EUROPEAN JOURNAL OF EMERGING CYBERSECURITY AND INFORMATION PROTECTION

AN ANALYTICAL SURVEY OF IMMERSIVE TECHNOLOGIES FOR ENHANCING CYBER SITUATIONAL AWARENESS

Dr. Nadia M. Suleiman
Department of Computer Science, King Saud University, Saudi Arabia

Dr. Henrik L. Olsen
Department of Electronic Systems, Aalborg University, Denmark

V0LUME01 ISSUE01 (2024)

Published Date: 22 December 2024 // Page no.: - 35-43

ABSTRACT

The escalating complexity and frequency of cyber threats necessitate advanced tools for effective cyber defense. Traditional security systems, often relying on two-dimensional displays, struggle to represent the multi-faceted nature of modern cyber data, potentially overwhelming human analysts and causing data occlusion. This has led to a growing interest in immersive technologies—Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR)—as a means to enhance Cyber Situational Awareness (Cyber SA). This paper presents a systematic survey of the current landscape of immersive systems designed for cybersecurity. We follow a structured review methodology to identify, categorize, and analyze existing research, focusing on applications in threat visualization, security operations, and professional training. Our findings indicate that immersive analytics can significantly improve data comprehension, facilitate collaborative analysis, and provide engaging educational experiences. Based on our synthesis of the literature, we propose a novel reference framework that maps specific immersive visualization and interaction techniques to the core levels of situational awareness: perception, comprehension, and projection. This framework serves as a guide for the design and analysis of future Immersive Cyber Situational Awareness (ICSA) systems. Finally, we discuss the primary challenges, identify key research gaps, and propose future directions, including the integration of Artificial Intelligence (AI) and the need for large-scale empirical studies to unlock the full potential of immersive technologies in strengthening global cyber defenses.

Keywords: Cybersecurity, Cyber Situational Awareness (Cyber SA), Immersive Analytics, Virtual Reality (VR), Augmented Reality (AR), Extended Reality (XR), Data Visualization, Security Operations Center (SOC).

INTRODUCTION

The digital landscape is increasingly defined by a persistent and evolving array of cyber threats. In the wake of global events like the COVID-19 pandemic, reliance on digital infrastructure has surged, concurrently expanding the attack surface for malicious actors [1, 2]. Modern commerce, heavily reliant on e-commerce and digital technologies like blockchain, further amplifies the stakes of maintaining robust security postures [3]. Consequently, cybercrime has become more sophisticated and prevalent, posing significant risks to individuals, organizations, and critical infrastructure [4, 7]. Reports from agencies like the FBI's Internet Crime Complaint Center show billions of dollars in losses annually, while industry analyses like the Verizon Data Breach Investigations Report highlight that a substantial portion of security incidents involves external actors and organized crime, underscoring the professionalization of cyber attacks [4, 5].

A critical factor in many security breaches is the human element. Human factors are consistently identified as a primary contributor to cybersecurity vulnerabilities, whether through error, negligence, or susceptibility to social engineering [6]. One analysis suggested that human error was responsible for the vast majority of data security incidents reported to the UK's Information Commissioner's Office, indicating a pervasive challenge [7]. To counteract these threats, cybersecurity professionals require a deep and intuitive understanding of their network environments. This is the core concept of Situational Awareness (SA), defined by Endsley as a three-stage process: the perception of elements in the environment, the comprehension of their meaning, and the projection of their status in the near future [8]. In the context of cybersecurity, this translates to Cyber Situational Awareness (Cyber SA)—a comprehensive understanding of the cyber environment that enables timely and effective defensive actions [10].

However, achieving a high level of Cyber SA is challenging. Security analysts are often inundated with vast streams of fast, dynamic, and heterogeneous data from disparate sources, which must be correlated and interpreted under immense time pressure. Traditional Security Operations

Centers (SOCs) rely on dashboards and 2D visualizations, which can be inadequate for representing the complex, high-dimensional nature of network traffic and threat data. This often leads to data occlusion and convolution, where important information is hidden or difficult to distinguish, thereby limiting an analyst's perception [11, 12]. The cognitive load associated with mentally stitching together information from multiple screens and terminals can lead to fatigue and missed indicators of an attack [14].

Recognizing these limitations, researchers have begun exploring immersive technologies—Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR), collectively known as Extended Reality (XR)—as a new paradigm for cyber defense [18, 60]. Immersive technologies offer the potential to move beyond flat screens, presenting data in three-dimensional, interactive, and collaborative virtual spaces [28, 70]. The hypothesis is that by mapping abstract cyber data to intuitive 3D visualizations, analysts can more readily perceive patterns, identify anomalies, and comprehend complex relationships within the data [16, 35]. Early systems have demonstrated the potential of AR for visualizing network operations and improving cognitive performance [11, 14], while mobile AR applications aim to bring cybersecurity data directly into the physical environment [12]. Similarly, VR has been used to create fully immersive environments for monitoring threat intelligence and training security personnel [15, 16, 17].

