Synthetic Environments for the Cyber Domain: A Survey on Advances, Gaps, and Opportunities

Emily Nack
Lieutenant Colonel Nathaniel D. Bastian, Ph.D.

ABSTRACT

The need to understand cyber vulnerabilities and information in real time is imperative and often mission-critical in battlefield scenarios. As technologies continue to evolve, a need arises for more time-efficient and effective solutions within the cyber domain. With the growing popularity of synthetic environment technologies such as Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) in a variety of fields, the question emerges: How can applications of this technology be applied to the field of cyber and what impact can they have? In this article, we survey the body of knowledge, both theoretical and empirical, of existing works exploring AR, VR, and MR technologies as solutions to common cyber challenges, as well as discuss the advances, gaps, and opportunities of this technology within the cyber domain.

CYBER APPLICATIONS OF SYNTHETIC ENVIRONMENTS

Synthetic environment technologies such as AR, VR, and MR allow users to experience a different reality, either by enhancing their perception of the real world (AR), creating a completely artificial environment (VR), or by combining elements of both (MR). These technologies have been used in various fields, including education, gaming, and healthcare, and have recently been adopted in the field of cybersecurity. We provide an overview of AR, VR, and MR in the cyber domain, highlighting the relevant technologies and their current applications within the field.

In Cybersecurity Training and Operations

AR, VR, and MR technologies have been increasingly used in cybersecurity training and operations due to their ability to provide analysts with realistic, immersive, and interactive environments.

Emily Nack is an Information Technology Specialist serving within the Data and Decision Sciences Division at the Army Cyber Institute (ACI) within the Department of Electrical Engineering and Computer Science at the United States Military Academy at West Point. She also serves as Research Lab Manager where she provides research and engineering technical support and systems management across the ACI's Intelligent Cyber-Systems and Analytics Research Lab, ACI's Internet of Things Research Lab, and ACI's Cyber Modeling and Simulation Research Lab. She holds an A.S. degree in Computer Information Systems from Hudson Valley Community College, along with a B.S. degree in Game Design and Development from the Rochester Institute of Technology.

AR technology has been utilized to enhance learners' understanding of complex cybersecurity concepts and scenarios by providing interactive visualizations of cyber threats and countermeasures. For instance, the use of AR technology, specifically Microsoft's HoloLens, was explored to aid human operators with computer network operations tasks.[1] Multiple applications were developed to demonstrate alternative approaches to network security operations by simulating environments and events that closely align with the daily tasks of operators. The AR-based cybersecurity training applications enabled users to visualize and interact with virtual cyber attacks and defense mechanisms in a real-world environment. This approach provided users with a visual representation of the threat landscape, enabling more engaging and interactive learning environments, and preparing users to make informed security decisions in the event of a real attack.

Both VR and MR technology have been used to create realistic and immersive simulations that allow users to practice defending against cyber attacks in a safe and controlled environment. The use of VR and MR to support defensive cyber operations and training was discussed, as researchers reviewed new capabilities being developed and theorized by the U.S. Army C5ISR Center Cybersecurity Service Provider (CSSP).[2] Several combined VR and MR environments were developed to facilitate collaboration between analysts and provide the virtual real estate needed to monitor cyberspace effectively. The Visual Intrusion Detection System (VIDS) was developed to visualize Intrusion Detection System (IDS) alerts in a three-dimensional (3D) space, allowing cybersecurity analysts to view, categorize, and find correlations between alerts quickly.[3] This provides analysts with the necessary visualizations to detect and defend efficiently against incoming cyber attacks.

LTC Nathaniel D. Bastian, Ph.D., is an Academy Professor and Cyber Warfare officer at the United States Military Academy at West Point. He serves as Division Chief, Data and Decision Sciences and Senior Research Scientist at the Army Cyber Institute (ACI) within the Department of Electrical Engineering and Computer Science, as well as Assistant Professor of Operations Research and Data Science with a dual faculty appointment in the Department of Systems Engineering and the Department of Mathematical Sciences. He also serves as the ACI's Chief Data Scientist, directing the ACI's Intelligent Cyber-Systems and Analytics Research Lab, Internet of Things Research Lab, Cyber Modeling and Simulation Research Lab, and Cognitive Security Research Lab. He has co-authored 90+ refereed publications, received $4M+ in externally-funded research monies, served as Visiting Research Fellow at the Johns Hopkins University Applied Physics Lab, and served as Distinguished Visiting Professor at the National Security Agency.

