Journal of *Cybersecurity and Privacy*

MDPI

Review

A Survey on Immersive Cyber Situational Awareness Systems

Hussain Ahmad [1], Faheem Ullah [2,*] and Rehan Jafri [3]

[1] School of Computer and Mathematical Sciences, The University of Adelaide, Adelaide 5005, Australia; hussain.ahmad@adelaide.edu.au
[2] College of Interdisciplinary Studies, Zayed University, Dubai 144534, United Arab Emirates
[3] Honeywell, Bracknell RG12 1EB, UK; rehan.jafri@honeywell.com
* Correspondence: faheem.ullah@zu.ac.ae

Abstract: Cyber situational awareness systems are increasingly used for creating cyber common operating pictures for cybersecurity analysis and education. However, these systems face data occlusion and convolution issues due to the burgeoning complexity, dimensionality, and heterogeneity of cybersecurity data, which damages cyber situational awareness of end-users. Moreover, conventional forms of human–computer interactions, such as mouse and keyboard, increase the mental effort and cognitive load of cybersecurity practitioners when analyzing cyber situations of large-scale infrastructures. Therefore, immersive technologies, such as virtual reality, augmented reality, and mixed reality, are employed in the cybersecurity realm to create intuitive, engaging, and interactive cyber common operating pictures. Immersive cyber situational awareness (ICSA) systems provide several unique visualization techniques and interaction features for the perception, comprehension, and projection of cyber situational awareness. However, there has been no attempt to comprehensively investigate and classify the existing state of the art in the use of immersive technologies for cyber situational awareness. Therefore, in this paper, we have gathered, analyzed, and synthesized the existing body of knowledge on ICSA systems. In particular, our survey has identified visualization and interaction techniques, evaluation mechanisms, and different levels of cyber situational awareness (i.e., perception, comprehension, and projection) for ICSA systems. Consequently, our survey has enabled us to propose (i) a reference framework for designing and analyzing ICSA systems by mapping immersive visualization and interaction techniques to the different levels of ICSA; (ii) future research directions for advancing the state of the art on ICSA systems; and (iii) an in-depth analysis of the industrial implications of ICSA systems to enhance cybersecurity operations.

Keywords: virtual reality; augmented reality; mixed reality; extended reality; cybersecurity; cyber situational awareness; cybersecurity education; cybersecurity training

Received: 9 April 2025
Revised: 28 May 2025
Accepted: 30 May 2025
Published: 12 June 2025

Citation: Ahmad, H.; Ullah, F.; Jafri, R. A Survey on Immersive Cyber Situational Awareness Systems. *J. Cybersecur. Priv.* **2025**, *5*, 33. https://doi.org/10.3390/jcp5020033

1. Introduction

With the drastic increase in cybercrime, especially after the outbreak of the COVID-19 pandemic [1], cybersecurity awareness, education, and training have become imperative for every individual. The pandemic alone contributed to a 400% increase in cybercrime incidents [2], coinciding with the accelerated digitization of services and global commerce. For instance, global retail e-commerce sales were valued at USD 5.8 trillion in 2023 [3], are projected to exceed USD 6.3 trillion in 2024, and are expected to surpass USD 8 trillion by 2027, creating an expanded attack surface for malicious actors [4]. This rise in online activity has been matched by a corresponding increase in cyber threats. In 2022, the FBI's

Internet Crime Complaint Center reported USD 10.3 billion in losses from cybercrime, up from USD 6.9 billion in 2021, across 800,944 reported incidents [4]. The 2024 Data Breach Investigations Report by Verizon Business found ransomware responsible for 23% of all breaches in 2023, while phishing simulations showed that 20% of users identified malicious emails, with 11% of those who clicked also reporting the incident [5]. Similarly, the Sophos State of Ransomware 2024 reported that 59% of organizations faced ransomware attacks in 2023, down slightly from 66% in the preceding two years. Critically, human error remains a central contributor to security breaches. A growing body of research links many incidents to a lack of cybersecurity training and user awareness [6]. One analysis found that 99% of data security incidents reported to the UK Information Commissioner's Office were caused by human error, suggesting that such incidents are far more common than currently acknowledged by the cybersecurity community [7]. In response, the field of cyber situational awareness is gaining increasing attention from researchers, practitioners, and educators, as it seeks to address the human element of cybersecurity by enhancing individuals' real-time understanding of cyber threats and decision-making under uncertainty.

Cyber situational awareness can be considered as an application of Endsley's situational awareness reference model [8] in the cybersecurity domain [9]. Cyber situational awareness refers to the identification, collection, analysis, and evaluation of cybersecurity data from a given system to make effective decisions for responding to potential cyber threats [10]. Traditional cyber situational awareness systems provide perception, comprehension, and projection of cyber environments to end users through two-dimensional displays (e.g., 2D screens) with limited interaction capabilities (e.g., mouse, keyboard, and monitor). These conventional visualization and interaction technologies limit users' cognition and understanding of cyber situations, which eventually deteriorates cyber situational awareness. For example, cybersecurity data complexities (e.g., fast, dynamic, and unpredictable data) and heterogeneity lead to data occlusion and convolution in traditional cybersecurity visualizations [11], which limits the perception of cyber situations [12,13]. Moreover, users suffer from mental effort and cognitive load when they need to shift their focus between multiple terminal windows to understand cyber situations and perform parallel activities through traditional visualization and interaction techniques of cyber situational awareness systems [14]. This issue was spotlighted during the surge of the COVID-19 pandemic when operators needed to monitor pandemic-related data and respond to cybersecurity alerts simultaneously [15].

To solve the abovementioned problems, immersive technologies based on extended reality are used to create effective cyber situational awareness for end-users [16–18]. Immersive cyber situational awareness systems refer to software and hardware systems that allow users to replace or expand their physical environments with virtual objects to create perception, comprehension, and projection of cybersecurity-relevant information within a system. ICSA systems provide several features for enhancing the cyber situational awareness of end-users [19]. While several related paradigms, such as digital twins, gamification, and the metaverse, share immersive characteristics, ICSA systems in this context are specifically grounded in extended reality technologies such as virtual, augmented, and mixed reality. These systems provide a range of features to enhance users' understanding of complex and evolving cyber threats. For example, ICSA systems present multidimensional cybersecurity data through different visualization techniques (e.g., metaphorical shapes, icons, and scatterplots) with an ability to arrange its multiple views through natural interaction features (e.g., gaze, gesture, and controller) in a spatial three-dimensional space around users for monitoring, analyzing and forecasting cyber situations. Moreover, a single immersive 3D display presents cybersecurity information in a unified manner, delivering a comprehensive cyber common operating picture while reducing cognitive load and eliminating the need

for multiple traditional data views to achieve situational awareness. Furthermore, ICSA systems provide engagement, entertainment, and enjoyment in cybersecurity education and training processes [20], which significantly increases cyber situational awareness with less cognitive load and mental effort. With the adoption of the *Industrial Revolution 4.0*, ICSA systems can be employed in a variety of settings, including Security Operation Centers, operations of Computer Emergency Response Teams, Incident Response Management, Network Security Operations, and Computer Network Defense, as well as in cybersecurity education and training.

Given the advantages of ICSA systems over traditional cyber situational awareness systems, researchers and practitioners have been putting a lot of effort into analyzing, designing, and evaluating visualization and interaction features of ICSA systems for a better understanding of cyber situational awareness. Therefore, the body of knowledge on ICSA systems has continuously been scatteredly expanding. Hence, we decided to collect, analyze, and synthesize the existing literature for systematizing and classifying the state of the art on ICSA systems. In this study, we have extracted, analyzed, and reported the existing literature on ICSA systems. In particular, our survey aims to review the visualization and interaction techniques, evaluation mechanisms, and levels of cyber situational awareness achieved for ICSA systems. The ICSA visualization and interaction techniques are then further analyzed in terms of the perception, comprehension, and projection phases of cyber situational awareness to propose a framework for designing and analyzing ICSA systems. Furthermore, this survey identifies future research directions for researchers and provides industrial insights for practitioners regarding ICSA systems.