Given the growing body of work in this area, a systematic synthesis is required. This survey aims to systematically review the body of research on immersive systems for Cyber SA. We seek to synthesize the current state of the art, identify the primary applications and system designs, evaluate the reported benefits, and consolidate the outstanding challenges. Our key contributions are:

- A detailed analysis and novel taxonomy of the visualization and interaction techniques used in ICSA systems.
- A categorization of existing research according to the three levels of Cyber SA: perception, comprehension, and projection.
- The proposal of a new reference framework to guide the design and evaluation of ICSA systems.
- An identification of key research gaps, future directions, and industrial implications for the field.

2. METHODS

To ensure a comprehensive and unbiased review of the literature, we adopted a systematic literature review (SLR) methodology, drawing upon established guidelines in software engineering and other fields [23]. Our review process was structured into three main phases: planning, execution, and analysis.

2.1. Research Questions

The review was guided by a set of research questions designed to structure the investigation into the current state of ICSA systems:

- RQ1: What are the primary visualization and interaction techniques used in ICSA systems? This question aims to identify and categorize the specific methods used to represent and manipulate data in immersive cybersecurity environments.
- RQ2: What levels of Cyber SA (perception, comprehension, projection) are facilitated by existing ICSA systems? This question seeks to analyze how current systems support the different cognitive stages of situational awareness based on Endsley's model.
- RQ3: How are ICSA systems empirically evaluated in the literature, and what are the key findings? This question intends to synthesize the validation methods, metrics, and outcomes reported in user studies to understand the proven benefits and limitations.
- RQ4: What are the key challenges, open research questions, and future directions for the field? This question aims to identify the primary obstacles and opportunities for advancing the state of the art in ICSA.

2.2. Search Strategy and Study Selection

We conducted a systematic search of the Scopus academic database, which provides broad coverage of peer-reviewed literature from other major databases like IEEE Xplore and ACM Digital Library [24, 25]. Our search query combined keywords related to immersive technologies and cybersecurity, such as: ("virtual reality" OR "augmented reality" OR "mixed reality" OR "immersive analytics") AND ("cybersecurity" OR "network security" OR "situational awareness" OR "threat intelligence").

The initial search yielded a large set of papers. We then applied a multi-stage filtering process based on the following predefined inclusion and exclusion criteria:

- Inclusion Criteria: Studies were included if they were published in English in a peer-reviewed journal or conference, focused on the design, development, or evaluation of an immersive system (VR, AR, MR) for a cybersecurity task, and presented either empirical evidence, a user study, or a detailed conceptual framework.
- Exclusion Criteria: Studies were excluded if immersive technology was not the primary focus, if they were non-peer-reviewed articles (e.g., editorials, keynotes, workshop summaries, book chapters), or if the full text was not accessible.

To ensure comprehensive coverage, we also employed the "snowballing" technique, where the reference lists of selected primary studies were manually scanned to identify additional relevant publications [26]. This iterative process helped uncover foundational work and recent studies that may have been missed by the initial keyword search, resulting in a final corpus of 72 relevant studies for analysis.

2.3. Data Extraction and Thematic Analysis

For each paper that met the inclusion criteria, we extracted relevant data pertaining to our research questions. This included the type of immersive technology used (VR/AR/MR), the specific cybersecurity application, system design details, evaluation methods (e.g., user study, performance metrics), key findings, and reported challenges.

To synthesize the extracted data, we employed thematic analysis, a qualitative method for identifying, analyzing, and reporting patterns (themes) within data [27]. We followed a multi-step process: (1) familiarizing ourselves with the data; (2) generating initial codes for visualization techniques, interaction features, and evaluation outcomes; (3) searching for broader themes by grouping related codes; (4) reviewing and refining these themes; and (5) defining and naming the final themes. This approach allowed us to structure the Results section around the dominant trends and topics in the literature.

3. Results: A Taxonomy of Immersive Techniques for Cyber SA

Our systematic review of the literature identified 72 relevant studies. The analysis of these papers revealed several key themes regarding the application, design, and evaluation of immersive systems for cybersecurity. This section presents a detailed taxonomy of the visualization and interaction techniques identified.

3.1. Visualization Techniques for ICSA

Immersive technologies provide unique capabilities for visualizing complex, multidimensional cybersecurity data. We identified 11 distinct visualization techniques used in the literature.

- Geographical Displays: These visualizations map cybersecurity data onto geographical representations, such as a 3D globe, to show the physical location of network assets, traffic origins, or attacks [11, 29, 30]. This leverages spatial reasoning to help analysts understand the global scope of their network.
- Metaphorical Displays: To make abstract data more comprehensible, some systems use metaphors. For instance, Delcombel et al. [31] used a 3D helix to represent periodic signals of cyberattacks, placing the user inside the structure for an unobstructed view.
- Node-Link Graphs: This is a common technique for visualizing network topologies, where nodes represent devices and links represent connections [29, 32, 33, 34, 35]. In an immersive 3D space, these graphs can be explored from multiple angles.
- Scatterplots: 3D scatterplots are used to show relationships between multiple data variables, aiding in the identification of clusters and outliers [36].
- 3D Bar Charts: These extend traditional bar charts into three dimensions, allowing for the comparison of multiple data series simultaneously [37].
- Volume Rendering: This technique uses 3D objects and models to represent cybersecurity concepts, common in both operational displays and educational games [11, 14, 15, 20, 29, 31-33, 38-45].
- Icons, Symbols, and Glyphs: To provide quick, at-a-glance information, many ICSA systems use icons to represent network components or user actions [12, 29, 41, 42, 45, 46, 47].
- Animation/Video Displays: Dynamic elements like animations are used to demonstrate processes or consequences, such as the propagation of a virus through a network [11, 46].
- 360° Pictures/Environments: Fully immersive 360° environments place the user within a comprehensive cyber common operating picture, often used in VR-based SOC simulations [16, 40, 48].
- 2D Displays in 3D Space: Many ICSA systems embed traditional 2D displays (like terminal windows or dashboards) as virtual screens within the 3D immersive space [14, 15, 29, 32, 33, 38-40, 47].
- List, Table, and Text Displays: For conveying precise instructions or logs, textual information is often presented on virtual tablets or pop-up panels [11, 12, 31, 33, 38-40, 45-47].

