view, please see Fig. 5.

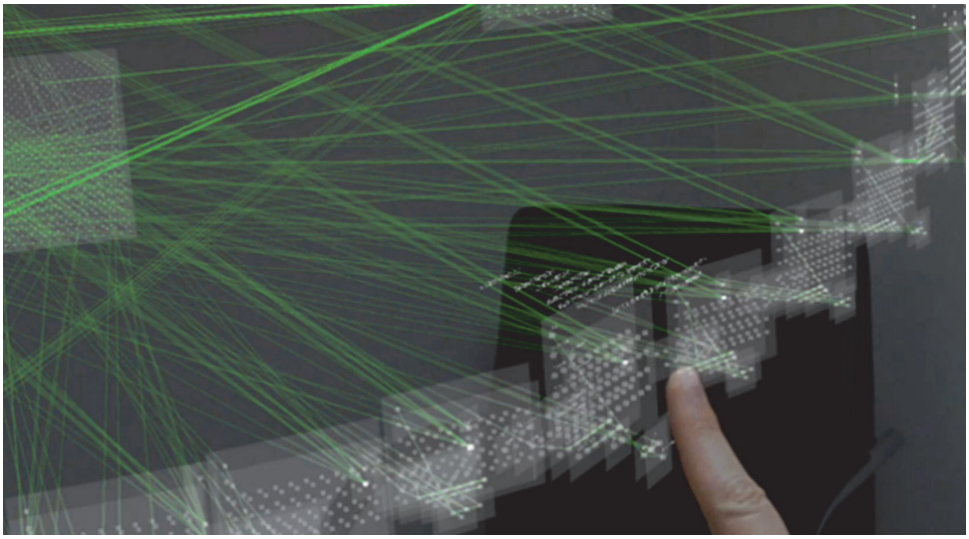


Fig. 4. MR view of Locked Shields 18 Partner Run network topology and network traffic visualization with VDE; user is selecting a Blue Team's network's visualization with index finger to have it enlarged and brought into the center of the view. Please see the video accompanying this paper for better perception: https://coda.ee/HCII22

visualization sub-groups to focus on, to enable textual labels, to hide enclosures, to enable update routines, colliders, etc. (Shneiderman Task Levels 2, 3, 4, 5, 7). Therefore, depending on user's direction and location amongst the visualization components and on the user's gaze (if eye-tracking is available), a visualization's details are either visible or hidden, and if visible, then either interactive or not.

The reasons for such a behavior are threefold:

1. Exposing the user to too many visual representations of the data objects will overwhelm them, even if occlusion is not a concern.
2. Having too many active objects may overwhelm the GPU/CPU of a standalone MR/VR headset - or even a computer rendering into a VR headset - due to the computational costs of colliders, joints, or other physics. (see "Optimizations" section, below)
3. By adjusting their location (and gaze), the user can:
   (a) See an overview of the entire dataset (Shneiderman Task Level 1),
   (b) Zoom on an item or subsets of items (Shneiderman Task Level 2),
   (c) Filter irrelevant items (Shneiderman Task Level 3),
   (d) Get details-on-demand for an item or subset of items (Shneiderman Task Level 4),
   (e) Relate between items or subsets of items. (Shneiderman Task Level 5).

Figure 7 and Fig. 8 show this behavior, while the video (https://coda.ee/HCII22) accompanying this paper makes understanding such MR interaction clearer than is possible from a screenshot, albeit less so than experiencing it with a MR headset.

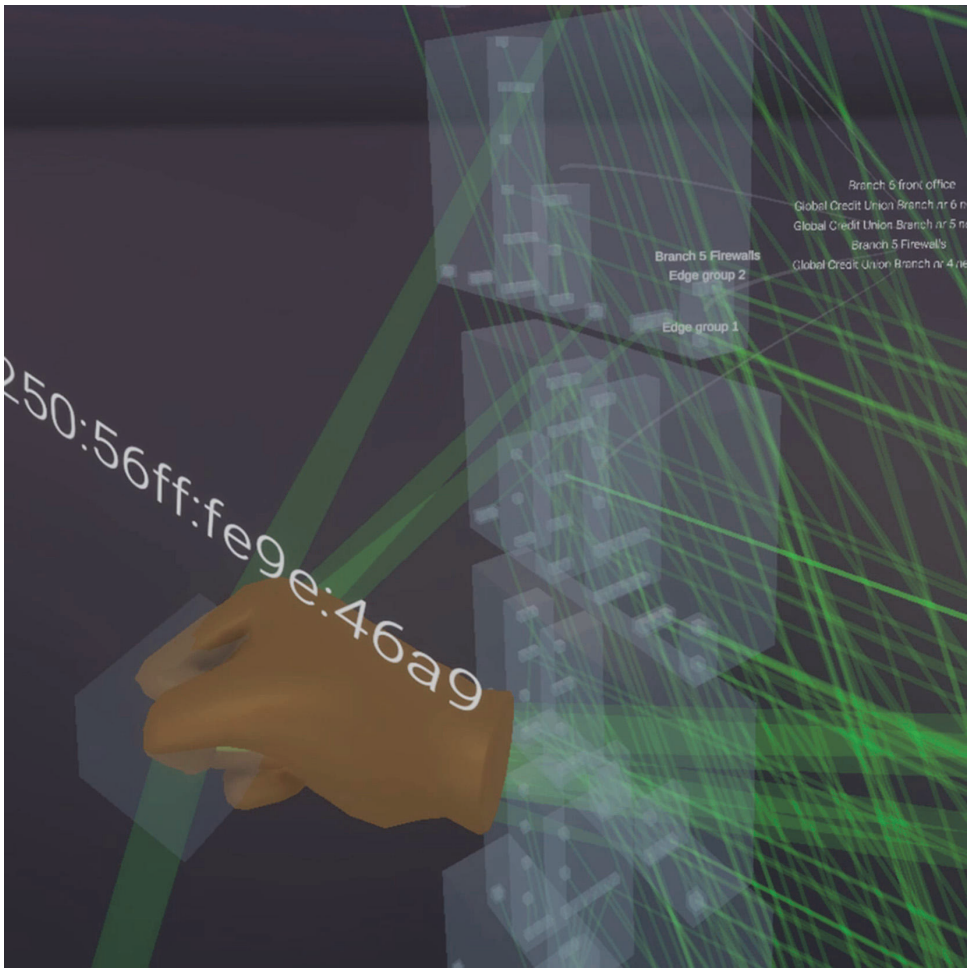


Fig. 5. In a VR environment, the user grabs a node, that is sized to sit into ones palm. For comparison with Mixed Reality view, please see Fig. 3.

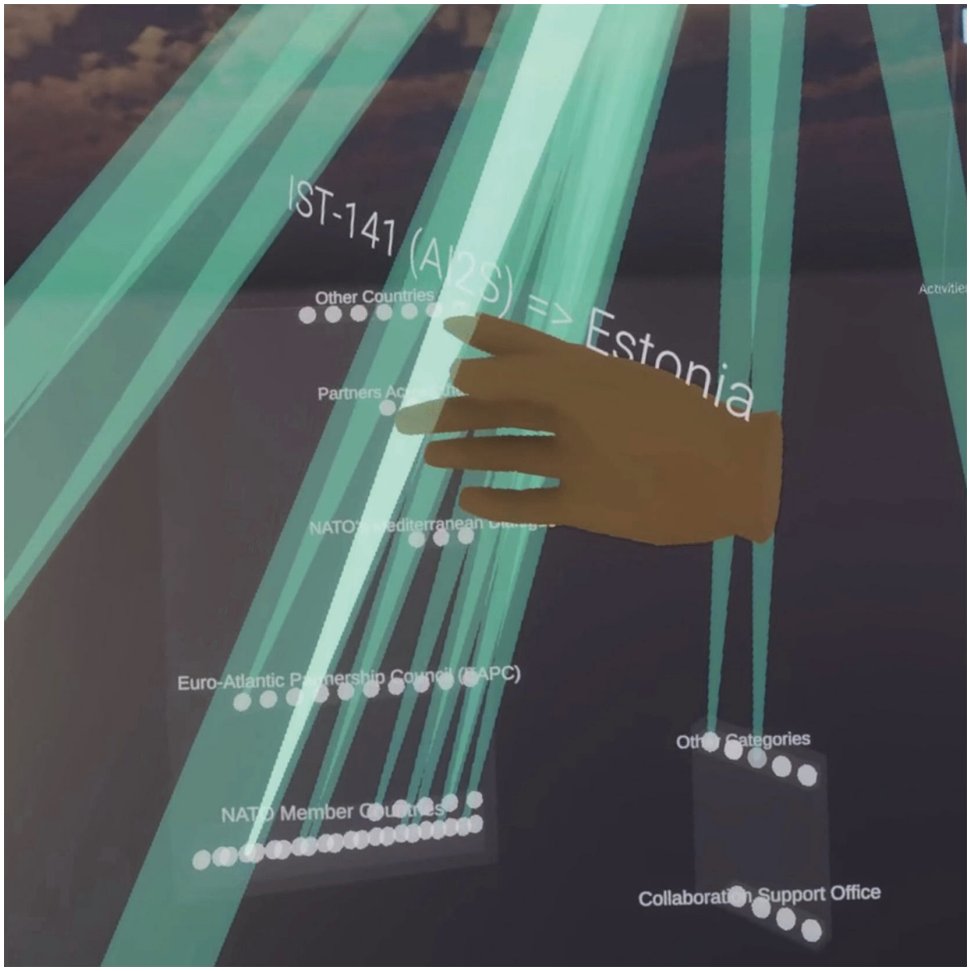


Fig. 6. User touches an edge with the index finger of Oculus avatar's hand, to learn details about that edge.

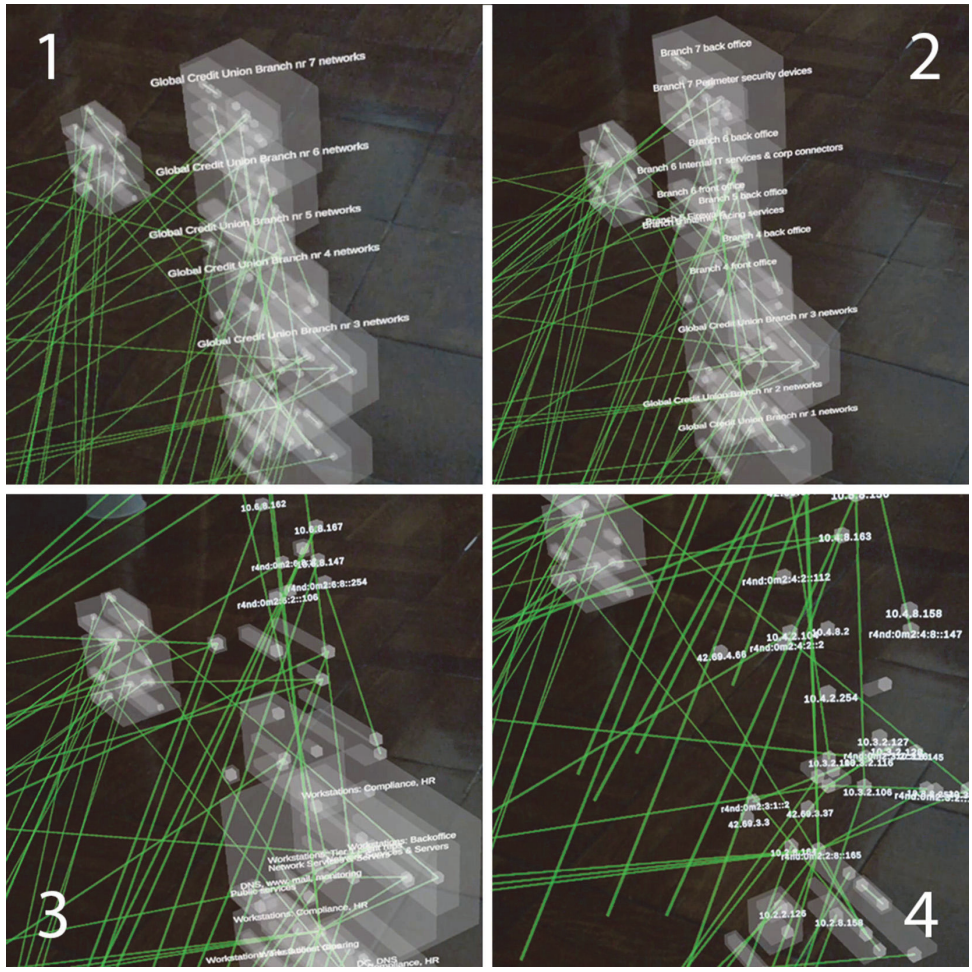


Fig. 7. Once user moves closer to a part of the visualization that might be of interest, textual labels are shown for upper tier groups first, while the rectangular representations of these groups are disappeared as the user gets closer, to enable focusing on the subgroups inside, and then the nodes with their IP addresses as labels. To convey the changes in visualization as the user moves, screenshots are provided sequentially, numbered 1–4. For comparison with Virtual Reality view, please see Fig. 8.

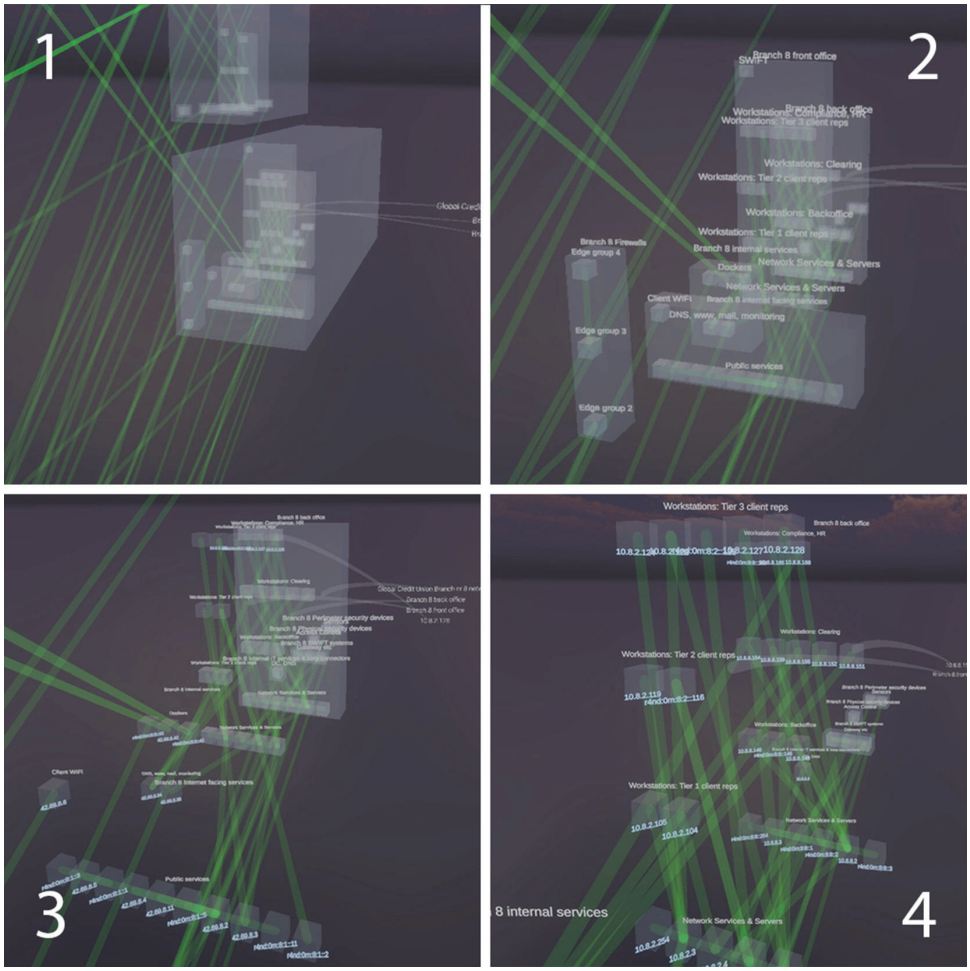


Fig. 8. Once user moves closer to a part of the visualization that might be of interest, textual labels are shown for upper tier groups first, while the rectangular representations of these groups are disappeared as the user gets closer, to enable focusing on the subgroups inside, and then the nodes with their IP addresses as labels. To convey the changes in visualization as the user moves, screenshots are provided sequentially, numbered 1–4. For comparison with Mixed Reality view, please see Fig. 7.

3.6 Textual Information

Text labels of nodes, edges, groups are a significant issue, as these are expensive to render due to their complex geometrical shapes and also risk the possible occlusion of objects which may fall behind them. Accordingly, text is shown in VDE only when necessary, to the extreme that a label is made visible only when the user's gaze is detected on a related object. Backgrounds are not used with text in order to reduce their occlusive footprint.

3.7 Optimizations

The basis for VDE: less is more.

Occlusion of visual representations of data objects is a significant problem for 3D data visualizations on flat screens. In VR/MR environments, occlusion can be mostly mitigated by stereoscopic perception of the (semi-transparent) visualizations of data objects and by parallax, but may still be problematic [5].

While occlusion in MR/VR can be addressed by measures such as transparency, transparency adds significant overhead to the rendering process. To optimize occlusion-related issues, VDE strikes a balance between the necessity of transparency of visualized objects, while adjusting the number of components currently visible (textual labels, reducing the complexity of objects that are farther from the user's viewpoint, etc.) based on the current load (measured FPS); on objects' relative positions in user's gaze (in-view, not-in-view, behind the user); and on the user's virtual distance from these objects. This XR-centric approach to semantic zooming proves a natural user experience, visually akin to the semantic zooming techniques used in online maps which smoothly but dramatically change the extent of detail as a function of zoom level (showing only major highways or the smallest of roads, toggling the visibility of street names and point of interest markers).

Although colors and shapes of the visual representations of data objects can be used to convey information about their properties, user feedback has confirmed that these should be used sparsely. Therefore, in most VDE layouts, the nodes (representing data objects) are visualized as transparent off-white cubes or spheres, and the latter only in case if the available GPU is powerful enough. Displaying a cube versus a sphere may seem a trivial difference, but considering the sizes of some of the datasets visualized (>10,000 nodes and >10,000 edges), these complexities add up quickly and take a significant toll.

4 Conclusion

Immersive visualization of large, dynamic node-link diagrams requires careful consideration of visual comprehensibility and computational performance. While many of node-link visualization idioms are well-studied in 2D flat screen visualizations, the opportunities and constraints presented by VR and MR environments are distinct. As the pandemic made a larger-scale study with many participants impossible, VDE instead underwent a more iterative review process, drawing input from representative users and domain expertise. The approach described herein reflects many iterations of performance testing and user feedback.

Optimizing user interactions for VDE presented the design challenge of providing an interface which intuitively offers an informative presentation of the node-link network both at a high-level "overview" zoom level and at a very zoomed "detail" view, with well-chosen levels of semantic zoom available along the continuum between these extremes. Constrained navigation further optimizes

the user experience, limiting confusion and motion sickness. Dynamic highlighting, through the selection and controller-based movement of individual notes, enhances the users' understanding of the data.

Acknowledgement. The authors thank Alexander Kott, Jennifer A. Cowley, Lee C. Trossbach, Matthew C. Ryan, Jaan Priisalu, and Olaf Manuel Maennel for their ideas and guidance. This research was partly supported by the Army Research Laboratory under Cooperative Agreement Number W911NF-17-2-0083 and in conjunction with the CCDC Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center. The material is based upon work supported by NASA under award number 80GSFC21M0002.

References

1. Batch, A., Elmqvist, N.: The interactive visualization gap in initial exploratory data analysis. IEEE Trans. Visual Comput. Graph. **24**(1), 278–287 (2018). https://doi.org/10.1109/TVCG.2017.2743990
2. Ben-Asher, N., Gonzalez, C.: Effects of cyber security knowledge on attack detection. Comput. Hum. Behav. **48**, 51–61 (2015). https://doi.org/10.1016/j.chb.2015.01.039. https://www.sciencedirect.com/science/article/pii/S0747563215000539
3. Casallas, J.S., Oliver, J.H., Kelly, J.W., Merienne, F., Garbaya, S.: Using relative head and hand-target features to predict intention in 3d moving-target selection. In: 2014 IEEE Virtual Reality (VR), pp. 51–56 (2014). https://doi.org/10.1109/VR.2014.6802050
4. Dübel, S., Röhlig, M., Schumann, H., Trapp, M.: 2d and 3d presentation of spatial data: a systematic review. In: 2014 IEEE VIS International Workshop on 3DVis (3DVis), pp. 11–18 (2014). https://doi.org/10.1109/3DVis.2014.7160094
5. Elmqvist, N., Tsigas, P.: A taxonomy of 3d occlusion management for visualization. IEEE Trans. Visual Comput. Graphics **14**(5), 1095–1109 (2008). https://doi.org/10.1109/TVCG.2008.59
6. Günther, T., Franke, I.S., Groh, R.: Aughanded virtuality - the hands in the virtual environment. In: 2015 IEEE Virtual Reality (VR), pp. 327–328 (2015). https://doi.org/10.1109/VR.2015.7223428
7. Johnson, D.M.: Introduction to and review of simulator sickness research (2005)
8. Kabil, A., Duval, T., Cuppens, N.: Alert characterization by non-expert users in a cybersecurity virtual environment: a usability study. In: De Paolis, L.T., Bourdot, P. (eds.) AVR 2020. LNCS, vol. 12242, pp. 82–101. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-58465-8_6
9. Kabil, A., Duval, T., Cuppens, N., Comte, G.L., Halgand, Y., Ponchel, C.: Why should we use 3d collaborative virtual environments for cyber security? In: 2018 IEEE Fourth VR International Workshop on Collaborative Virtual Environments (3DCVE), pp. 1–2 (2018). https://doi.org/10.1109/3DCVE.2018.8637109
10. Kang, H.J., Shin, J.h., Ponto, K.: A comparative analysis of 3d user interaction: How to move virtual objects in mixed reality. In: 2020 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), pp. 275–284 (2020). https://doi.org/10.1109/VR46266.2020.00047
11. Kullman, K.: Creating useful 3d data visualizations: Using mixed and virtual reality in cybersecurity (2020). https://coda.ee/MAVRIC, 3nd Annual MAVRIC Conference

12. Kullman, K., Ben-Asher, N., Sample, C.: Operator impressions of 3d visualizations for cybersecurity analysts. In: 18th European Conference on Cyber Warfare and Security. Coimbra, Portugal (2019)
13. Kullman, K., Cowley, J., Ben-Asher, N.: Enhancing cyber defense situational awareness using 3d visualizations. In: 13th International Conference on Cyber Warfare and Security, Washington, DC (2018)
14. Kullman, K.: Virtual data explorer. https://coda.ee/
15. Kullman, K., Buchanan, L., Komlodi, A., Engel, D.: Mental model mapping method for cybersecurity. In: HCI (2020)
16. Kullman, K., Engel, D.: Interactive stereoscopically perceivable multidimensional data visualizations for cybersecurity. J. Defence Secur. Technol. **4**(3), 37–52 (2022). 10.46713/jdst.004.03
17. Lu, F., Davari, S., Lisle, L., Li, Y., Bowman, D.A.: Glanceable ar: evaluating information access methods for head-worn augmented reality. In: 2020 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), pp. 930–939 (2020). https://doi.org/10.1109/VR46266.2020.00113
18. Miyazaki, R., Itoh, T.: An occlusion-reduced 3d hierarchical data visualization technique. In: 2009 13th International Conference Information Visualisation, pp. 38–43 (2009). https://doi.org/10.1109/IV.2009.32
19. Munzner, T.: Visualization Analysis and Design. AK Peters Visualization Series. CRC Press (2015). https://books.google.de/books?id=NfkYCwAAQBAJ
20. Pruett, C.: Lessons from the frontlines modern vr design patterns (2017). https://developer.oculus.com/blog/lessons-from-the-frontlines-modern-vr-design-patterns, unity North American Vision VR/AR Summit
21. Roberts, J.C., Ritsos, P.D., Badam, S.K., Brodbeck, D., Kennedy, J., Elmqvist, N.: Visualization beyond the desktop-the next big thing. IEEE Comput. Graphics Appl. **34**(6), 26–34 (2014). https://doi.org/10.1109/MCG.2014.82
22. Shneiderman, B.: The eyes have it: a task by data type taxonomy for information visualizations. In: Proceedings 1996 IEEE Symposium on Visual Languages, pp. 336–343 (1996). https://doi.org/10.1109/VL.1996.545307
23. Whitlock, M., Smart, S., Szafir, D.A.: Graphical perception for immersive analytics. In: 2020 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), pp. 616–625 (2020). https://doi.org/10.1109/VR46266.2020.00084
24. Yu, D., Liang, H.N., Fan, K., Zhang, H., Fleming, C., Papangelis, K.: Design and evaluation of visualization techniques of off-screen and occluded targets in virtual reality environments. IEEE Trans. Visual Comput. Graphics **26**(9), 2762–2774 (2020). https://doi.org/10.1109/TVCG.2019.2905580

Appendix 7

Publication VII

Varga, Margaret; Liggett, Kristen K.; Bivall, Petter; Lavigne, Valérie; Kullman, Kaur; Camossi, Elena; Ray, Cyril; Arkin, Ethem; Krilavičius, Tomas; Mandravickaitė, Justina; Winkelholz, Carsten; Träber-Burdin, Susan; Jayaram, Shivas; Panga, Marius; Acharya, Nikhil; (2022). NATO IST STO-141 Workgroup Final Report: Exploratory Visual Analytics. Science and Technology Organization of the North Atlantic Treaty Organization. DOI: 10.14339/STO-TR-IST-141

Note that included here are only the two chapters of the report where I was one of the co-authors. Full report is available from sto.nato.int[2].

[2] https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-IST-141/$$TR-IST-141-ALL.pdf

NORTH ATLANTIC TREATY
ORGANIZATION

SCIENCE AND TECHNOLOGY
ORGANIZATION

AC/323(IST-141)TP/1079

www.sto.nato.int

STO TECHNICAL REPORT **TR-IST-141**

Exploratory Visual Analytics

(Analyse visuelle exploratoire)

This is the Technical Report of the NATO IST-141 Research Task Group
“Exploratory Visual Analytics.”