Our Contributions In summary, our survey makes the following contributions.

- It provides an overarching analysis of ICSA visualization and interaction techniques identified in the literature. Each visualization and interaction technique is reported in the context of perception, comprehension, and projection of ICSA systems. The visualization and interaction techniques are categorized based on a novel taxonomy separately.
- It gives a comprehensive analysis of the situational awareness levels achieved for ICSA in the literature. For the first time, each level of situational awareness is described in the context of ICSA. The existing literature is categorized based on the defined levels of ICSA (i.e., perception, comprehension, projection).
- It presents a high-level investigation of evaluation mechanisms used to validate ICSA systems. Each evaluation mechanism has been critically examined, focusing on ICSA usability evaluation, user demographics, performance, and cognition metrics. The evaluation mechanisms are categorized based on the methodology employed for validating ICSA systems.
- It presents a combined analysis of ICSA visualization/interaction techniques, evaluation mechanisms, and levels of ICSA. This thorough analysis leads to the development of a reference framework for designing and evaluating ICSA systems. Additionally, the analysis suggests future research directions and highlights the industrial implications of ICSA systems.

Survey Structure: The rest of this survey is organized as follows. Section 2 presents the research methodology to conduct this survey study. Sections 3–5 report ICSA visualization/interaction techniques, evaluation mechanisms, and levels of ICSA, respectively. Section 6 proposes the developed framework based on the analysis of our research findings. This section also describes the potential future research directions and industrial implications for ICSA systems. Lastly, the conclusion of this survey is presented in Section 7.

2. Research Methodology

This section reports the research methodology used to conduct this survey study. We extract, analyze, and synthesize the existing state of the art on ICSA systems using the following five-step research methodology.

2.1. Research Questions

This survey aims to provide an overview of the existing state of the art on ICSA systems. We designed a set of three research questions (RQs) to review the existing literature on ICSA systems. Table 1 presents the research questions along with their motivations.

Table 1. Research questions of this survey.

Research Question	Motivation
RQ1:What are the visualization and interaction techniques used by ICSA systems?	To identify visualization techniques and interaction features used by immersive technologies for cyber situational awareness.
RQ2: What level of cyber situational awareness is facilitated by immersive technologies in ICSA systems?	To identify perception, comprehension, and projection of cyber situational awareness in ICSA systems.
RQ3: How are ICSA systems evaluated?	To identify evaluation techniques for validating ICSA systems.

2.2. Search Strategy

We devised a comprehensive search strategy for extracting as many relevant studies as possible from the Scopus search engine. The search strategy is composed of the following steps.

- *Search Method:* We first designed an inclusive search string containing the terms related to our research questions. Then, we ran the search string on Scopus to retrieve the maximum number of relevant studies on ICSA systems.
- *Search Terms:* Our search string included all the terms that are relevant to the research objectives (i.e., RQs) of this survey. Figure 1 shows the developed search string that is mainly composed of two parts: (i) the first part consisted of different "*immersive technologies*", and (ii) the second part contained the synonyms and relevant terms of "*cybersecurity*" and "*cyber situational awareness*". It is important to note that the terms were searched in the title, keywords, and abstract of the papers available at Scopus to identify and extract the relevant literature on ICSA systems.
- *Data Sources:* Similar to [21], we used the Scopus search engine only to identify the relevant literature on ICSA systems for this survey. This is mainly because of the observations reported in [22–25], which justify that Scopus indexes a large amount of peer-reviewed papers and journals indexed by many other digital databases such as IEEE Xplore, ACM Digital Library, Science Direct, SpringerLink, and Wiley Online Library.

```
TITLE-ABS-KEY (("Virtual reality" OR "Augmented reality" OR "Mixed reality " OR "Extended reality") AND (cybersecurity
OR cyber-security OR "network security" OR "computer security" OR (cyber AND ( securi* OR awareness OR educat* OR
picture OR learn* OR train* OR defense OR intelligen* OR attack OR threat OR visualization ))))
```

Figure 1. Search string for this survey with an asterisk (*) wildcard to capture word variants.

2.3. Inclusion and Exclusion Criteria

We devised inclusion and exclusion criteria to select the most relevant studies on ICSA systems for this survey. We included the peer-reviewed papers that can answer our defined research questions. Moreover, we included the study that is written in the English language only, irrespective of its publication date. All other types of literature, such as workshop articles, editorials, keynotes, tutorial summaries, panel discussions, books, and reviews,

are out of the scope of this survey. Table 2 presents the inclusion and exclusion criteria of this survey. The criterion was applied in the study selection process to retrieve the most pertinent papers, as described in the next phase.

Table 2. Inclusion and exclusion criteria for this survey.

Inclusion Criteria
I1: A study that is related to the use of immersive technologies for cybersecurity purposes
I2: A study is selected irrespective of its publication date
Exclusion Criteria
E1: A study that is written in a language other than English
E2: Books, workshop articles and non-peer-reviewed papers
E3: Full text is not accessible

2.4. Study Selection

We identified, selected, and extracted the existing state-of-the-art ICSA systems through a six-step process. The phases of the study selection process are briefly described as follows.

- *Automatic Search:* We ran our search string on the Scopus search engine to identify existing literature on ICSA systems. As a result, we retrieved 3536 potential studies.
- *Title-Based Selection:* We analyzed the title of the 3536 studies. If a paper title was relevant to the research questions of this survey, we included that paper. In case we were not sure about the relevance of a paper, that paper was transferred to the next phase. At the end of this phase, we had 327 papers.
- *Duplication Removal:* As we only consulted one database (i.e., Scopus) to retrieve the existing literature, no duplicate study was found during our study selection process.
- *Abstract-Based Selection:* We thoroughly read the abstracts and conclusions of the remaining 327 studies to check their relevance to our research questions. Here, we also applied the inclusion and exclusion criteria (Table 2) to the abstracts of papers. Consequently, this phase reduced the pool of papers from 327 to 139.
- *Full-Text-Based Selection:* We read the full text of 139 studies, and applied the inclusion and exclusion criteria on them. As a result, we obtained 36 relevant studies.
- *Snowballing:* We performed forward and backward snowballing [26] on the 36 studies to identify more literature on ICSA systems. This gave us 7 potentially relevant studies that were then passed through our inclusion and exclusion criteria. Consequently, we finalized 43 relevant studies for this survey.

2.5. Data Extraction and Synthesis

In this section, we report the data extraction and synthesis process of this survey. First, we extracted the data relevant to our research questions from the finalized 43 studies. Then, we analyzed and synthesized the extracted data to answer the research questions of this survey. The details of each process are as follows.

2.5.1. Data Extraction

We formulated a list of data items according to our research questions for extracting relevant details from the retrieved studies. Table 3 presents the data extraction form containing the list of data items prepared for this survey. The data items D1 to D8 present demographic details of the extracted literature. For example, title (D1), author(s) (D2), and publication type (D5) of papers represent the demographic data of the existing literature.

Similarly, the data items D9 to D12 correspond to our research questions. For example, the details of visualization techniques and interaction features were collected against data items D9 and D10, respectively, to answer RQ1. We papered a Microsoft Excel spreadsheet to save the extracted information against each data item for further analysis.

Table 3. Data extraction form of this survey.

ID	Data Item	Description	Research Questions
D1	Title	The title of the paper	Demographic data
D2	Author(s)	The author(s) of the paper	Demographic data
D3	Venue	The publication venue	Demographic data
D4	Year	The year of the publication	Demographic data
D5	Publication type	The type of publication (e.g., journal paper, conference paper)	Demographic data
D6	Area of focus	The focus of the paper in ICSA domain	Demographic data
D7	Target user(s)	The intended user(s) (e.g., security analyst)	Demographic data
D8	Software and hardware tools	The software/hardware tools used for ICSA systems	Demographic data
D9	Visualization techniques	The visualization techniques for ICSA systems	RQ1
D10	Interaction techniques	The interaction techniques for ICSA systems	RQ1
D11	Cyber situational awareness level	The level of cyber situational awareness achieved for ICSA systems	RQ2
D12	Evaluation mechanisms	The evaluation mechanisms used to validate ICSA systems	RQ3
D13	Future work	The reported future work	Discussion

2.5.2. Data Synthesis

We used descriptive statistics to analyze the demographic attributes (i.e., D1 to D8), while the other data items (i.e., D9 to D13) were analyzed by using thematic analysis [27]. The thematic analysis methodology identifies themes in the extracted data, interprets the themes, and draws conclusions. As per the thematic analysis guidelines reported by Braun and Clarke [27], we followed the five-step approach to perform thematic analysis on the data items D9 to D13.