Comparative Analysis of Visualization Techniques: Each technique offers distinct advantages and disadvantages. Geographical displays and node-link graphs excel at showing structural relationships but can suffer from visual clutter in dense networks. Metaphorical displays are intuitive but may require a learning curve if the metaphor is not universally understood. Analytical visualizations like scatterplots and 3D bar charts are powerful for data analysis but can increase cognitive load. Icons and animations are excellent for engagement and high-level understanding but lack analytical depth. The most effective ICSA systems often use a hybrid approach, combining multiple techniques to balance immersion, clarity, and analytical power.

3.2. Interaction Techniques for ICSA

Effective interaction is critical for exploring and making sense of immersive visualizations. We identified nine common interaction techniques.

- Select: The fundamental act of choosing an object or option, accomplished through various modalities like gaze, gesture, or controllers [11, 12, 20, 29-33, 36-40, 42, 45-47, 50-52].
- Navigate: Moving through the immersive environment, often via physical movement, controller joysticks, or teleportation [11, 20, 29-33, 38-40, 46, 47, 50].

- Details on Demand: This allows users to retrieve more detailed information about a selected object [11, 12, 20, 29-33, 37-40, 45-47, 53, 54].

- Arrange/Change: Users can manipulate the environment by moving, rotating, or scaling visualizations to customize their workspace [29-33, 36, 37, 39, 40, 46].

- Filter: This enables users to show or hide data based on specific criteria to reduce visual clutter [29, 31, 32].

- Extract/Share: In collaborative environments, users can extract data or visualizations to share them with teammates [32, 50].

- Aggregate/Relate: This involves combining multiple data points to create higher-level information or to identify relationships [31, 32, 36, 37].

- Annotate: Users can add their own textual or graphical notes directly onto visualizations in the 3D space [31, 32].

- Record: Some systems allow for the recording of user interactions or data trends over time for post-incident analysis [33].

Comparative Analysis of Interaction Techniques: There are trade-offs among these techniques. Gesture and gaze interactions are natural and hands-free but may lack the precision of controller-based inputs. Unconstrained navigation can enhance immersion but also risks causing disorientation or cybersickness. The most successful ICSA systems provide multiple, complementary interaction methods, allowing users to choose the best tool for the task at hand.

4. Levels of Immersive Cyber Situational Awareness

Drawing on Endsley's widely accepted model [8], we categorized the surveyed literature based on the level of situational awareness each ICSA system aims to support. The majority of studies [11, 12, 14, 15, 20, 30-33, 36, 37, 39-47, 51, 53, 58-62] focus on the foundational level of Perception. A smaller, yet significant, number of studies [29, 31-34, 37, 38, 46, 54, 63-65] address the more advanced level of Comprehension. The highest level, Projection, remains the least explored, with only a few studies [11, 35, 38, 46] attempting to address it.

4.1. Level 1: Perception

Perception is the foundational level, answering the question, "What is happening?" It involves monitoring the environment to detect and recognize key elements. The majority of ICSA systems focus on this level. They use immersive visualizations to provide a holistic overview of the cyber environment, helping users perceive threats, vulnerabilities, and network status at a glance. For example, displaying real-time threat alerts on a global map provides perception of an ongoing attack campaign [15]. Similarly, using distinct icons for different types of malware helps with rapid recognition [41]. The primary goal of perception-level systems is to present data in a way that is quickly and easily digestible, leveraging the full 3D space to avoid the data occlusion common on 2D screens [12, 58, 61].

4.2. Level 2: Comprehension

Comprehension goes beyond perception to answer the question, "What does it mean?" This level involves analyzing and integrating information to understand the significance of events and the relationships between them. ICSA systems support comprehension by providing interactive tools for data exploration. For instance, the 3D Cyber COP system allows analysts to filter and aggregate alerts to distinguish between false positives and genuine threats, thereby comprehending the true security state [33]. Interactive bar charts that allow for comparative analysis of network traffic help analysts understand why a particular spike is anomalous [37]. This level is about turning raw data into actionable insights through tasks like pattern analysis, data clustering, and visual correlation [34, 64].

4.3. Level 3: Projection

Projection is the highest level of SA, answering the question, "What will happen next?" It involves extrapolating from current information to predict future states. This level remains significantly underexplored in ICSA research. Supporting projection is inherently complex, as it requires predictive modeling and the visualization of hypothetical scenarios. A few systems have begun to address this. For example, an AR application that uses animations to show the negative consequences of clicking on a phishing link helps users project the outcome of their actions [46]. A 3D mixed reality visualization that improves team communication has been shown to enhance their ability to anticipate the adversary's next move [35]. However, most systems lack the integration with real-time simulation or predictive analytics needed for robust projection. This represents a major gap and a critical area for future research.