To summarize, AR, VR, and MR technologies have been increasingly used in cybersecurity training and operations to provide users with realistic, immersive, and interactive learning experiences. These technologies enable users to practice their cybersecurity skills in a safe and controlled environment and enhance their understanding of complex cybersecurity concepts and scenarios.

Network Security Monitoring and Data Visualizations

AR, VR, and MR technologies are changing the field of network security monitoring and data visualization by making it easier and more efficient to analyze security threats. These technologies offer new ways to visualize and interact with complex data, allowing analysts to identify potential security risks quickly.

AR technology enables visualizations of network traffic and security events. One developed application is a 3D network visualizer that displays network topologies from both a global and local perspective.[1] Users are prompted with randomly generated alerts that simulate emergent problems requiring attention. When users interact with alerts, a local network topology is imported and dynamically generated, including routers, switches, and computers represented as 3D objects interconnected via links. As the HoloLens enables eye-tracking, users can glance over the topology, with individual objects and links highlighted when observed. Interacting with objects reveals mockups of different network diagnostic windows, emulating actions that cybersecurity analysts take when visualizing data and monitoring security risks. This environment provides analysts with a more intuitive and interactive view of the network and can help identify network traffic anomalies and respond to potential security threats.

VR technology can create immersive environments for network and data visualization. With VR, users can explore data and network structures in a 3D space, allowing for more intuitive interaction with the information. VRNetzer is an interactive data exploration platform that facilitates the visualization and analysis of large-scale, complex data, allowing users to gain a deeper understanding of the information presented.[4] Although not designed with cybersecurity in mind, VRNetzer's functionality is powerful and can enable analysts to parse through complex data and identify cyber vulnerabilities efficiently.

MR technology combines aspects of AR and VR technologies, providing a more immersive and interactive environment for data visualization. Researchers explored the use of MR as an improved approach to visualizing big data.[5] By using MR for visualization, access to large amounts of data is convenient and can provide a view from multiple perspectives, allowing for smooth navigation and minimal perceptual inaccuracies in data analysis. Such visualization provides the necessary infrastructure to improve network security monitoring and reduce the time it takes to understand fully the complexity of cybersecurity data.

Overall, AR, VR, and MR technologies are revolutionizing the way security professionals visualize and analyze network data. These technologies provide increasingly sophisticated tools for identifying and mitigating security threats, improving analysts' workflow and reducing response times. As these technologies continue to evolve, they will play a significant role in network security monitoring and data visualization.

Cyber Incident Response and Situational Awareness

AR, VR, and MR technologies can enhance situational awareness and improve decision-making in cyber incident response. By providing analysts with a more comprehensive and immersive view of the cyber threat landscape, these technologies can enable faster and more effective threat detection and response.

AR technology can offer real-time information overlays, including alerts and threat information, improving situational awareness and enabling faster response times. For instance, researchers proposed an Augmented Reality-based framework that uses AR to present data, make forecasts, conduct analyses, and support decision-making.[6] This framework can help cybersecurity specialists in high-performance computing (HPC) environments combat the increasing cyber-physical threats that HPC data centers with heterogeneous compute servers and networks face. The framework sends notifications to an AR device to alert analysts of any hardware issues, and a navigation tool helps locate the damaged device. Once located, a 3D visualization tool can reveal the issue and, in the future, detailed animations can demonstrate how to fix the detected issues. Using AR to provide a visual representation of cyber infrastructure helps analysts understand the scope and impact of threats to physical systems.