Published February 2023

Distribution and Availability on Back Cover

NORTH ATLANTIC TREATY
ORGANIZATION

SCIENCE AND TECHNOLOGY
ORGANIZATION

AC/323(IST-141)TP/1079

www.sto.nato.int

STO TECHNICAL REPORT **TR-IST-141**

Exploratory Visual Analytics

(Analyse visuelle exploratoire)

This is the Technical Report of the NATO IST-141 Research Task Group
“Exploratory Visual Analytics.”

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published February 2023

Copyright © STO/NATO 2023
All Rights Reserved

ISBN 978-92-837-2396-7

Single copies of this publication or of a part of it may be made for individual use only by those organisations or individuals in NATO Nations defined by the limitation notice printed on the front cover. The approval of the STO Information Management Systems Branch is required for more than one copy to be made or an extract included in another publication. Requests to do so should be sent to the address on the back cover.

Table of Contents

List of Figures

List of Tables

List of Acronyms

2D	Two-Dimensional
3D	Three-Dimensional
ACM	Association for Computing Machinery
AI	Artificial Intelligence
AIS	Automatic Identification System
APP	Allied Procedural Publication
AR	Augmented Reality
ARL	U.S. Army Research Laboratory
ASCII	American Standard Code for Information Interchange
C2	Command and Control
C5ISR	Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, Reconnaissance
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CC	Creative Commons
CCDC	Combat Capabilities Development Command
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDX	Cyber Defence Exercise
CFD	Computational Fluid Dynamics
C-IED	Counter Improvised Explosive Device
CMRE	Centre for Maritime Research and Experimentation
CNN	Convolutional Neural Network
COE	Centre of Excellence
Cranfield-SAS	Cranfield Situation Awareness Scale
CSO	Collaboration Support Office
CSSP	Cyber Security Service Provider
CT	Computed Tomography
datAcron	Big Data Analytics for Time Critical Mobility Forecasting
DDOS	Distributed Denial-of-Service
DGMs	Deep Generative Models
DKOE	Decision Knowledge Operational Effectiveness
DNS	Domain Name System
DoD	Department of Defense
DQN	Deep Q-Network
DRDC	Defence Research & Development Canada
DS	Decision Support
EID	Ecological Interface Design
ESS	Earth System Science
GANs	Generative Adversarial Networks
GUI	Graphical User Interface
HFM	Human Factors and Medicine
HPC	High Performance Computing
IA	Information Analysis
IED	Improvised Explosive Device

IEEE	Institute of Electrical and Electronics Engineers
IMO	International Maritime Organization
IST	Information Systems Technology
ITU-R	International Telecommunication Union – Recommendation
IVIS	Interactive Visualizations
KIA	Killed in Action
LIME	Local Interpretable Model-agnostic Explanations
LRP	Layer-wise Relevance Propagation
LSTM	Long Short-Term Memory
MARS	Mission Awareness Rating Scale
MIL-STD	Military Standard
MLP	Multi-Layer Perceptron
MOD	Ministry of Defence
MPoLIS	Maritime Patterns-of-Life Information Service
MR	Mixed Reality
MSA	Maritime Situational Awareness
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NMEA	National Marine Electronic Association
NMSG	NATO Modelling and Simulation Group
OSeaM	Open Sea Map
OSM	Open Street Map
PCP	Parallel Coordinates Plot
QUASA	Quantitative Analysis of Situation Awareness
RNN	Recurrent Neural Network
RTG	Research Task Group
RTO	Research and Technology Organization
SA	Situation Awareness
SABARS	Situation Awareness Behavioral Rating Scale
SAGAT	Situation Awareness Global Assessment Technique
S-AIS	Satellite AIS
SAR	Search and Rescue
SART	Situation Awareness Rating Technique
SAS	System Analysis and Studies
SA-SWORD	Situation Awareness Subjective Workload Dominance
SAVANT	Situation Awareness Verification and Analysis Tool
SME	Subject Matter Expert
SN	Social Networks
SNA	Social Network Analysis
SOM	Self-Organizing Map
SPAM	Situation Present Assessment Method
STANAG	Standardization Agreement
SWAT	Subjective Workload Assessment Technique

T-AIS	Terrestrial AIS
TCT	Trajectory Contingency Tables
TLG	Timeline Graphs
TLX	Task Load Index
t-SNE	t-distributed Stochastic Neighbor Embedding
UCD	User-Centered Design
UI	User Interface
UK	United Kingdom
US	United States
UX	User Experience
VA	Visual Analytics
VAST	Visual Analytics Science and Technology
VDE	Virtual Data Explorer
Vids	Visual Intrusion Detection System
VizSec	Visualization for Cyber Security
VMS	Vessel Monitoring System
VR	Virtual Reality
VRDAE	Virtual Reality Data Analysis Environment
VTK	Visualization Toolkit
WIA	Wounded in Action
xR	Extended Reality

Acknowledgements

We would like to acknowledge the invaluable support and guidance from our mentor and IST Panel Chair Dr. Michael Wunder and IST Panel Vice Chair Col. Dr. Nikolai Stoianov, UK IST panel representatives Mr. Simon Baker and Prof. Bob Madahar, also the invaluable support from Col. (rtd) Philippe Soète, Ms. Aysegul Apadin, Ms. Agata Fernandes Swiatkiewicz, Ms. Armelle Dutruc and Mr. Bernard Garcin from CSO.

IST-141 Membership List

CHAIR

Dr. Margaret VARGA*
University of Oxford
UNITED KINGDOM
Email: margaret.varga@zoo.ox.ac.uk

MEMBERS

Mr. Ethem ARKIN*
Aselsan
TURKEY
Email: earkin@aselsan.com.tr

Dr. Petter BIVALL*
Swedish Defence Research Agency (FOI)
SWEDEN
Email: petter.bivall@foi.se

Dr. Elena CAMOSSI*
CMRE
CMRE – Centre for Maritime Research and Experimentation
Email: lena.camossi@cmre.nato.int

Mr. Kaur KULLMAN*
Estonian Ministry of Defense
ESTONIA
Email: kaur@ieee.org

Dr. Tomas KRILAVIČIUS*
Vytautas Magnus University (Vytauto Didziojo Universitetas)
LITHUANIA
Email: tomas.krilavicius@krilas.lt

Mrs. Valérie LAVIGNE*
Defence Research and Development Canada – Valcartier
CANADA
Email: valerie.lavigne@drdc-rddc.gc.ca

Dr. Kristen LIGGETT*
Air Force Research Laboratory, Airman Systems Directorate
UNITED STATES
Email: kristen.liggett@us.af.mil

Dr. Virginijus MARCINKEVIČIUS*
Vilnius University
LITHUANIA
Email: virginijus.marcinkevicius@mii.vu.lt

Mr. Cyril RAY*
Ecole navale (French Naval Academy)
FRANCE
Email: cyril.ray@ecole-navale.fr

Ms. Susan TRAEBER-BURDIN*
Fraunhofer FKIE
GERMANY
Email: susan.traeber-burdin@fkie.fraunhofer.de

Dr. Carsten WINKELHOLZ*
Fraunhofer FKIE
GERMANY
Email: carsten.winkelholz@fkie.fraunhofer.de

*** Contributing or Supporting Author**

ADDITIONAL CONTRIBUTORS

Mr. Nikhil ACHARYA*
Fraunhofer FKIE
GERMANY
Email: nikhil.acharya@fkie.fraunhofer.de

PANEL/GROUP MENTOR

Dr. Michael WUNDER
Fraunhofer-FKIE
GERMANY
Email: michael.wunder@fkie.fraunhofer.de

*** Contributing or Supporting Author**

Exploratory Visual Analytics

(STO-TR-IST-141)

Executive Summary

Information superiority is one of the primary enablers for military dominance; the exploitation of all relevant information from multiple sources is a key factor for NATO's information superiority. Visualization and visual analytics research are essential to address the needs of the 2015 NATO targets of emphasis in Information Analysis (IA) and Decision Support (DS): IA&DS-1 on Decision Support and IA&DS-2 on Big Data and Long Data Processing and Analysis.

Visual analytics is the science of analytical reasoning facilitated by interactive visual interfaces. The IST-141/RTG-66 group investigated, researched, and fostered collaborations in visual analytics and visualization – facilitating knowledge extraction and data analysis for timely situation awareness and effective decision making. The objectives of IST-141 were thus to research, develop and apply exploratory visual analytics techniques:

1) To exploit and make sense of large and complex data, i.e., Big data;
2) To help make tacit knowledge explicit;
3) To provide acute situation awareness; and
4) To support informed decision making across a wide range of defence domains including cyber, maritime, genomics, and social media domains, as well post analysis and in situ visualization for simulation data.

In addition, IST-141 facilitated the interest in, as well as the uptake and exploitation of, visual analytics technologies within and beyond NATO through:

1) Organizing and presenting at one NATO Specialists' Meeting (IST-HFM-154: Cyber Symbology) and one NATO inter-panel and inter-group workshop (IST-178: Big Data Challenges: Situation Awareness and Decision Support).
2) Lecturing on two NATO Lecture Series (IST-143 and IST-170) during 2016 – 2019 in eight different countries.
3) Contributing to, and participating in, NATO CSO activities organized by others and initiating/participating in joint activities.
4) Presenting at many prestigious international conferences, workshops, and seminars such as IEEE VIS.
5) IST-141 members also work widely outside the group in collaborations with IST-108, IST-129, IST-177, IST-ET-094, IST-ET-099, IST-SAS-102, HFM-259, HFM-294, SAS-124, SAS-117 and SAS-139.

The group generated 32 publications.

Analyse visuelle exploratoire

(STO-TR-IST-141)

Synthèse

La supériorité en matière d'information est l'un des principaux outils de prédominance militaire ; l'exploitation de toutes les informations pertinentes de multiples sources est un facteur clé pour l'OTAN dans ce domaine. Les recherches sur la visualisation et l'analyse visuelle sont essentielles pour atteindre les objectifs prioritaires de l'OTAN en 2015 dans le domaine de l'analyse de l'information (AI) et de l'aide à la décision (DS) (IA&DS-1 sur l'aide à la décision et IA&DS-2 sur les données massives et le traitement et l'analyse de données longues).

L'analyse visuelle est la science du raisonnement analytique facilitée par des interfaces visuelles interactives. Le groupe IST-141/RTG-66 a mené des études et des recherches et favorisé des collaborations en analyse visuelle et visualisation, en facilitant l'extraction des connaissances et l'analyse des données afin d'établir une connaissance de la situation opportune permettant une prise de décision efficace. Les objectifs de l'IST-141 étaient donc d'étudier, mettre au point et appliquer des techniques d'analyse visuelle :

1) Pour exploiter et donner un sens aux données vastes et complexes, autrement dit, aux données massives ;
2) Pour faciliter l'explicitation de l'implicite ;
3) Pour fournir une connaissance de la situation précise ; et
4) Pour favoriser une prise de décision éclairée dans une large palette de domaines de la défense, y compris le cyberdomaine, le domaine maritime, la génomique et les médias sociaux, ainsi pour la post-analyse et la visualisation in situ des données de simulation.

De plus, l'IST-141 a renforcé l'intérêt pour et facilité l'essor et l'exploitation des technologies d'analyse visuelle au sein de l'OTAN et en dehors, par :

1) L'organisation d'une réunion des spécialistes (IST-HFM-154, « Cybersymbologie ») et d'un séminaire intercommission et intergroupe (IST-178, « Défis des données massives : connaissance de la situation et aide à la décision ») et la présentation d'exposés à ces occasions ;
2) L'intervention dans deux séries de conférences OTAN (IST-143 et IST-170) entre 2016 et 2019 dans huit pays ;
3) La contribution et la participation aux activités du CSO de l'OTAN organisées par d'autres et le lancement ou la participation à des activités conjointes ;
4) La présentation d'exposés dans un grand nombre de conférences et séminaires internationaux prestigieux, tels que VIS de l'IEEE ;
5) Les membres de l'IST-141 travaillent par ailleurs largement en dehors du groupe, au sein de collaborations avec l'IST-108, l'IST-129, l'IST-177, l'IST-ET-094, l'IST-ET-099, l'IST-SAS-102, le HFM-259, le HFM-294, le SAS-124, le SAS-117 et le SAS-139.

Le groupe a produit 32 publications.

Chapter 1 – INTRODUCTION

Margaret Varga
University of Oxford / Seetru Ltd.
UNITED KINGDOM

Petter Bivall
Swedish Defence Research Agency
SWEDEN

Kristen K. Liggett
Air Force Research Laboratory
UNITED STATES

Valérie Lavigne
Defence Research and Development Canada
CANADA

1.1 BACKGROUND

Information superiority is one of the key elements for military dominance; the exploitation of all relevant information from multiple sources is a crucial factor for NATO's information superiority. Visualization and Visual Analytics research are essential to address the needs of the 2015 NATO targets of emphasis in Information Analysis (IA) and Decision Support (DS): IA&DS-1 on Decision Support and IA&DS-2 on Big Data and Long Data Processing and Analysis.

Visual Analytics (VA) is the science of analytical reasoning facilitated by interactive visual interfaces [1]. There are three main components of VA, namely, interactive visualization, analytical reasoning, and computational analysis [2]. In the context of VA considered by the Group:

- Visualization is concerned with the use of interactive visual representations of data to amplify cognition [3], while;
- Analytical reasoning and computation analysis work to support data exploration, analysis and understanding.

1.2 OBJECTIVES OF THE NATO IST-141 RTG

The NATO IST-141/RTG66 Research Task Group (RTG) Exploratory Visual Analytics investigated, researched and fostered collaborations in knowledge extraction/discovery and data analysis for timely situation awareness to support effective decision making. The Group explored how visualization conveys information effectively: leveraging human perception and enhancing human cognition, i.e., bringing together visualization and the user's mental model (see Chapter 2 and [4]). The objectives of IST-141 were thus to research, develop and apply exploratory visual analytics techniques:

1) To exploit and make sense of large and complex data sets, i.e., Big data;
2) To help make tacit knowledge explicit;
3) To provide acute situation awareness, and
4) To support informed decision making in a wide range of different defence domains, such as maritime, social media, genomics, and cyber domains as well as post analysis and in situ visualization for simulation data.

1.3 AIM OF THE REPORT

The aim of this IST-141 Research Task Group technical report is to discuss the work conducted by the Group to research, develop and apply exploratory visual analytics to data sets relating to:

- Improvised explosive devices resources (NATO C-IED COE);
- Social media; and
- Cyber and maritime and intelligence operations.

The work demonstrates the effectiveness of Exploratory VA in detecting, monitoring, analyzing, and understanding large and complex datasets, i.e., big data, for situation awareness and decision support.

This report will also discuss the work of the Group on:

1) Research and development of visualization and visual analytics technologies.
2) Raising awareness of the Group's work:
   - By presenting papers at prestigious international conferences, e.g., IEEE VIS; and
   - Contributing to two NATO lecture series (IST-143 and IST-170).
3) Facilitating the exploitation and application of visual analytics and visualization technologies in NATO defence and security domains, and beyond.
4) Broadening the horizon of the understanding and exploration of visualization and visual analytics.
5) Leveraging the generation of new ideas.
6) Developing NATO inter-Panel/inter-Group collaborations through:
   - Organization (and presentation of the Group's work therein) of one joint Panel NATO Specialists' meeting (IST-HFM-154: Cyber Symbology) and one NATO inter-Panel / inter-Group Workshop (IST-178: Big Data Challenges – Situation Awareness and Decision Support);
   - Participating in NATO activities organized by others; and
   - Organizing joint meetings with numerous RTGs from different Panels.

1.4 REPORT STRUCTURE

The chapters in the report summarize work conducted during the course of this RTG.

Chapter 2 discusses human factors considerations for visual analytics. It begins by defining human factors and describes the human factors / user-centered design process. It discusses some common myths about the design process for designers to be aware of and avoid. Users of visual analytics systems are many and diverse, so knowing the user for any project is of utmost importance to ensure that the output product is both useful and usable. References to standards, guidelines, heuristics, and best practices for how to optimally display information are provided. Included in the chapter is a discussion and figures depicting the advantages of using stereoscopic three-dimensional visualizations for particular data sets. Finally, there is a section on how to evaluate the usefulness and usability of visualizations. Included are resources for situation awareness and workload metrics.

Chapter 3 discusses Information visualization and visual analytics in the maritime domain.

Chapter 4 and Chapter 5 are concerned with social media data and simulation data.

Chapter 6 discusses the interactions between visual analytics and deep learning.

Chapter 7 discusses the Group's work in cyber situation awareness and cyber symbology.

Chapter 8 and Chapter 9 explore the application of visual analytics and visualization to NATO data such as:

- IED (NATO C-IED COE); and
- NATO HFM-259 data.

These two chapters discuss the development of, and resulting design principles for, web-based access to these datasets for a wide range of users from the general public to researchers and policy makers, i.e., people from different backgrounds and with varying levels of expertise and knowledge. The analysis of IED data adopted an interactive storytelling approach to engage the general public, and the visual analytics / visualizations of the HFM-259 data are also suitable for public engagement.

Chapter 10 draws conclusions and makes recommendations.

1.5 REFERENCES

[1] Thomas, J.J. and Cook, K.A. (Eds.) (2005). Illuminating the Path: The Research and Development Agenda for Visual Analytics. National Visualization and Analytics Center.

[2] Keim, D., Andrienko, G., Fekete, J.D., Görg, C., Kohlhammer, J. and Melançon, G. (2008). Visual Analytics: Definition, Process, and Challenges. 10.1007/978-3-540-70956-5_7.

[3] Card, S., Mackinlay, J. and Shneiderman, B. (1999). Readings in Information Visualization: Using Vision to Think. Morgan Kaufmann Publishers.

[4] Tory, M. and Moller, T. (2004). Human Factors in Visualization Research. In IEEE Transactions on Visualization and Computer Graphics, 10(1), pp. 72-84, Jan – Feb 2004.

Chapter 2 – HUMAN FACTORS CONSIDERATIONS FOR VISUAL ANALYTICS

Kristen K. Liggett
Air Force Research Laboratory
UNITED STATES

Kaur Kullman
Cognitive Data OÜ
ESTONIA

2.1 DEFINING HUMAN FACTORS

According to the International Ergonomics Association, "Ergonomics (or human factors) is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data, and other methods to design in order to optimize human well-being and overall system performance" [1]. California State University Long Beach, Department of Psychology, defines human factors as " …a scientific discipline which examines human behavior and capabilities in order to find the best ways to design products, equipment and systems for maximum safe, effective, satisfying use by humans" [2]. While there are many definitions of human factors in the literature, these two are highlighted because they focus on the consideration of human capabilities in the design of things with which humans interact to maximize *effective performance* and *user satisfaction*. One of the first books published on human factors was an engineering textbook entitled "Human Factors in Engineering and Design" [3]. It was first published in 1957 and is now in its 7th edition. Seminal work in human factors was organized into The Handbook of Human Factors [4]. The book entitled "The Psychology of Everyday Things" (more recently published as "The Design of Everyday Things" [5]) was written in 1988 to introduce these concepts to a wider, non-technical, audience. Although the human factors discipline has been around for quite some time, it is occasionally "rediscovered" and, at various times, has been rebranded as user-centered design, user-driven development, User Experience (UX) design, human-centered design, human engineering, cognitive systems engineering, and most recently, design thinking.

2.2 DETERMINING WHAT TO PRESENT

2.2.1 User-Centered Design

User-Centered Design (UCD) is the cornerstone of the human factors discipline and has been used effectively in many domains, including designs of work support systems for aircraft cockpits, unmanned aerial vehicle control stations, automotive dashboards, nuclear power plant control rooms, space vehicle controls, hospital medical record systems, and many more safety-critical applications.

At the most basic level, UCD is a design approach that definitively places the user at the center of all design activities (Figure 2-1). According to William Hudson of the Interaction Design Foundation [6], UCD is "an iterative design process in which designers focus on the users and their needs in each phase of the design process. UCD calls for involving users throughout the design process via a variety of research and design techniques so as to create highly usable and accessible products for them." The process starts with a deep understanding of the user and their work. This analysis informs the designer of what to present to the user and *drives* the design process. The analysis phase of the design process also provides designers an opportunity to establish a relationship between the design team and the end-users of the product being designed. These users will supply the design team with valuable information about the work domain, including the overall goal of the work, tasks necessary to accomplish it, the objectives, order, and dependencies of those tasks, information requirements, etc. The design team can use techniques such as interviews, observations, task analysis, and workflow diagramming to gather information for further

analysis. One such technique, goal-directed task analysis, is a procedure of interviews and knowledge elicitation methods that seeks all information related to goals of operators, and the information needed to achieve them in a technologically agnostic manner [7]. Information collection and subsequent analysis help the design team understand the tasks and stakeholders, the information, and decisions to be supported, current sources of information, gaps in current processes, and information gaps. Ultimately, the analysis phase will allow members of the design team to determine how to best support the work processes of end-users in a way that facilitates their cognitive and perceptual needs.

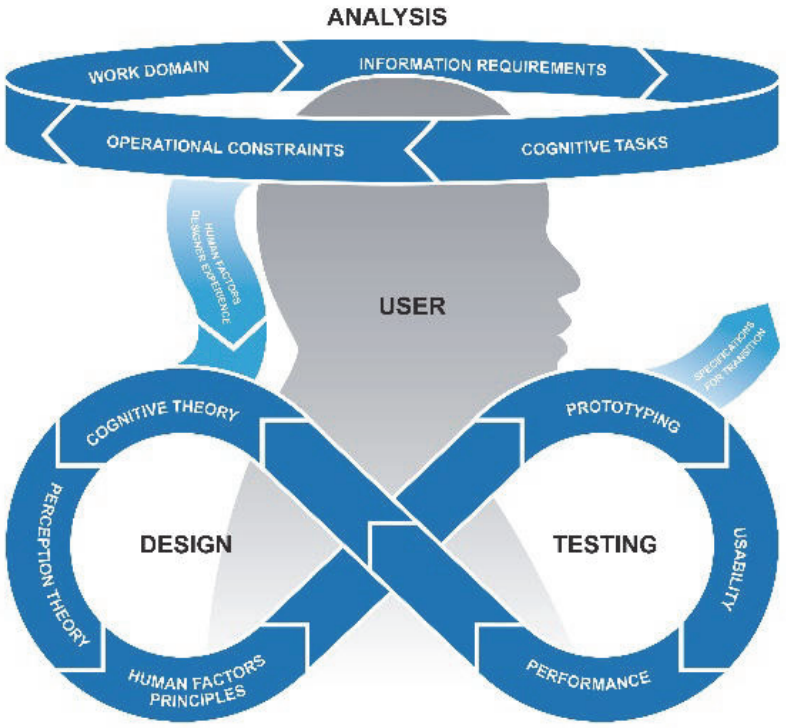


Figure 2-1: User-Centered Design.

Next, and most challenging, is the conversion of information gathered during the analysis phase into initial design concepts (represented by the arrow from the Analysis to Design and Testing Phase in Figure 2-1). This step represents the integration of information gathered in the analysis phase with foundational empirical knowledge of human perception (vision theory, color theory, etc.) and cognition (encoding theory, memory theory, information processing theory, multiple resource theory, attention theory, etc.) guided by human factors design principles that represent decades of research in determining the most effective ways to display information for different uses. Unfortunately, this essential step often lacks a proper foundation, and developers proceed directly to the generation of visualizations without a complete understanding of the work or of how to apply psychological research to best support the end-users' cognitive capabilities, task goals, or workflow. Too often, complex designs are created under misguided notions, such as that providing end-users vast amounts of information will allow them to find what they need when they need it, that training or documentation will allow users to bridge gaps, or that users' knowledge and/or expertise about the work itself will be sufficient to allow them to tailor the work aids, interfaces, and/or visualizations in

a way that will support them in their work. Historically, this traditional approach has resulted in systems that fail to provide the expected performance improvements or in systems that are not used at all because they *add* to rather than *support* work.

Once the information from the analysis phase is converted into an initial design, the design team can begin developing the visualization/tool interfaces as well as the tool functionality. The design team will determine sources of required data to support the visualizations and consider methods of effectively accessing the data. The design team will also determine appropriate task allocation to include how automation might be employed. Interaction with end-users is critical for refining initial designs during the design and testing phases. If the previous steps have been done well, designs will require fewer iterations. During this phase, products are tested, refined, and tested again as needed to ensure maximum utility and usability. Latter evaluation involves user-in-the-loop testing with operationally representative scenarios consisting of representative user tasks that have been developed from information gained in the analysis phase.

When UCD is employed by developers with design experience who understand human capabilities and limitations and basic human factors design principles, the resulting designs are effective and intuitive and have a high degree of user acceptance. These designs support workflow without adding unwanted workload.

2.2.2 Myths About Design

Often, tools are built based on factors other than user needs, such as when developers try to find new ways to make use of existing technology or to make use of a new and innovative technology. Other times, user needs drive design, but the designs are not based on a thorough evaluation of the users' processes and goals. While these types of development are not useless, they do not generally lead to the most effective tools and often lead to tools that get shelved because they either don't fit into the users' work processes or because they provide a service that the user doesn't really require. Three common "myths" about how to provide capability are often employed by developers as excuses for circumventing the user-centered design process:

- **Design Myth #1:** Just ask the users what they want and give it to them.
- **Design Myth #2:** Give users access to everything they could possibly need, and they will find what they need when they need it.
- **Design Myth #3:** Allow users to design their own visualizations and interfaces by making everything customizable and letting them choose how they want things to look and behave.

There is solid empirical evidence that indicates that these "myths" are not only inaccurate but can even be dangerous if employed in the design of critical systems.

Design Myth #1 – Give the Users What They Say They Want

While it may be true that users know what they want, that knowledge is often limited by experience (constraints they currently work within) and the lack of knowledge of what is possible. It has been said that if Henry Ford had asked people what they wanted, they would have said 'faster horses' [8]. While there is some debate as to whether this is an actual quote from Ford, it illustrates the fact that getting user input involves more than just asking people what they want. The more important information for designers to obtain when the users are excited about telling them what they want (and they will be!) is the understanding of ***why*** they are asking for specific things. It is up to designers to probe users for goals, constraints, and motivations. Yes, faster horses may be the users' interpretation of a requirement, but the underlying reason for this request is so they can get from point A to point B faster. Analysis activities as described above supply the design team with a valuable knowledge for design. Using this knowledge, designers can provide tools that allow users to perform work in the best possible way using current technology and sometimes provide requirements that expand current technology rather than tools that just allow them to marginally improve upon current work processes that have been defined and limited by the constraints of past tools and technologies (i.e., faster horses).