5. Evaluation of ICSA Systems

The literature employs various user-experience research methods to evaluate the effectiveness of ICSA systems. These evaluations consistently show that immersive technologies can enhance user performance and cognition, but they also reveal methodological limitations. The most common evaluation methods are user studies involving questionnaires (e.g., with Likert scales), usability instruments (like the System Usability Scale - SUS), and cognitive load assessments (such as the NASA-TLX and SART) [14, 15, 33, 38]. These are often supplemented by objective performance metrics, including task completion time, accuracy, response rates, and memory recall tests [39, 42, 48].

The findings consistently report that ICSA systems lead to higher user engagement, better memory retention in training scenarios [40, 41], and improved performance on tasks like anomaly detection compared to traditional interfaces [14]. For example, a study by Beitzel et al. [14] using a Capture the Flag exercise with 7 male participants found that AR improved performance (e.g., total elapsed time, response time) and cognitive outcomes (e.g., mental demand, frustration). Another study by Salazar et al. [42] with 208 participants found that AR-based games improved both performance (knowledge acquisition, vulnerability detection) and cognition (confidence). Similarly, a study by Rana et al. [48] with 100 participants demonstrated that VR training was more effective than traditional video-based methods based on task completion time and accuracy.

However, some studies note that benefits can be influenced by user demographics, such as gender or prior experience, suggesting that one-size-fits-all solutions may not be optimal [15, 41]. A significant limitation in the current body of research is the reliance on small-scale user studies, which limits the statistical power and generalizability of the findings. Furthermore, there is a lack of standardized evaluation frameworks, making it difficult to compare results across different studies.

6. A Reference Framework for Designing and Analyzing ICSA Systems

Based on our analysis, we propose a reference framework to guide the development and evaluation of ICSA systems. This framework maps visualization and interaction techniques to the three levels of situational awareness. The goal is to help developers select appropriate features to meet specific cognitive objectives.

Conceptual Framework:

● Level 1: Perception (Monitoring & Recognition)

○ Visualization Techniques: Node-link graphs, Geographical displays, 3D Iconography, Volume rendering, 2D displays in 3D space, Text summaries/tables. These techniques provide a clear, high-level overview of the system's state.

○ Interaction Techniques: Select (via Gaze, Controller, Gesture), Navigate, Scroll. These are fundamental interactions for observing and moving through the environment.

● Level 2: Comprehension (Analysis & Interpretation)

○ Visualization Techniques: Metaphors, Scatterplots, 3D Bar Charts, Parallel Coordinate Plots. These visualizations support deeper analysis and comparison.

○ Interaction Techniques: Details on Demand, Filter, Arrange/Change, Aggregate/Relate, Annotate, Zoom. These interactions allow users to drill down into data, reduce clutter, and build a mental model of the situation.

● Level 3: Projection (Prediction & Forecasting)

○ Visualization Techniques: Animations, Flow visualizations, Temporal data displays (e.g., showing historical trends and predicted future paths). These techniques help visualize change over time and hypothetical outcomes.

○ Interaction Techniques: Extract/Share, Record. These support collaborative "what-if" scenario planning and retrospective analysis to inform future predictions.

This framework provides a structured approach for designers. For example, a system designed primarily for real-time monitoring (Perception) should prioritize clear node-link graphs and simple navigation. A system for forensic analysis (Comprehension) would need powerful filtering and details-on-demand capabilities. A system for strategic planning (Projection) would require tools for collaborative scenario modeling.

7. DISCUSSION

The results of our systematic review indicate that immersive technologies represent a vibrant and rapidly evolving frontier in cybersecurity. This section synthesizes our findings, discusses the overarching challenges, and outlines promising directions for future work.

7.1. Synthesis of Findings and Implications

The primary implication of our findings is that immersive analytics offers a compelling alternative to the traditional, screen-based paradigms that have dominated SOCs. By leveraging the human brain's innate capacity for spatial reasoning, 3D visualizations can transform abstract data streams into tangible, explorable landscapes [67]. This can reduce cognitive load and foster a deeper level of Cyber SA [10, 57]. The ability to create collaborative virtual environments where teams can jointly analyze a threat is particularly powerful, potentially accelerating incident response [50, 56]. Furthermore, the application of XR in education is profoundly impactful, making learning active, engaging, and memorable, which can help cultivate a more skilled cybersecurity workforce [9, 17].

7.2. Limitations and Challenges

Despite the promising results, the widespread adoption of ICSA systems is hindered by several significant challenges.

1. Usability and Human Factors: This is a frequently cited challenge. Issues such as cybersickness, visual fatigue, and a steep learning curve for complex interaction techniques can negate the potential benefits [44]. Designing intuitive controls and minimizing cognitive overload are critical research problems [33].

2. Scalability: Cybersecurity data is characterized by immense volume and velocity. Visualizing an entire enterprise network in real-time without overwhelming the user or the hardware is a major technical hurdle. Most current prototypes operate on limited datasets.