VR and MR technology can provide a 3D visualization of the cyber environment, allowing incident responders to see attack surfaces and understand potential attack vectors in a more

immersive way. It can also help with post-incident analysis by recreating cyber incidents, allowing responders to identify the root cause, determine the scope of the attack, and develop strategies to prevent similar incidents in the future. For instance, this was explored in the Vids Cyber Defense Visualization Project, which is an interactive 3D environment for visualizing network Intrusion Detection System (IDS) data.[3] Vids builds upon an earlier visualization project, called VIDS,[2] which focused solely on visualizing IDS alerts in a 3D space. Vids is currently implemented as a 2D representation of a 3D space, allowing the platform to be used for testing and visualization concepts and gathering feedback from users. In the long term, the platform is intended to integrate with a VR or MR environment. Vids has several uses that enable cyber incident response and situational awareness, including providing a visual reference model to explain events or incidents, identifying "known unknowns" or "unknown unknowns" through multidimensional analysis, and enabling collaboration among multiple parties involved in different stages of research, development, or user chains.

Leveraging the power of AR, VR, and MR technologies in cyber incident response and situational awareness empowers organizations to not only stay ahead of evolving cyber threats, but also enhance their overall cybersecurity posture. By integrating these technologies into their strategies, organizations can significantly mitigate the impact of cyber attacks and protect critical assets and information from sophisticated adversaries. The immersive and comprehensive view provided by AR, VR, and MR enables analysts to make faster and more informed decisions, detect threats more effectively, and respond with greater agility.

GAPS, OPPORTUNITIES, AND CURRENT EFFORTS

The use of AR, VR, and MR technologies in the cyber domain has the potential to improve cyber defense significantly by enhancing situational awareness, enabling effective training, and improving incident response accuracy and speed. However, there are still significant gaps in understanding how to fully leverage these technologies for cybersecurity. This section will explore new opportunities for utilizing AR, VR, and MR to address cybersecurity challenges and bridge these gaps. Specifically, it will focus on utilizing these technologies to further enhance cybersecurity training, network visualization, and situational awareness. By highlighting these new opportunities, this section aims to provide insights into how these technologies can effectively address the evolving challenges presented within the cyber domain.

Serious Games for Improved Cybersecurity Training and Awareness

The combination of AR technology and serious games offers numerous opportunities for cybersecurity training and awareness. One of the key advantages of leveraging this technology is the ability to provide hands-on training experiences that simulate real-world cyber threats and attack scenarios, enabling users to develop practical skills and a deeper understanding

of cybersecurity concepts. A good example is the "CybAR" game,[7] which creates a virtual training environment where users can experience the consequences of careless cybersecurity habits and learn how to defend against them. Additionally, the gamification of cybersecurity training can make it more engaging and enjoyable for learners, promoting the retention of information and development of critical thinking and problem-solving skills. "CybAR" was designed as a competitive game, utilizing gamification elements such as point systems, leader boards, and achievements to motivate players to continue playing and increase their awareness of cybersecurity practices.

Furthermore, AR technology can create more immersive and realistic training environments, increasing motivation and interest in the field. While the "Red vs Blue, Cyber-security Simulator" game[8] does not utilize AR, the implementation of the technology could enhance realism and facilitate remote collaboration and teamwork among players. The game splits players into three teams (White, Red, and Blue), which must work together to strategize cyber attacks and defenses, promoting decision-making at the operational cybersecurity level.

AR and serious games can also be used to raise awareness about cyber threats and best practices for cybersecurity, educating employees and the general public about the importance of cybersecurity and how to protect against cyber attacks. "Riskio" is a good example, providing an active learning environment where players build knowledge on cybersecurity attacks and defenses by playing the roles of both attacker and defender of critical assets in a fictitious organization, raising awareness about cybersecurity threats and mitigation tactics.[9]

Overall, the combination of AR and serious games has exciting potential for improving cybersecurity training and awareness. Future research can further explore the impact of this technology on cybersecurity education and its potential for providing high-quality and scalable cybersecurity training and awareness programs.

Real-Time Network Visualization Using Mixed Reality

With today's constantly evolving threat landscape, real-time network visualization plays a critical role in responding to emerging threats and preventing catastrophic data breaches. However, despite the potential benefits of using MR technology for real time network visualization in cybersecurity, there are currently few applications that exist. This may be due to the challenges of implementing MR and displaying large amounts of data in real-time. As this technology continues to advance, approaches and potential opportunities for using MR can be explored.