- *Familiarizing with Data:* We obtained an initial understanding of the extracted visualization techniques (D9), interaction features (D10), levels of cyber situational awareness (D11), and evaluation mechanisms (D12) for ICSA systems.
- *Generating Initial Codes:* We developed a rudimentary list of similar visualization techniques, interaction features, cyber situational awareness levels, and evaluation mechanisms for ICSA systems. In some cases, we re-examined the retrieved studies to verify the developed list.
- *Searching for Themes:* We categorized the initial codes for each data item into potential themes. For example, visualization techniques based on icons are combined under the theme of "Iconic Displays".
- *Reviewing and Refining Themes:* We analyzed the identified themes against each other to detect similar and irrelevant themes. For example, spatial visualizations and geometric visualizations were merged with each other due to their same characteristics.
- *Defining and Naming Themes:* A clear and concise name was defined for each theme.

3. Visualization and Interaction Techniques

This section addresses *RQ1: What are the visualization and interaction techniques used by ICSA systems?* It examines the specific visualization techniques and interaction features employed by immersive technologies to enhance cyber situational awareness. Section 3.1 discusses the visualization techniques, while Section 3.2 outlines the interaction features used in ICSA systems.

3.1. Visualization Techniques for ICSA

Immersive technologies provide several unique features for complex and multidimensional cybersecurity data visualization to enhance the understanding of end-users. For example, these features include spatial immersion, situated analytics, embodied data exploration, collaboration, multisensory presentation, and engagement for complex data presentation and analysis [28]. This enhances the perception, comprehension, and projection of cyber situational awareness for end-users. To answer RQ1, we identified 11 distinguishable visualization techniques of immersive technologies from the existing literature used for creating cyber situational awareness. Table 4 presents the identified visualization techniques along with their corresponding literature. In the following, we report the details of each visualization technique for ICSA.

Table 4. Identified immersive visualization techniques and their sources.

Visualization Techniques	Papers
Geographical Displays	[11,12,29,30]
Metaphorical Displays	[31]
Node-Link Graphs	[29,32–35]
Scatterplots	[36]
Three-Dimensional Bar Charts	[37]
Volume	[11,14,15,20,29,31–33,38–45]
Icons/Symbols/Glyphs	[12,29,41,42,45–47]
Animation/Video Displays	[11,46,47]
360° Pictures	[45,48]
Two-Dimensional Displays	[14,15,29,32,33,38–40,47]
List/Table/Text Displays	[11,12,31,33,38–40,45–47]

Geographical Displays: ICSA systems use geographical displays to represent cybersecurity data for creating cyber situational awareness. Geographical displays refer to the visualizations that present cybersecurity data with their geographical locations (e.g., position coordinates of longitude and latitude). The spatial information helps end-users (e.g., cybersecurity experts, trainees, and analysts) to understand a cyber situation, which facilitates their decision-making and execution of action plans accordingly. For instance, an immersive 3D Network Visualizer application, developed by Beitzel et al. [29], displays networks' topology with their geographic coordinates. In each network topology, network nodes and edges are overlaid onto a real-world globe based on their geographical locations, as presented by Figure 2. It can also be seen that cybersecurity alerts/flags are placed on corresponding nodes and edges, which facilitates end-users in monitoring and detecting cybersecurity anomalies in large-scale networks.

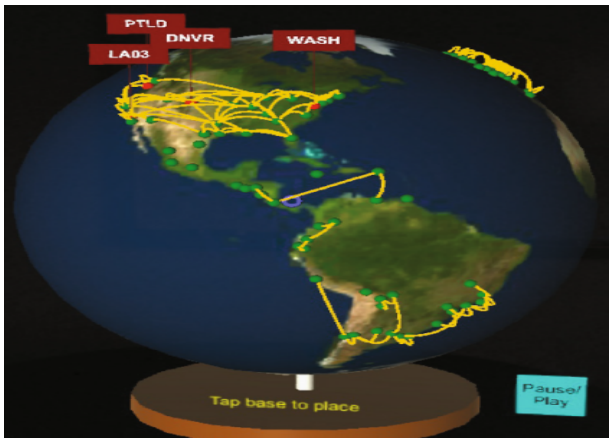

Figure 2. Geographical display [29].

Metaphorical Displays: Cybersecurity visualizations leverage metaphors to represent cyber situations in a comprehensible manner. Metaphorical displays provide clarity and context of cyber situations without any data occlusion. For example, Delcombel et al. [31] developed a helix structure to display arranged, organized, and systematized cybersecurity data. The 3D helical representation, presented by Figure 3, helps users in monitoring and detecting periodic signals of cyberattacks. A user is placed inside the helix, surrounded by cybersecurity data, to obtain insights into cyber situations with proper context and less obstruction.

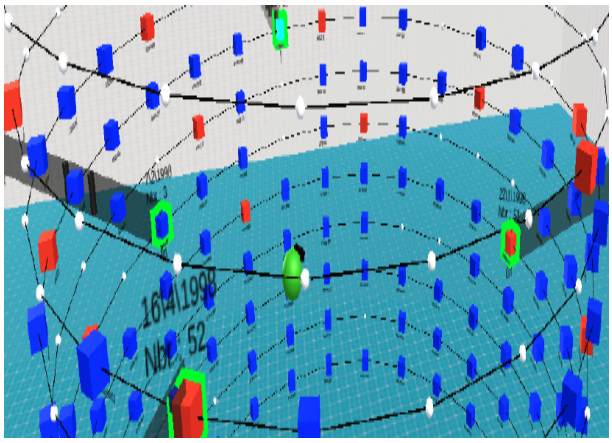

Figure 3. Metaphorical display [31].

Node-Link Graphs: Large-scaled network topologies are presented by node-link graphs to identify and understand how nodes (e.g., entities) are connected with each other. This provides an overview of network topologies, where nodes and their links are drawn as points and lines, respectively. For instance, the 3D Cyber COP prototype, developed by Kabil et al. [32], presents a holistic view of network topologies through node-link graphs for cybersecurity coordinators, which provides them with an understanding of network security state. Similarly, the 3D Network Visualizer application [29] contracts node-link graphs for showing network assets and their relationships with each other. Figure 4 shows the node-link graphs developed by the 3D Network Visualizer application for cyber situational awareness.

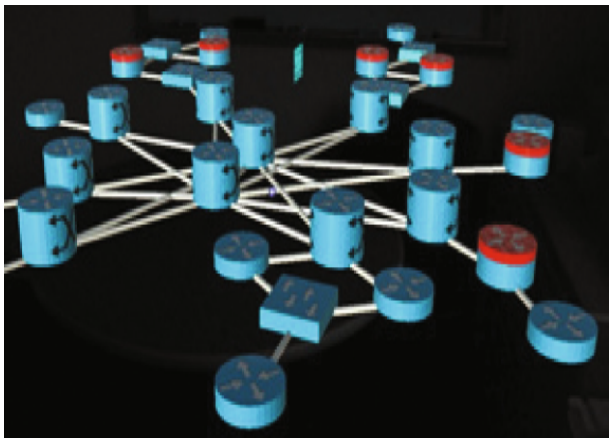

Figure 4. Node-linkgraph [29].

Scatterplots: Cybersecurity data need to be correlated with different cybersecurity parameters for a better understanding of cyber situations. For this purpose, immersive three-dimensional scatterplots are used to display relationships among cybersecurity data. Moreover, additional cybersecurity information can be visualized through different colors, shapes, and sizes of objects in scatterplots. An interesting example of immersive scatterplots is reported in [36], where different sets of network traffic data are displayed through scatterplots for different networks (Figure 5). The color, shape, and size of data objects present different cybersecurity parameters (e.g., anomalous and normal traffic data) for better perception and analysis of cyber situations.