3. Integration with Existing Workflows: Immersive

systems must interface with existing SOC tools like SIEMs and threat intelligence platforms. The challenges of achieving seamless integration are both technical and procedural [21, 22].

4. Lack of Standardized Evaluation: The field lacks standardized benchmarks and evaluation methodologies, making it difficult to compare the effectiveness of different systems. More rigorous, longitudinal studies are needed [63].

5. Security of Immersive Systems: XR systems themselves introduce new vulnerabilities, including data privacy concerns related to the biometric and behavioral data they collect [71].

6. Methodological Limitations of this Survey: This review was limited to the Scopus database and excluded non-peer-reviewed literature, which may have omitted some relevant work. Additionally, a formal quality assessment of the included studies was not performed.

7.3. Industrial Implications

ICSA systems have significant potential for the cybersecurity industry. In addition to training, they can enhance real-time collaboration in SOCs and assist in troubleshooting by allowing analysts to explore data interactively. However, industries must address the security and privacy risks. Sensitive data captured by immersive platforms (e.g., gaze patterns, user behavior) must be protected through robust measures like encryption and multifactor authentication [71]. A real-world parallel can be seen in frameworks like SCOUT for critical infrastructure protection, which fuses cyber-physical data for situational awareness [72]. Integrating such systems with immersive interfaces could be a powerful next step for industry.

7.4. Future Research Directions

Based on the identified gaps, we propose the following directions for future research:

- Focus on Projection: As highlighted by our framework, there is a critical need for research into visualization and interaction techniques that explicitly support the projection level of SA. This includes developing methods for predictive analysis and "what-if" scenario modeling in immersive environments.

- Integrating Advanced Visualization and Interaction: Researchers should explore more advanced techniques not yet common in ICSA, such as flow visualizations for mapping data movement [66], Kohonen maps for visualizing high-dimensional data [67], and 3D heatmaps for intuitive data comparison [68].

- Large-Scale User Studies: To validate the utility of these systems, the field must move beyond small-scale lab experiments. Longitudinal studies that deploy ICSA systems in realistic SOC environments with a diverse range of participants are needed to understand their practical impact.

- Integration of AI and LLMs: The synergy between AI and immersive visualization is a largely untapped area. AI can pre-process and filter data, highlighting critical events for the analyst. LLMs could enable natural language interaction, allowing analysts to ask complex questions about the network, with the results visualized immersively [13, 49].

- Adaptive Interfaces: Future systems should move towards adaptive interfaces that can dynamically adjust the visualization's complexity based on the user's cognitive state, expertise, and current task, potentially using biometric sensors to infer cognitive load.

8. CONCLUSION

Immersive technologies are poised to significantly advance the field of Cyber Situational Awareness. By moving beyond the limitations of 2D screens, ICSA systems offer a more intuitive, engaging, and powerful way to visualize and interact with complex cybersecurity data. This survey has provided a systematic overview of the state of the art, presenting a detailed taxonomy of visualization and interaction techniques and categorizing them according to the levels of situational awareness they support. We have proposed a reference framework to guide future design and highlighted the critical need for more research into the projection level of SA, large-scale empirical evaluation, and the integration of AI. While significant challenges in usability, scalability, and security remain, the ongoing innovation in this space suggests that the virtual and augmented worlds will play an increasingly critical role in defending our digital one.

REFERENCES

[1] Williams, C.M.; Chaturvedi, R.; Chakravarthy, K. Cybersecurity risks in a pandemic. J. Med. Internet Res. 2020, 22, e23692.

[2] Arogbodo, M. Impacts of the COVID-19 Pandemic on Online Security Behavior Within the UK Educational Industry. 2022.

[3] Mouna, B.; Yassine, M. Business Leadership in E-Commerce in the USA: The Impact of Blockchain Technology. Bus. Ethics Leadersh. 2024, 8, 116–128.

[4] Kuzior, A.; Tiutiunyk, I.; Zieli ́nska, A.; Kelemen, R. Cybersecurity and cybercrime: Current trends and threats. J. Int. Stud. 2024, 17, 220.

[5] 2024 Data Breach Investigations Report. 2024.

[6] Thirupathi, L.; Vasundara, B.; Sundaragiri, D.; Ch, V.B.; Gugulothu, R.; Pulyala, R. Understanding and Addressing Human Factors in Cybersecurity Vulnerabilities. In Human Impact on Security and Privacy: Network and Human Security, Social Media, and Devices; IGI Global: Hershey, PA, USA, 2025; pp. 13–38.

[7] Button, M.; Shepherd, D.; Blackbourn, D.; Sugiura, L.; Kapend, R.; Wang, V. Assessing the seriousness of cybercrime: The case of computer misuse crime in the

United Kingdom and the victims' perspective. Criminol. Crim. Justice 2025, 25, 670–691.

[8] Endsley, M.R. Design and evaluation for situation awareness enhancement. Proc. Hum. Factors Soc. Annu. Meet. 1988, 32, 97–101.

[9] Ullah, F.; Ye, X.; Fatima, U.; Akhtar, Z.; Wu, Y.; Ahmad, H. What Skills Do Cyber Security Professionals Need? arXiv 2025, arXiv:2502.13658.

