

This work was written as part of one of the author's official duties as an Employee of the United States Government and is therefore a work of the United States Government. In accordance with 17 U.S.C. 105, no copyright protection is available for such works under U.S. Law.

Public Domain Mark 1.0

<https://creativecommons.org/publicdomain/mark/1.0/>

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

**Please provide feedback**

Please support the ScholarWorks@UMBC repository by emailing [scholarworks-group@umbc.edu](mailto:scholarworks-group@umbc.edu) and telling us what having access to this work means to you and why it's important to you. Thank you.

## 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.

© 2019, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.

**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 1<sup>st</sup> and 3<sup>rd</sup> 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.

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).

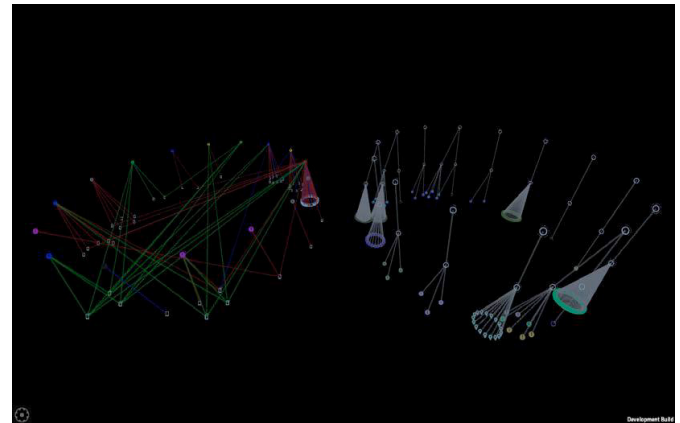
VRDAE will function as an operating environment for other tools (for network and data visualization, but also for others), abstracting user interaction and collaboration. Hence VRDAE's focus being more on user interaction, user experience and user interface design.

### 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

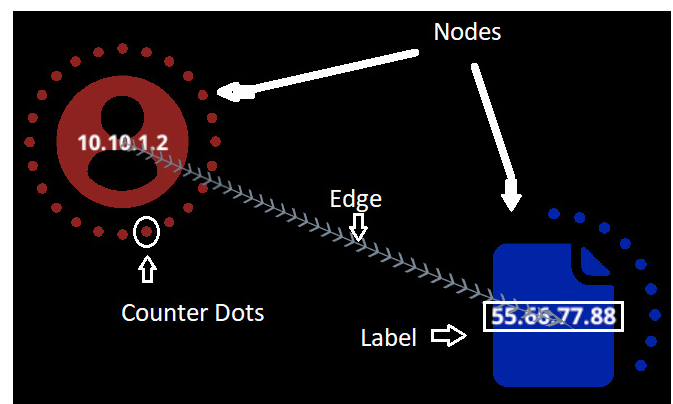
these layout states without reloading the underlying data nor recalculating the visualization.

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.

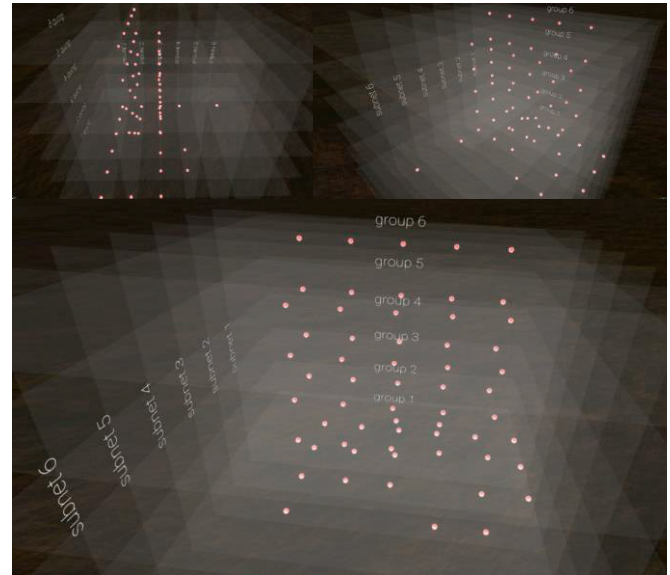
The Vids project aims to demonstrate a new direction in 3D interactive visualization for the Army. Faced with ever-increasing data volumes, new solutions are needed to maintain network situational understanding. Visualizations are one way to enable the Warfighter or network defender to process, and most 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.