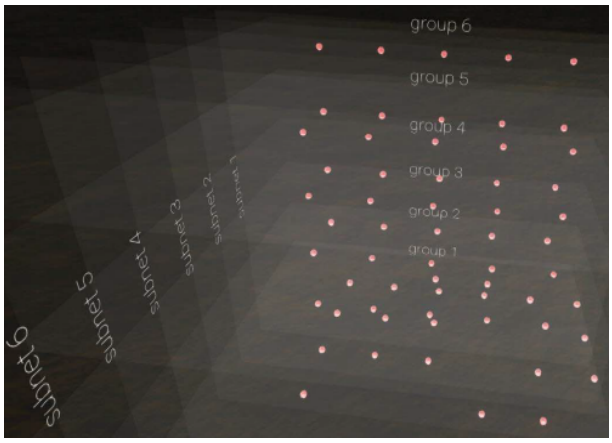

Figure 5. Scatterplot [36].

Three-Dimensional Bar Charts: Three-dimensional bar charts refer to the representation of information with rectangular bars of different widths, heights, and colors presenting the corresponding cybersecurity data in an immersive three-dimensional space. These charts are mostly used to perform a comparative analysis of multidimensional data in the cybersecurity realm. For instance, Beitzel et al. [37] developed a prototype application, called MINER, to perform a network anomaly analysis with 3D bar charts (Figure 6). The unique design of these 3D bar charts allows for a more intuitive and time-efficient identification of irregularities within network data. By presenting the information in this visually accessible manner, MINER enhances the cyber situational awareness of its end-users.

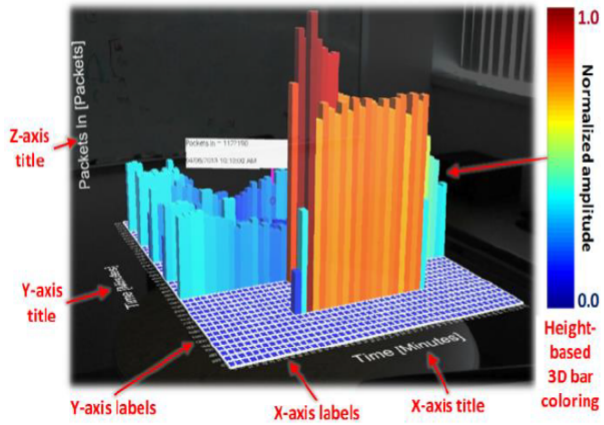

Figure 6. Three-dimensional bar chart [37].

Volume: Volume refers to the 3D object representations of cybersecurity data, encompassing assets, cyberattacks, and countermeasures, to aid end-users in understanding and managing cyber situations. For example, Figure 7 presents the cartoonish 3D models and virtual shields that are used to show cybersecurity threats and countermeasures, respectively, in an AR-based serious game reported in [42]. Similarly, 3D round-shaped objects (e.g., spheres) of red and green colors to indicate faulty and normal equipment, respectively, are used in debug UIs developed to detect anomalies in high-performance computing environments [11]. The literature reporting the use of *volume* in ICSA systems is presented in Table 4.

Figure 7. Volume rendering [42].

Icons/Symbols/Glyphs: ICSA systems use icons, symbols, or glyphs to represent cybersecurity data for better perception and comprehension by end-users. Our survey shows that this immersive visualization technique is extensively used in ICSA systems for cyber situational awareness (Table 4). For instance, an AR-based application, reported in [46], uses icons to indicate objects for navigating into the application, such as the *trash-bin icon* for delete and the *open icon* for open operation, as presented by Figure 8. Moreover, other different icons, such as email and trashcan icons, are used to open and delete an email. Similarly, the 3D Network Visualizer applications use icons to show a variety of network components, including switches, computers, and routers [29]. The use of icons, symbols, or glyphs increases the understanding and perception of cyber situations by end-users.

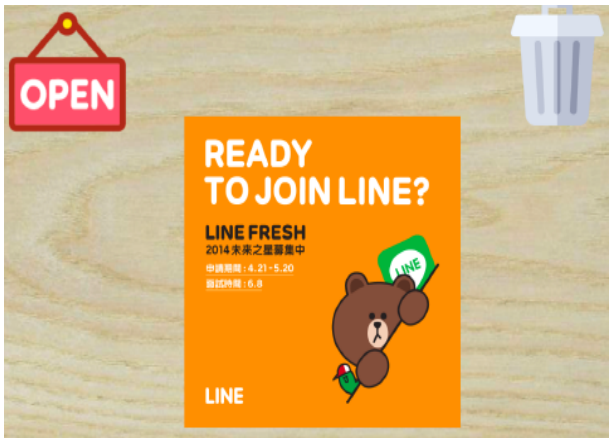

Figure 8. Icons [46].

Animation/Video Displays: ICSA systems use animations and videos to display cybersecurity information (e.g., impacts of cyberattacks, and countermeasures' implementation process) for enhancing cyber situational awareness of end-users. For example, Sukhija et al. [11] presented a concept of animation in their developed AR-based framework for fixing anomalies in large-scale infrastructures. For instance, animations include instructions to fix an anomaly to enhance cybersecurity. Similarly, the application on phishing education [49], developed by Chiou et al. [46], uses animations to demonstrate the impacts (e.g., the disappearance of applications, photos, or emails) of phishing attacks. This sort of information enables end-users to predict cyber situations caused by their actions.

360° Pictures: Immersive visualizations employ 360° pictures to disseminate cyber situational awareness to end-users. 360° pictures present an overall and comprehensive view of cyber situations, which enhances the cyber situational awareness of end-users. A potential use of 360° pictures is highlighted in [48], in which 360° pictures are used to detect cybersecurity vulnerabilities in a given system. The identification of cybersecurity vulnerabilities indicates the severity of a cyber situation [13]. It also leads to the identification of potential countermeasures for eradicating the detected vulnerabilities.

Two-Dimensional Displays: ICSA systems use two-dimensional displays for cybersecurity 2D data visualization in a 3D spatial space around end-users. For example, focusing on a single display of information, Korkiakoski et al. [15] developed an AR application that shows cybersecurity data (e.g., threats and severity levels) through a virtual 2D event information panel along with physical monitors that show operational information, as presented by Figure 9. Similarly, the node-link graphs, presented in [29], display network data (i.e., command terminal windows and Wireshark displays) through 2D displays in an immersive 3D space. Two-dimensional displays are usually integrated with 3D visualization techniques in ICSA systems to enhance the cyber situational awareness of end-users.

List/Table/Text Displays: ICSA systems need to display cybersecurity information through long-text, list, or tabular format. Therefore, immersive technologies employ lists, tables, or text summaries to represent cybersecurity information for enhancing the cyber situational awareness of end-users. For example, the VR system developed in [39] provides textual instructions for entering, navigating, and inspecting a virtual data center through a virtual tablet. Moreover, operational and security protocols are provided to end-users through the tablet for detecting and fixing an anomaly in the data center. Similarly, an AR-based cybersecurity awareness game [45] provides textual instructions to end-users regarding how to play the game (Figure 10); also, it gives an explanation behind each step taken by users in a textual format to raise their cybersecurity awareness.

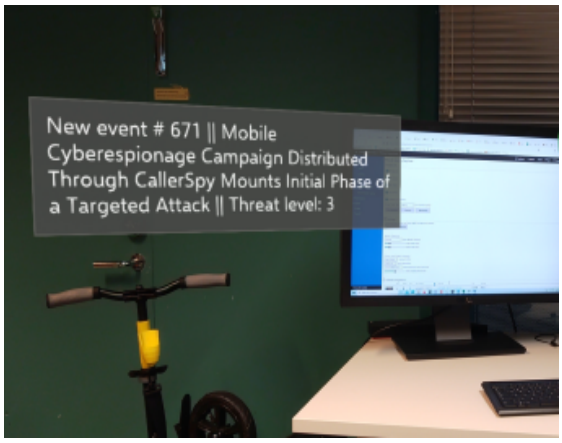

Figure 9. Two-dimensional display [15].