Design Myth #2 – Give Users Access to Everything and They Will Find What They Need

This myth stems from the frequent requirement for users to go to a variety of sources to obtain needed information. Designing a system that collects and stores all of this information is an incremental improvement, but that capability alone certainly does not provide an optimal solution. Many dashboards are designed using this myth, and they are frequently not effective for particular users due to the large amount of time and cognitive effort required to sort through and filter information. Often these complex designs are created under the misguided notion that training or documentation will allow users to bridge the gap between the excessive amounts of information and their ability to process excessive amounts of information. As previously mentioned, the most challenging step in UCD is the conversion of domain knowledge obtained during the analysis phase into initial design concepts. This step requires the integration of information gathered in the analysis phase with foundational empirical knowledge of human perception (vision theory, color theory, etc.) and cognition (encoding theory, memory theory, information processing theory, multiple resource theory, attention theory, etc.) guided by human factors design principles that represent decades of empirical research to determine the most effective ways to display information for different uses. This foundational knowledge and experience in applying it to design prevents the creation of complex designs that overtax users' perception and cognition. Design teams must also determine sources of required data to support the interfaces and visualizations and consider methods of effectively accessing those data. Through these activities, a design team can provide an effective tool that will guide users to information they need when they need it, and training and documentation needs will be minimal.

Design Myth #3 – Make Everything Customizable and Let the User Design

One problem with this notion that users typically do not have the time or ability to customize their interfaces. More importantly, multiple studies have been conducted that illustrate that there is often a disconnect between configurations that people say they like best and those with which they perform most effectively [9]. While there are some features of visualizations and interfaces that can and even should remain flexible, the choice of many features is optimal only when their designs and configuration are primarily dependent on workflow needs and goals and fitted to human perceptual and cognitive needs. As indicated above, the conversion of 'work needs' to 'work aids' requires both a deep understanding of the work and a foundational knowledge of human perceptual and cognitive processes along with knowledge of human factors design principles. Users cannot be expected to have this foundational knowledge and should not be made responsible for design. On the other hand, users do have a deeper understanding of the work than can be obtained by the designer, which is why interaction with end-users is critical for refining initial designs. User involvement has the added advantage of ensuring user buy-in. Users often end up preferring things that are best for them when they feel they have been allowed an adequate amount of input into the design process.

2.2.3 Users of Visual Analytics Systems

There are many different types of users of visual analytics systems – but there is **always** a user. The point of visual analytics is to leverage the capabilities of the human visual system to understand complex data. So, whether the users are skilled analysts looking for new insights into complex data sets or the general public trying to understand COVID-19 pandemic information, there are goals, objectives, and tasks unique to each user group. The user groups for visual analytics systems need to be identified and analyzed, and results must be considered when deciding the presentation and interaction details of a visual analytics system. For instance, expert analysts may want to understand information about optimization constraints on algorithms used to process data sets (how do results change if the optimization parameters are weighted differently), while non-experts may want to understand relative comparisons based on personal interests (how does the number of cases/deaths in my state compared to the number in my family's states?). In both of these situations, the presentation of information and how each user group will interact with the information will be very different. If a system will be used by multiple types of users, having a mechanism to tailor the presentation and interaction prior to use based on some initial questionnaire information could allow for pre-use tailoring of the

system. While it is certainly more work to tailor a system to accommodate more than one user group or tailor a system at all, the benefits in terms of portraying useful information and providing a means to explore the data can increase dramatically. Designing a visual analytics system independent of user considerations will lead to unsatisfactory results in terms of both usefulness and usability. One size fits ~~all~~ none.

2.3 DETERMINING HOW TO PRESENT IT

2.3.1 Standards, Guidelines, Heuristics, and Best Practices

Once user analyses have been completed and the designer has identified requirements for what to present, focus now shifts to how to present it. This is an equally important design challenge. There are many resources that designers can reference for guidance in this area. Also, past design experience (examples of things that have worked successfully in the past for a similar requirements) should be considered. Reference documents relevant to human factors design typically come in the form of standards. When there are not established standards, guidelines, best practices, and heuristics suffice. Guidelines are often a useful set of Dos and Don'ts. Best Practices are techniques that have shown to be consistently better than other techniques. Heuristics are general rules of thumb. Jakob Nielsen has generated a useful set of 10 heuristics for user interface design [10].

As mentioned in Section 2.1, the Handbook of Human Factors [4] is a great starting place for guidance and examples of how to display information. There are also numerous design standards that have been produced to guide the designer. The United States (US) Department of Defense MIL-STD-1472 is a military design standard on human engineering [11]. The Ministry of Defence (MOD) Standard 00-250 [12] provides design guidance for the MOD defence acquisition contracts. The International Organization for Standardization established a standard on human-centered design for interactive systems [13] that focuses on ways in which both hardware and software components of interactive systems can enhance human-system interaction. These are just a few of the standards relative to human factors design in existence today. Of particular interest to visual analytics system designers may be the National Institute of Standards and Technology (NIST) Human Engineering Design Criteria Standards [14]. This standard was developed for the Department of Homeland Security and specifically considers use of products by diverse users' groups (civil servants, public health officials, travelers, first responders, and the general public). Visual analytics systems have diverse user groups as well, as pointed out in Section 2.2.3, Table 2-1 shows common topics in many of these standards.

Table 2-1: Common Human Factors Design Standard Topics.

Accessibility	Alarms/Warnings/ Cautions	Anthropometry and Biomechanics	Audio Displays	Communications
Controls	Controls and Display Integration	Dialogue Principles	Environmental Factors	Error Management
Feedback	Forms and Data Entry	Hazards and Safety	Help/Instructions/ Tutorials/Training	Information Coding
Input Devices	Labels	Physical Accommodation	Selection Methods	Signs, Symbols, and Markings
Software Elements	System Status	Use of Automation	Visual Displays	Workstation/Work space Layout

Each Topic has sub-topics. For instance, Visual Displays is commonly broken down into display content and display hardware. This topic was selected for this example because, in visual analytics, 3D representation of data can be essential to understanding the data.

2.3.2 Example: Stereoscopically Perceivable 3D Data Visualizations for Cyber Security

Customized, stereoscopically perceivable 3D visualizations, aligned with cybersecurity analysts' internalized representations of their data, may enhance their capability to understand the state of their networked systems in ways that flat displays with either text, 2D or perspective 3D visualizations cannot afford. For these visualizations to be useful and usable, those need to be aligned to analysts' internalized understanding (mental model) of their data. Section 2.2 described methods for extracting analysts' implicit and explicit understanding of the data that they work with, to create useful, interactive, and importantly for this section, stereoscopically perceivable visualizations that would assist them with their tasks.

Although there have been quite a few recent attempts to utilize Augmented Reality (AR), Mixed Reality (MR) and Virtual Reality (VR) headsets for data visualization, those are usually geared towards showing users the usual (flat) 2D visualizations in Extended Reality (xR) environments or are using relational graphs to show clusters and their relations in 3D. These visualizations can be useful for an initial familiarization phase with a dataset, when a Subject Matter Expert (SME) is trying to learn the functional topology and common behaviors of that dataset but are not particularly useful for interactive data exploration after the user has already gained initial understanding of the topology, relations of its entities and their groups (of groups [of groups (of groups)]) and their expected behavior. Following is a brief overview of a tool, Virtual Data Explorer, which enables the creation of stereoscopically perceivable 3D visualizations and their exploration in mixed or virtual reality environment.

2.3.3 Virtual Data Explorer

For a data visualization that is composed of data-shapes (representations of groups (of groups) of entities in predetermined locations) or their constellations to be useful, the SME must be able to readily map familiar 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 a SME is intimate with the composition of the visualization and its relation to the underlying dataset or source, can this SME use that visualization to extract information from the underlaying data. To explore the usability of such visualizations, Virtual Data Explorer (VDE) software was created. VDE, which may be employed for visualizing cybersecurity specific datasets, is described in more detail in Refs. [15], [16], [17]. Figure 2-2 through Figure 2-5 show how VDE displays cyber data from the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Locked Shields Cyber Defence Exercise (CDX). These figures depict a) Functional topology of entities present in computer networks (22 blue teams, red team's networks, and the game network infrastructure, etc.) that is overlaid with b) Network traffic visualization, where edges (green lines) represent sessions that were observed between entities during a time window, with each edge's opacity referring to the session count between two entities. For detailed explanation of VDE and exercise, see Refs. [15] and [16].

Creation of VDE was partly supported by the Army Research Laboratory under Cooperative Agreement Number W911NF-17-2-0083 and in conjunction with the CCDC Command, Control, Computers, communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.

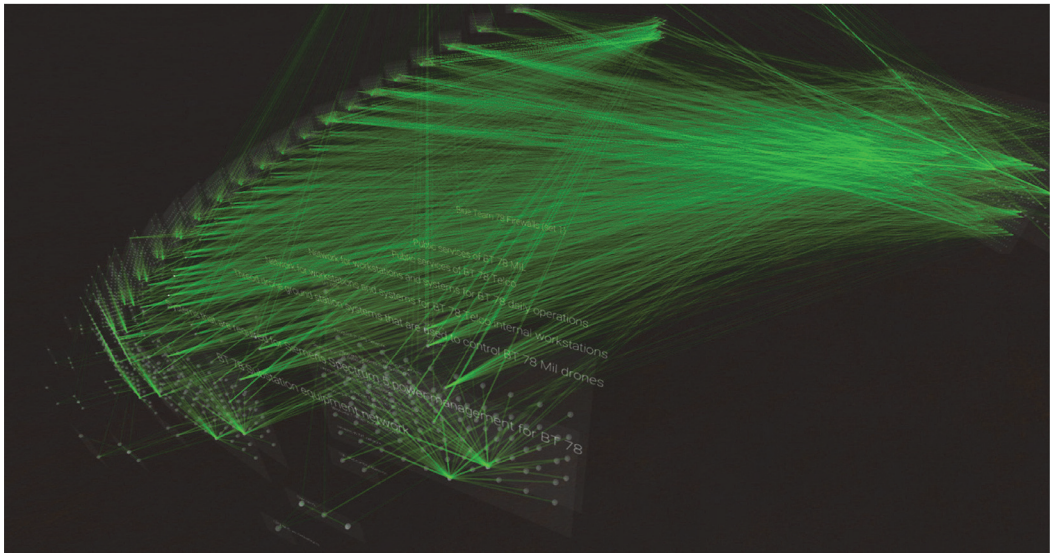


Figure 2-2: NATO CCDCOE Locked Shields CDX Networks Topology Rendered from NATO CCDCOE Locked Shields 2018 Partner Run Dataset, Overlaid with Activity. (Source: Ref. [17].)

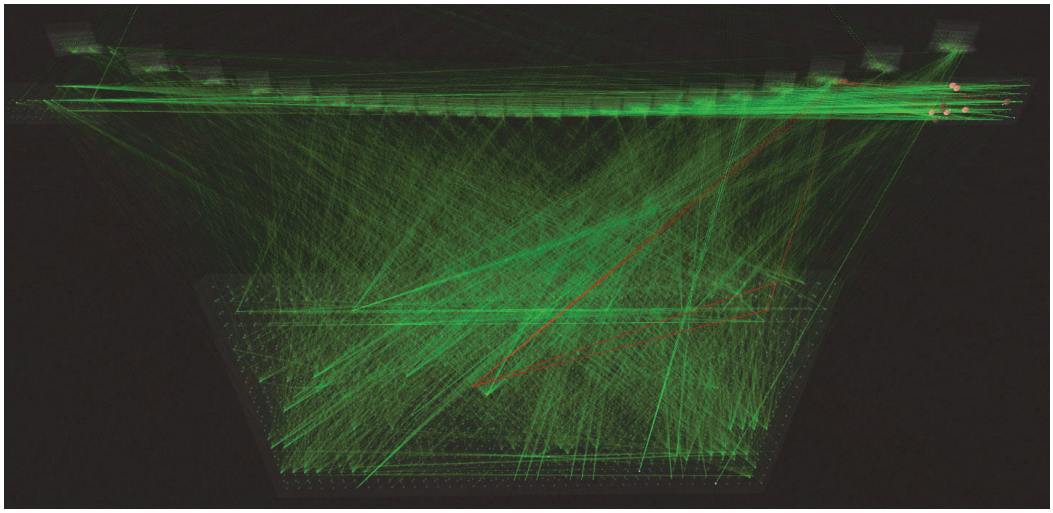


Figure 2-3: Same Constellation as 2-2, but Camera Viewpoint Turned 90 Degrees Clockwise and Moved Behind the "Simulated Internet" Data-Shape; Highlighted (Red) Are Edges Illustrating the Connections of Red Team Activities in Third Blue Team's Drone Control Nodes. (Source: Ref. [17].)

Figure 2-4: Display of a Blue Team's Network Topology and Observed Connections During a Time Window.

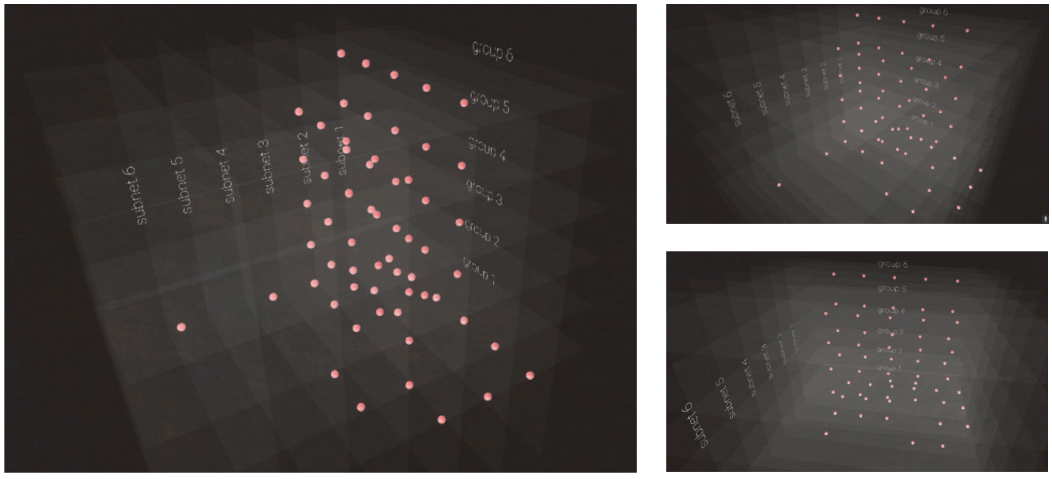


Figure 2-5: Display of a Blue Team's Network Layout Where Entities' Positions on XYZ Axes are Determined by: Z) The Group this Entity Belongs to (a Subnet); Y) Subgroup (a Functional Group in that Subnet: Servers, Networks Devices, Workstations); X) Entity's Sequential (Arbitrary) Position in that Subgroup (for Example the Last Octet of its IP Address). (Source: Refs. [17], [18].)

2.4 EVALUATING DESIGN EFFECTIVENESS

The evaluation of design effectiveness (usefulness and usability) is the final phase of the human factors design process. Once again, users, playing the role of evaluation participants, are essential for meaningful testing. Designing an experiment to evaluate the effectiveness of a design with representative user tasks is the best way to confirm the fit between the user and their work with the visualization/interface/tool that was designed. Measures of human performance, situation awareness, and workload are the three most common metrics for evaluation.

2.4.1 Subjective versus Objective Human Performance Measures

Both subjective and objective measures have a role in evaluation. Subjective measures consist primarily of opinions gathered via questionnaires and interviews and are very helpful early on in the design process. They can point out missing features and bring attention to problems with visualization features, such as labelling, and mismatches between user expectations and feature implementation. However, subjective metrics are limiting and are prone to user biases. For instance, users may not positively rate designs with which they are unfamiliar. Objective measures of performance are typically gathered during an experiment in which a participant must perform a representative task or tasks and quantitative metric such as time and accuracy are recorded. Task analysis information from the analysis phase should provide specific user tasks with which to evaluate performance. Accuracy can be characterized in a number of ways to include a correctness score, number of corrects, number of errors, error rate, false alarm rate, deviations from optimum, percent correct, percent errors, ratio of number correct to number of errors, etc. Time can be characterized as reaction time to a stimulus, search time, marking speed, time to complete a task, etc.

2.4.2 Situation Awareness Measures

Situation Awareness (SA) is simply defined as “being aware of what is happening around you and understanding what that information means to you now and in the future.” [7]. As with human performance measures, there are both subjective SA measures (qualitative opinion data) as well as objective SA measures (quantitative performance data – typically, accuracy of responses to task-relevant probe questions). While self-report SA gathered with subjective SA measures can be useful, objective measures of SA are deemed as more helpful in determining the user’s actual awareness of the situation pertinent to performing a particular task [19]. Table 2-2 shows a partial list of both subjective and objective measures of SA.

Table 2-2: Measures of SA.

Subjective	Objective
Situation Awareness Rating Technique (SART)	Situation Awareness Global Assessment Technique (SAGAT)
Situation Awareness Subjective Workload Dominance (SA-SWORD)	Quantitative Analysis of SA (QUASA)
China Lake Situational Awareness	SA Analysis Tool (SAVANT)
Situation Awareness Behavioral Rating Scale (SABARS)	Situation Present Assessment Method (SPAM)
Mission Awareness Rating Scale (MARS)	Cranfield SA Scale (Cranfield-SAS)

2.4.3 Workload Measures

Workload indicates the level of work that a person is exerting while performing a task. Performance and workload are not negatively correlated (lower workload results in higher performance and higher workload results in lower performance) rather, the relationship between workload and performance is an inverted-U shape. Therefore, there is an optimum range of user workload that results in the highest performance. Too much workload leads to information overload and performance errors; not enough workload leads to boredom and performance errors. As with SA, there are a number of subjective workload measures and objective workload measures [7]. Subjective measures of workload include NASA's Task Load Index (TLX), Subjective Workload Assessment Technique (SWAT), and the Cooper-Harper Scale. Objective measures include physiological measures such as electro-encephalograms and performance measures including task errors and measures of space capacity using secondary tasks.

2.5 SUMMARY

The field of visual analytics focuses on analytical reasoning facilitated by interactive visual interfaces. These interfaces are essential to understanding the analytical techniques applied to data. Therefore, it is of utmost important to design those interfaces using human factors and the user-centered design process. Once the user or users of the visual analytics systems are defined, the phases of analysis, design, and evaluation as described in this chapter can help lead the design team to a system that is both useful and usable.

2.6 REFERENCES

[1] International Ergonomics Association (IEA). What is Ergonomics? https://iea.cc/what-is-ergonomics/ Accessed 10 Apr 2020.

[2] California State University Long Beach. Department of Psychology. Option in Human Factors. http://www.cla.csulb.edu/departments/psychology/ms-human-factors/ Accessed 10 Apr 2020.

[3] Sanders, M., and McCormick, E. (1993). Human Factors in Engineering and Design, 7th Edition, McGraw Hill.

[4] Salvendy, G. (Ed.) (2012). Handbook of Human Factors and Ergonomics, 4th Edition, Wiley.

[5] Norman, D. (2013). The Design of Everyday Things, Basic Books.

[6] Interaction Design Foundation. https://www.interaction-design.org/ Accessed 10 Apr 2020.

[7] Endsley, M., and Jones, D. (2012). Designing for Situation Awareness: An Approach to User-Centered Design, 2nd Edition, CRC Press, p. 13.

[8] Roth, C. (13 Mar 2017). Why Henry Ford's Most Famous Quote is Dead Wrong. https://www.entrepreneur.com/article/290410 Accessed 01 Apr 2020.

[9] Eltin, L.S., Martin, C.G., Cantor, S.B., and Rubenstein, E.B. (5 June 1999). Influence of Data Display Formats on Physician Investigators' Decisions to Stop Clinical Trials: Prospective Trial with Repeated Measures. BMJ.; 318(7197): 1527-1531. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC27896/ Accessed 01 Apr 2020.

[10] Nielsen, J. (24 Apr 1994, updated 15 Nov 2020). 10 Usability Heuristics for User Interface Design. https://www.nngroup.com/articles/ten-usability-heuristics/

[11] Department of Defense Design Criteria Standard: Human Engineering, MIL-STD-1472F, (23 Aug 1999). http://everyspec.com/MIL-STD/MIL-STD-1400-1499/MIL-STD-1472F_208/ Accessed 01 Apr 2020.

[12] Human Factors for Designers of Systems DEF STAN 00-25, Ministry of Defence Standard 00-250 (22 Oct 2012).

[13] ISO. Ergonomics of Human-System Interaction – Part 210: Human-Centred Design for Interactive Systems ISO 9241-210:2019 (Jul 2019). https://www.iso.org/standard/77520.html Accessed 10 Apr 2020.

[14] Furman, S., Theofanos, M., and Wald, H. (Apr 2014). Human Engineering Design Criteria Standards Part 1: Project Introduction and Existing Standards. DHS S&T TSD Standards Project https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7889.pdf Accessed 01 Apr 2020.

[15] Kullman, K., Ben-Asher, N., and Sample, C. (2019). Operator Impressions of 3D Visualizations for Cybersecurity Analysts. ECCWS 2019 18th European Conference on Cyber Warfare and Security, Coimbra, 2019.

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

[17] Kullman, K., Ryan, M., and Trossbach, L. (2019). VR/MR Supporting the Future of Defensive Cyber Operations. 14th IFAC Symposium on Analysis Design and Evaluation of Human Machine Systems, Tallinn, 2019.

[18] Kullman, K., Buchanan, L., Komlodi, A., and Engel, D. (2020). Mental Model Mapping Method for Cybersecurity. 22nd International Conference on Human-Computer Interaction, Copenhagen, 2020.

[19] Gawron, V. (2019). Human Performance and Situation Awareness Measures, 3rd Edition, CRC Press.

Chapter 7 – CYBER SITUATION AWARENESS

Margaret Varga
University of Oxford
UNITED KINGDOM

Carsten Winkelholz and Susan Träber-Burdin
FKIE
GERMANY

Petter Bivall
Swedish Defence Research Agency
SWEDEN

Kaur Kullman
Cognitive Data OÜ
ESTONIA

7.1 INTRODUCTION

We have become more and more dependent on the ever-expanding Internet with its growing complexities and inter-dependencies. While on the one hand we benefit from its immensely powerful infrastructure, we are vulnerable to cyber-attacks which can happen anytime, anywhere and can cause widespread service degradation and network destruction [1], [2], [3], [4].

In 2008, NATO set up the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) in Tallinn [3]. The strategic concept document of NATO 2020 states – responding to the rising danger of cyber-attacks:

> *NATO must "accelerate efforts to respond to the danger of cyber-attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence."* [5].

Cyber Situation Awareness (SA) is vital in support of making informed decisions for maintaining a stable, safe and secure environment [6], [7]. The enhancement of the cyber operators' situation awareness is thus a crucial objective for any user interface design [8], [9], [10], [11], [12].

In addressing parts of the challenges associated with cyber SA the IST-141 group organized an inter-Panel specialists' meeting, IST-HFM-154, on cyber symbology, in Dayton, Ohio (2016). The aim of the meeting was to gather experts, users, and stakeholders to discuss and progress the development of symbols used for cyber information in a NATO context.

This chapter summarizes the work conducted in the IST-141 group regarding cyber SA and cyber symbology, including studies conducted by the IST-141 group in exploring, developing, and comparing user-centered and system-based approaches to facilitate cyber SA.

7.2 CYBER SITUATION AWARENESS

Endsley's work on SA provides an established definition of SA, in particular for dynamic environments:

> *Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future* [13].

Ensley considered that there are three stages of SA, namely: 1) Perception; 2) Comprehension; and 3) Projection [13]. This links cognitive psychology with human factors (see Chapter 2: Human Factors Considerations for Visual Analytics) in the sense making process, and this is particularly important in complex situations such as the cyber domain. In cyber operations Endsley's three stages of SA are closely interlinked and are undertaken in round the clock operations. The necessary awareness covers the network infrastructure in both the physical and the virtual domains. The analysts need to be able to detect, recognize, identify, and communicate trends, patterns, violations, and anomalies in an intuitive and timely manner [5].

Indeed, cyber SA is concerned with the human cognitive process and the processing of data. In the complex and dynamic cyber environment, the quality and the speed of human decision making can be greatly enhanced by acute situation awareness. This chapter reports our study on exploring, developing, and comparing different human machine interface design approaches applicable in addressing the analysis and presentation as well as the use of cyber symbology for cyber SA.

7.3 HUMAN MACHINE INTERFACE DESIGN APPROACHES

Different approaches to human machine interface design can be developed and applied to address the different operational and users' needs, for example:

- User-centered approaches; and
- System-based approaches, such as the Ecological Interface Design (EID).

These two approaches provide SA in a different manner. The user-centered approach is concerned with the users' and the tasks' needs, the users' skills, and limitations, as well as their mental models [8], [14]. While, the EID focuses on the system [15], [16], [17], [18], [19], [20], [21] with the aim to show the complex relationships in the system to the user in a readily informative manner. It is a user interface design particularly suitable for real-time dynamic and complex socio-technical systems [18], [21], [22].

Figure 7-1 and Figure 7-2 show examples of user-centered and system-based approaches for cyber security, details of the work can be found in Refs. [23], [24], [25].

An initial evaluation by analysts was carried out for the user-centric and the EID approaches developed in this study. It was found that the user-centric visualization approach provided an effective means of analyzing, detecting, discovering, and identifying patterns, anomalies, violations, and threats; as well as correlating events, Figure 7-1. The resulting intuitive visualizations are suitable for the provision of detailed information on the performance of network components, such as IPs, ports, protocols, packages, CPU load, disk, and memory usages, etc. The EID visualization, on the other hand, portrayed the logical network topology, the functionalities of the network, depicting the relationships and dependencies between servers, firewalls, etc. It provided a visualization that guided the users to understand the functioning of the network. Once users became familiar with the patterns of the 'normal situation,' they could readily detect any changes from the normal patterns, Figure 7-2. Therefore, in the EID concept, analysts easily saw the operational aspects of the network, i.e., the big picture. The two approaches complement each other in providing awareness and information of different aspects of the network situation [26].