One proposed approach to using MR for visualizing real-time data for cyber situational awareness was discussed, as authors developed a prototype for displaying network data as a holographic overlay on physical network devices.[10] In their proposed model, live data was

indexed in real time using IDS, Security Incident Event Message (SIEM), and Unified Threat Management (UTM) to detect threats. A Simultaneous Localization and Mapping (SLAM) algorithm was then used to map the environment, and unique tags with MAC addresses were placed on machines to identify their physical locations when a threat was detected. The model utilized Microsoft HoloLens to identify suspicious activities and guide the user to their location, where information was augmented on the device using surface detection. This prototype demonstrated the potential of MR for real-time network visualization and highlighted the benefits of displaying network data in a more intuitive and immersive way.

Two use cases that demonstrate the benefits of using MR technology for visualizing real-time Internet of Things (IoT) data were proposed.[11] The first use case was for smart cities where IoT devices collected real-time data on temperature, humidity, and noise throughout the city. The data was then filtered, aggregated, and visualized on a 3D map of the city using MR technology. The second use case was for cybersecurity, in which an MR application was used to filter incoming real-time data based on Indicators of Compromise (IOC) and to visualize the propagation of malware among infected devices during a cyber attack. Both of these use cases highlighted the advantages of using MR to visualize real-time IoT data, including faster and more intuitive data analysis, improved decision-making, and better communication between users.

While these opportunities demonstrate the potential of MR for real-time network visualization in cybersecurity, there is still much work to be done to realize fully the potential of this technology. Further research is needed to explore the effectiveness of MR-based network visualizers in real-world cybersecurity scenarios and to address the challenges of displaying large amounts of data in real time. However, with the increasing need for real-time network monitoring and the continued advancements in MR technology, it is likely that MR-based network visualizers will become an important tool for cybersecurity professionals in the future.

Visualizing Geospatial Data with Augmented Reality

AR technology has the potential to be a powerful tool for visualizing geospatial data in the field of cybersecurity. By using AR, cybersecurity professionals can quickly and accurately understand the location of threats and their potential impact, allowing them to take faster and more effective actions.

One potential application of AR for geospatial data visualization is in the visualization of cyber threats and attacks in real time, overlaid on a map. This idea was minimally explored with the 3D Network Visualizer app, which mapped network topologies at the global view, displaying interconnected nodes and edges atop a 3D globe. By using gesture-based input capabilities, users could scale and rotate the globe, while random nodes were selected from

the network topology to simulate emergent alerts. When further inspected by the user, the local network view for the affected node would be displayed, allowing users to understand and respond to the alert. This functionality coupled with real-time geospatial data could help cybersecurity professionals identify the location of attacks and their potential impact on critical infrastructure, enabling faster and more effective response.

To enhance situational awareness in both physical and cyber spaces, AR can be used to create immersive experiences that visualize geospatial data. This can be especially important in critical infrastructure and other areas where visualizing the location of threats and their potential impact is crucial. As an example, a cybersecurity team could use AR to display real-time data on the physical location of devices on a network, along with their status and vulnerabilities. This concept was discussed in various studies, where authors described unique frameworks for visualizing geospatial data in both operational and defensive settings.[6,10,12] By utilizing AR technology to create immersive experiences that visualize geospatial data, cybersecurity professionals can gain a better understanding of the physical locations and status of threats in real time, allowing them to take faster and more effective actions.

Overall, the integration of AR with geographical data presents a range of opportunities for improving cybersecurity, from real-time threat visualization to enhanced situational awareness and training. As the technology continues to advance, it will be interesting to see how these opportunities are further developed and applied in real-world contexts.

Digital Twin Technology with AR for Increased Cyber Situational Awareness

Digital twin technology and AR offer significant opportunities to enhance cyber situational awareness. Digital twins are virtual representations of physical objects or systems that can simulate their behavior and performance in real time. This enables predictive analytics, remote monitoring, and maintenance.[13] AR can provide a visual overlay of digital twin data onto the physical world, allowing for more intuitive and interactive access to information. Combining these two technologies provides cybersecurity professionals with a comprehensive understanding of cyber threats, empowering them to take faster and more effective actions.