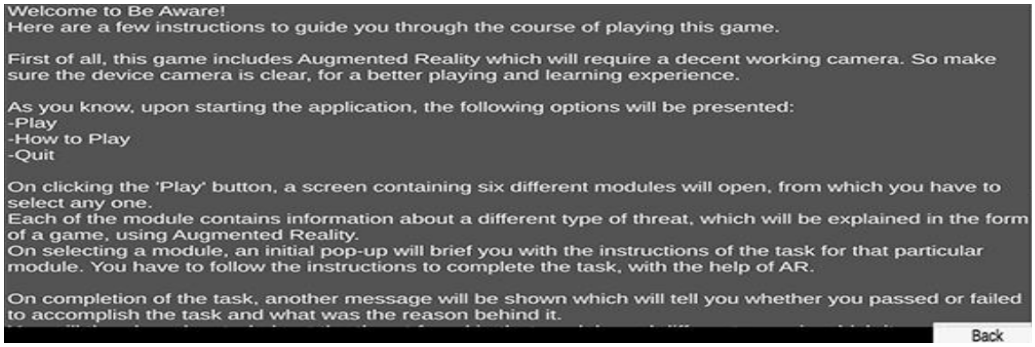

Figure 10. Text display [45].

Comparative Analysis of Visualization Techniques for ICSA: To address the depth of analysis, we critically compare the identified visualization techniques based on their effectiveness, limitations, and contextual relevance in ICSA systems. Geographical displays and node-link graphs are effective for representing distributed infrastructures and visualizing relationships within large-scale networks. They support spatial reasoning and structural understanding but can become visually dense in complex or highly dynamic environments. Metaphorical displays, such as 3D helices, provide intuitive and engaging representations for temporal or sequential data, enhancing pattern recognition. However, their abstract nature may require a learning curve and can limit immediate interpretability. Scatterplots and 3D bar charts support precise, multidimensional analysis and are well suited for anomaly detection and performance comparison. These methods, while analytically powerful, can become cognitively demanding as data volume increases. Icons, symbols, and glyphs are frequently used for intuitive labeling and quick recognition, especially in user-friendly or educational settings, though they may oversimplify nuanced data. Animations and video displays are highly effective for illustrating causal effects, user actions, and attack consequences, making them suitable for training and awareness. Yet, they often lack interactivity and analytical flexibility. Volumetric displays and 360° environments provide a strong sense of immersion and are useful in exploratory tasks or narrative-driven simulations but may offer limited value for real-time monitoring or detail-oriented analysis. Two-dimensional panels and textual displays, though less immersive, support detailed information delivery and are often used in conjunction with other techniques to provide explanations or procedural guidance. Overall, the optimal use of these techniques depends on the user's role (e.g., analyst and trainee), task complexity, and the desired balance between engagement, clarity, and analytical depth. Hybrid approaches that combine complementary visualization methods can offer more robust support for cyber situational awareness across varying operational contexts.

3.2. Interaction Techniques for ICSA

An interaction technique refers to an approach to interact with immersive visualizations for creating and maintaining cyber situational awareness for a given system. We have identified nine interaction techniques for ICSA systems through the existing literature. Table 5 presents the identified interaction techniques with their corresponding literature. In the following, we describe each interaction technique of ICSA systems for creating cyber situational awareness.

Table 5. Identified immersive interaction techniques and their sources.

Interaction Techniques	Papers
Select	[11,12,20,29–33,36–40,42,45–47,50–52]
Navigate	[11,20,29–33,38–40,46,47,50]
Details on Demand	[11,12,20,29–33,37–40,45–47,53,54]
Arrange/Change	[29–33,36,37,39,40,46]
Filter	[29,31,32]
Extract/Share	[32,50]
Aggregate/Relate	[31,32,36,37]
Annotate	[31,32]
Record	[33]

Select: Users engage with ICSA systems by selecting objects or options to carry out tasks such as organizing and interacting with cybersecurity data, thereby enhancing their cyber situational awareness. Immersive technologies provide several ways for the selection task in ICSA systems. This includes touch selection [12], gaze selection [37], point selection [20], gesture selection [29], controller selection [39], and custom marker selection [42]. These natural interactions make the selection task easier for end-users than the traditional mouse and keyboard selection, in which investigation of large-scale networks becomes cumbersome when users try to reach a specific node [50].

Navigate: Navigation refers to the interactions that help users move in ICSA systems to gain cybersecurity awareness. Most immersive technologies employ head tracking to enable their users to navigate ICSA systems with physical movements [20]. Head tracking provides a natural experience of moving around 3D virtual elements for obtaining a comprehensive perception and comprehension of cyber situational awareness [50]. Similarly, immersive technologies use selection techniques with virtual objects, allowing users to navigate ICSA systems. For example, users point and click on 3D arrows to navigate around a VR environment presented in [39]. Another navigation technique is zooming, which provides users with zoom-in and zoom-out capabilities for navigating ICSA environments.

Details on Demand: Users of ICSA systems need the necessary details of cybersecurity data for understanding, analyzing, and forecasting cyber situations. Therefore, immersive technologies offer *details on demand* capability in ICSA systems to display detailed information about cybersecurity data, when required by end-users. For instance, the 3D Network Visualizer application shows the detailed network traffic, through command terminal windows and Wireshark displays, on top of nodes in a node-link graph to diagnose a network cyber situation [29].

Arrange/Change: Organization of cybersecurity data provides insights of cyber situations to end-users. Therefore, ICSA systems enable users to arrange and change cybersecurity data, statistics, and views in a comprehensible manner so that they can perceive cyber situations with minimum cognitive load. This includes information highlighting, changing

attribute mapping, and changing representations (i.e., customization) of cybersecurity visualizations, which enhances users' cyber situational awareness. For example, users can change angles between radial data and helix of the helical visualization, proposed in [31], to visualize cybersecurity data with clarity.

Filters: Filters enable users to define inclusion and exclusion criteria within cybersecurity visualizations, allowing them to concentrate on the most relevant data and enhance their cyber situational awareness. For instance, the Network Feed application, proposed in [29], allows users to filter network traffic types (e.g., UDP, ICMP, and TCP) to obtain specific insights into cyber situations.

Extract/Share: ICSA systems allow users to extract and share cybersecurity reports, status, and visualizations with each other for creating collaborative environments to estimate cyber situational awareness. Moreover, the collaborative assessment of cyber situational awareness facilitates the identification, selection, and preparation of an optimal action plan for achieving desired cyber situations. For instance, the 3D Cyber COP prototype, developed by Kabil et al. [32], shares different cybersecurity data visualizations with operators according to their roles (e.g., analyst, coordinator, and client). It also provides cybersecurity report extraction capability to coordinators at any given instance to perform collaborative analysis for estimating cyber situations in real time.

Aggregate/Relate: ICSA systems enable users to aggregate cybersecurity data to make sense of what is going on in cyberspace. Recalling the example of the 3D Cyber COP prototype, cybersecurity experts combine raw data to create potential cyber incident scenarios [32]. This helps users predict possible cyber situations and prepare possible action plans accordingly.

Annotate: Annotation refers to the addition of graphical or textual information on cybersecurity visualizations for a better understanding of cyber situational awareness. The metaphorical display of cybersecurity information allows users to add additional information on a given space beyond the helix [31]. Similarly, the 3D Cyber COP application enables cybersecurity analysts to share their analysis with each other by adding visual cues on cyber assets [32]. In this way, all the stakeholders involved in cybersecurity operations can obtain the same picture of cyberspace, which facilitates the execution of cybersecurity operations in a collaborative manner.

Record: ICSA systems allow users to save their interaction logs and cybersecurity data trends for estimating the cyber situations of a given system. Historical data help users in detecting anomalies and predicting cyber situations. For example, the 3D Cyber COP application shows a system's parameter details (e.g., status, trend, and history) through a two-dimensional graph on a virtual 2D screen to help analysts in assessing cyber situational awareness [33].