Figure 7-1: User-Centric Approach.

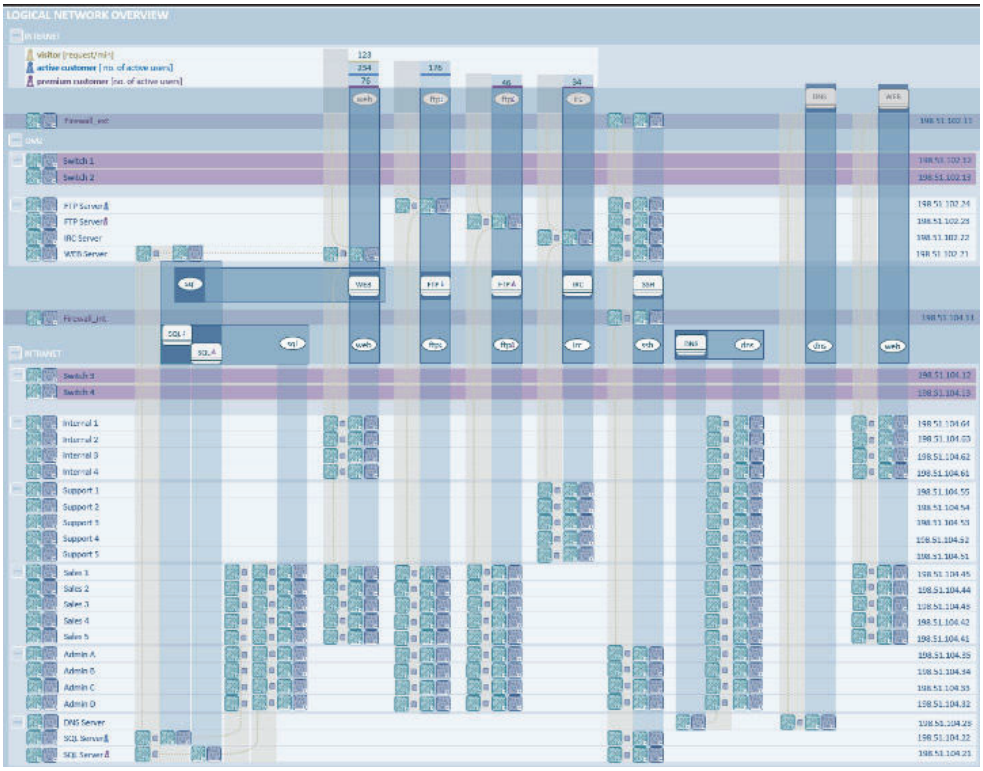


Figure 7-2: System-Based – Ecological Interface Design.

7.4 SYMBOLOGY

Some symbols were created in the above system-based approaches. What is a symbol? A symbol is a representation of an object, idea, emotion, relationship or thought, etc. It can be composed of a combination of words, gestures, sounds, ideas, or visual images. However, users need to learn what they mean and how to associate the symbols with their meaning before they can use them. For example, CO_2 (Carbon dioxide) is an acidic colorless gas with a molecular structure composed of one carbon atom and two oxygen atoms. Some suggest that symbols can be made more intuitive and easier to remember by using pictorial or iconic representations.

In general, symbols that represent physical objects are easy to construct and use; but there is not a natural physical representation for abstract representations of tasks, ideas, actions, thoughts, applications, etc. Symbols can thus be complex, but the key advantage of using a symbol is that it can be given very specific meaning and has great potential as an information carrier. A set of symbols can be created for specific purposes, domains, or applications, and in the case of the cyber domain, to provide an intuitive means of accurately conveying, for example, a networks' status and to make it easier for different users with different backgrounds and levels of expertise to understand the situation of the network.

7.4.1 Symbology, Geo-Spatial and Cyber-Spatial Thinking

Traditionally military operations have always been carried out on the ground, in the air or space, on the water surface or below. In all cases, it has been possible to keep track of the units, activities and events using symbols on a map, that is, the geo-spatial aspect has always been a prominent part of the information flow. The symbol standards used in the United States and by NATO [13], [28], [29], have been developed with these conditions in mind, and with adaptations suitable for military fallback approaches, such as the requirement that all symbols should be possible to draw by hand directly on a map. Cyber, on the other hand, does not follow the geo-spatial boundaries and carries a very different set of challenges when visualized.

Military operations in the geo-spatial world have fairly clear boundaries; an airplane cannot travel indefinitely far in a matter of seconds, a certain number of troops can be expected to be spread out over a limited space, a missile only reaches targets within its range, etc. Cyber is connected to hardware executing instructions and mediating data, but cyber-spatial operations have little to no restrictions with respect to space or time as the structure is more based on activities and abilities of the computational hardware [30], processor microcode [31], peripherals firmware [32], various layers of software [33], [34], and last, but not least, the cyber operators. A server can be located anywhere in the world, activities can move from one country to another in seconds, and automated systems can survey an adversary's network continuously for months. When working with cyber, these differences require a move from geo-spatial thinking to cyber-spatial thinking. How this transition should be achieved and how the visual representations and cyber symbology are to be designed to support the cyber-spatial thinking is a topic for both ongoing and future research. Figure 7-3 aims to illustrate the move from geo-spatial to cyber-spatial using two of the many different types of representations available.

Additionally, the manner in which users interpret symbols, and thus become aware of the situation, its effect and impact, differs a lot between geo-spatial and cyber-spatial representations (symbology). To complicate things further, there are also cases when geo-spatial and cyber-spatial merge, raising a need to relate the cyber situation to missions and operations in the physical space as well as in the logical space [28]. The following is our list of challenges adapted from Refs. [23], [35]:

a) How do icons compare with symbols in conveying the required information?

b) When to use symbols and when to use icons and in what operations/activities/domain(s)/layers ?

c) How to decide what is the intuitive way to depict multiple cyber elements and their associated situations?

d) How to decide what is the intuitive way to depict multiple cyber situations?

e) How much information and detail are necessary for and from different user groups and different operational needs?

f) How to show the temporal elements of a situation?

g) Should cyber symbols be superimposed on geo-spatial maps and / or should other aspects such as the network architecture be included?

h) Scalability.

i) How can user (system) performance be evaluated?

j) User identification and requirement capturing.

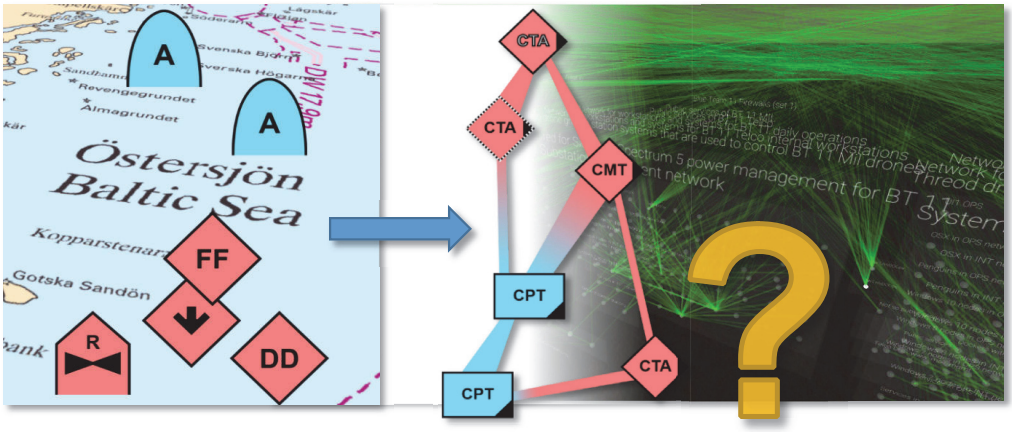


Figure 7-3: Moving from Geo-Spatial to Cyber-Spatial Visual Representations is a Requirement for Successful Cyber SA. How the cyber-spatial representations should be designed is still a topic for research. Left: Traditional geo-spatial symbols; right: alternatives for cyber-spatial representations, including an example from Ref. [36].

7.4.2 MIL-STD-2525D and NATO APP-6

Military Standard (MIL-STD)-2525D is a major document defining the rules and requirements for the development and display of joint military symbology in the US within the Department of Defense (DoD) and non-DoD entities across all services and functions. It is mainly concerned with geographic-centric representation of the physical layer and covers a very wide range of military symbology applications and requirements and includes civilian unit / organization symbols [37]. In June 2014, an initial set of cyber symbols were added to MIL-STD- 2525D through the addition of Appendix L [27].

NATO Standardization Agreement (STANAG) Allied Procedural Publication (APP) 6 is the joint NATO Standard on Military Symbology for maps. The symbols provide a standard set of common operational symbols (Command, Communications and Control Measures symbols) which have been designed to enhance NATO's interoperability in joint and combined (different forces Air/Land/Sea/etc., units, organizations, and nationalities) military operations. It can be used in electronic / automated display systems and manual applications. The symbology consists of graphical symbols for visual representation of physical objects, activities, or events. The symbols are applicable in multi-chrome and monochrome and can be hand drawn. APP-6 also recognizes the need for cyberspace symbology [29].

APP-6 and MIL-STD-2525 aim to develop a comprehensive joint military symbology that is common to both organizations, which covers physical (units, equipment), non-physical (planning) or predicted locations with temporarily assigned characteristics or validity [27], [29], [38]. A 'building block' approach is used to represent their symbology: an icon-based symbol is used to depict units, equipment, installations, activities, and meteorological occurrences, etc. which are located within and around a virtual bounding octagon concept. The octagon can be composed of 1) Frames; 2) Icons; 3) Modifiers and 4) Amplifiers, as well as color, graphics, and alphanumeric representations. Such symbols can be assimilated by users much more readily and effectively than a text (language) based communication, which can be prone to misunderstanding, misinterpretation and imprecision, ambiguity as well as slowness of transmission [37].

The main advantage of these two standards is that they are familiar to the military, thus the incorporation of cyber symbols can be readily accepted; the disadvantages are the adaptation / extension of physical symbols into the non-physical aspects of the cyber domain is complex and may result in misinterpretation.

7.4.3 Other Cyber Symbology Approaches

McCroskey and Mock [39] developed a MIL-STD-2525 compliant symbol set that addresses the lack of effective communication between the physical and cyber domains, having highlighted the risk that decisions on strategic and mission planning will be made without awareness of the network situation, and thus could endanger warfighters. Their MIL-STD-2525 compliant symbol set is concerned with the display of cyber information in the Logical and Persona layers of cyberspace. The advantage of their proposed MIL-STD 2525D compliant cyberspace operational graphics approach is that it is more likely to be accepted by the existing military users. It provides a means to convey cyber information that is relevant to commanders who are unfamiliar with the technical aspects of the cyberspace that affects their decision making. The disadvantage is that it follows a 'pre-cyber' symbology approach which could bound the way symbols could be developed, and therefore, also, the need to show how the physical and logical networks relate to each other.

Examples of standardized geo-spatial symbols and non-standardized cyber-spatial symbols are presented in Figure 7-4.

Geo-spatial	Description	Cyber-spatial	Description
	Friendly airborne fixed wing.		*Shellcode action*, a remote control action.
	Hostile airborne rotary wing.		*Scanner action*, actions aimed at mapping out a network or gaining information about computers.
	Friendly surface vessel.		*Exploit action*, attacks aimed at acquiring privileges on computers.

Figure 7-4: Examples of MIL-STD-2525D Geo-Spatial Symbols (Left) and Cyber-Spatial Symbols Created Independently in the Absence of a Standard (Right). Cyber symbols designed by Jennifer Bedhammar and Oliver Johansson, to be published in a master's thesis at Linköping University, used under permission.

Varga et al. [23] used spider diagrams as a symbol to represent the dynamics of all the parameters on a map of an internal network (an intranet) for each internal host. This provides an intuitive means for the user to visualize the problems readily as they arise, and thus make informed decision to mitigate the problems [23].

In addition to showing the variation (deviation from norm) of parameters for each host, spider diagrams also show characteristic shapes for different states, and these may be recognized easily by an experienced operator. Such visualizations provide a first step in providing diagnostics information. The advantage of this approach is that it provides an effective means of communicating the dynamic status of the logical network which is applicable in both the military and civil domains. The disadvantage is that there is a need to map the different spider diagrams with diagnostic information. However, this approach is non-compliant with any existing Standards, therefore acceptance into the military operation is not straightforward.

Fugate and Gutzwiller [40] also identified that the characteristics of cyberspace operations differ from those in the physical domain, and it is therefore problematic to regard cyberspace representation as a subset of the physical domain operational picture. They consider that re-using the physical space for cyberspace (MIL-STD-2525D) makes it difficult for users familiar with the physical domain, and associated representation, to differentiate the two, i.e., when cyberspace information is treated as physical information it could lead to misinterpretation and hence mis-informed decision making. While their approach is inspired by MIL-STD-2525 they did not restrict their approach to using physical domain symbology to depict cyber effects and actions for cyber threats. They consider a cyber-attack incident reflects the attacker's approach and motivation and designed three symbols to represent three different entities in a cyber incident, namely, devices, users, and software. They represent a device by a square, while a circle represents a user and a hexagon represents software. Vulnerability in a device is indicated by a broken outline. Each entity is also associated with a trust element, which can be unknown, trusted, untrusted, threat or insider. They also address the scalability issue. The advantage of their approach is it can represent a cyber incident based on the three entities. The disadvantage is that, once again, their approach is not compliant with any existing Standards, and therefore adoption into the military domain is not straightforward.

It can be seen, from the above, that there are some possible approaches towards some of the identified cyber symbology challenges, e.g., d) and f). Many of the challenges remain completely open and unaddressed.

7.5 CONCLUSIONS

This chapter discussed the user-centered and system-based approaches to providing different types, levels and perspectives of cyber SA. Cyber symbology was also discussed.

An initial evaluation found that the user-centric approach to SA provides an effective means of analyzing, detecting, discovering, and identifying patterns, anomalies, violations, and threats, as well as correlating events. The visualizations are suitable for the provision of detailed information on the performance of network components.

The EID approach, on the other hand, provides an effective visualization to guide users in their understanding of how networks should function compared to how these networks are actually functioning; thus, analysts can easily see the operational aspects of the network, i.e., the big picture.

The two approaches complement each other in providing awareness and information on different aspects of the network situation.

Cyber symbology has the potential to enable visualization of cyber situation, though there are not yet clear methodologies or solutions as to how it can best be achieved. This chapter lays out cyber symbology challenges

and questions that must be answered by future research; thus, providing a foundation and context for future research programs to develop military cyber symbology.

7.6 REFERENCES

[1] Ablon, L., and Bogart, A. (2017). Zero Days, Thousands of Nights; The Life and Times of Zero-Day Vulnerabilities and Their Exploits. Santa Monica: RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf

[2] Kott, A., Wang, C. and Erbacher, R.F. (Eds.) (Jan 2015). Cyber Defense and Situational Awareness. Springer.

[3] Geers, K. (2011). Strategic Cyber Security, CCD COE Publication, ISBN 978-9949-9040-7-5.

[4] Peng, T., Leckie, C., and Ramamohanarao, K. (2007). Survey of Network-Based Defense Mechanisms Countering the Dos and DDos Problems. ACM Computing Survey, 39(1), 3.

[5] NATO 2020: Assured Security; Dynamic Engagement, 17th May 2010. https://www.nato.int/cps/en/natolive/official_texts_63654.htm.

[6] D'Amico, A., and Whitley, K. (2008). The Real Work of Computer Network Defense Analysts: The Analysis Roles and Processes that Transform Network Data Into Security Situation Awareness. In Proceedings of the Workshop on Visualization for Computer Security (VizSec 2007), Springer, Berlin, pp. 19-37.

[7] Franke, U., and Brynielsson, J. (2014). Cyber Situational Awareness – A Systematic Review of the Literature. Computer and Security, 26, pp. 18-31, Elsevier.

[8] Endsley M.R., and Jones, D.G. (2004). Designing for Situation Awareness: An Approach to User Centered Design, Second Edition, CRC Press, ISBN 9781420063554.

[9] Grégoire, M. and Beaudoin, L. (2004). Visualisation for Network Situational Awareness in Computer Network Defence. NATO IST-043 Visualisation and the Common Operational Picture, Toronto, Sept 2004.

[10] Lahmadi, A., and Beck, F. (2015). Powering Monitoring Analytics with ELK Stack. 9th International Conference on Autonomous Infrastructure, Management and Security, June 2015, Ghent, Belgium.

[11] Lavigne, V., and Gouin, D. (2014). Visual Analytics for Cyber Security and Intelligence. The Journal of Defence Modeling and Simulation: Applications, Methodology, Technology, April 2014. http://dms.sagepub.com/content/11/2/175.

[12] Varga, M.J., Winkelholz, C., Träber-Burdin, S., and Bivall, P. Cyber Situation Awareness, International conference of Cyber Defence, 13th – 14th April, 2018, Sofia, Bulgaria. (invited).

[13] Endsley, M.R. Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors, 37(1), pp. 32-64, March 1995.

[14] McKenna, S., Staheli, D., and Meyer, M. (2015). Unlocking User-Centered Design Methods for Building Cyber Security Visualizations. IEEE Symposium on Visualization for Cyber Security (VizSec), 2015.

[15] Bennett, K.B. (2014). VEILS: An Ecological Interface for Computer Network Defense. Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting, 2014.

[16] Burns, C.M., Kuo, J., and Ng, S. (2003). Ecological Interface Design: A New Approach for Visualizing Network Management. Computer Networks 43, pp. 369-388, Elsevier.

[17] Burns, C.M. (2000). Putting It All Together: Improving Display Integration in Ecological Displays. Human Factors 42, pp. 224-241.

[18] Rasmussen, J., and Vicente, K.J. (1989). Coping with Human Errors Through System Design: Implications for Ecological Interface Design. International Journal of Man-Machine Studies, 31, pp. 517-534.

[19] Rasmussen, J. (1985). The Role of Hierarchical Knowledge Representation in Decision Making and System Management. IEEE Transactions on Systems, Man and Cybernetics, 15, pp. 234-243.

[20] Rasmussen, J. (1983). Skills, Rules, Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man and Cybernetics, 13, pp. 257-266.

[21] Rasmussen, J. (1974). The Human Data Processor as a System Component. Bits and Pieces of a Model. Risø National Library, Risø-M No. 1722.

[22] Vicente, K., and Rasmussen, J. (1992). Ecological Interface Design: Theoretical Foundations, IEEE Transactions on Systems, Man and Cybernetics 22, pp.1-18.

[23] Varga, M.J., Winkelholz, C., and Träber-Burdin, S. (2019). An Exploration of Cyber Symbology. IEEE VizSec, 23rd Oct 2019, Vancouver, Canada.

[24] Varga, M.J., Winkelholz, C., and Träber-Burdin, S. (2018). An Exploration of User Centered and System Based Approaches to Cyber Situation Awareness. 15th IEEE Symposium on Visualization for Cyber Security (VizSec), 22nd Oct 2018, Berlin, Germany.

[25] Varga, M.J., Winkelholz, C., and Träber-Burdin, S. (2018). Exploration of User Centered and System Based Approaches to Cyber Situation Awareness. NATO HFM-288 Research Workshop on Integrated Approach to Cyber Defence: Human in the Loop, 16th – 18th Apr 2018, Sofia, Bulgaria.

[26] Varga, M.J., Winkelholz, C., and Träber-Burdin, S. (2017). Exploration of User Centered and System Based Approaches to Cyber Situation Awareness. 14th IEEE Symposium on Visualization for Cyber Security (VizSec), 2 Oct 2017, Phoenix, USA.

[27] Department of Defense (2014). Interface Standard Joint Military Symbology, MIL-STD-2525D, 10 June 2014. M.R., Endsley. Toward a theory of situation awareness in dynamic systems. Human Factors, 37(1), 32-64, March 1995.

[28] Joint Publication 3-12, Cyberspace Operations, 8 June 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf Accessed 26 May 2019

[29] NATO. (2011). Allied Procedure Publication (APP) – 6(c) NATO Joint Military Symbology, May 2011. https://web.archive.org/web/20150921231042/http://armawiki.zumorc.de/files/NATO/APP-6(C).pdf

[30] Intel. (n.d.). Intel Product Security Center Advisories. https://www.intel.com/content/www/us/en/security-center Accessed 02 May 2020.

[31] Bitdefender (02 Oct 2020). LVI-LFB Side-Channel Attack. https://www.bitdefender.com/business/cyber-threats/lvi-lfb-attack.html Accessed 28 Apr 2020.

[32] Cojocar, L., Kim, J., Patel, M., Tsai, L., Saroiu, S., Wolman, A., and Mutlu, O. (2020). Are We Susceptible to Rowhammer? An End-to-End Methodology for Cloud Providers. 41st IEEE Symposium on Security and Privacy (S&P). Internet, 2020. Retrieved from https://www.microsoft.com/en-us/research/publication/are-we-susceptible-to-rowhammer-an-end-to-end-methodology-for-cloud-providers/

[33] Carnegie Mellon University. (n.d.). Beware of Compiler Optimizations. Retrieved from https://wiki.sei.cmu.edu/confluence/display/c/MSC06-C.+Beware+of+compiler+optimizations. Accessed on April 28, 2020.

[34] MITRE Corporation. (n.d.). ATT&CK Matrix for Enterprise. https://attack.mitre.org/ Accessed 28 Apr 2020.

[35] Varga, M.J., Winkelholz, C., Träber-Burdin, S., Liggett, K., Werner, K., Bivall, P., and Lavigne, V.A (2016). A Consideration of the Application of Icons and Symbols in Cyber Situation Awareness. NATO IST-HFM-154 Cyber Symbology Specialists' Meeting, 28th – 30th Nov 2016, Dayton, USA.

[36] Kullman, K., Ryan, M., and Trossbach, L. (2019). VR/MR Supporting the Future of Defensive Cyber Operations, NATO Computer Aided Analysis, Exercise, Experimentation Forum, 2019.

[37] Andrews, M., and Loveridge, S. (2016). Joint Symbology Standard Management in the Military Domain. NATO IST-HFM-154 Specialists' Meeting on Cyber Symbology, 28th – 30th Nov 2016.

[38] McGrane, B., Bohling, J., and Eple, M. (2016). Development, Distribution and Management of a Common Cyber Symbology for Joint Military Planning and Operations. NATO IST-HFM-154, Cyber Symbology Specialists' Meeting, 28th – 30th November 2016, Ohio, USA.

[39] McCroskey, E.D. and Mock, C.A. (2017). Operational Graphics for Cyberspace. Joint Force Quarterly 85, 2nd Quarter, 2017.

[40] Fugate, S.F., and Gutzwiller, R.S. (2016). Rethinking Cyberspace Symbology. NATO IST-HFM-154, Cyber Symbology Specialists' Meeting, USA, November 2016.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-IST-141 AC/323(IST-141)TP/1079	ISBN 978-92-837-2396-7	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Exploratory Visual Analytics

7. Presented at/Sponsored by

This is the Technical Report of the NATO IST-141 Research Task Group "Exploratory Visual Analytics."

8. Author(s)/Editor(s)	9. Date
Multiple	February 2023
10. Author's/Editor's Address	**11. Pages**
Multiple	124

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Artificial intelligence; Batch processing; Counter Improvised Explosive Device (C-IED); Decision support; Deep learning; Exploratory visual analytics; Improvised Explosive Device (IED); Maritime situation awareness; Network analysis; Simulation analysis; Situation awareness; Social media; Storytelling; Trend analysis; Visualization

14. Abstract

Information superiority is one of the primary enablers for military dominance; the exploitation of all relevant information from multiple sources is a key factor for NATO's information superiority. Visualization and visual analytics research are essential to address the needs of the 2015 NATO targets of emphasis in Information Analysis (IA) and Decision Support (DS): IA&DS-1 on Decision Support and IA&DS-2 on Big Data and Long Data Processing and Analysis.

Visual analytics is the science of analytical reasoning facilitated by interactive visual interfaces. The Group investigated, researched and fostered collaborations in knowledge extraction and data analysis for timely situation awareness to support effective decision making. The IST-141 group researched, developed and applied exploratory visual analytics techniques: 1) To exploit and make sense of large and complex data sets, i.e., Big Data; 2) To help make tacit knowledge explicit; 3) To provide acute situation awareness, and 4) To support informed decision making across a wide range of defence and security application domains including cyber, maritime, genomics and social media domains, as well as post analysis and in situ visualization for simulation data.

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS
STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document
Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and
Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2396-7

Appendix 8

Publication VIII

Ask, Torvald F.; Kullman, Kaur; Sütterlin, Stefan; Knox, Benjamin J.; Engel, Don; Lugo, Ricardo G.; (2023). A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. Front. Big Data 6:1042783. DOI: 10.3389/fdata.2023.1042783

frontiers | Frontiers in Big Data

TYPE Original Research
PUBLISHED 27 January 2023
DOI 10.3389/fdata.2023.1042783

Check for updates

OPEN ACCESS

EDITED BY
Mohammed Saqr,
University of Eastern Finland, Finland

REVIEWED BY
Martin Drasar,
Masaryk University, Czechia
Zhi Liu,
Central China Normal University, China

*CORRESPONDENCE
Torvald F. Ask
✉ torvaldfask@gmail.com

SPECIALTY SECTION
This article was submitted to Cybersecurity and Privacy, a section of the journal Frontiers in Big Data

RECEIVED 13 September 2022
ACCEPTED 10 January 2023
PUBLISHED 27 January 2023

CITATION
Ask TF, Kullman K, Sütterlin S, Knox BJ, Engel D and Lugo RG (2023) A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. *Front. Big Data* 6:1042783. doi: 10.3389/fdata.2023.1042783

COPYRIGHT
© 2023 Ask, Kullman, Sütterlin, Knox, Engel and Lugo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness

Torvald F. Ask[1,2]*, Kaur Kullman[3,4], Stefan Sütterlin[2,5,6], Benjamin J. Knox[1,2,7], Don Engel[4] and Ricardo G. Lugo[1,2]

[1]Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway, [2]Faculty of Health, Welfare and Organization, Østfold University College, Halden, Norway, [3]Doctoral School of Information and Communication Technology, Institute of Computer Science, Tallinn University of Technology, Tallinn, Estonia, [4]Center for Space Sciences and Technology, University of Maryland, Baltimore County, Baltimore, MD, United States, [5]Faculty of Computer Science, Albstadt-Sigmaringen University, Sigmaringen, Germany, [6]Centre for Digital Forensics and Cybersecurity, Tallinn University of Technology, Tallinn, Estonia, [7]Norwegian Armed Forces Cyber Defense, Oppland, Norway

Background: Cyber defense decision-making during cyber threat situations is based on human-to-human communication aiming to establish a shared cyber situational awareness. Previous studies suggested that communication inefficiencies were among the biggest problems facing security operation center teams. There is a need for tools that allow for more efficient communication of cyber threat information between individuals both in education and during cyber threat situations.