One potential application of digital twin technology and AR for cyber situational awareness is in visualizing cyber-physical systems (CPS) and IoT devices.[13] These systems and devices are increasingly prevalent in critical infrastructure, and cybersecurity professionals need to understand their behavior and vulnerabilities to protect against cyber threats. Digital twins offer a key advantage: users can analyze the environment based on geography, sensing, and timing to identify vulnerabilities in tactical operations.[14] For example, users can evaluate the effectiveness of observation posts in detecting targets or explore multiple phenomena, including physical, cyber, and human behavioral effects. These analyses can help users target specific areas of concern and minimize overall system costs.

By creating a digital twin of CPS and IoT devices, cybersecurity professionals can simulate their behavior and monitor for anomalies in real time. AR can then overlay this data onto the physical world, providing a visual representation of the CPS or IoT device and its status. This enables cybersecurity professionals to identify potential threats quickly and respond accordingly. AR can also be dynamic, adaptive, and persistent, and can be used to signal the presence of sensors that are not apparent or in low-visibility areas, indicate positions of critical resources or assets, suggest defensive positions, and identify and label enemy forces for training and testing purposes.[14]

The integration of digital twin technology and AR offers a promising avenue for improving cyber situational awareness. With the ability to represent physical systems virtually and overlay critical cybersecurity information onto the real world, cybersecurity professionals can more effectively understand and respond to potential threats. As these technologies continue to evolve, it will be exciting to see how they are further leveraged in practical contexts to enhance cybersecurity and protect against emerging threats.

Novel Approaches to Addressing Research Gaps and Opportunities

As we researched current applications and the advances/gaps in using AR, VR, and MR technologies within the cyber domain, it quickly became apparent that there were limited tangible solutions which exist for real-time network visualization and threat detection and mitigation. Here we discuss the work we have done in developing a real-time network visualizer using AR technology. Our research aims to address the gaps and opportunities presented earlier in this article, particularly exploring real-time network and geospatial data visualization. Traditional network visualizations often involve 2D static representations that can be challenging for users to interpret in real time. Our work uses AR technology to create an interactive and dynamic visual representation of network data. By leveraging the capabilities of AR, our visualizer allows users to experience network data in a more intuitive and engaging way, enabling interaction with data and exploration of network relationships in real time.