Comparative Analysis of Interaction Techniques for ICSA: To strengthen the depth of analysis, we compare the identified interaction techniques in ICSA systems by evaluating their effectiveness, limitations, and application contexts. Selection techniques, such as gesture-, gaze-, touch-, and controller-based inputs, are foundational and vary in precision and ease of use. Gesture and gaze offer natural and immersive control, well suited for hands-free environments, but may lack accuracy in dense data scenes. Touch and controller-based methods provide higher precision, making them more suitable for tasks requiring detailed manipulation. Navigation through head tracking and point-and-click movement enhances spatial orientation and immersion, but may lead to fatigue or disorientation during prolonged use. Zoom-based navigation supports focus on specific elements but can interrupt global situational awareness if not smoothly integrated. Details-on-demand interactions enable users to access supplementary data when needed, supporting analysis without overwhelming the visual interface. However, excessive layering can increase visual

complexity. Arrange/change and filter techniques empower users to tailor data views, reduce cognitive load, and focus on relevant threats, especially beneficial in high-volume or mission-critical environments. Extract/share, aggregate/relate, and annotate promote collaboration and shared understanding across teams, though their effectiveness relies on intuitive design and role-based coordination. Lastly, recording supports retrospective analysis and anomaly detection, adding long-term value to situational awareness efforts.

In summary, each interaction technique presents trade-offs between intuitiveness, accuracy, effort, and collaboration. The most effective ICSA systems adopt a hybrid interaction design that aligns techniques with user roles (e.g., analysts, coordinators) and operational needs, thereby enhancing usability and the overall quality of cyber situational awareness.

4. Levels of Immersive Cyber Situational Awareness

This section answers *RQ2: What level of cyber situational awareness is facilitated by immersive technologies in ICSA systems?* Given the wide acceptance of Endsley's situational awareness model [8] in several domains (e.g., paramedicine [55], military realm [56], and cybersecurity [57]), we leveraged Endsley's situational awareness model for assessing cyber situational awareness in immersive environments. Accordingly, we have defined and identified the three levels (i.e., perception, comprehension, and projection) of situational awareness for ICSA through the existing literature. Table 6 presents the ICSA levels with their corresponding literature. In the following, we describe the definition and details for each ICSA level.

Table 6. Identified levels of ICSA from existing literature.

Levels of ICSA	Papers
Perception	[11,12,14,15,20,30–33,36,37,39–47,51,53,58–62]
Comprehension	[29,31–34,37,38,46,54,63–65]
Projection	[11,35,38,46]

4.1. Perception

Perception is the fundamental phase of SA, which enables users to answer the question *what is happening in cyber environments?* For immersive environments, perception refers to the monitoring, detection, and recognition of cybersecurity data (e.g., attack vectors, vulnerabilities, and countermeasures) that provide users with a holistic picture of cyber situations. Immersive visualization and interaction techniques help users create and maintain their perception of cyber situational awareness in ICSA systems. For instance, the immersive display, proposed in [15], shows an overview of ongoing cyber threats with their severity levels for COVID-19 information systems, which provides security experts with an overall perception of cyber situations. Similarly, the VR-based cybersecurity game, developed by Jin et al. [41], uses icons for cyberattacks and defenses to help users recognize cybersecurity elements, which enhances the perception of end-users for cyber situational awareness. Table 6 presents the reviewed studies that address the perception level of cyber situational awareness for ICSA systems.

4.2. Comprehension

Though the perception level of situational awareness provides a basic understanding of cyber situations, comprehension conveys extensive knowledge about cyberspace to end-users. The comprehension level of situational awareness enables users to answer the questions "*Why is it happening?*" and "*What is its meaning?*" ICSA systems enable users to explore, analyze, and investigate cyber situations through interactive visualizations. For

example, the 3D Cyber COP model allows non-experts to distinguish between malicious alerts and false positives through different visualization and interaction techniques [33]. Similarly, Beitzel et al. [37] presents interactive bar charts for comparative analysis to detect anomalies in network traffic. The comprehension level of ICSA covers data analysis tasks that include, but are not limited to, data clustering, anomaly detection, pattern analysis, visual search, comparative analysis, and data enrichment. Table 6 presents the literature that reports the use of immersive technologies to enhance cyber situational awareness.

4.3. Projection

Projection refers to the ability to anticipate future cyber states, helping users answer critical questions such as "*What will happen next?*" and "*What can I do?*" Immersive technologies offer promising avenues to support this level by reducing cognitive load and enabling more intuitive mental simulation of evolving threats. For example, the AR-based cybersecurity education application developed by Chiou et al. [46] visualizes the impact of phishing attacks through animations (e.g., disappearance of emails or applications) when incorrect decisions are made. Such feedback mechanisms help users internalize cause–effect relationships and anticipate the consequences of similar actions in real-world settings. However, compared with the perception and comprehension levels, the projection level remains underexplored in the literature. As summarized in Table 6, only a few studies have attempted to address this cognitive layer using immersive approaches. This gap largely stems from the inherent complexity of modeling predictive scenarios, the need for contextual reasoning, and the challenge of visualizing hypothetical outcomes in a manner that remains usable and comprehensible. Additionally, most existing systems lack integration with real-time threat intelligence or dynamic simulation capabilities, which are essential for forward-looking decision support. Addressing this limitation requires future ICSA systems to incorporate mechanisms such as predictive overlays, temporal data visualizations, or simulation-driven digital twins, which could enhance the system's ability to support proactive cybersecurity planning and threat mitigation.

5. Evaluation Mechanisms for ICSA Systems

This section answers *RQ3: How are ICSA systems evaluated?* From the reviewed studies, we identified that researchers have employed various user-experience research methods to assess ICSA systems. These methods include questionnaires, surveys, situational awareness evaluation techniques, and usability evaluation mechanisms.

User-oriented studies have provided comprehensive insights into several key aspects. They report on users' demographics, including factors such as gender and ethnicity, which help in understanding the diversity of participants involved in the studies. Performance metrics such as threat response time and task completion time are also analyzed, offering quantitative measures of user efficiency and effectiveness when interacting with ICSA systems. Additionally, cognition parameters such as distraction levels and memory retention are evaluated, providing valuable data on the cognitive impact of using immersive technologies for cyber situational awareness.

The findings from these studies consistently indicate that ICSA systems significantly enhance users' performance and cognitive capabilities. By improving threat detection and response times and reducing cognitive load, ICSA systems enable users to manage cybersecurity tasks more effectively. Table 7 provides a detailed summary of the evaluation mechanisms employed in the existing literature. While we reference all the evaluation mechanisms used, due to space constraints, we have not included every individual study. However, the evaluation methods mentioned are representative of those commonly cited across multiple studies. The table includes the demographics of the users involved, the

specific performance and cognition metrics assessed, and the overall results. Consistent findings across studies confirm that immersive technologies improve user performance and cognition.

Table 7. Evaluation mechanisms for ICSA systems.