Methods: In the present study, we compared how the visual representation of network topology and traffic in 3D mixed reality vs. 2D affected team performance in a sample of cyber cadets ($N = 22$) cooperating in dyads. Performance outcomes included network topology recognition, cyber situational awareness, confidence in judgements, experienced communication demands, observed verbal communication, and forced choice decision-making. The study utilized network data from the NATO CCDCOE 2022 Locked Shields cyber defense exercise.

Results: We found that participants using the 3D mixed reality visualization had better cyber situational awareness than participants in the 2D group. The 3D mixed reality group was generally more confident in their judgments except when performing worse than the 2D group on the topology recognition task (which favored the 2D condition). Participants in the 3D mixed reality group experienced less communication demands, and performed more verbal communication aimed at establishing a shared mental model and less communications discussing task resolution. Better communication was associated with better cyber situational awareness. There were no differences in decision-making between the groups. This could be due to cohort effects such as formal training or the modest sample size.

Conclusion: This is the first study comparing the effect of 3D mixed reality and 2D visualizations of network topology on dyadic cyber team communication and cyber situational awareness. Using 3D mixed reality visualizations resulted in better cyber situational awareness and team communication. The experiment should be repeated in a larger and more diverse sample to determine its potential effect on decision-making.

KEYWORDS

mixed reality, 3D network topology visualization, cyber team communication, Virtual Data Explorer, shared mental model, cyber situational awareness, human factors, cybersecurity

1. Introduction

Decision-making in Cyber Threat Situations (CTSs) is subject to many challenges due to the interconnectedness between decision-making agents and assets in cyber and physical space, and the high levels of uncertainty inherent to the cyber domain (Jøsok et al., 2016). This results in decision-making often having to be made on an insufficient information basis which makes it difficult to predict the impact of decisions on own and third-party assets, as well as on adversarial behavior (Jøsok et al., 2016). Other challenges to decision-making include competence differences between analyst-level and decision-making personnel (Knox et al., 2018), which are roles that often are assigned to different individuals within organizations doing cybersecurity operations (e.g., Security Operation Centers; SOCs).

Due to the interconnectedness between assets and decision-making agents in the cyber and physical domains and the resulting human-human and human-machine interactions, cybersecurity operations unfold in a complex sociotechnical system. According to the Situational Awareness (SA) model (Figure 1A) proposed by Endsley (1988, 1995), establishing SA for decision-making in sociotechnical systems is achieved in three levels, where all levels must be achieved in order to have full SA.

SA Level 1 is the perception stage and involves perceiving the elements in a situation. SA Level 2 is the comprehension stage and involves understanding the relationship between the perceived elements. SA Level 3 involves using the understanding of the relationship between the elements to predict future states of the system that the situation is occurring in, and how those future states will be affected by decision-making (Endsley, 1995).

In a cybersecurity setting, SA is increasingly referred to as Cyber SA (CSA; Barford et al., 2009; Franke and Brynielsson, 2014). Extending on the formal definition of SA (Endsley, 1988), CSA is considered a subset of SA and can in general terms be defined as "*the perception of the elements in the [cyber] environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future*" (Franke and Brynielsson, 2014, p. 4). It should be noted, however, that it is acknowledged that actions in the physical domain may influence events in cyberspace and *vice versa* (Jøsok et al., 2016). Consequently, stakeholders and decision-makers are often required to have a SA that simultaneously accounts for the impact of decisions in both the cyber and the physical domain.

Seven requirements for achieving CSA for cyber defense decision-making have been suggested (Barford et al., 2009). These requirements can be arranged under the SA model proposed by Endsley (Figure 1B). To achieve SA Level 1 during a CTS, one must have perceived indicators of compromise allowing for (1) awareness of the current situation; (2) awareness of the impact of the attack; (3) awareness of adversarial behavior; and (4) awareness of the quality and trustworthiness of CSA information. To achieve SA Level 2, one must have (5) awareness of why and how the current situation is caused (e.g., if it is an automatic or directed attack), and (6) awareness of how situations evolve. To achieve SA Level 3, one must be able to (7) assess plausible future outcomes.

Decision-making in CTSs is based on communication between human agents that often differ in technical competence (Knox et al., 2018). The point of communication is to establish a shared CSA between the analyst and the decision-maker such that the decision-maker can make good cyber defense decisions. This communication happens in the form of the analyst communicating a Recognized Cyber Picture (RCP) which is based on the analyst's CSA and contains carefully selected and actionable cyber threat information tailored to the needs of the recipient (Ahrend et al., 2016; Staheli et al., 2016; Ask et al., 2021a). A recent review of performance-related factors in SOC teams suggested that insufficient communication was among the biggest challenges faced by SOC team analysts but also one of the least researched topics (Agyepong et al., 2019). Another recent review (Ask et al., 2021a) that specifically looked at communication between humans in CTSs found that (a) there were no common best practices for information sharing; (b) technological aids (e.g., visualization tools and information sharing platforms) were not suited to fit the needs of the analysts; (c) there was a lack of studies simultaneously assessing individual- and team-level performance metrics; and (d) there was a general need for developing shared mental models for effective cyber threat communication.

In contrast to many other working environments, the personnel working within the cyber domain (NATO Cooperative Cyber Defense Center of Excellence, 2016) do not have direct sensory access to the space where events are taking place. In other words, when cyber personnel such as analysts are establishing CSA they are essentially trying to predict the future state of an environment they cannot directly observe. Instead, they are dependent on (1) tools that can detect and visualize events and activities in their cyber domain; and (2) their own mental models of that space. This may be a source of friction when relaying information between individuals because different individuals may have different mental models of the same phenomena, with corresponding differences in their understanding of the causal relationships contributing to those phenomena. This may affect what information different individuals think is important during a cyber threat situation (Ask et al., 2021a). For instance, previous research on the RCP needs of local- and national-level stakeholders in Sweden showed that no one listed knowledge about adversarial behavior as important for their RCPs (Varga et al., 2018). If awareness of adversarial behavior is required for achieving SA Level 1 during a CTS and is necessary to make good cyber defense decisions (Barford et al., 2009), then ignoring information of adversarial behavior may result in an insufficient CSA. Thus, stakeholders may have a mental model of causal relationships during a CTS that affect what kind of prioritizations they have and decisions that they make based on those prioritizations (Ask et al., 2021a).

While developing shared mental models have been suggested to ensure successful RCP communication during CTSs (Steinke et al., 2015; Ask et al., 2021a), little is known about the effect of visualization tools for cyber threat information communication and shared CSA such as how network topology is represented visually. The mammalian brain has evolved a neural architecture with an innate ability to process and understand information that relates to time and space (Eichenbaum, 2014; Ray and Brecht, 2016; Berggaard et al., 2018). Typical representations of network topology are in two dimensions (2D), which loses temporal and spatial relationships between nodes in the network, in addition to not scaling well with increased (but often necessary) complexity. Virtual Reality (VR) and Mixed Reality (MR) tools that are able to visualize CSA-relevant information such as network topology as 3D objects in space and time, may aid in the development of shared mental models for efficient RCP communication between technical and non-technical personnel (Kullman et al., 2018, 2019a,b, 2020). For instance, SA level 3 is the most vital stage for decision-making and appears to

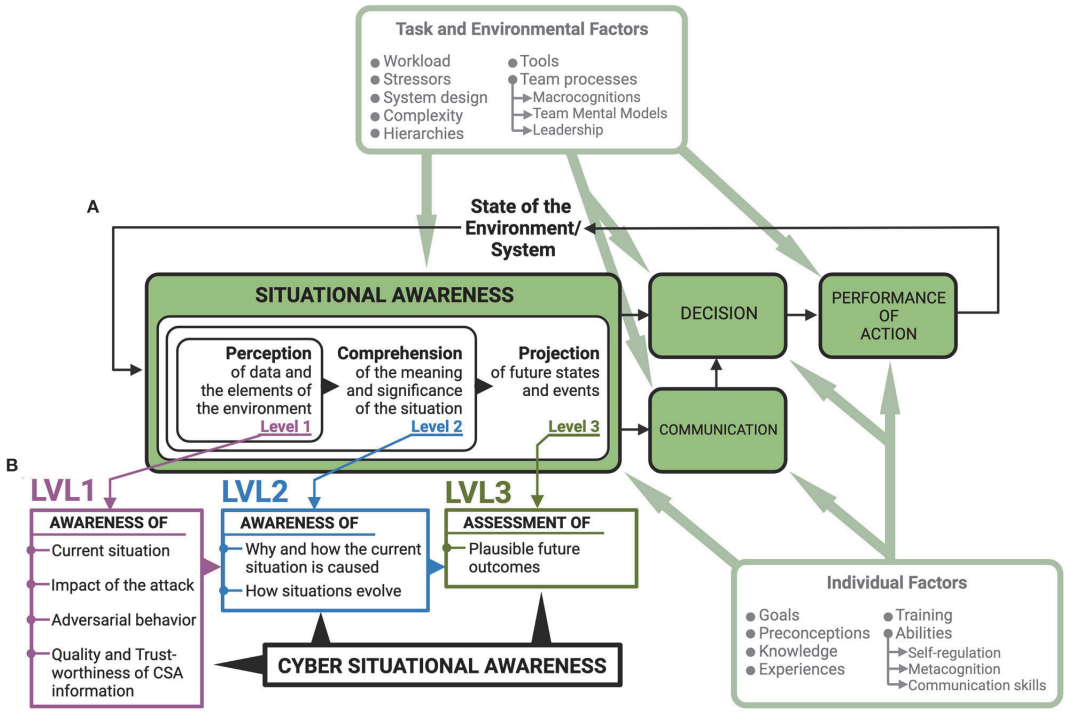


FIGURE 1
Situational Awareness model with suggested requirements for achieving Cyber Situational Awareness. **(A)** Situational Awareness is achieved in three stages (Endsley, 1995). To account for the separation between analysts and decision-makers in SOCs (Knox et al., 2018; Ask et al., 2021a), a "communication" element has been added to the model. **(B)** Seven requirements that can be organized under the Endsley model need to be met to achieve Cyber Situational Awareness for cyber defense (Barford et al., 2009). Establishing Cyber Situational Awareness, communicating for shared Cyber Situational Awareness, and decision-making based on Cyber Situational Awareness is influenced by individual factors such as emotion, metacognition, self-regulation, and communication skills (Jøsok et al., 2016, 2019; Knox et al., 2017, 2018; Ask et al., 2021b, 2023; Sütterlin et al., 2022) and task and environmental factors such as team-processes including macrocognitions, team mental models, and leadership (Jøsok et al., 2017; Ask et al., 2021a). Modified from Lankton (2007).

be the stage that is the most dependent on human working memory (Gutzwiller and Clegg, 2013). 3D visualizations of network topology in VR/MR may leverage automatic neurocognitive processes for encoding spatial information (Stackman et al., 2002; Angelaki and Cullen, 2008; Moser et al., 2008) when individuals are establishing a shared mental model of events in the network. If this allows CTS information to be encoded more efficiently (e.g., Legge et al., 2012; Wagner et al., 2021), it may also allow for more working memory capacity to be allocated to sharing knowledge about the course and impact of current and future events. Reducing the load on working memory may in turn support establishing shared SA level 3 (Gutzwiller and Clegg, 2013) for decision-making in CTSs (Kullman et al., 2019a).

Studies on VR navigation in humans and mice (Bohbot et al., 2017; Safaryan and Mehta, 2021) showed that they were able to generate brain waves in areas relevant for navigation, attention, learning, and memory (Winson, 1978; Seager et al., 2002). Similarly, previous VR research in humans showed that participants were able to use knowledge about the relationship between geometrical shapes in abstract space to navigate that space in a first-person VR navigation task (Kuhrt et al., 2021). This may further indicate that 3D visualizations that allow for exploring and interacting with network data in a way that facilitates spatial encoding of CSA information could leverage neurocognitive processes (Stackman et al., 2002; Angelaki and Cullen, 2008; Moser et al., 2008) that are currently underused in cyber defense.

The Virtual Data Explorer (VDE; Kullman et al., 2018, 2019a) was developed to visualize network topology in a manner that is idiosyncratic to the mental models that analysts use to conceptualize the network (Figure 2). Based on interviews with expert analysts, the VDE is able to visualize the relationship between nodes in an actual network in space and time (Kullman et al., 2018, 2019a,b, 2020). The visualizations produced by the VDE are interactive and can be shared between individuals, even remotely, thus allowing for collaborative development of shared mental models of events in the network. The VDE may therefore be a useful aid in the knowledge-transfer between technical and non-technical personnel such that shared CSA can be achieved to facilitate good cyber defense decision-making (Kullman et al., 2019a).

The VDE uses two distinct sets of information to visualize network topology: (1) the nodes included in a set of network traffic, and (2) mockup connections during a specified time-window or an

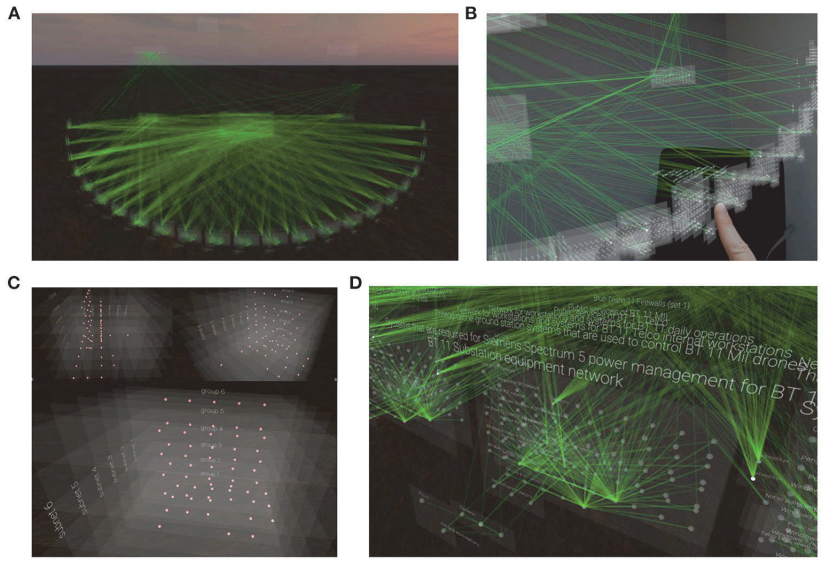


FIGURE 2
Visualization of network topography using the Virtual Data Explorer app. **(A)** Full overview of the metashape of the actual network that was used during the NATO CCDCOE 2018 Locked Shields event as visualized in VR using the VDE app. **(B)** An individual interacting with the network topography in MR. **(C)** A close-up of nodes in the network from different angles and without the edges representing the connections between them. **(D)** A close-up of Blue Team nodes in the network with descriptive information and the edges that connect them. Images taken from Kullman et al. (2019a).

attack path (Kullman et al., 2018). For the sake of clarity, we want to specify that the VDE is not a tool for carrying out forensic analyses. Instead, by visualizing network topology in time and space according to the mental model of the operator (Kullman et al., 2018, 2019a), the VDE may be a neuroergonomic tool for analysts to deepen their own understanding of how a CTS relates to the network they are tasked with defending, and for sharing CSA in complex working environments such as cybersecurity (Kullman and Engel, 2022a,b).

In the present study, we assess the effect of 3D visualization of network topology on communication and collaboration for CSA and cyber defense decision-making. The aim of this study is to determine if a 3D MR representation of a network attack, visualized by VDE is better than a 2D representation for (1) achieving Cyber Situational Awareness; (2) cyber team communication; and (3) decision-making among cooperating dyads during a simulated CTS.

2. Materials and methods

2.1. Ethics statement

This study was conducted under the Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations (ACDICOM) project.[1] The present study conformed to institutional guidelines and was eligible for automatic approval by the Norwegian Social Science Data Services' (NSD) ethical guidelines for experimental studies. Participation was voluntary and all participants were informed about the aims of the study; the methods applied; that they could withdraw from participation at any time and without any consequences; and that, if they did so, all the data that was gathered from them would be deleted. After volunteering to participate in the study, participants were asked to provide informed consent on the first page of an online form where baseline data was collected. Participants were asked to generate and remember a unique participant ID that they would use during data collection for the duration of the study.

2.2. Participants and design

This experiment employed a pseudo-randomized head-to-head design using VDE in the experimental condition and the packet capture software Arkime (formerly Moloch) as the control condition. Participants ($N = 22$, mean age = 22.5, female = 5) were cyber cadets recruited from the Norwegian Defense University College, Cyber Academy (NDCA). Half of the cadets were specializing in military Information Communication Technology (ICT) systems while the other half were specializing in cyber operations.

The study consisted of two parts distributed over 3 days, where day one was used for gathering informed consent, and collecting demographic and baseline cognitive trait data. Results related to the cognitive data will be reported elsewhere. Day two and three was used for the experiment. After providing informed consent and filling out initial questionnaires, participants were randomized in dyads and allocated to either the VDE or the Arkime condition. During the experiment, dyads had to collaborate to familiarize themselves

1 RCN #302941. Project website: https://www.hiof.no/hvo/vlo/english/research/projects/acdicom/.

with the network topology and to identify indicators of compromise. The participants in the VDE condition used HoloLens 2 (Microsoft) for the MR visualizations of network topology as their only aid. The participants in the Arkime condition also had a 2D schematic illustration of the network topology available to them in paper format.

The network topology and activity used for this experiment was visualized using network data from the 2022 Locked Shields Cyber Defense Exercise (CDX) provided by the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE). The experiment lasted for approximately 2 h per dyad.

2.3. HoloLens 2

Microsoft HoloLens 2 (Microsoft, Redmond, DC) has become the most common MR headset to be used for various research studies, fielded by enterprises and governments for Interactive Stereoscopically Perceivable Multidimensional Data Visualizations (ISPMDV; see Kullman and Engel, 2022b for an introduction), where its mostly used for either geospatial or natively spatial datasets. For the purposes of this study, HoloLens 2 was chosen for its capabilities, ease of software development, and existing compatibility with VDE.

2.4. The Virtual Data Explorer and visualization of network topology

VDE (Kullman et al., 2018, 2019a,b, 2020; [https://coda.ee/]) enables a user to perceive the spatial layout of a dataset, for example the topology of a computer network, while the resulting ISPMDV (Kullman and Engel, 2022a,b) can be augmented with additional data, like TCP/UDP session counts between network nodes. Users can customize ISPMDV layouts using textual configuration files that are parsed by a VDE Server and used while showing the visualization by a VDE Client.

VDE functionality is decoupled to server and client components in order to accommodate timely processing of large query results (from the user's dataset) in a more powerful environment (than a wireless MR headset) before data is visualized either by a VR or MR headset. The VDE Server also acts as a relay to synchronize the visualizations (e.g., grabbed objects position in connected users' views) between connected users' sessions so that a connected user's actions manipulating a visual representation of data can be synchronized with other connected users working with that same dataset.

Only a subset of VDE capabilities was employed in the present study: the dataset was preloaded to the headset along with the application (to avoid any possible networking related issues) while VDE Server was used only to facilitate multi-user sessions.

A previous study indicated that there was a need for more experimental collaboration between cognitive scientists and CDX organizers (Ask et al., 2021a). For this study, a NATO CCDCOE Locked Shields 2022 CDX Blue Team's network topology was visualized for the participants with VDE and overlaid with edges (network session counts) between cubes (networked entities). Within view at any given time (depending on user's location and direction) were up to 958 nodes and groups, with up to 789 edges.

All study participants perceived the ISPMDV being positioned in the same location and direction in the room where the study was conducted (see Figure 3A, image on the left). Participants did not have the capability to reposition the visualization components permanently, but they could grab (pinch) a node to better understand its connections while temporarily moving the node around. Once the participant let go of the node, it returned smoothly to its initial location.

As the study participants did not have prior knowledge of Locked Shields 2022 networks and topology, the topology visualization they experienced was not created based on their mental models (as would be the suggested course of using VDE after employing mental model mapping method for cybersecurity; Kullman et al., 2020). Instead, the participants received an introduction about the topology as described in the task one procedures (Section 2.7.1.).

2.5. Arkime packet capture software

Arkime (v3.4.2 [https://arkime.com/]) was used for preparing the dataset from Locked Shields 2022 network traffic both for the VDE ISPMDV view, as well as for the comparative group that used 2D and textual information. Participants were given access to an Arkime instance and taught the basics of using its interface (Sessions and Connections tabs). In the Connections tab, participants had a 2D graph view (see Figure 3B, image on the right) onto the exact same set of nodes and edges that VDE participants had with HoloLens. When participants hoovered over the edges connecting nodes (hosts) to each other, the amount of traffic was displayed on a left-hand panel as described in the task two procedures (Section 2.7.2.).

2.6. Hardware functionality and operational stability

The HoloLens 2 headsets had a tendency to overheat after a period of use, upon which the Windows Operating System running the headset froze the VDE application. This left the network visualization flickering in the user's view. As this issue only started to manifest during the second half or the 1st day of the study, we suspected that the problem originated from thermal issues. To keep the study going, we relied on three HoloLens 2 headsets, of which two were used by a dyad on the floor while the third one was being charged. Rapid charging and then discharging while the headset's GPU and CPU were being heavily utilized by the VDE application seemed to have been too much for the headset's thermal dissipator. Switching a participant's malfunctioning headset during a trial was sub-optimal, hence we needed a more sustainable setup. The solution for the HoloLens 2 overheating problem was to use power delivery capable battery packs. The setup on the 2nd day was for the users to wear the headsets, while having battery packs in their pockets that were connected to the headsets with power delivery capable cables. This allowed the headsets to be used uninterrupted for the duration of a given dyad's trial.

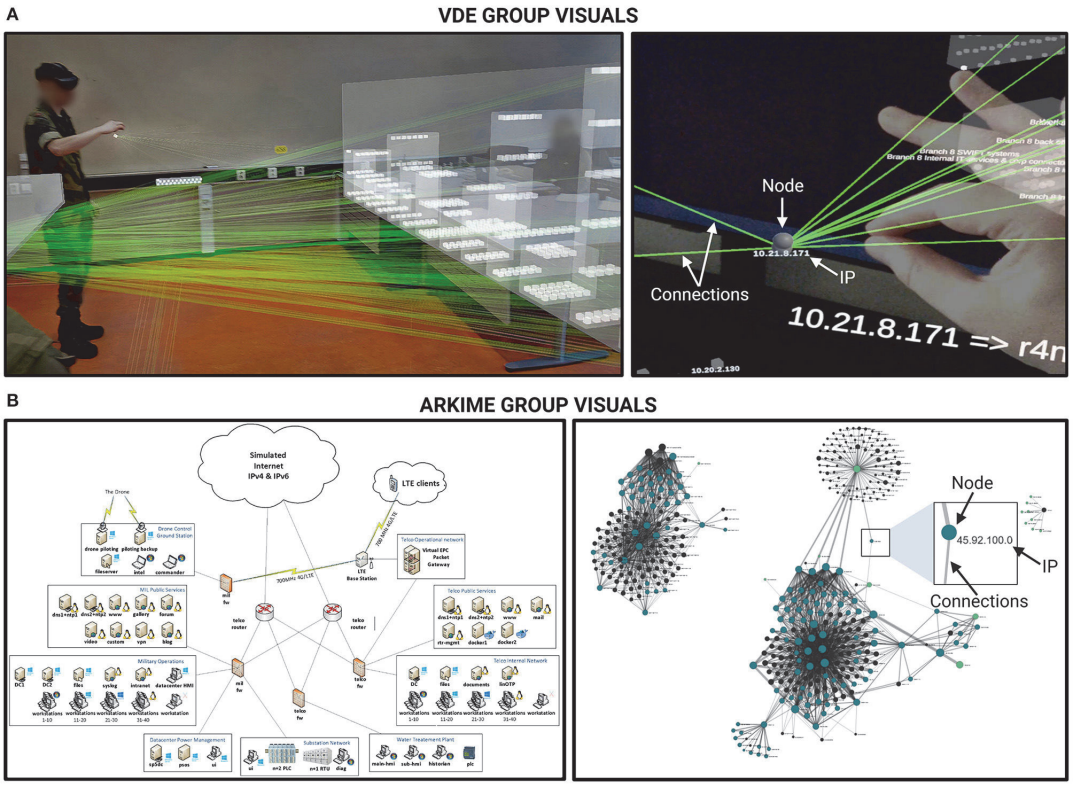


FIGURE 3
Overview of the visualization tools used in each condition. **(A)** The Virtual Data Explorer (VDE) representation of the network topology. The first image in the panel (left-hand side) depicts an overview of the network layout used in the present study. The second image (right-hand side) is a representative close-up (taken from Kullman and Engel, 2022a). White arrows have been superimposed on the image on the right to indicate node/hosts, edges that represent connections between nodes, and the host IP address. **(B)** Images depicting the 2D network topology as shown in the Arkime condition. The first image in the panel (left-hand side) depicts an approximation of the 2D representation of network topology as shown in the paper schematics. The second image (right-hand side) depicts a graph representation of the network topology as shown in the Arkime software, where dots are hosts and edges are the connections between them. Participants could zoom in, select nodes to see exclusive connections, session number, and so on. Black arrows have been superimposed on the image on the right to indicate node/host, edges that represent connections between nodes, and the host IP address.