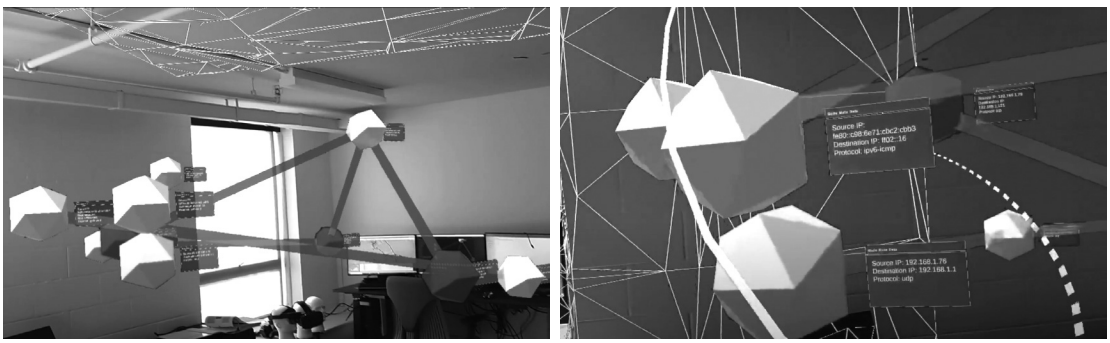

Figure 1: Real-Time AR Network Visualizer

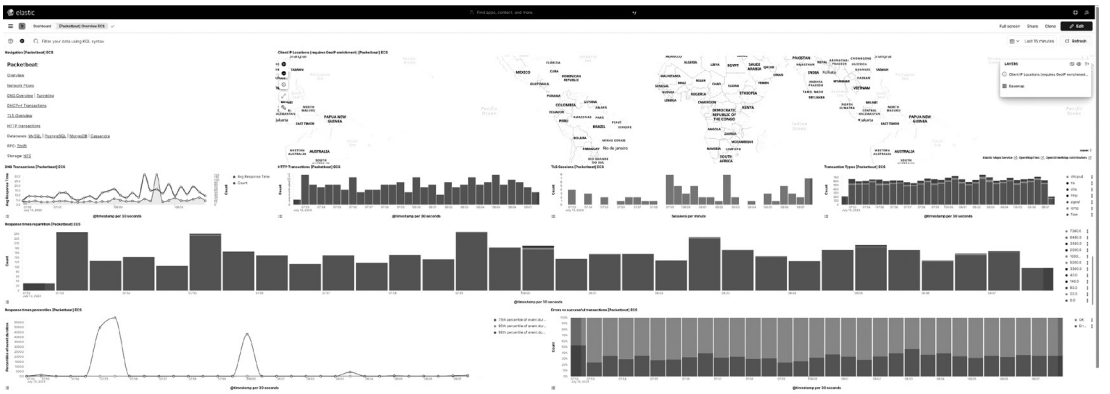

Figure 2: Packetbeat Dashboard in Kibana Visualizing Real-Time Network Data

Our network visualizer, as seen in Figure 1, was developed in Unity and uses data collected from Elasticsearch's Packetbeat,[15] pictured in Figure 2, to create game objects dynamically in real time that represent source and destination IPs as nodes and their communication via edges. As data is updated, the game objects are updated with new information, reconnecting source nodes to their appropriate destinations and recoloring game objects based on protocol. As of now, the visualizer creates the game objects at random positions within the room, spatially mapped using Microsoft HoloLens' built-in capabilities and Microsoft's Mixed Reality ToolKit[16] to update the mapping in Unity in real time. This allows game objects to be properly scaled within the room space and allows for physics-based collision using object detection.

In the future, we plan to use geospatial data to map the game objects based on location. With Elasticsearch's Packetbeat, location data can be collected, which presumably means we should be able to extract geospatial data and assign it to game objects in the same way we do for network data. We also plan to use our visualizer for threat detection and mitigation by generating alerts and highlighting anomalous nodes for the user to explore further. We can leverage security tools like Suricata,[17] which can be configured to send intrusion detection data to Elasticsearch and write custom scripts to access and store the data within Unity. Alerts can be generated and visualized based on the signature-based rules Suricata offers, and users can drill down into suspect nodes, potentially performing actions to mitigate threats directly from the AR visualizer.

There is still much work to be done to help address the gaps of using AR for real-time data visualization and threat detection and mitigation in the cyber domain, but with our research we have proved that it can be done. The future work planned for the visualizer, including the integration of geospatial data and the generation of alerts and highlighting of anomalous nodes, demonstrates the potential for continued advancements in AR technology for cybersecurity. By leveraging AR technology, real-time data visualization and threat detection in

the cyber domain can become more accessible and intuitive, leading to more effective cybersecurity practices. Furthermore, the use of Elasticsearch's Packetbeat and security tools like Suricata highlights the potential for integrating existing cybersecurity tools with AR technology for real-time threat detection and mitigation. This integration can provide a more comprehensive approach to cybersecurity and help identify and address threats in a timely and effective manner. Our work contributes to the advancement of AR technology in cybersecurity and provides a foundation for further research and development in this field.

CONCLUSIONS AND FUTURE WORK

As technology continues to advance, new tools and techniques have emerged to improve our ability to combat cyber threats. One area of development in this field is the use of synthetic environment technologies like AR, VR, and MR in cybersecurity. While these technologies have the potential to transform how we approach cyber defense by enhancing situational awareness, enabling more effective training and improving the accuracy and speed of incident response, there are still gaps in our understanding of how best to apply them to this field. This article explored the current state of research in this area and has identified both the gaps associated with AR, VR, and MR in the cyber domain and new opportunities for how this technology can enhance the field.