[10] Barford, P.; Dacier, M.; Dietterich, T.G.; Fredrikson, M.; Giffin, J.; Jajodia, S.; Jha, S.; Li, J.; Liu, P.; Ning, P.; et al. Cyber SA: Situational awareness for cyber defense. In Cyber Situational Awareness; Springer: Berlin/Heidelberg, Germany, 2010; pp. 3–13.

[11] Sukhija, N.; Haser, C.; Bautista, E. 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), Chicago, IL, USA, 28 July–1 August 2019 ; pp. 1–4.

[12] Mattina, B.; Yeung, F.; Hsu, A.; Savoy, D.; Tront, J.; Raymond, D. MARCS: Mobile augmented reality for cybersecurity. In Proceedings of the 12th Annual Conference on Cyber and Information Security Research, Oak Ridge, TN, USA, 4–6 April 2017; pp. 1–4.

[13] Chopra, S.; Ahmad, H.; Goel, D.; Szabo, C. ChatNVD: Advancing Cybersecurity Vulnerability Assessment with Large Language Models. arXiv 2024, arXiv:2412.04756.

[14] Beitzel, S.; Dykstra, J.; Huver, S.; Kaplan, M.; Loushine, M.; Youzwak, J. Cognitive performance impact of augmented reality for network operations tasks. In Advances in Human Factors in Cybersecurity; Springer: Berlin/Heidelberg, Germany, 2016; pp. 139–151.

[15] Korkiakoski, M.; Sadiq, F.; Setianto, F.; Latif, U.K.; Alavesa, P.; Kostakos, P. Using smart glasses for monitoring cyber threat intelligence feeds. In Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, The Hague, The Netherlands, 8–11 November 2021; pp. 630–634.

[16] Munsinger, B.; Beebe, N.; Richardson, T. Virtual reality for improving cyber situational awareness in security operations centers. Comput. Secur. 2023, 132, 103368.

[17] Alnajim, A.M.; Habib, S.; Islam, M.; AlRawashdeh, H.S.; Wasim, M. Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. Symmetry 2023, 15, 2175.

[18] Abu Deeb, F. Enhancing Cybersecurity with Extended Reality: A Systematic Review. J. Comput. Inf. Syst. 2024, 1–15.

[19] Skorenkyy, Y.; Kozak, R.; Zagorodna, N.; Kramar, O.; Baran, I. Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. J. Phys. Conf. Ser. 2021, 1840, 012026.

[20] Puttawong, N.; Visoottiviseth, V.; Haga, J. VRFiWall virtual reality edutainment for firewall security concepts. In Proceedings of the 2017 2nd International Conference on Information Technology (INCIT), Nakhonpathom, Thailand, 2–3 November 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.

[21] Dissanayake, N.; Jayatilaka, A.; Zahedi, M.; Babar, M.A. Software security patch management-A systematic literature review of challenges, approaches, tools and practices. Inf. Softw. Technol. 2022, 144, 106771.

[22] Shahin, M.; Babar, M.A.; Zhu, L. Continuous integration, delivery and deployment: A systematic review on approaches, tools, challenges and practices. IEEE Access 2017, 5, 3909–3943.

[23] Kitchenham, B.; Pretorius, R.; Budgen, D.; Brereton, O.P.; Turner, M.; Niazi, M.; Linkman, S. Systematic literature reviews in software engineering–a tertiary study. Inf. Softw. Technol. 2010, 52, 792–805.

[24] Zahedi, M.; Shahin, M.; Babar, M.A. A systematic review of knowledge sharing challenges and practices in global software development. Int. J. Inf. Manag. 2016, 36, 995–1019.

[25] Shahin, M.; Babar, M.A.; Chauhan, M.A. Architectural design space for modelling and simulation as a service: A review. J. Syst. Softw. 2020, 170, 110752.

[26] Wohlin, C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, London, UK, 13–14 May 2014.

[27] Braun, V.; Clarke, V. Using thematic analysis in psychology. Qual. Res. Psychol. 2006, 3, 77–101.

[28] Dwyer, T.; Marriott, K.; Isenberg, T.; Klein, K.; Riche, N.; Schreiber, F.; Stuerzlinger, W.; Thomas, B.H. Immersive analytics: An introduction. In Immersive Analytics; Springer: Berlin/Heidelberg, Germany, 2018; pp. 1–23.

[29] Beitzel, S.; Dykstra, J.; Toliver, P.; Youzwak, J. Exploring 3d cybersecurity visualization with the microsoft hololens. In Proceedings of the International Conference on Applied Human Factors and Ergonomics, Los Angeles, CA, USA, 17–21 July 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 197–207.

[30] Ma, C.; Kulshrestha, S.; Shi, W.; Okada, Y.; Bose, R. E-learning material development framework supporting VR/AR based on linked data for IoT security education. In Proceedings of the International Conference on Emerging Internetworking, Data & Web Technologies, Tirana, Albania, 15–17 March 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 479–491.

[31] Delcombel, N.; Kabil, A.; Duval, T.; Pahl, M.O. CyberCopter: A 3D helical visualisation for periodic signals

of cyber attacks. In Proceedings of the VR4Sec 2021 (Security for XR and XR for Security), Virtual, 6 August 2021.

[32] Kabil, A.; Duval, T.; Cuppens, N.; Le Comte, G.; Halgand, Y.; Ponchel, C. 3D cybercop: A collaborative platform for cybersecurity data analysis and training. In Proceedings of the International Conference on Cooperative Design, Visualization and Engineering, Hangzhou, China, 21–24 October 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 176–183.