2.7. Procedure

The study was conducted at the NDCA. The two experimental conditions were conducted in parallel, one dyad at a time, and in separate rooms that were secluded from other activities. The experiment consisted of two parts. In the first part, one participant from each dyad was introduced to the network topology which they then had to explain to the other participant in the dyad. In the second part, participants in each dyad had to collaborate to identify indicators of compromise. Measurements were done thrice; baseline measures upon arrival and then outcome measures after each part of the experiment. For the outcome measures after each part, participants filled out questionnaires assessing task success, confidence in answers, and how they experienced communicational, coordination, emotional, and performance monitoring load related to their teamwork. After part two the participants also had to answer some CSA-related questions that they were not explicitly asked to solve in the task instructions they were given. During the experiment, verbal communication and the time dyads spent on finishing each task was scored by observers. Figure 4 shows an overview of the study and each part of the experiment.

2.7.1. Task one: Understanding the network topology

Upon arriving at the experiment, both participants in the dyad were given a link to the online form which they accessed with laptops. The dyads in the VDE condition spent a few minutes having the HoloLenses they were going to use calibrated to their eyes before filling out the questionnaires. The dyads were referred to as teammates for the duration of the experiment.

After filling out the questionnaires related to the baseline-measurements the form presented a prompt telling the participant to pause and wait for instructions. After both participants were done filling out the questionnaires, one participant was asked to wait outside the room until summoned by the experimenter. The other

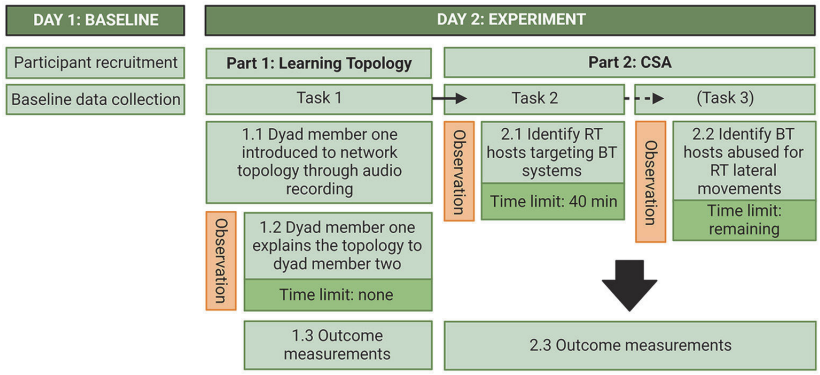


FIGURE 4
Overview of the experiment. RT, Red Team; BT, Blue Team; CSA, Cyber Situational Awareness; VDE, Virtual Data Explorer.

participant in the dyad was then either told to put on the HoloLenses (if in the VDE condition) to see the 3D representation of the network topology or seated at a table where the 2D schematics of the network topology was depicted (Arkime condition).

Upon confirming that they saw a network in front of them, the participants were played an English audio recording explaining that what they saw was the network that the Blue Team had to defend during the Locked Shields 2022 CDX. The recording lasted for 3 min and 30 seconds. It was explained to them what nodes each segment in the network consisted of, what was considered normal activity, where known Red Team nodes were, and which nodes were unknown. In the VDE condition, the participant was instructed to walk through the nodes and also how to interact with the nodes to probe for further information (e.g., touch node to see the IP address or pinch node to lift up in order to see which nodes it was connected to).

The briefing was only given once (which was stated in the beginning of the recording). After the recording was over, the participant was given the instruction that their task would be to explain the network topology to their teammate. They were instructed to get confirmation from their teammate that they had understood the topology upon which they would either (1) re-explain if their teammate did not understand or (2) let the experimenter know that they had completed the task. After confirming that they had understood the task, the other participant in the dyad was summoned and then the first participant was told to start at their convenience. In the VDE condition, the participant that was summoned was told to put on their HoloLens and confirm that they saw the network representation in front of them before the first participant in the dyad was given the signal to start. There were no time constraints on this task.

After signaling that the task was over, the participants were instructed to access their laptops and continue filling out the questionnaires until getting to a prompt asking them to wait for further instructions. In the VDE condition, the participants were instructed to remove their HoloLenses while answering the questionnaires.

2.7.2. Task two: Identifying Red Team hosts targeting Blue Team systems

After both participants were done filling out the questionnaires, they received the instructions for the second task. In the VDE condition, both participants were told to put on their HoloLenses again. This time the 3D representation of the network topology was updated with more edges connecting each node. The edges varied in brightness depending on the number of sessions (traffic) associated with the connections.

In the Arkime condition, both participants were introduced to a graph representation of the Blue Team network topology in Arkime. They were instructed (1) that they could select nodes to see their associated IP addresses and communications targets (represented by edges between the nodes); and (2) that they could see the session count (amount of traffic) associated with each connection by hovering over the edges connecting each node. The edges varied in thickness depending on the amount of traffic associated with the connection.

The dyads were then instructed to collaborate to find the top five Red Team hosts (nodes) targeting Blue Team systems according to the amount of traffic associated with each connection. For this task, they were given pen and paper to note the IP address associated with each identified Red Team host. The dyads were instructed to confirm with each other when they were done with the task before notifying the experimenter.

Both conditions saw the same network, with the same number of nodes and edges and the same amount of traffic. Participants in the VDE condition could not see the session count associated with each connection but could only use the edge brightness as cue. The participants had 40 min to finish the task, although this was not disclosed to them.

Upon notifying the experimenter that they had finished the task, the participants were given the instructions for the third task. If the time ran out before a dyad could finish the task, they were stopped by the experimenter and told to finish the last set of questionnaires.

2.7.3. Task three: Identifying Blue Team hosts abused for Red Team lateral movements

For the third task, the dyads were instructed to collaborate to find evidence, if any, of Red Team lateral movements and to note down the top five Blue Team hosts that were possibly abused for that purpose according to the amount of traffic associated with the connection.

The dyads were told that they had a time limit and what the duration of that time limit was (which was the time remaining from the 40 min they had to finish the previous task). As for the previous task, they were instructed to confirm amongst each other that they had finished the task before signaling to the experimenter that they were done.

After completing the task (or if the time ran out), the dyads were instructed to complete the last set of questionnaires. This was done individually. They were allowed to look at their notes from tasks two and three when answering questions about hosts and IP addresses but were not allowed to communicate or collaborate when answering the questionnaires.

After the Arkime group was done with the experiment, they also did the first task of the VDE condition, receiving instructions as described previously. The roles for task one were the same as in the Arkime condition, meaning that the participant who explained the topology to their teammate in the Arkime condition also did so in the VDE condition. Initially, we wanted the Arkime group to run through the entire experiment in the VDE condition as well. Due to time constraints and the experiment needing to be conducted on the same day, this was limited to completing the first task. Data related to these measurements will be reported elsewhere.

2.8. Data measures

2.8.1. Understanding the network topology

Per definition (Endsley, 1988; Franke and Brynielsson, 2014), to acquire CSA during a CTS in a cyber environment, one must necessarily know the normal state of the environment. To assess the participants' understanding of the network topology, we used a questionnaire partly inspired by the CSA for Analysts Questionnaire (Lif et al., 2017). The CSA questionnaire asks participants to draw a description of the network topology with sources and targets of attack. As our measurements were collected digitally, we employed a forced choice questionnaire where participants had to choose the one of four images that had the most correct 2D depiction of the network topology they had reviewed. The images varied in how connections between Blue Team segments were depicted, while some network segments were missing from the incorrect topology images. To avoid problems with resolution, the images were numbered and presented on laminated A3 paper while the participant provided their answers in the online form. Correct answers were scored as 1 and incorrect answers were scored as 0.

Our initial plan was to have two sets of forced choice questionnaires (in two different formats) that both conditions had to answer. One set would include the 2D schematics that were used in the forced choice questionnaire administered in the present study, while the other set of network topology images would be based on the 3D representation in VDE. Each set of questionnaires would therefore favor the condition where the format matched the condition (e.g., the 2D images favor the Arkime condition where 2D representations of the network topology is part of the tools available to the participants). The idea was that, if one condition performed better on the forced choice set that favored the other condition, this would say something about the level of understanding of the network topology that the participants were able to extract from either the 2D schematics or the VDE representation. However, due to time restraints, we could only use one set of forced choice questionnaires. As the current forced choice questionnaire favors the Arkime condition, it also serves as a test for whether the VDE representation induces overconfidence if the VDE group performs worse on this test than the Arkime group but is more or equally confident in their answers.

2.8.2. CSA item 1: Adversarial behavior

To assess the outcome of task two, one of the items asked: "What are the possible Red Team hosts that were targeting the Blue Team systems?". The participants had to write down the five IP addresses that they identified during task two. The answers were used to generate three variables: (1) total number of hosts identified, (2) total number of correctly identified hosts, and (3) total number of sessions associated with correctly identified hosts.

2.8.3. CSA item 2: Impact of the attack

To further assess the participants' CSA, they were asked to "Choose Blue Team segments in which the Red Team has been trying to compromise Blue Team hosts". For this item, the participants were given a multiple-choice questionnaire listing five Blue Team segments that were possibly affected. The participants could choose as many as they wanted. Because all of the segments were affected, answers on this item were scored by adding up all the segments that were chosen by the participants giving a numerical score ranging from 0 (the minimum of correct answers) to 5 (the maximum of correct answers).

2.8.4. CSA item 3: Situational report

To assess their comprehension of the cyber threat situation (awareness of the current situation, what caused it, and how it may evolve), participants were asked to answer three qualitative, open-ended questions. The questions were taken from a SITREP developed by one of the co-authors for use in cyber defense exercises. The questions included: "(1) Describe the activity you saw (specific but not overly detailed)", "(2) What type of incident do you think it was?", and "(3) If you could suggest anything - which actions should be done?".

The answers were blinded and scored individually by one of the co-authors who participated at Locked Shields 2022 exercise and had access to the ground truth of the dataset used. The answers were scored on a 5-point scale ranging from 0 (not correct/irrelevant) to 1 (correct/relevant). The answers were given an overall k-score ranging from 0 (not thorough) to 9 (thorough) to indicate the level of thoroughness combined in the answers to all three questions.

2.8.5. CSA item 4: Adversarial behavior and impact of attack

To measure the outcome of task three, participants were asked: "If any, what were the indicators of Red Team lateral movements in Blue

Team networks? Name BT hosts that were (possibly) (ab)used for that purpose." The participants had to write down the IP addresses that they identified during task three. Answers on this item were used to generate three variables: (1) total number of hosts identified, (2) total number of correctly identified hosts, and (3) total number of sessions associated with correctly identified hosts.

Because the information required to solve task three was available to all participants at all times from the initiation of task two, all participants had to answer this item regardless of whether they were given the opportunity to solve task three or not.

2.8.6. Confidence in answers

After each question, participants were asked to rate how confident they were in their answers on a 11-point scale ranging from 0 to 100%.

2.8.7. Decision-making forced-choice task

To assess the effect of condition on decision-making, participants were asked to answer a forced-choice decision-making question with four possible alternatives. The item asked: "If you could only pick one course of action, which would you pick?". The four alternatives were: (1) Cut off all connectivity from the friendly networks to outside, (2) Start incident response on selected hosts, (3) Launch attacks against the hosts that the suspected adversaries might be using, or (4) Cut off connectivity to a selection of network segments. An additional question was asked: "If you picked 4, what would be your suggested network segments?". Each choice was used to generate four variables scored as 0 (not chosen) and 1 (chosen).

2.8.8. Team workload questionnaire (select items)

The Team Workload Questionnaire (TWLQ; Sellers et al., 2014) was used to assess how participants experienced workload demands on team tasks during the exercise. The items are scored on an 11-point Likert scale ranging from very low to very high. High scores indicate higher levels of subjective workload. The TWLQ consists of six subscales divided on two dimensions, the Teamwork component (communication, coordination, team performance monitoring) and Task-Team component (time-share, team emotion, team support). For the purpose of the present study, we were mainly interested in the communication demand item as an indicator of whether the VDE would reduce communication demands. We were also interested in the items related to coordination demand, demand for controlling their own emotions, and demand for monitoring their own performance. The four TWLQ items were administered two times; the first at the end of task one and the second at the end of the experiment.

2.8.9. Structured observation

Structured observation was performed to assess the frequency of occurrence for four verbal communication behaviors: (1) Orient, Locate, Bridge (OLB) processes, (2) perceptual shared mental modeling, (3) task resolution, and (4) communication dysfunction.

OLB behaviors included communication behaviors related to perspective taking and grounded communication to achieve a shared understanding of the situation in accordance with the OLB model (Knox et al., 2018). Some examples included when members of the dyads asked questions to probe each other's understanding of what was communicated; adjusted language (from technical to less technical) to make sure the recipient understood the significance of what was communicated; and gave each other updates to maintain a mutually shared overview of what they were doing and discovering at any given moment.

Perceptual shared mental model behaviors included verbal communication related to achieving a shared perception of anything related to the task. Examples included utterances such as "Come here and look at this," "When I stand here I see x," "Do you see this node? It is communicating with that node over there," and so on.

A previous observational study indicated that team communication related to task resolution was different between well- and poor-performing teams during a CDX (Jariwala et al., 2012). In our study, task resolution behaviors included verbal communication related to the status or completion of the specific tasks that they were assigned. Examples included participants in the dyad asking each other "How many hosts have we found now?", "How many hosts did we have to find again?", and "Should we say that we have completed the task?".

Communication dysfunction behaviors included communication where participants in the dyad talked over/interrupted each other, did not answer each other's questions, argued, went too long (over 2 min) without communicating, and so on. Examples included instances where a participant started explaining what they were seeing and the other participant interrupting them to talk about what they were seeing.

Two observers/coders, one per condition, were used for the scoring of items. Score per dyad was determined by noting frequency of behavioral occurrence during the experiment. The coders agreed how to categorize the behaviors prior to the experiment, and the same coders were used throughout the experiment to ensure reliability. To assess inter-rater reliability, both observers simultaneously scored one of the dyads followed by performing a two-way mixed, absolute, single measures intra-class correlation (ICC) analysis on the raw scores for each item (Shrout and Fleiss, 1979; Hallgren, 2012). Inter-rater reliability was excellent (ICC = 0.871; Cicchetti, 1994). The observers also noted the time (minutes) spent to finish each task.

2.8.10. User experience measurements

To measure the experience participants had with using the HoloLens 2 and the VDE, we administered the User experience in Immersive Virtual Environment questionnaire (Tcha-Tokey et al., 2016). This data will be reported elsewhere.

2.8.11. Cognitive tests and self-report measures

We collected a range of cognitive trait and state data including measurements that have been identified as relevant for performance in previous studies on cyber cadets and cyber security personnel (Knox et al., 2017; Lugo and Sütterlin, 2018; Jøsok et al., 2019; Ask et al., 2021b; Sütterlin et al., 2022). For instance, positive moods and overconfidence has been found to be associated with poorer metacognitive judgments of CSA during a cyber engineering exercise (Ask et al., 2023), and in detecting cyber threats not directly related to network intrusion (Sütterlin et al., 2022). Conversely, self-regulation abilities measured through self-report and neurophysiological indicators were found to predict

cognitive flexibility in terms of mental context shifting during a cyber defense exercise (Knox et al., 2017; Jøsok et al., 2019) and better metacognitive judgements of performance (Ask et al., 2023), respectively. Furthermore, metacognition, self-regulation, and cognitive flexibility are necessary for establishing and communicating CSA (Jøsok et al., 2016; Knox et al., 2018; Endsley, 2020; Ask et al., 2023). Cognitive data was collected with tests and self-report questionnaires on both days of the experiment. The cognitive data collected on day one included cognitive styles, cognitive flexibility, emotion regulation, vividness of mental imagery, and rumination. The cognitive data collected during the experiment included affective states (baseline) and metacognition (projections for how well they thought they would perform at baseline and correction of how well they thought they had performed after the experiment was over). As noted, the results related to the cognitive data will be reported elsewhere.

2.9. Data analysis

The data were summarized and presented in tables using mean (M) and standard deviations (SD) for continuous and numerical variables, and frequency (count) and percentage (%) for ordinal variables.

The Shapiro-Wilk test of normality and confirmatory visual inspection revealed that most variables were not normally distributed. The exceptions included part one communication demands, part one coordination demands, part one performance monitoring demands, confidence in CSA 1 answers, confidence in CSA 3 descriptions, part two emotion demands, part two performance monitoring demands, and task two OLB. Non-parametric tests were performed for all subsequent analyses except for those variables.

For the non-parametric analyses, the Kruskal-Wallis H test was used for comparisons between the VDE group and the Arkime group. Results were presented as H statistic (degrees of freedom; df), p-values, and effect size. Effect size (η^2) for Kruskal-Wallis H test was calculated as $(H - k + \text{df})/(n - k)$; where H was the Kruskal-Wallis statistic, k was the number of groups, and n was the total number of observations ($n = 22$). Dunn's *Post-Hoc* test was used to assess significant relationships for non-parametric variables between groups and was reported as z-statistic and Bonferroni adjusted p-values (p_{bonf}).

For the parametric analyses, one-way ANOVAs were performed. Results for ANOVA were reported as F statistic(df), p-values, and effect size. Effect size (ω^2) for ANOVA was calculated as [sum of squares between $-$ (k – 1) mean square within]/(sum of squares total + mean square within). Tukey's *post hoc* test was used to assess significant relationships for parametric variables between groups and was reported as mean difference (MD) and p_{bonf}.

Between-group differences were visualized in interval plots with 95% confidence intervals.

The relationship between communication variables that were significantly different between the groups and CSA variables that were significantly different between the groups were assessed with Spearman correlation (2-tailed) on z-transformed variables. Results were visualized in a heat map and presented as correlation coefficients (ρ) and p-values. Separate regression analyses were performed for significant relationships. Results were reported as standardized beta (β), p-values, adjusted R^2 (R^2_{Adj}), and F(df) statistics.

Alpha levels for hypothesis testing were set at the 0.05 level for all analyses. All data were analyzed using JASP version 0.15 (JASP Team, 2021).

3. Results

Table 1 presents descriptive statistics of participant characteristics and experimental outcome measurements.

3.1. The effect of VDE on cyber situational awareness

3.1.1. Baseline network topology recognition

Kruskal-Wallis H test was performed to assess the differences of condition on task one outcome variables. Table 2 shows the results of the comparisons between the VDE group and the Arkime group on selecting the correct image depiction of the network topology, confidence in image selection, and TWLQ item responses.

The Kruskal-Wallis test showed that the VDE group selected the correct network topology image significantly different from the Arkime group ($p = 0.009$). Dunn's *post hoc* test showed that the VDE group selected the correct network topology image significantly less than the Arkime group ($z = -2.63$, $p_{\text{bonf}} = 0.004$).

The Kruskal-Wallis test showed that the confidence in image selection was significantly different between the VDE group and the Arkime group ($p = 0.006$). Dunn's *post hoc* test showed that the VDE group was significantly less confident in their image selection than the Arkime group ($z = -2.73$, $p_{\text{bonf}} = 0.003$).

No significant differences were observed on any of the TWLQ items measured after the completion of task one.

3.1.2. Red team movements, attack severity, and situational reports

Kruskal-Wallis H test was performed to assess the differences in the effect of condition on task two and three outcome variables. Table 3 shows the results of the comparisons between the VDE group and the Arkime group on identifying Red Team hosts targeting Blue Team systems, identifying affected blue team segments, assessment of the observed activity, assessment of what incident it was, suggestions of what actions to do as response, identifying Blue Team hosts abused for Red Team lateral movements, confidence in responses, and TWLQ item responses.

Two dyads, one from VDE group and one from Arkime group, spent >40 min on exploring the topology in task one. The dyad in the VDE group spent the least amount of time of all dyads on finishing task two (15 min). The dyad in the Arkime group could not finish task two in <40 min. The maximum amount of time spent to finish task two was 35 min. Thus, the amount of time the dyads had to finish task three ranged from five to 25 min.

There were no significant differences between the groups with respect to finishing task two within the 40-min time limit ($p = 0.495$). In general, the VDE group had higher scores than the Arkime group

TABLE 1 Descriptive statistics ($N = 22$).

	Total			VDE			Arkime		
Variables	M	SD	Count (%)	M	SD	Count (%)	M	SD	Count (%)
Age	22.59	1.36		22.50	1.44		22.70	1.33	
Gender (male)			17 (77.27)			7 (58.33)			10 (100.00)
Military IT systems			13 (59.01)			8 (66.66)			5 (50.00)
Cyber operations			9 (40.90)			4 (33.33)			5 (50.00)
Part 1									
Select correct image	0.59	0.50	13 (59.09)	0.33	0.49	4 (33.33)	0.90	0.31	9 (90.00)
Confidence in choice	61.36	35.49		41.66	33.25		85.00	21.21	
Communication demand	5.90	1.95		5.91	1.73		5.90	2.28	
Coordination demand	4.90	1.82		5.25	1.60		4.50	2.06	
Emotional demand	3.81	3.01		3.66	2.93		4.00	3.26	
Performance monitoring demand	5.13	2.03		4.66	1.96		5.70	2.05	
Part 2									
CSA 1 total RT hosts	3.36	1.62		4.41	1.16		2.10	1.10	
CSA 1 correct RT hosts	2.59	2.01		4.00	1.34		0.90	1.19	
CSA 1 RT hosts total traffic	26525.77	28681.35		48583.25	20069.14		56.80	104.19	
CSA 1 confidence	41.81	26.30		54.16	23.14		27.00	22.63	
Finished task 2 < 40 min	0.72	0.56	16 (72.72)	0.66	0.49	8 (66.66)	0.80	0.42	8 (80.00)
CSA 2 total BT segments	1.59	0.73		2.00	0.73		1.10	0.31	
CSA 2 confidence	40.90	29.09		52.50	26.32		27.00	27.10	
CSA 3 SITREP—activity	0.62	0.36		0.77	0.31		0.45	0.35	
CSA 3 SITREP—incident	0.60	0.42		0.72	0.40		0.45	0.40	
CSA 3 SITREP—actions	0.52	0.42		0.60	0.44		0.42	0.39	
CSA 3 SITREP—K-score	5.04	3.25		6.16	3.29		3.70	2.79	
CSA 3 confidence	38.63	22.52		47.50	19.59		28.00	22.01	
CSA 4 total BT hosts	0.96	1.61		1.50	1.97		0.30	0.67	
CSA 4 correct BT hosts	0.81	1.53		1.33	1.87		0.20	0.63	
CSA 4 BT hosts total traffic	640.54	1086.05		732.50	1040.58		530.20	1184.88	
CSA 4 confidence	40.90	32.05		56.66	27.08		22.00	27.80	
Communication demand	7.63	0.84		7.33	0.77		8.00	0.81	
Coordination demand	6.72	1.77		6.50	2.23		7.00	1.05	
Emotional demand	4.63	2.59		4.41	2.93		4.90	2.23	
Performance Monitoring demand	6.09	2.11		5.91	2.39		6.30	1.82	
Forced decision-making									
Decision 1	0.04	0.21	1 (4.54)	0.08	0.28	1 (8.33)	0.00	0.00	0 (0.00)
Decision 2	0.90	0.29	20 (90.90)	0.83	0.38	10 (83.33)	1.00	0.00	10 (100.00)
Decision 3	0.00	0.00	0 (0.00)	0.00	0.00	0 (0.00)	0.00	0.00	0 (0.00)
Decision 4	0.04	0.21	1 (4.54)	0.08	0.28	1 (8.33)	0.00	0.00	0 (0.00)

CSA, Cyber situational awareness; RT, Red team; BT, Blue team; SITREP, Situational report.

on all performance outcomes and lower scores on all team workload measures during the second part of the experiment, although not all of these differences were significantly different between the groups.

3.1.3. CSA 1: Identifying RT hosts targeting BT systems

The Kruskal-Wallis H test showed that the total number of identified Red Team hosts targeting Blue Team systems was

TABLE 2 Task 1 comparisons between VDE and Arkime ($N = 22$).

Variables	Kruskal-Wallis test			Dunn's *post hoc*	
	H (1)	p	η^2	z	p_{bonf}
Select the correct image	6.916	**0.009**	0.295	−2.630	**0.004**
How confident are you about this?	7.469	**0.006**	0.323	−2.733	**0.003**
Emotional demand	0.059	0.808	−0.047	-	-
	One-way ANOVA			Tukey's *post hoc*	
	F (1)	p	ω^2	MD	p_{bonf}
Performance monitoring demand	1.442	0.244	0.020	-	-
Communication demand	0.000	0.985	0.000	-	-
Coordination demand	0.919	0.349	0.000	-	-

η^2, Effect size; p_{bonf}, Bonferroni adjusted p-values; Bold, significant differences; ω^2, Effect size; MD, Mean difference.

TABLE 3 Comparison of task two and task three results between VDE and Arkime ($N = 22$).

Variables	Kruskal-Wallis test			Dunn's *post hoc*	
	H (1)	p	η^2	z	p_{bonf}
CSA 1. Number of identified possible RT hosts that were targeting the BT systems	11.603	**<0.001**	0.530	3.406	**<0.001**
CSA 1. Correctly identified RT hosts that were targeting the BT systems	12.867	**<0.001**	0.593	3.587	**<0.001**
CSA 1. Correctly identified RT hosts that were targeting the BT systems—traffic total	15.822	**<0.001**	0.741	3.978	**<0.001**
CSA 2. Compromised BT Segments correctly identified	8.863	**0.003**	0.393	2.977	**0.001**
CSA 2. How confident are you about this?	4.121	**0.042**	0.156	2.030	**0.021**
Finished task 2 on time	0.467	0.495	−0.026	-	-
CSA 3. SITREP—Describe the activity you saw	4.035	**0.045**	0.151	2.009	**0.022**
CSA 3. SITREP—What incident do you think it was?	2.743	0.098	0.087	-	-
CSA 3. SITREP—Which actions should be done?	0.988	0.320	−0.000	-	-
CSA 3. SITREP—Thoroughness K-score	3.044	0.081	0.102	-	-
CSA 4. Total BT hosts abused for RT lateral movements	1.735	0.188	0.037	-	-
CSA 4. Correctly identified BT hosts abused for RT lateral movements	3.681	0.055	0.134	-	-
CSA 4. BT hosts abused for RT lateral movements—Traffic	0.515	0.473	−0.024	-	-
CSA 4. How confident are you about this?	6.651	**0.010**	0.282	2.579	**0.005**
Communication demand	3.919	**0.048**	0.145	−1.980	**0.024**
Coordination demand	0.029	0.866	−0.048	-	-
	One-way ANOVA			Tukey's *post hoc*	
	F (1)	p	ω^2	MD	p_{bonf}
CSA 1. How confident are you about this?	7.667	**0.012**	0.233	27.458	**0.012**
CSA 3. SITREP—How confident are you about the descriptions above?	4.832	**0.040**	0.148	19.500	**0.040**
Emotion demand	0.182	0.674	0.000	-	-
Performance monitoring demand	0.172	0.682	0.000	-	-

η^2, Effect size; p_{bonf}, Bonferroni adjusted p-values; Bold, significant differences; CSA, Cyber situational awareness; RT, Red Team; BT, Blue Team; SITREP, Situational report; ω^2, Effect size; MD, Mean difference.

significantly different between the VDE and the Arkime group ($p < 0.001$). Dunn's *post hoc* test showed that the VDE group identified significantly more Red Team hosts targeting Blue Team systems compared to the Arkime group ($z = 3.40$, $p_{bonf} < 0.001$).