Paper	Evaluation Mechanism	Users' Demographics	Performance Metrics	Cognition Metrics	Results
Mattina et al. [12]	Questionnaire		User time-on-task; User fact recall		Users' performance is improved
Korkiakoski et al. [15]	SART Questionnaire; Analysis of variance with *p*-value Test	6 participants; 3 males and 3 females	No. of completed tasks		Understanding of situational awareness depends on gender
Alqahtani et al. [38]	Questionnaire with five-point Likert scale	91 participants; 59% male and 41% female; Age between 18 and 65			AR-based game increases cyber situational awareness
Beitzel et al. [14]	Capture the flag exercise; Post-task survey; NASA TLX Assessment	7 participants; 7 male; Age is between 34 and 60; Ethnicity: Caucasian	Total elapsed time; Average response time; Countermeasure failure rate; Success EOIs; Failed EOIs	Mental demand; Physical demand; Temporal demand; Frustration	AR improves both performance and cognition of users
Seo et al. [39]	Questionnaire	25 participants		Memory test	Interactive immersion in VR is beneficial for long-term memorization of cyber situational awareness
Chu et al. [40]	Questionnaire; Interview	6 participants with no cybersecurity knowledge		Memory test	Cyber situational awareness training through VR is more engaging than video training.
Jin et al. [41]	Questionnaire with 5-point Likert scale; Analysis of variance with *p*-value Test	181 participants; 123 male and 58 female			Immersive game-based learning for cyber situational awareness is more effective for males than females
Kabil et al. [33]	SUS usability questionnaire; Analysis of variance with *p*-value Test; Cybersickness questionnaire	30 participants with no cybersecurity knowledge		Physiological disorder	Users had good performance with no discomfort
Salazar et al. [42]	Questionnaire with 5-point Likert scale	208 participants; Age between 14 and 19	Knowledge acquisition; Vulnerability detection; Defense preparation	Confidence in technology	AR-based games improve both performance and cognition
Rana et al. [48]	Post-task quiz and survey with statistical analysis (t-test)	100 participants with cybersecurity knowledge			VR cybersecurity training is more effective than video-based methods
Delcombel et al. [31]	SUS usability questionnaire	8 participants; 3 male and 5 female; Age: 23 to 30	Task completion time; Task accuracy		Users' task performance is enhanced in immersive environments
Kaleem et al. [47]	Pre- and post-task survey with 5-point Likert scale and statistical analysis	20 participants			AR has a positive impact on cybersecurity learning
Kasurinen et al. [44]	Pre- and post-task survey		task completion time; No. of unforced errors		VR learning environments is beneficial for understanding cyber situational awareness
Puttawong et al. [20]	Pre- and post-task survey	Participants have cybersecurity knowledge			VR environments are productive for cybersecurity education
Kommera et al. [61]	Pre- and post-task survey; Satisfaction survey				AR provides insights in cybersecurity forensic education

A comparative synthesis of evaluation mechanisms used across ICSA systems reveals significant variation in methodology, metrics, and study scope (Table 7). The majority of studies employed questionnaire-based assessments, including Likert scales, usability instruments such as the SUS, and cognitive load measures like NASA-TLX and SART. These were often supplemented by objective performance metrics, such as task completion time, accuracy, response rates, and fact recall. A smaller subset incorporated statistical validation techniques, including ANOVA and t-tests, to establish the significance of observed differences. Consistent across studies is the finding that immersive technologies, particularly AR and VR, enhance user engagement, comprehension, and task performance. For instance, Beitzel et al. [14] and Salazar et al. [42] demonstrated improved cognitive processing and decision-making efficiency through AR-based interfaces. Similarly, enhanced memory retention and long-term learning outcomes were observed in immersive training environments (e.g., Seo et al. [39], Rana et al. [48]). However, the influence of user demographics, such as prior experience or gender, was evident in certain studies (e.g., Jin et al. [41], Chu et al. [40]), suggesting that personalization and adaptive interaction may be necessary for broader effectiveness.

Despite generally positive outcomes, current evaluations often lack methodological consistency and longitudinal scope. Few studies perform comparative analysis across multiple interaction or visualization techniques, and collaborative functionalities, critical in operational cybersecurity settings, are rarely assessed empirically. These observations underscore the need for more standardized, multidimensional evaluation frameworks that incorporate cognitive, performance, and usability metrics across diverse user groups and usage contexts in future ICSA research.

6. Discussion

This section reports an analysis of our research findings described in Sections 3–5. We develop a reference framework by mapping the ICSA visualization and interaction techniques with different levels of ICSA (perception, comprehension, and projection). This framework aids researchers and practitioners in designing and evaluating ICSA systems using immersive technologies for cyber situational awareness. Furthermore, based on our research findings, we suggest future research directions to further advance the field of ICSA systems.

6.1. A Reference Framework for Designing and Analyzing ICSA Systems

Unlike the traditional cyber situational awareness frameworks [57], there exists no framework for the designing elements (i.e., interaction and visualization techniques) of ICSA systems to create perception, comprehension, and projection of cyber situational awareness. This gap in the literature and practice presents significant challenges for developers and practitioners working on ICSA systems, as they lack a standardized guide to create systems that effectively enhance the perception, comprehension, and projection of cyber situational awareness. The absence of such a framework leads to several specific issues. Developers, when faced with a multitude of available features and options, often find it difficult to identify the most suitable visualization and interaction techniques for their specific objectives, such as improving user comprehension. This difficulty can result in inefficiencies and increased costs during both the design and operational phases of ICSA systems. Without a clear framework, the process of trial and error becomes more prevalent, which can delay development timelines and inflate budgets. Also, the lack of a structured approach can lead to inconsistencies in system performance and user experience, undermining the efficacy of ICSA systems in real-world applications. For instance, a developer aiming to design an ICSA system with a primary focus on enhancing user perception might

struggle to select the appropriate visualization techniques that provide clear and immediate insights into cyber threats. Similarly, interaction techniques that facilitate quick and intuitive user responses might be overlooked or misapplied. These challenges are exacerbated when considering the need to balance multiple design elements simultaneously, such as ensuring that the system is both comprehensive and comprehensible.

To address these significant challenges, we have undertaken the task of mapping visualization and interaction techniques (detailed in Section 3) to the different levels of ICSA (outlined in Section 4). This mapping process has culminated in the development of a reference framework that categorizes existing interaction and visualization techniques according to the three critical levels of ICSA: perception, comprehension, and projection. Figure 11 illustrates this framework, demonstrating the immersive visualization and interaction techniques applicable at each level of ICSA. For instance, basic visualization techniques such as *volume* and interaction features like *select* are essential components at the perception level of cyber situational awareness. These techniques are utilized within our framework to enhance the perception level of ICSA, providing users with clear and immediate insights into cyber threats. Our reference framework is designed to aid developers and practitioners in identifying the most suitable visualization and interaction techniques when designing and operating ICSA systems for specific purposes, whether it be for perception, comprehension, or projection. By offering a structured approach, this framework ensures that the selection and implementation of these techniques are efficient and effective, ultimately enhancing the overall design and functionality of ICSA systems. Moreover, the framework plays a crucial role in facilitating anomaly detection and mitigation processes within ICSA systems. Categorizing immersive techniques based on their applicability to different levels of situational awareness enables the creation of more robust systems that can promptly identify and respond to anomalies. This capability is particularly important in the dynamic field of cybersecurity, where timely and accurate situational awareness is critical to preventing and addressing cyber threats.

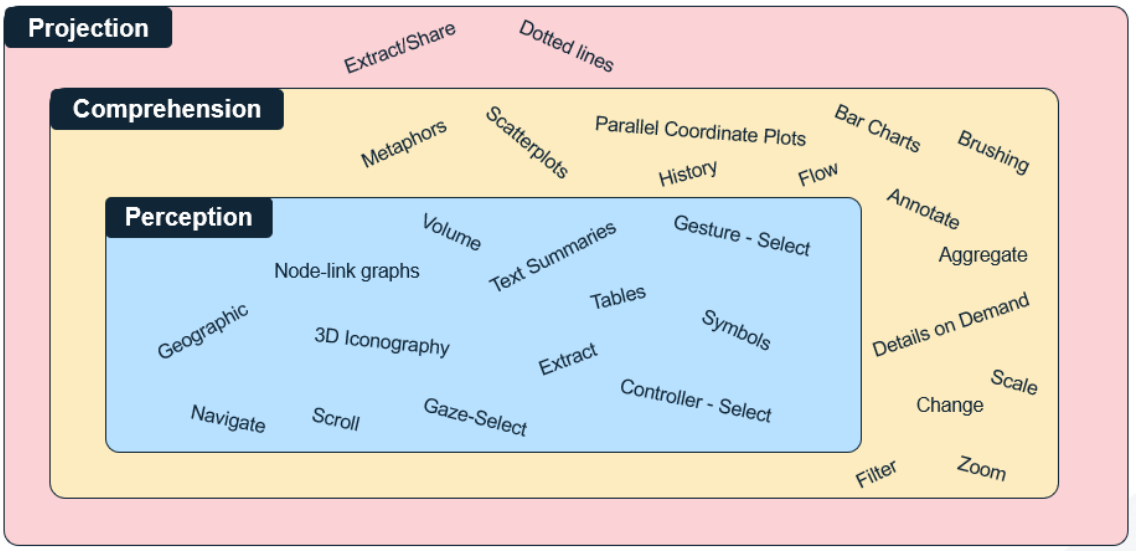

Figure 11. Reference framework for designing and analyzing ICSA systems.