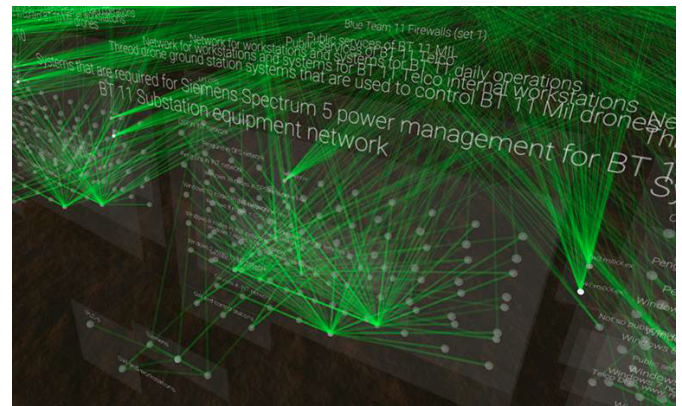
In the context of VDE:

- 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.



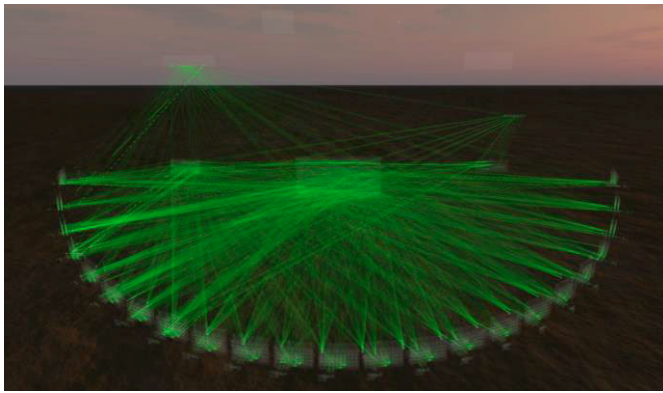
**Fig 3.** Viewing same data-shape from three different angles. Reddish spheres are nodes that were present in a sample used to generate a Blue Team's networks data-shape.

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.

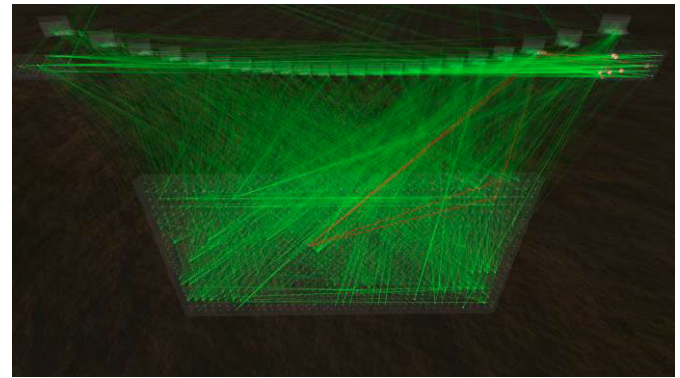


**Fig. 5.** VDE: VR view of Locked Shields 18 Partner Run network topology and network traffic using VDE; displaying an overall view of the meta-shape – a data-shape consisting of multiple data-shapes. Detailed description of this layout is found in (Kullman, Cowley, & Ben-Asher, Enhancing Cyber Defense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

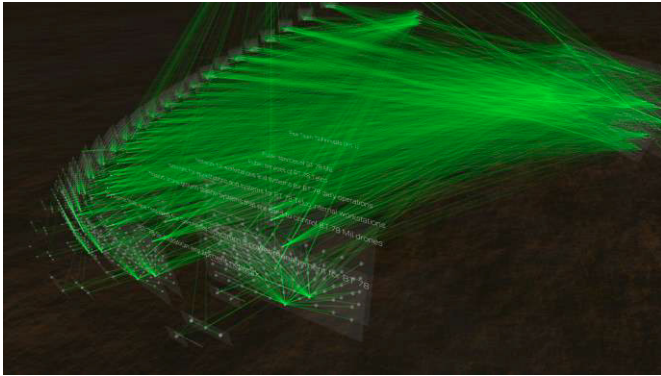
- Understand the principles of how does a computer network function; specifically, how is such a network set up in the environment, that the author of this visualizations needs to protect;
- Understand of the logical grouping of networked entities and their topology but also networked entities and stakeholders' goals (e.g. corporate, employees, external {friendly, neutral, malicious} actors, etc.);
- Understanding the expected behavior of the above actors and how it should and would reflect on network data;
- 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 axes available to encode data, we chose to use two of those axes 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=NYINCwAAQBAJ>
- 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*.