The Kruskal-Wallis H test showed that the total number of correctly identified Red Team hosts targeting Blue Team systems was significantly different between the VDE group and the Arkime group ($p < 0.001$). Dunn's *post hoc* test showed that the VDE group identified significantly more correct Red Team hosts targeting Blue

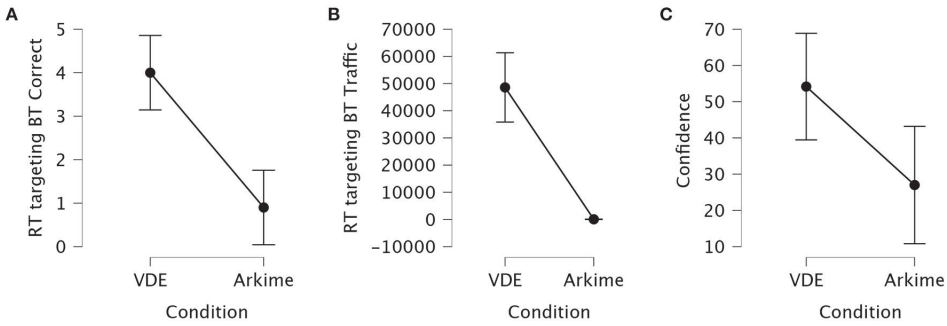


FIGURE 5
Interval plots for the differences in identifying Red Team hosts targeting Blue Team systems. **(A)** Correctly identified Red Team hosts. **(B)** Traffic associated with correctly identified Red Team hosts. The number of sessions associated with correctly identified hosts ranged from 27,083 to 75,554 in the VDE group while ranging from 0 to 254 in the Arkime group. **(C)** Confidence in answers. Whiskers are 95% confidence intervals.

Team systems compared to the Arkime group ($z = 3.58$, $p_{bonf} < 0.001$). Figure 5A shows interval plots for the differences in correctly identified Red Team hosts targeting Blue Team systems.

The Kruskal-Wallis H test showed that the activity associated with the correctly identified Red Team hosts targeting Blue Team systems was significantly different between the VDE group and the Arkime group ($p < 0.001$). Dunn's *post hoc* test showed that the VDE group identified significantly more highly-active Red Team hosts targeting Blue Team systems compared to the Arkime group ($z = 3.97$, $p_{bonf} < 0.001$). Figure 5B shows interval plots for the differences in the traffic associated with correctly identified Red Team hosts targeting Blue Team systems.

One-Way ANOVA showed that confidence in having correctly identified Red Team hosts targeting Blue Team systems was significantly different between the VDE group and the Arkime group ($p = 0.012$). Tukey's *post hoc* test showed that the VDE group was significantly more confident in having correctly identified Red Team hosts targeting Blue Team systems compared to the Arkime group ($MD = 27.45$, $p_{bonf} = 0.012$). Figure 5C shows interval plots for the differences in how confident participants were in having identified the correct hosts.

3.1.4. CSA 2: Identifying compromised BT segments

The Kruskal-Wallis H test showed that the number of identified Blue Team segments compromised by the Red Team was significantly different between the VDE group and the Arkime group ($p = 0.003$). Dunn's *post hoc* test showed that the VDE group identified significantly more Blue Team segments that were compromised by the Red Team compared to the Arkime group ($z = 2.97$, $p_{bonf} = 0.001$).

The Kruskal-Wallis H test showed that confidence in having correctly identified Blue Team segments compromised by the Red Team was significantly different between the VDE group and the Arkime group ($p = 0.042$). Dunn's *post hoc* test showed that the VDE group was significantly more confident in having correctly identified Blue Team segments compromised by the Red Team compared to the Arkime group ($z = 2.03$, $p_{bonf} = 0.021$). Figure 6 shows interval plots for differences between the VDE group and the Arkime group in having identified compromised Blue Team segments and confidence in having identified compromised Blue Team segments.

3.1.5. CSA 3: Situational report

The Kruskal-Wallis H test showed that the accuracy score for the description of what type of activity they saw was significantly different between the VDE group and the Arkime group ($p = 0.045$). Dunn's *post hoc* test showed that the VDE group had a significantly higher accuracy score compared to the Arkime group ($z = 2.00$, $p_{bonf} = 0.022$).

The accuracy score for the description of type of incident it was ($p = 0.098$), the relevance score for the suggestion of actions that should be done ($p = 0.320$), and the thoroughness k-score ($p = 0.081$) were not significantly different between the groups.

One-Way ANOVA showed that confidence in the SITREP descriptions was significantly different between the VDE group and the Arkime group ($p = 0.040$). Tukey's *post hoc* test showed that the VDE group had a significantly higher confidence in their SITREP answers compared to the Arkime group ($MD = 19.50$, $p_{bonf} = 0.040$).

3.1.6. CSA 4: Identifying BT hosts abused for RT lateral movements

The Kruskal-Wallis H test showed that neither the total number of Blue Team hosts abused for Red Team lateral movements ($p = 0.188$), the number of correctly identified Blue Team hosts abused for Red Team lateral movements ($p = 0.055$), nor the number of sessions associated with correctly identified Blue Team hosts abused for Red Team lateral movements ($p = 0.473$) were significantly different between the groups, although the difference in the number of correctly identified Blue Team hosts abused for Red Team lateral movements approached significance.

The Kruskal-Wallis H test showed that confidence in the answers was significantly different between the VDE group and the Arkime group ($p = 0.010$). Dunn's *post hoc* test showed that the VDE group had a significantly higher confidence in their answers compared to the Arkime group ($z = 2.57$, $p_{bonf} = 0.005$).

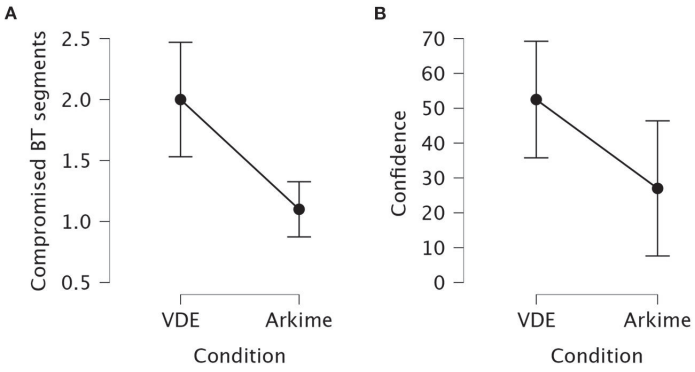


FIGURE 6
Interval plots for the differences in identifying compromised Blue Team systems. **(A)** Identified compromised Blue Team systems. **(B)** Confidence in having identified compromised Blue Team segments. Whiskers are 95% confidence intervals.

3.2. The effect of VDE on cyber team communication

3.2.1. Self-reported communication demands

The Kruskal-Wallis *H* test showed that the communication demands during part two of the experiment was significantly different between the VDE group and the Arkime group ($p = 0.048$). Dunn's *post hoc* test showed that the VDE group experienced significantly lower communication demands compared to the Arkime group ($z = -1.98$, $p_{bonf} = 0.024$). No other TWLQ measures were significantly different between the groups. Figure 7A shows interval plots displaying differences in part two communication demands between the groups.

3.2.2. Observation of communication behaviors

Kruskal-Wallis *H* tests and One-Way ANOVAs were used to assess differences on the observed verbal communication scores between the VDE group and the Arkime group. Table 4 presents the result of the comparisons. Figures 7B–D shows interval plots for between-group differences in task two OLB communication, task two task resolution communication, and task two communication dysfunction.

The Kruskal-Wallis *H* test showed that the VDE group had significantly different task one OLB scores compared to the Arkime group ($p = 0.042$). Dunn's *post hoc* test showed that the VDE group performed significantly more OLB communications during task one compared to the Arkime group ($z = 2.03$, $p_{bonf} = 0.021$). No other comparisons from task one were significant.

The one-way ANOVA showed that the VDE group had significantly different task two OLB scores compared to the Arkime group ($p = 0.028$). Tukey's *post hoc* test showed that the VDE group performed significantly more OLB communications during task two compared to the Arkime group ($MD = 5.16$, $p_{bonf} = 0.028$).

The Kruskal-Wallis *H* test showed that the VDE group had significantly different task two task resolution scores compared to the Arkime group ($p < 0.001$). Dunn's *post hoc* test showed that the VDE group performed significantly less task resolution communications during task two compared to the Arkime group ($z = -3.99$, $p_{bonf} < 0.001$). The Kruskal-Wallis *H* test showed that the VDE group had significantly different task two communication dysfunction scores compared to the Arkime group ($p = 0.043$). Dunn's *post hoc* test showed that the VDE group had significantly less communication dysfunction during task two compared to the Arkime group ($z = -2.02$, $p_{bonf} = 0.021$). The Kruskal-Wallis *H* test showed that the VDE group had significantly different task two Time-to-finish scores compared to the Arkime group ($p < 0.001$). Dunn's *post hoc* test showed that the VDE group had significantly lower time-to-finish scores during task two compared to the Arkime group ($z = -3.60$, $p_{bonf} < 0.001$).

Perceptual shared mental models were not significantly different between the groups. No comparisons were significantly different between groups with respect to task three observational scores.

3.2.3. Relationship between communication variables and CSA items

Spearman correlations were performed to assess the relationship between communication variables and CSA variables that were significantly different between the VDE group and the Arkime group. Figure 8 presents a heat map showing the results from the correlational analysis.

Task one OLB scores were significantly and positively correlated with task two OLB scores ($p = 0.035$), total number of identified Red Team hosts targeting Blue Team systems ($p = 0.009$), total number of correctly identified Red Team hosts targeting Blue Team systems ($p = 0.005$), and identifying compromised Blue Team segments ($p = 0.018$).

Task two OLB scores were significantly and positively correlated with total number of correctly identified Red Team hosts targeting Blue Team systems ($p = 0.048$).

Task two Task resolution scores were significantly and positively correlated with task two Communication dysfunction ($p = 0.018$), communication demands ($p = 0.024$), and negatively correlated with total number of identified Red Team hosts targeting Blue Team systems ($p < 0.001$), total number of correctly identified Red Team

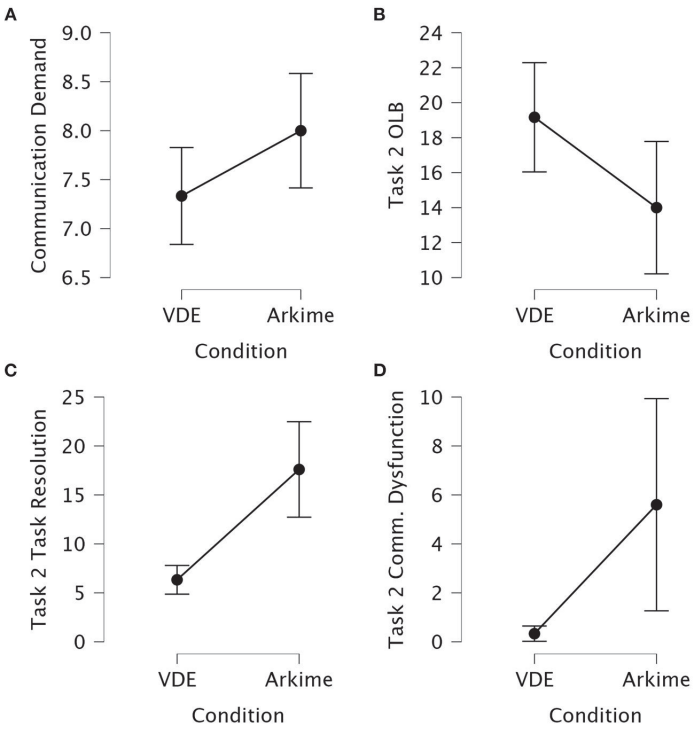


FIGURE 7
Interval plots for between-group differences in self-reported and observed communication variables. **(A)** Self-reported communication demands after part two of the experiment. **(B)** Observed task two OLB communication. **(C)** Observed task two task resolution communication. **(D)** Observed task two communication dysfunction. Whiskers are 95% confidence intervals.

hosts targeting Blue Team systems ($p < 0.001$), total amount of traffic associated with correctly identified Red Team hosts targeting Blue Team systems ($p < 0.001$), identifying compromised Blue Team segments ($p = 0.002$), and confidence in having identified Blue Team hosts abused for Red Team lateral movements ($p = 0.039$).

Task two communication dysfunction scores were significantly and negatively correlated with the accuracy score for the description of what type of activity they saw ($p = 0.010$), and confidence in having identified Blue Team hosts abused for Red Team lateral movements ($p = 0.027$).

Part two communication demands were significantly and negatively correlated with total number of correctly identified Red Team hosts targeting Blue Team systems ($p = 0.039$), and identifying compromised Blue Team segments ($p = 0.031$).

No other correlations were significant.

Separate linear regressions were performed for significant correlations. Significant results are shown in Table 5. Task two task resolution was a significant negative predictor of total number of identified Red Team hosts targeting Blue Team systems ($p < 0.001$), total number of correctly identified Red Team hosts targeting Blue Team systems ($p = 0.002$), total amount of traffic associated with correctly identified Red Team hosts targeting Blue Team systems ($p < 0.001$), and identifying compromised Blue Team segments ($p = 0.008$). No other relationships were significant.

Task two communication dysfunction was a significant negative predictor of the accuracy score for the description of what type of activity they saw ($p = 0.012$), and confidence in having identified Blue Team hosts abused for Red Team lateral movements ($p = 0.012$).

Communication demands was a significant negative predictor of the total number of correctly identified Red Team hosts targeting Blue Team systems ($p = 0.034$). No other relationships were significant.

3.3. The effect of VDE on decision-making

All the participants except two ($n = 20$) picked the "Start incident response on selected hosts" option on the forced-choice decision-making task. Thus, there was no difference between the groups. The other two participants, both in the VDE condition but not in the same dyad, picked the "Cut off all connectivity from the friendly networks to outside" and the "Cut off connectivity to a selection of network segments" options.

4. Discussion

Cyber defense decision-making during CTSs is based on human communication aiming to establish a shared CSA between

TABLE 4 Comparison of observational scores between VDE and Arkime ($N = 22$).

Variables	M ± SD	Kruskal-Wallis test			Dunn's *post hoc*	
		H (1)	*p*	η^2	z	p_{bonf}
Task 1 OLB	10.45 ± 13.00	4.145	**0.042**	0.157	2.036	**0.021**
Task 1 perceptual shared mental models	9.00 ± 11.75	0.461	0.497	−0.026	-	-
Task 1 task resolution	6.36 ± 11.08	0.000	1.000	−0.50	-	-
Task 1 communication dysfunction	0.27 ± 0.63	0.000	1.000	−0.50	-	-
Task 1 time to finish (min)	11.72 ± 15.46	0.000	1.000	−0.50	-	-
Task 2 perceptual shared mental models	16.90 ± 5.54	0.018	0.894	−0.049	-	-
Task 2 task resolution	11.45 ± 7.46	15.968	**<0.001**	0.748	−3.996	**<0.001**
Task 2 communication dysfunction	2.72 ± 4.80	4.101	**0.043**	0.155	−2.025	**0.021**
Task 2 time to finish (min)	28.90 ± 9.12	13.013	**<0.001**	0.600	−3.607	**<0.001**
Task 3 OLB	6.09 ± 8.79	0.916	0.339	−0.004	-	-
Task 3 perceptual shared mental models	5.45 ± 7.96	1.162	0.281	0.008	-	-
Task 3 task resolution	3.00 ± 3.59	0.898	0.343	−0.005	-	-
Task 3 communication dysfunction	0.90 ± 1.54	1.825	0.177	0.041	-	-
Task 3 time to finish (min)	6.27 ± 7.09	0.299	0.585	−0.035	-	-
		One-way ANOVA			Tukey's *post hoc*	
		F (1)	*p*	ω^2	MD	p_{bonf}
Task 2 OLB	16.81 ± 5.62	5.625	**0.028**	0.174	5.167	**0.028**

η^2, Effect size; p_{bonf}, Bonferroni adjusted *p*-values; Bold, significant differences; OLB, Orient, Locate, Bridge; ω^2, Effect size; MD, Mean difference.

TABLE 5 Linear regressions ($N = 22$).

Predictor	Dependent variable	β	*p*	R^2_{Adj}	*F* (1)
Task two task resolution	RT hosts targeting BT systems total	−0.763	<0.001	0.561	27.845
Task two task resolution	RT hosts targeting BT systems correct	−0.630	0.002	0.366	13.142
Task two task resolution	RT hosts targeting BT systems traffic	−0.665	<0.001	0.415	15.889
Task two task resolution	Identifying compromised BT segments	−0.547	0.008	0.264	8.534
Task two communication dysfunction	SITREP—Describe the activity you saw	−0.524	0.012	0.238	7.553
Task two communication dysfunction	BT hosts abused for RT lateral movements confidence	−0.525	0.012	0.239	7.594
Communication demands	RT hosts targeting BT systems correct	−0.454	0.034	0.166	5.178

RT, Red team; BT, Blue team; SITREP, Situational report.

analyst-level and decision-making personnel (Knox et al., 2018). Communication for shared CSA is one of the main problems facing SOC team analysts (Knox et al., 2018; Agyepong et al., 2019; Ask et al., 2021a). Current visualization tools to support achieving a shared understanding of the CTS include 2D graphs and schematics of network topology. These visualization tools do not scale well with increasing complexity. Furthermore, SA level 3 appears to be the SA stage most dependent on human working memory (Gutzwiller and Clegg, 2013). The mammalian brain has developed an innate ability to understand time and space (Eichenbaum, 2014; Ray and Brecht, 2016; Berggaard et al., 2018). 3D representations of network topology may leverage automatic spatial sensory processes (Stackman et al., 2002; Angelaki and Cullen, 2008; Moser et al., 2008) that reduce load on working memory during communication. Thus, 3D visualizations may be more neuroergonomic than 2D representations by facilitating more efficient communication and shared situational understanding during CTSs, which could support decision-making (Kullman et al., 2019a). In this study, we compared how the representation of a network topology in 3D MR (Kullman et al., 2018, 2020) vs. 2D affected topology recognition, CSA, team communication and decision-making in a sample of cyber cadets.

In the first part of the experiment, the Arkime group performed better than the VDE group on the task where participants had to identify the correct depiction of the network topology among four 2D schematics. This finding was not surprising as the correct depiction was in the same format as the 2D schematic the Arkime group had used to familiarize themselves with the topology.

3D visualizations of network topology are expected to be neuroergonomic in the sense that they leverage innate neurocognitive processes that encode spatial information. Additionally, the VDE

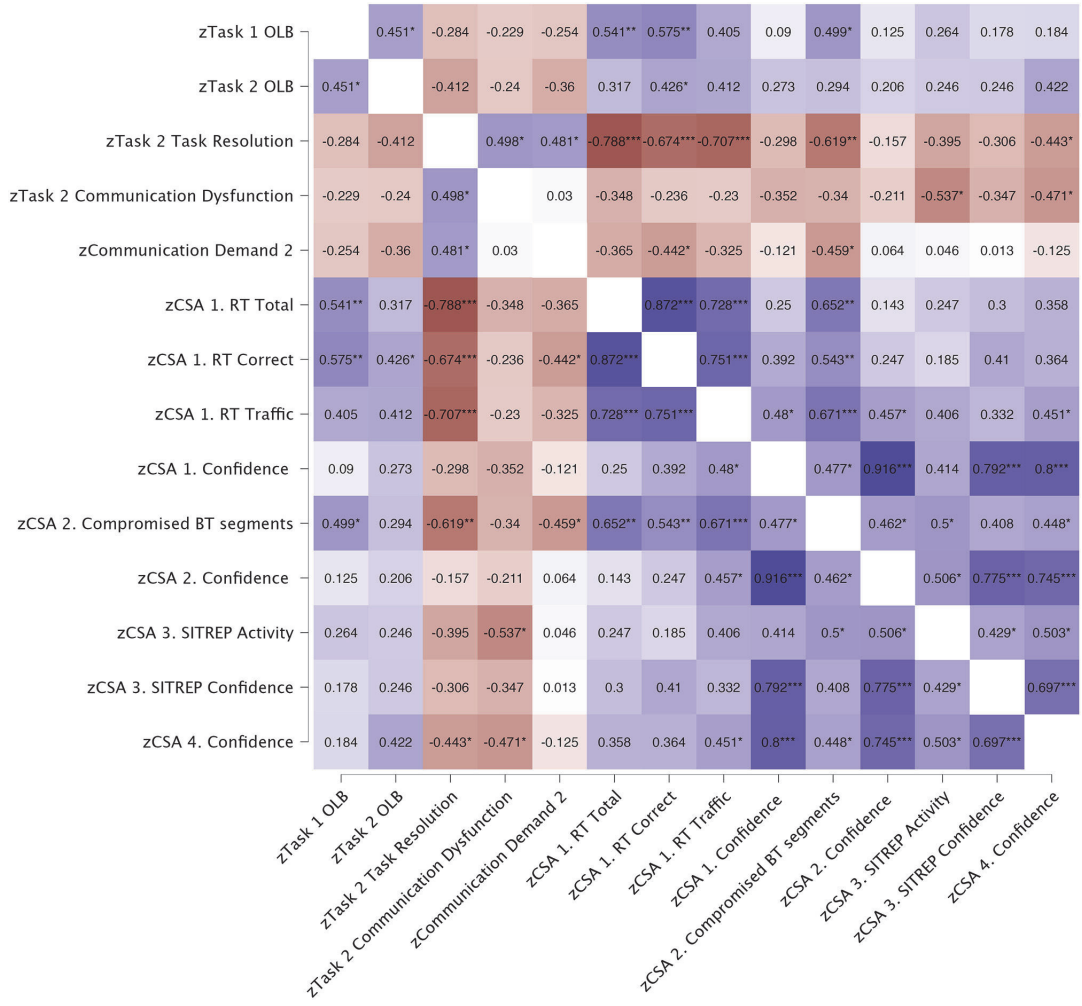


FIGURE 8
Heat map showing results from Spearman (ρ) correlations. All correlations are 2-tailed. Blue color indicates positive correlations. Red color indicates negative correlations. *$p < 0.050$, **$p < 0.010$, ***$p < 0.001$. OLB, Orient, Locate, Bridge (Knox et al., 2018); CSA, Cyber situational awareness; RT, Red team; BT, Blue team; SITREP, Situational report.

visualizes network data based on the mental model that operators have of the network they are defending (Kullman et al., 2020). While both being neuroergonomic and conserving connections and sessions between nodes, the topological layout as visualized in the VDE does not represent the actual reality of the network. This may be problematic if the 3D visualizations contribute to a false sense of confidence in one's understanding of the topology by virtue of being visually persuasive. For instance, previous studies on cyber cadets have shown that high self-confidence in combination with intuitive decision-making can have detrimental effects on performance when counterintuitive decisions are required (Lugo et al., 2016). Interestingly, while performing worse, the VDE group was also less confident in their answers on the topology recognition task. Thus, the 3D visualizations did not give a false sense of confidence with respect to topology recognition.

Awareness of adversarial behavior is suggested to be necessary for achieving CSA for cyber defense decision-making (Barford et al., 2009) although non-technical stakeholders may underestimate the importance of such information (Varga et al., 2018). This may have severe consequences for decision-making if analyst-level personnel and decision-makers have different mental models of the CTS and the network, especially if analyst-level personnel are not aware of this discrepancy during RCP communication (Ask et al., 2021a). Because the VDE allows for visualizing, thus sharing the mental models that the analyst have of the network topology (Kullman et al., 2018, 2020), this potential gap in information requirements (Varga et al., 2018) may be bridged more efficiently if adversarial

behavior can be visualized during RCP sharing. While non-technical personnel were not included in the present study, the VDE group outperformed the Arkime group on all metrics when they were tasked to identify the top five Red Team hosts targeting Blue Team systems. This was true for correctly identifying Red Team hosts targeting Blue Team systems, but especially apparent for the traffic associated with the identified Red Team hosts where the differences in the session number associated with the identified connections differed in the tens of thousands. Moreover, the VDE group identified the connection with the highest amount of associated traffic while the Arkime group did not. Considering that the Arkime group could see the session number associated with the connections when hovering over the edge connecting the nodes while the VDE group had to go by edge brightness alone, this difference in performance is arguably the most salient of the experimental results.

Considering the role of working memory in SA (Gutzwiller and Clegg, 2013), it could be that using edge brightness as a cue for traffic provided an advantage over having access to actual session statistics due to complexity reduction freeing up cognitive resources. Albeit being allowed to write down their discoveries (e.g., host IP, session number), having the actual statistics available may result in deliberately or habitually engaging in analytical procedures that require the application of additional cognitive processes. This may include processes that tax attention allocation and working memory which could be detrimental to performance in a working environment that is already taxing on cognitive resources (Champion et al., 2012; Sawyer and Hancock, 2018). Alternatively, or additionally, it could be that having the network topology fixed in space and at a scale where participants could walk from node to node, facilitated a method of loci/memory palace-effect (Legge et al., 2012; Wagner et al., 2021), due to the spatial encoding of information (Stackman et al., 2002; Angelaki and Cullen, 2008; Moser et al., 2008). By using edge brightness as the singular attentional cue combined with a spatial layout, the VDE may have improved performance by allowing for increased ease of visuo-cognitive processing of the state of the network. But what if participants were tasked to find the bottom five Red Team hosts (e.g., rare or ambiguous signals) targeting Blue Team systems (with session number above zero)? For instance, would edge brightness then be distracting, or would the differences in performance remain? This question should be addressed in future studies.