To leverage these technologies fully, future work should focus on exploring innovative ways to integrate them into existing cybersecurity workflows. This may involve developing new software and hardware solutions that are specifically designed for cyber defense, as well as incorporating existing AR, VR, and MR technologies into current cybersecurity training and simulation programs. Additionally, it is important to continue exploring the potential of these technologies for threat hunting, incident response, and other key areas of cyber defense. By staying up to date with the latest advancements in AR, VR, and MR technology, we can unlock the full potential of these technologies to better protect our digital assets and critical infrastructure.

NOTES

1. Beitzel, Steve, Josiah Dykstra, Paul Toliver, and Jason Youzwak. "Exploring 3d Cyberse-curity Visualization with the Microsoft Hololens." In International Conference on Applied Human Factors and Ergonomics, 197-207. Springer, 2017.
2. Kullman, Kaur, Matt Ryan, and Lee Trossbach. "VR/MR Supporting the Future of Defen-sive Cyber Operations." IFAC-PapersOnLine 52, no. 19 (2019): 181-86.
3. Edwards, Joshua, and Gregory Shearer. "Vids Cyber Defense Visualization Project." In Vids Cyber Defense Visualization Project. ICF, 2020.
4. Pirch, Sebastian, Felix Müller, Eugenia Iofinova, Julia Pazmandi, Christiane V. R. Hütter, Martin Chiettini, Celine Sin, et al. "The VRNetzer Platform Enables Interactive Network Analysis in Virtual Reality." *Nature Communications* 12, no. 1 (2021): 1-14.
5. Olshannikova, Ekaterina, Aleksandr Ometov, Yevgeni Koucheryavy, and Thomas Olsson. "Visualizing Big Data with Augmented and Virtual Reality: Challenges and Research Agenda." *Journal of Big Data* 2, no. 1 (2015): 1-27.
6. Sukhija, Nitin, Cory Haser, and Elizabeth Bautista. "Employing Augmented Reality for Cybersecurity Operations in High Performance Computing Environments." In Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (Learning), 1-4, 2019.
7. Alqahtani, Hamed, and Manolya Kavakli-Thorne. "Design and Evaluation of an Augment-ed Reality Game for Cyberse-curity Awareness (CybAR)." Information 11, no. 2 (2020): 121.
8. Yamin, Muhammad Mudassar, Basel Katt, and Mariusz Nowostawski. "Serious Games as a Tool to Model Attack and Defense Scenarios for Cyber-Security Exercises." *Computers & Security* 110 (2021), 102450 .
9. Hart, Stephen, Andrea Margheri, Federica Paci, and Vladimiro Sassone. "Riskio: A Seri-ous Game for Cyber Security Awareness and Education." Computers & Security 95 (2020), 101827 .
10. Joshi, Tapas Dipakkumar. "A Mixed-Reality Approach for Cyber-Situation Awareness." Florida Tech, 2017.
11. Andrade, Tiago, and Daniel Bastos. "Extended Reality in Iot Scenarios: Concepts, Applica-tions and Future Trends." In 5th Experiment International Conference (Exp. at'19), 107 -12. IEEE, 2019.
12. Kammerer, Klaus, Rüdiger Pryss, Kevin Sommer, and Manfred Reichert. "Towards Con-text-Aware Process Guidance in Cyber-Physical Systems with Augmented Reality." In 4th International Workshop on Requirements Engineering for Self-Adaptive, Collaborative, and Cyber Physical Systems (RESACS), 44-51. IEEE, 2018 .
13. Böhm, Fabian, Marietheres Dietz, Tobias Preindl, and Günther Pernul. "Augmented Reali-ty and the Digital Twin: State-of-the-Art and Perspectives for Cybersecurity." *Journal of Cybersecurity and Privacy* 1, no. 3 (2021): 519-38.
14. Raybourn, Elaine M., and Ray Trechter. "Applying Model-Based Situational Awareness and Augmented Reality to Next-Generation Physical Security Systems." *In Cyber-Physical Systems Security*, 331-44. Springer, 2018.
15. Elasticsearch. "Packetbeat: Network Analytics Using Elasticsearch," 2023. https://www.elastic.co/beats/packetbeat.
16. Microsoft. "MRTK2-Unity Developer Documentation." 2022.
17. Suricata. "Suricata," n.d., https://suricata.io/.