[33] Kabil, A.; Duval, T.; Cuppens, N. Alert characterization by non-expert users in a cybersecurity virtual environment: A usability study. In Proceedings of the International Conference on Augmented Reality, Virtual Reality and Computer Graphics, Lecce, Italy, 7–10 September 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 82–101.

[34] Kullman, K.; Asher, N.B.; Sample, C. 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, Coimbra, Portugal, 4–5 July 2019; ACPI: Reading, UK, 2019; pp. 257–266.

[35] Ask, T.F.; Kullman, K.; Sütterlin, S.; Knox, B.J.; Engel, D.; Lugo, R.G. A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. Front. Big Data 2023, 6, 1042783.

[36] Kullman, K.; Cowley, J.; Ben-Asher, N. 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, 8–9 March 2018; pp. 369–378.

[37] Beitzel, S.; Dykstra, J.; Toliver, P.; Youzwak, J. Network anomaly analysis using the Microsoft HoloLens. Proc. Hum. Factors Ergon. Soc. Annu. Meet. 2018, 62, 2094–2098.

[38] Alqahtani, H.; Kavakli-Thorne, M. Design and evaluation of an augmented reality game for cybersecurity awareness (cybar). Information 2020, 11, 121.

[39] Seo, J.H.; Bruner, M.; Payne, A.; Gober, N.; McMullen, D.; Chakravorty, D.K. Using virtual reality to enforce principles of cybersecurity. J. Comput. Sci. Educ. 2019, 10, 81–87.

[40] Chu, E.S.; Payne, A.; Seo, J.H.; Chakravorty, D.; McMullen, D. Data center physical security training VR to support procedural memory tasks. In Proceedings of the International Conference on Human-Computer Interaction, Orlando, FL, USA, 26–31 July 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 353–358.

[41] Jin, G.; Tu, M.; Kim, T.H.; Heffron, J.; White, J. Game based cybersecurity training for high school students. In Proceedings of the ACM Technical Symposium on Computer Science Education, Baltimore, MD, USA, 21–24 February 2018; pp. 68–73.

[42] Salazar, M.; Gaviria, J.; Laorden, C.; Bringas, P.G. Enhancing cybersecurity learning through an augmented reality-based serious game. In Proceedings of the 2013 IEEE Global Engineering Education Conference (EDUCON), Berlin, Germany, 13–15 March 2013; pp. 602–607.

[43] Garae, J.; Ko, R.K.; Kho, J.; Suwadi, S.; Will, M.A.; Apperley, M. Visualizing the new zealand cyber security challenge for attack behaviors. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, Australia, 1–4 August 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1123–1130.

[44] Kasurinen, J. Usability issues of virtual reality learning simulator in healthcare and cybersecurity. Procedia Comput. Sci. 2017, 119, 341–349.

[45] Sharma, A.; Palrecha, D.; Parekh, M. Security Awareness Game (Augmented Reality). In Proceedings of the International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur, India, 26–28 February 2019.

[46] Chiou, Y.M.; Shen, C.C.; Mouza, C.; Rutherford, T. Augmented Reality-Based Cybersecurity Education on Phishing. In Proceedings of the 2021 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), Taichung, Taiwan, 15–17 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 228–231.

[47] Faisal, K.; Nikitha, K.; Portia, P. Augmented Reality Mobile Forensic Laboratory (AMFL). In Proceedings of the 10th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2019), Orlando, FL, USA, 12–15 March 2019.

[48] Rana, S.; Alhamdani, W. Exploring the Need to Study the Efficacy of VR Training Compared to Traditional Cybersecurity Training. Int. J. Comput. Inf. Eng. 2014.

[49] Goel, D.; Ahmad, H.; Jain, A.K.; Goel, N.K. Machine Learning Driven Smishing Detection Framework for Mobile Security. arXiv 2024, arXiv:2412.09641.

[50] Kabil, A.; Duval, T.; Cuppens, N.; Le Comte, G.; Halgand, Y.; Ponchel, C. Why should we use 3d collaborative virtual environments for cyber security? In Proceedings of the 2018 IEEE Fourth VR International Workshop on Collaborative Virtual Environments (3DCVE), Reutlingen, Germany, 19 March 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–2.

[51] Korkiakoski, M.; Antila, A.; Annamaa, J.; Sheikhi, S.; Alavesa, P.; Kostakos, P. Hack the Room: Exploring the potential of an augmented reality game for teaching cyber security. In Proceedings of the Augmented Humans International Conference 2023, Glasgow, UK, 12–14 March 2023; pp. 349–353.

[52] Manoharan, A.; Sriskantharajah, A.; Herath, H.;

Guruge, L.; Yasakethu, S. MetaHuman based phishing attacks in the metaverse realm: Awareness for cyber security education. Educ. Inf. Technol. 2025, 1–27.

[53] Chakal, K.; Korkiakoski, M.; Mehmood, H.; Anagnostopoulos, T.; Alavesa, P.; Kostakos, P. Augmented Reality Integration for Real-Time Security and Maintenance in IoT-Enabled Smart Campuses. In Proceedings of the 2023 IEEE 31st International Conference on Network Protocols (ICNP), Reykjavik, Iceland, 10–13 October 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6.