Interestingly, and without knowing that they had outperformed participants in the Arkime group, some of the participants in the VDE condition expressed that they would have liked to have session number available for inquiry. This may further suggest that taxing habitual or procedural (e.g., trained) cognitive processes could have contributed to performance differences between the groups. In a realistic scenario, however, the VDE would not be used to replace packet capture software or any investigative tools. Instead, the SOC analysts would have all their usual tools available to them, while the VDE would be an additional tool that analysts could use to interact with network data according to their information processing needs (Kullman and Engel, 2022a,b). If analysts would prefer to inquire about session statistics, they could either probe for that through common means or incorporate it in VDE. This, in turn, serves to deepen their understanding of the cyber environment they are operating within on their own terms, either for themselves or when communicating with team analysts, decision-makers, or stakeholders (Kullman et al., 2019a).

Awareness of the impact of an attack is also suggested to be necessary for achieving CSA for good cyber defense decision-making (Barford et al., 2009). In the present study, the VDE group identified more Blue Team segments that were compromised by the Red Team than the Arkime group. Given the level of uncertainty that is inherent to the cyber domain (Jøsok et al., 2016), this difference in impact awareness may be advantageous when attempting to reduce the level of experienced uncertainty both when attempting to understand the situation but also perhaps when evaluating the trustworthiness of CSA information, especially for non-technical personnel. The latter is also suggested to be important for achieving CSA for cyber defense decision-making (Barford et al., 2009).

To assess the potential effect of VDE on RCP communication, we asked participants to provide a short situational report based on three open-ended questions which were later used to generate three scores based on accuracy and relevance. In line with Barford et al. (2009), the questions were aimed at measuring (a) awareness of the current situation by describing the activity they saw, (b) what caused it by describing what type of incident it was, and (c) how the situation may evolve by suggesting which actions should be taken. A k-score was generated based on the overall thoroughness of the situational report. Although the VDE group scored higher than the Arkime group on all four measures, only the activity description score was significantly different between the groups.

In the present study, the VDE group identified more Blue Team hosts that were abused for Red Team lateral movements. However, this was not significantly different between the groups (although the number of correctly identified abused Blue Team hosts approached significance). Considering the difference in performance on task two, the lack of difference in performance on task three could be due to the time limit that the participants had to work under. It could also be due to the limited sample size. This will have to be addressed in future studies.

During the second part of the experiment, the VDE group was more confident in their answers than the Arkime group on all CSA measures. This should be considered in light of the fact that the VDE group performed significantly better than the Arkime group on several of the performance outcomes while having higher scores on all performance outcomes (although not all were significantly different). The outcome measures for the fourth CSA question (the question relating to task three) was the only measure where not one of the scores were significantly different between the groups. When also considering the lower confidence scores when the VDE group actually performed worse than the Arkime group, it could indicate that these performance estimations are well-founded. A second interpretation could be that the cyber cadets have good metacognitive accuracy irrespective of the conditions they were assigned to. Previous studies on cyber cadets have indicated that they are similar in their cognitive profiles (Lugo and Sütterlin, 2018), and that cyber cadets with higher metacognitive accuracy have better CSA, while overconfident cyber cadets have worse CSA (Ask et al., 2023). Assessing the metacognitive accuracy of the participants with respect to performance outcomes will be addressed in the study examining the cognitive measures that were taken during the experiment.

It is important to restate here that the VDE is not a tool for conducting forensic analyses *per se*. It is a neuroergonomic tool for visualizing network topology in accordance with the analyst's mental model of the network (Kullman and Engel, 2022a,b). This allows the analyst to not have to spend working memory on mentally maintaining or navigating the representation of their mental models when they are seeking to understand a CTS. Because individuals collaborating in VDE will have the same spatial mental model of the network (Kullman and Engel, 2022a,b), less mental effort may be required to ground communication, thus making knowledge transfer more efficient. While the experimental tasks and preliminary nature of the present study does not capture traditional SOC activities with sufficient realism, it still goes some way in capturing how the VDE influences communication processes when individuals are collaborating to establish CSA.

During the second part of the experiment, participants in the VDE condition experienced a lower communication demand compared to participants in the Arkime condition, suggesting that the VDE improves communication efficiency. Thus, when considering that communication inefficiencies are one of the biggest but least researched problems facing SOC team analysts (Agyepong et al., 2019; Ask et al., 2021a), this finding may indicate that the VDE could aid in solving some of those communication problems.

Previous studies have indicated that task-related communication is different between poor and well performing cyber teams during CDXs (Jariwala et al., 2012; Ask et al., 2023) but that expert cyber analysts communicate less than novice cyber analysts (Buchler et al., 2016; Lugo et al., 2017). This could indicate that experts communicate more effectively (e.g., are better at OLB processes; Knox et al., 2018) and more readily achieve a shared mental model of the tasks they are solving and of the cyber threat situation (Ask et al., 2023). A recent review found that there was a lack of studies characterizing the communication in cyber defense settings such as the purpose of communication and the type of communication (Ask et al., 2021a). In the present study, we noted the frequency of dyadic verbal communication as they related to OLB processes, task resolution, achieving a shared perceptual mental model, and communication dysfunction. We found that the VDE group performed significantly more OLB communication (which are aimed at achieving a shared understanding of a situation; Knox et al., 2018) during task one and task two, while the Arkime group performed significantly more task resolution communications and had more communication dysfunctions during task two. In our regression analysis, both observed and self-reported communication variables that were scored higher in the Arkime group compared to the VDE group were negative predictors of CSA scores. This could indicate that the VDE facilitates more efficient cyber team communication and should be assessed further in future studies. The possibility for using VDE in remote dyadic cooperation should also be assessed in future studies to assess whether these potential effects are present when body language cues are not available to the participants.

In the present study, almost all participants picked the same decision regardless of assigned condition or individual performance. This is likely due to cohort effects such as training but could also potentially be due to the specific cognitive profiles that the cyber engineering profession selects for Lugo and Sütterlin (2018). This could explain why the relevance score for the actions suggested in the situation report were not different between the groups. Future studies should include a more diverse sample to avoid potential confounding influences on the effect of VDE on decision-making. Because the VDE visualizations are established through an interview with the user of the visualizations (the analysts; Kullman et al., 2018, 2020), the 3D layout of the network topology in VDE is generated through user-centric cooperative-design principles. Due to the participants not being familiar with the network they were working with in the current experiment, the 3D layout was predefined. Usually, a cyber analyst will know the network they are operating within, thus, there is always a possibility that the unfamiliarity of the network made participants choose "safer" and similar decision-making options.

4.1. Limitations and future perspectives

The present study has a few limitations. The VDE group had higher scores on all performance measures and lower scores on all team workload measures during the second part of the experiment, although not all of these were significantly different. It is hard to say whether differences would have reached significance with a larger sample size. Considering this possibility, the experiment should be repeated in a larger sample.

With most behavioral experiments, there is a question of whether the experimental design produces results that can be generalized to a real-world setting. Due to being high stakes and unfolding in a complex working environment, defensive cyber operations can be stressful and often entail being exposed to a number of distractors (e.g., security alerts that are false positives) that may degrade performance over time (Champion et al., 2012; Sawyer and Hancock, 2018). Future studies should therefore include more distractors to ensure that results have high ecological value. This could include explicating time limits on all tasks, or exposing participants to periodic security alerts and increasing indicators of compromise (scenario injections). This in turn would allow the assessment of how taxing different senses and cognitive systems affect VDE vs. Arkime usability for CSA generation, team communication, and decision-making. Furthermore, applying the VDE in a setting that captures SOC tasks with more realism, including analyst-to-decision-maker communication will be necessary to fully validate the potential usability of the VDE for achieving a shared CSA.

While the overall performance of the HoloLens 2 was good, there were some instances where the HoloLens 2 headsets overheated which negatively affected application's stability and forced a few minute-long breaks while the headset was being replaced. Wearing a battery pack that provided the HoloLens 2 device with additional power appeared to solve the problem but the form factor of the battery pack and absence of dedicated gear (the participants kept the battery in their pocket) made it a somewhat awkward experience. This should be addressed in future research to ensure a more seamless experience that works under various conditions.

5. Conclusions

In the present study, a collaborative, 3D mixed reality representation of a network topology and network attack provided better CSA compared to using paper-based, 2D topology schematics and graph representation in the packet capture software Arkime.

The most apparent difference was in the detection of the top five Red Team hosts targeting Blue Team systems. The traffic associated with the identified Red Team hosts in the mixed reality condition differed in the tens of thousands. This is remarkable, as participants in the mixed reality condition could only use edge brightness as a cue for traffic while participants in the Arkime condition could see the actual session number statistics. Observed and self-reported communication was better for dyads in the VDE condition and was associated with their CSA. This may suggest that the VDE has neuroergonomic benefits when SOC team analysts need to communicate for shared CSA. Although participants in the mixed reality condition had higher CSA, we were not able to measure its effect on decision-making. This could be due to cohort effects such as training or the modest sample size. Finally, the experimental tasks and preliminary nature of the study does not reflect SOC tasks with sufficient realism. Thus, to truly assess the potential effects of VDE on communication for shared CSA, the study should be repeated in a naturalistic setting with a larger and more diverse sample.

Data availability statement

The datasets presented in this article are not readily available because access to raw and processed data is restricted in accordance with agreement between the researchers and the Norwegian Defense University College, Cyber Academy (NDCA).

Ethics statement

Ethical review and approval was not required for the study on human participants in accordance with the local legislation and institutional requirements. The patients/participants provided their written informed consent to participate in this study.

Author contributions

TA: experimental design, data collection, statistical analysis, and writing the original draft, review, and editing. KK: development of the data visualization application, experimental design, and writing, review, and editing of the original draft. SS: experimental design, review, and editing of original draft. BK: experimental design, data collection, review, and editing of original draft. DE: writing, review, and editing. RL: experimental design, data collection, statistical analysis, and writing, review, and editing of original draft. All authors approved the final draft of the manuscript.

Funding

This study was funded by the Norwegian Research Council (project #302941). Development of the Virtual Data Explorer was partly supported by the Army Research Laboratory under Cooperative Agreement No. W911NF-17-2-0083 and in conjunction with the CCDC Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center. Development of the Virtual Data Explorer is partly supported by NASA under Award No. 80GSFC21M0002.

Acknowledgments

A huge thank you to the Norwegian Defense Cyber Academy for help with facilitating the experiment and to the NATO CCDCOE for giving us access to the Locked Shields 2022 network data. A preprint of this manuscript is available *via* PsyArXiv (Ask et al., 2022).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P. (2019). Challenges and performance metrics for security operations center analysts: a systematic review. *J. Cyber Security Technol.* 4, 125–152. doi: 10.1080/23742917.2019.1698178

Ahrend, J. M., Jirotka, M., and Jones, K. (2016). "On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge," in *2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. (London, UK). doi: 10.1109/CyberSA.2016.7503279

Angelaki, D. E., and Cullen, K. E. (2008). Vestibular system: the many facets of a multimodal sense. *Ann. Rev Neurosci.* 31, 125–150. doi: 10.1146/annurev.neuro.31.060407.125555

Ask, T. F., Knox, B. J., Lugo, R. G., Helgetun, I., and Sütterlin, S. (2023). Neurophysiological and emotional influences on team communication and metacognitive cyber situational awareness during a cyber engineering exercise. *Front. Human Neurosci.* 16, 1092056. doi: 10.3389/fnhum.2022.1092056

Ask, T. F., Kullman, K., Sütterlin, S., Knox, B. J., Engel, D., and Lugo, R. G. (2022). A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. *PsyArXiv [Preprint]*. doi: 10.31234/osf.io/sphgn

Ask, T. F., Lugo, R. G., Knox, B. J., and Sütterlin, S. (2021a). "Human-human communication in cyber threat situations: a systematic review," in *HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning and Culture. HCII 2021*, ed C. Stephanidis (Cham: Springer), 21–43. doi: 10.1007/978-3-030-90328-2_2

Ask, T. F., Sütterlin, S., Knox, B. J., and Lugo, R. G. (2021b). "Situational states influence on team workload demands in cyber defense exercise," in *HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning and Culture. HCII 2021*, ed C. Stephanidis (Cham: Springer), 3–20. doi: 10.1007/978-3-030-90328-2_1

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., et al. (2009). "Cyber SA: situational awareness for cyber defense," in *Cyber Situational Awareness Advances in Information Security*, eds S. Jajodia, P. Liu, V. Swarup and C.Wang (Cham: Springer) 3–13. doi: 10.1007/978-1-4419-0140-8_1

Berggaard, N., Bjerke, I., Paulsen, A. E. B., et al. (2018). Development of parvalbumin-expressing basket terminals in layer II of the rat medial entorhinal cortex. *eNeuro* 5, e0438. doi: 10.1523/ENEURO.0438-17.2018

Bohbot, V. D., Copara, M. S., Gotman, J., and Ekstrom, A. D. (2017). Low-frequency theta oscillations in the human hippocampus during real-world and virtual navigation. *Nat. Commun.* 8, 14415. doi: 10.1038/ncomms14415

Buchler, N., Fitzhugh, S. M., Marusich, L. R., Ungvarsky, D. M., Lebiere, C., and Gonzalez, C. (2016). Mission command in the age of network-enabled operations: social network analysis of information sharing and situation awareness. *Front. Psychol.* 7, 937. doi: 10.3389/fpsyg.2016.00937

Champion, M. A., Rajivan, P., Cooke, N. J., and Jariwala, S. (2012). "Team-based cyber defense analysis," in *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in situation Awareness and Decision Support* (New Orleans, LA. USA), 218–221. doi: 10.1109/CogSIMA.2012.6188386

Cicchetti, D. V. (1994). Guidelines, criteria, and rules of thumb for evaluating normed and standardized assessment instruments in psychology. *Psychol. Assess.* 6, 284–290. doi: 10.1037/1040-3590.6.4.284

Eichenbaum, H. (2014). Time cells in the hippocampus: a new dimension for mapping memories. *Nat. Rev. Neurosci.* 15, 732–744. doi: 10.1038/nrn3827

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. In: *Proceedings of the Human Factors Society 32nd Annual Meeting* (Santa Monica, CA) 97–101. doi: 10.1177/154193128803200221

Endsley, M. R. (1995). Toward a theory of Situation Awareness in dynamic systems. *J. Hum. Factors Ergon. Soc.* 37, 32–64. doi: 10.1518/001872095779049543

Endsley, M. R. (2020). The divergence of objective and subjective situation awareness: a meta- analysis. *J. Cogn. Eng. Decis. Mak.* 14, 34–53. doi: 10.1177/1555343419874248

Franke, U., and Brynielsson, J. (2014). Cyber situational awareness - a systematic review of the literature. *Comput. Security* 46, 18–31. doi: 10.1016/j.cose.2014.06.008

Gutzwiller, R. S., and Clegg, B. A. (2013). The role of working memory in levels of situation awareness. *J. Cogn. Eng. Decis. Mak.* 7, 141–154. doi: 10.1177/1555343412451749

Hallgren, K. A. (2012). Computing inter-rater reliability for observational data: An overview and tutorial. *Tutor. Quant Methods Psychol.* 8, 23–34. doi: 10.20982/tqmp.08.1.p023

Jariwala, S., Champion, M., Rajivan, P., and Cooke, N. J. (2012). Influence of Team Communication and Coordination on the Performance of Teams at the iCTF Competition. *Proc. Human Factors Ergon. Soc. Ann. Meet.* 56, 458–462. doi: 10.1177/1071181312561044

JASP Team (2021). *JASP (Version 0.15)* [Computer software].

Jøsok, Ø., Knox, B. J., Helkala, K., Lugo, R. G., Sütterlin, S., and andWard, P. (2016). "Exploring the hybrid space," in *Augmented Cognition 2016. Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence),* eds D. D. D. Schmorrow and C. M. M. Fidopiastis (Cham: Springer), 9744, 178–188. doi: 10.1007/978-3-319-39952-2_18

Jøsok, Ø., Knox, B. J., Helkala, K., Wilson, K., Sütterlin, S., Lugo, R. G., et al. (2017). Macrocognition applied to the Hybrid Space: Team environment, functions and processes in Cyber Operations. in *International Conference on Augmented Cognition* (Cham: Springer), 486–500. doi: 10.1007/978-3-319-58625-0_35

Jøsok, Ø., Lugo, R., Knox, B. J., Sütterlin, S., and Helkala, K. (2019). Self-regulation and cognitive agility in cyber operations. *Front. Psychol.* 10, 875. doi: 10.3389/fpsyg.2019.00875

Knox, B. J., Jøsok, Ø., Helkala, K., Khooshabeh, P., Ødegaard, T., Lugo, R. G., et al. (2018). Socio-technical communication: The hybrid space and the OLB model for science-based cyber education. *Milit. Psychol.* 30, 350–359. doi: 10.1080/08995605.2018.1478546

Knox, B. J., Lugo, R. G., Jøsok, Ø., Helkala, K., and Sütterlin, S. (2017). "Towards a cognitive agility index: the role of metacognition in human computer interaction," in *HCI International 2017 - Posters' Extended Abstracts* (Cham: Springer) 330–338. doi: 10.1007/978-3-319-58750-9_46

Kuhrt, D., St. John, N. R., Bellmund, J. L. S., Kaplan, R., and Doeller, C. F. (2021). An immersive first-person navigation task for abstract knowledge acquisition. *Sci. Rep.* 11, 5612. doi: 10.1038/s41598-021-84599-7

Kullman, K., Asher, N. B., and Sample, C. (2019b). "Operator impressions of 3D visualizations for cybersecurity analysts," in *Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019: University of Coimbra, Portugal,* ed. Cruz, Tiago; Simoe, Paulo. (Reading, UK: ACPI) 257–266.

Kullman, K., Buchanan, L., Komlodi, A., and Engel, D. (2020). "Mental model mapping method for cybersecurity," in *HCI for Cybersecurity, Privacy and Trust. HCII 2020*, eds. A. Moallem (Cham, Springer). doi: 10.1007/978-3-030-50309-3_30

Kullman, K., Cowley, J. A., and Ben-Asher, N. (2018). "Enhancing cyber defense situational awareness using 3D visualizations," in *Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018: National Defense University, Washington DC, USA* (Washington DC: Academic Conferences and Publishing International Limited) 369–378.

Kullman, K., and Engel, D. (2022a). "User interactions in virtual data explorer," in *Augmented Cognition. HCII 2022,* eds. D.D. Schmorrow, C.M. Fidopiastis (Cham: Springer) 13310. doi: 10.1007/978-3-031-05457-0_26

Kullman, K., and Engel, D. (2022b). Interactive stereoscopically perceivable multidimensional data visualizations for cybersecurity. *J. Defence Secur. Technol.* 4, 37–52. doi: 10.46713/jdst.004.03

Kullman, K., Ryan, M., and Trossbach, L. (2019a). VR/MR supporting the future of defensive cyber operations. *IFAC-PapersOnLine* 52, 181–186. doi: 10.1016/j.ifacol.2019.12.093

Lankton, P. (2007). Endsley's model of situational awareness [jpg]. Available online at: https://en.wikipedia.org/wiki/File:Endsley-SA-model.jpg (accessed September 13, 2022).

Legge, E. L., Madan, C. R., Ng, E. T., and Caplan, J. B. (2012). Building a memory palace in minutes: equivalent memory performance using virtual versus conventional environments with the Method of Loci. *Acta Psychol.* 141, 380–390. doi: 10.1016/j.actpsy.2012.09.002

Lif, P., Granasen, M., and Sommestad, T. (2017). "Development and validation of technique to measure cyber situation awareness," in *2017 International Conference on Cyber Situational Awareness, Data Aanalytics and Assessment (Cyber SA)*, (London, UK). doi: 10.1109/CyberSA.2017.8073388

Lugo, R., Kwei-Nahr, P., Jøsok, Ø., Knox, B. J., Helkala, K., and Sütterlin, S. (2017). "Team workload demands influence on cyber detection performance," in *13th International Conference on Naturalistic Decision Making* (Bath, UK) 223–225.

Lugo, R. G., and Sütterlin, S. (2018). Cyber officer profiles and performance factors. *International Conference on Engineering Psychology and Cognitive Ergonomics* (Cham: Springer). 181–190. doi: 10.1007/978-3-319-91122-9_16

Lugo, R. G., Sütterlin, S., Knox, B. J., Jøsok, Ø., Helkala, K., and Lande, N. M. (2016). The moderating influence of self-efficacy on interoceptive ability and counterintuitive decision making in officer cadets. *J. Mil. Stud.* 7, 44–52. doi: 10.1515/jms-2016-0005

Moser, E. I., Kropff, E., and Moser, M. B. (2008). Place cells, grid cells, and the brain's spatial representation system. *Ann. Rev Neurosci.* 31, 69–89. doi: 10.1146/annurev.neuro.31.061307.090723

NATO Cooperative Cyber Defense Center of Excellence (2016). NATO Recognizes cyberspace as a 'domain of operations' at the Warsaw summit. Available online at: https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html (accessed September 13, 2022).

Ray, S., and Brecht, M. (2016). Structural development and dorsoventral maturation of the medial entorhinal cortex. *eLife* 5, e13343. doi: 10.7554/eLife.13343.019

Safaryan, K., and Mehta, M. R. (2021). Enhanced hippocampal theta rhythmicity and emergence of eta oscillation in virtual reality. *Nat. Neurosci.* 24, 1065–1070. doi: 10.1038/s41593-021-00871-z

Sawyer, B. D., and Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors.* 60, 597–609. doi: 10.1177/0018720818780472

Seager, M. A., Johnson, L. D., Chabot, E. S., Asaka, Y., and Berry, S. D. (2002). Oscillatory brain states and learning: Impact of hippocampal theta-contingent training. *Proc. Nat. Acad. Sci USA.* 99, 1616–1620. doi: 10.1073/pnas.032662099

Sellers, J., Helton, W. S., Näswall, K., Funke, G. J., and Knott, B. A. (2014). Development of the team workload questionnaire (TWLQ). *Proc. Hum. Factors Ergon. Soc. Annu. Meet.* 58, 989–993. doi: 10.1177/1541931214581207

Shrout, P. E., and Fleiss, J. L. (1979). Intraclass correlations: Uses in assessing rater reliability. *Psychol. Bull.* 86, 420–428. doi: 10.1037/0033-2909.86.2.420

Stackman, R. W., Clark, A. S., and Taube, J. S. (2002). Hippocampal spatial representations require vestibular input. *Hippocampus* 12, 291–303. doi: 10.1002/hipo.1112

Staheli, D., Mancuso, V., Harnasch, R., Fulcher, C., Chmielinski, M., Kearns, A., et al. (2016). "Collaborative data analysis and discovery for cyber security," in *SOUPS 2016: Twelfth Symposium on Usable Privacy and Security* (Denver, CO).

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., et al. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. *IEEE Secur. Privacy* 13, 20–29. doi: 10.1109/MSP.2015.71

Sütterlin, S., Lugo, R., Ask, T., Veng, K., Eck, J., Fritschi, J., et al. (2022). "The role of IT background for metacognitive accuracy, confidence and overestimation of deep fake recognition skills," in *Augmented Cognition. HCII 2022.* Lecture Notes in Computer Science, eds D. D. Schmorrow and C. M. Fidopiastis (Cham: Springer) 13310, 103–119. doi: 10.1007/978-3-031-05457-0_9

Tcha-Tokey, K., Christmann, O., Loup-Escande, E., and Richir, S. (2016). Proposition and validation of a questionnaire to measure the user experience in immersive virtual environments. *Int. J. Virtual Real.* 16, 33–48. doi: 10.20870/IJVR.2016.16.1.2880

Varga, S., Brynielsson, J., and Franke, U. (2018). "Information Requirements for National Level Cyber Situational Awareness," in *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (Barcelona, Spain) 774-781. doi: 10.1109/ASONAM.2018.8508410

Wagner, I. C., Konrad, B. N., Schuster, P., Weisig, S., Repantis, D., Ohla, K., et al. (2021). Durable memories and efficient neural coding through mnemonic training using the method of loci. *Sci. Adv.* 7, eabc7606. doi: 10.1126/sciadv.abc7606

Winson, J. (1978). Loss of hippocampal theta rhythm results in spatial memory deficit in the rat. *Science* 201, 160–163. doi: 10.1126/science.663646

Curriculum vitae

Personal data

Name:	Kaur Kullman
Citizenship:	Estonian

Contact data

E-mail:	tees.en@coda.ee

Education

2015–2023	Tallinn University of Technology – PhD
2007–2012	University of Tartu – MA
1998–2007	University of Tartu – BA

Language competence

Estonian	native
English	fluent
German	basic
Russian	basic
Finnish	basic

Professional employment

2020– …	University of Maryland, Baltimore County, Center for Space Sciences and Technology, Visiting Faculty Research Assistant
2017–2020	US Army Research Laboratory, Researcher
2012–2017	Estonian Information System Authority, Cybersecurity Expert
2007–2012	AS Lõhmus Haavel & Viiseman / LHV Pank, Chief Security Officer

Elulookirjeldus

Isikuandmed

Nimi:	Kaur Kullman
Kodakondsus:	Eesti

Kontaktandmed

E-post:	tees.ee@coda.ee

Hariduskäik

2015–2023	Tallinna Tehnikaülikool – PhD
2007–2012	Tartu Ülikool – MA
1998–2007	Tartu Ülikool – BA

Keelteoskus

eesti keel	emakeel
inglise keel	kõrgtase
saksa keel	algtase
vene keel	algtase
soome keel	algtase

Teenistuskäik

2020– …	University of Maryland, Baltimore County, Center for Space Sciences and Technology, Visiting Faculty Research Assistant
2017–2020	US Army Research Laboratory, Researcher
2012–2017	Riigi Infosüsteemi Amet, Küberturbe Ekspert
2007–2012	AS Lõhmus Haavel & Viiseman / LHV Pank, Turvajuht

ISSN 2585-6901 (PDF)
ISBN 978-9949-83-967-4 (PDF)