[54] Bernsland, M.; Moshfegh, A.; Lindén, K.; Bajin, S.; Quintero, L.; Solsona Belenguer, J.; Rostami, A. Cs: No–an extended reality experience for cyber security education. In Proceedings of the 2022 ACM International Conference on Interactive Media Experiences, Aveiro, Portugal, 22–24 June 2022; pp. 287–292.

[55] Hunter, J.; Porter, M.; Williams, B. Towards a theoretical framework for situational awareness in paramedicine. Saf. Sci. 2020, 122, 104528.

[56] Riley, J.M.; Endsley, M.R.; Bolstad, C.A.; Cuevas, H.M. Collaborative planning and situation awareness in Army command and control. Ergonomics 2006, 49, 1139–1153.

[57] Onwubiko, C. Understanding Cyber Situation Awareness. Int. J. Cyber Situational Aware. 2016, 1, 11–30.

[58] Alqahtani, H.; Kavakli-Thorne, M. Exploring factors affecting user's cybersecurity behaviour by using mobile augmented reality app (CybAR). In Proceedings of the 2020 12th International Conference on Computer and Automation Engineering, Sydney, Australia, 14–16 February 2020; pp. 129–135.

[59] Shen, C.C.; Chiou, Y.M.; Mouza, C.; Rutherford, T. Work-in-progress-design and evaluation of mixed reality programs for cybersecurity education. In Proceedings of the 2021 7th International Conference of the Immersive Learning Research Network (iLRN), Eureka, CA, USA, 17 May–10 June 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–3.

[60] Wagner, P.; Alharthi, D. Leveraging VR/AR/MR/XR Technologies to Improve Cybersecurity Education, Training, and Operations. J. Cybersecur. Educ. Res. Pract. 2023, 2024, 7.

[61] Kommera, N.; Kaleem, F.; Harooni, S.M.S. Smart augmented reality glasses in cybersecurity and forensic education. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28–30 September 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 279–281.

[62] Chen, W.; He, Y.; Tian, X.; He, W. Exploring cybersecurity education at the K-12 level. In Proceedings of the SITE Interactive Conference, Online, 26–28 October 2021; Association for the Advancement of Computing in Education (AACE): Chesapeake, Virginia, 2021 ; pp. 108–114.

[63] Kullman, K.; Ryan, M.; Trossbach, L. VR/MR supporting the future of defensive cyber operations. IFAC-PapersOnLine 2019, 52, 181–186.

[64] Veneruso, S.V.; Ferro, L.S.; Marrella, A.; Mecella, M.; Catarci, T. CyberVR: An interactive learning experience in virtual reality for cybersecurity related issues. In Proceedings of the International Conference on Advanced Visual Interfaces, Salerno, Italy, 28 September–October 2020; pp. 1–8.

[65] Kaneko, K.; Tsutsumi, Y.; Sharma, S.; Okada, Y. PACKUARIUM: Network packet visualization using mixed reality for detecting bot IoT device of DDoS attack. In Advances in Internet, Data and Web Technologies, Proceedings of the 8th International Conference on Emerging Internet, Data and Web Technologies (EIDWT-2020), Kitakyushu, Japan, 24–26 February 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 361–372.

[66] Homps, F.; Beugin, Y.; Vuillemot, R. ReViVD: Exploration and filtering of trajectories in an immersive environment using 3D shapes. In Proceedings of the 2020 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), Atlanta, GA, USA, 22–26 March 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 729–737.

[67] Kraus, M.; Fuchs, J.; Sommer, B.; Klein, K.; Engelke, U.; Keim, D.; Schreiber, F. Immersive analytics with abstract 3D visualizations: A survey. Comput. Graph. Forum 2022, 41, 201–229.

[68] Kraus, M.; Angerbauer, K.; Buchmüller, J.; Schweitzer, D.; Keim, D.A.; Sedlmair, M.; Fuchs, J. Assessing 2d and 3d heatmaps for comparative analysis: An empirical study. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 25–30 April 2020; pp. 1–14.

[69] Benko, H.; Ishak, E.W.; Feiner, S. Collaborative mixed reality visualization of an archaeological excavation. In Proceedings of the Third IEEE and ACM International Symposium on Mixed and Augmented Reality, Arlington, VA, USA, 2–5 November 2004; IEEE: Piscataway, NJ, USA, 2004; pp. 132–140.

[70] Fonnet, A.; Prie, Y. Survey of immersive analytics. IEEE Trans. Vis. Comput. Graph. 2019, 27, 2101–2122.

[71] Alismail, A.; Altulaihan, E.; Rahman, M.H.; Sufian, A. A systematic literature review on cybersecurity threats of virtual reality (vr) and augmented reality (ar). In Data Intelligence and Cognitive Informatics: Proceedings of ICDICI 2022, Tirunelveli, Tamil Nadu, 6–7 July 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 761–774.

[72] Cantelli-Forti, A.; Capria, A.; Saverino, A.L.; Berizzi, F.; Adami, D.; Callegari, C. Critical infrastructure protection system design based on SCOUT multitech seCurity system for intercOnnected space control groUnd staTions. Int. J. Crit. Infrastruct. Prot. 2021, 32, 100407.