To strengthen the practical relevance of the proposed framework, we have mapped specific techniques to the three levels of situational awareness using concrete examples from the surveyed literature. For instance, the 3D Cyber COP system [32] uses gesture and controller-based selection to support perception-level tasks, such as monitoring network assets and responding to alerts. In the CyberCopter system [31], features like spatial annotation and object arrangement help users explore helical data structures, making it

easier to understand complex temporal patterns, supporting the comprehension level. At the projection level, the immersive capture-the-flag scenario by Beitzel et al. [14] includes extract and share functionalities, allowing users to collaboratively forecast potential threats and coordinate responses. These examples validate the framework's structure and show how various immersive techniques are applied in real-world ICSA systems to address different cognitive goals across the situational awareness spectrum.

6.2. Future Research Areas

Through the analysis of our research findings, we have identified potential future research directions for researchers aimed at improving the existing state of ICSA systems.

Projection of ICSA. The projection phase is a critical component of ICSA, enabling users to anticipate future cyber events and formulate appropriate response strategies. However, as highlighted in our proposed framework (Figure 11), there is a notable gap in the use of immersive visualization and interaction techniques specifically tailored for this phase. Most existing solutions focus heavily on perception and comprehension, while projection remains underexplored. We encourage researchers and system designers to address this gap by developing immersive methods that support forecasting and predictive analysis within virtual environments. Enhancing the projection phase will provide users with a more holistic situational understanding, improving their ability to proactively respond to emerging cyber threats.

Integrating Advanced Immersive Visualization and Interaction Techniques. Immersive technologies provide a powerful array of visualization and interaction methods that remain largely untapped in the context of ICSA. Integrating advanced techniques such as flow visualizations, Kohonen maps, 3D heatmaps, import interactions, and spatial navigation (drive interactions) can significantly enrich users' understanding of cybersecurity data.

Flow visualizations [66] are particularly useful for mapping data movement across networks, allowing users to detect abnormal patterns and suspicious activity. Kohonen map representations [67], also known as self-organizing maps, provide a means of visualizing high-dimensional data in a two-dimensional space, which can be instrumental in identifying clusters and anomalies in large datasets. Heatmap visualizations [68] employ a three-dimensional approach to represent data, where color gradients indicate data intensity and the height of the map reflects the magnitude of specific metrics. This method offers an intuitive understanding of data variations and hotspots. Import interactions [69] involve the ability to seamlessly bring external data into the immersive environment, enhancing the user's capacity to analyze and correlate diverse data sources. Drive interactions [70] refer to the techniques that enable users to navigate through the virtual space effectively, providing them with a more immersive and interactive experience.

The incorporation of these advanced visualization and interaction techniques into the ICSA domain can significantly enhance the capability of developers and practitioners to design and operate ICSA systems. By leveraging these techniques, users can gain deeper insights into cyber threats and network activities, enabling more effective monitoring, analysis, and response. Furthermore, we strongly advocate for the continuous development and integration of new visualization and interaction techniques tailored specifically for cyber situational awareness in immersive environments. This ongoing innovation is essential to keep pace with the evolving nature of cyber threats and to ensure that ICSA systems remain robust, intuitive, and effective.

Large-Scale User Study: As discussed in Section 5, many ICSA systems are evaluated through user studies involving a relatively small number of participants. While these studies provide useful early-stage insights, they limit the broader applicability of findings. For example, systems tested with only a few users may not reflect the needs of large-scale

infrastructures that involve multiple roles, varied operational contexts, and diverse user profiles. Feedback from a small group can overlook usability challenges and functional gaps that only emerge in more complex or realistic environments. This restricts the generalizability and scalability of current ICSA systems. To overcome these limitations, we advocate for large-scale user studies during the design and evaluation of ICSA systems. Such studies should involve a wider range of participants, ideally representative of the actual end-user base, including individuals with different expertise levels, demographic backgrounds, and operational settings. Larger studies offer several advantages. They increase the validity of findings, provide broader and more diverse feedback, and help identify issues that are not visible in controlled or limited testing. They also enhance generalizability, making it possible to apply findings across different organizational and infrastructure scales. Incorporating large-scale evaluations can lead to more robust, user-adaptable ICSA systems that are well suited to real-world deployment. By capturing richer insights, these studies support better design decisions and improve the reliability, usability, and effectiveness of immersive cybersecurity solutions.

6.3. Industrial Implications of ICSA Systems

Our study highlights the growing potential of immersive technologies in the cybersecurity industry, following their success in domains such as gaming, education, healthcare, and entertainment. Technologies like virtual reality and augmented reality are now being applied to cybersecurity awareness and technical training. These immersive systems create engaging, hands-on learning environments that improve the skills and preparedness of cybersecurity professionals by simulating realistic threat scenarios. Beyond training, immersive technologies enhance how security teams visualize and interpret complex cybersecurity data. This includes network traffic patterns, alerts, threat indicators, and infrastructure topologies. By presenting data in an intuitive and spatial manner, ICSA systems help reduce cognitive load and improve decision-making. They also support real-time collaboration within Security Operations Centers and Network Operations Centers, enabling teams to coordinate responses more effectively during incidents.

ICSA systems can further assist in troubleshooting and operational monitoring. Their interactive interfaces allow analysts to explore data collaboratively and identify issues more efficiently. However, despite these advantages, the use of immersive technologies introduces new challenges, particularly in terms of security and privacy. Immersive platforms often capture sensitive data, such as user behavior, gaze patterns, and biometric identifiers. If not properly secured, these data may be vulnerable to misuse or attack [71]. It is therefore essential to implement strong safeguards. These include encryption of data in transit and at rest, multifactor authentication, endpoint protection, and well-defined privacy policies. Ensuring secure configurations of immersive environments is also critical to reducing the attack surface.

A compelling real-world example that reflects the foundational objectives of ICSA systems is SCOUT [72], a Critical Infrastructure Protection framework that delivers intelligent cyber situational awareness for industrial systems. Although SCOUT does not employ immersive interfaces, it exemplifies how integrated cyber-physical monitoring, real-time threat detection, and coordinated response capabilities can support critical environments. The architectural principles of SCOUT, particularly its fusion of security and operational data, mirror the core goals of ICSA. Integrating such systems with immersive technologies could further enhance operator situational awareness by enabling interactive exploration of attack paths, anomalies, and system states within 3D virtual environments.

In summary, immersive technologies offer significant value to cybersecurity operations. When paired with robust security and privacy measures, ICSA systems can enhance train-

ing, improve threat comprehension, and enable faster, more informed incident response, while minimizing associated risks.

6.4. Limitations

This survey provides a structured synthesis of ICSA systems; however, several methodological and practical limitations should be acknowledged.

First, the literature search was limited to the Scopus database. While Scopus is a widely recognized and comprehensive indexing source, this constraint may have excluded relevant studies indexed in other databases such as IEEE Xplore, ACM Digital Library, or Web of Science. Future reviews could benefit from a multidatabase search strategy to ensure broader coverage and minimize selection bias. Second, this study excluded workshop papers, white papers, and other non-peer-reviewed sources. Although this choice supports academic rigor, it may have omitted valuable early-stage insights and innovations, particularly from industry and interdisciplinary research, where immersive technologies often emerge. Third, the 43 selected studies were included based on topical relevance without a formal quality assessment. Treating all studies equally may limit the ability to weigh the reliability or strength of individual findings.

Beyond these methodological constraints, several broader issues emerged from the reviewed literature. Many user studies were based on small participant samples, often fewer than 30 individuals, limiting the generalizability and statistical robustness of reported outcomes, particularly those concerning usability, cognition, and engagement. This limitation warrants stronger emphasis in future analyses, especially when interpreting system effectiveness. In terms of scope, while this survey focuses on XR modalities such as AR and VR, it does not explicitly account for immersive environments like digital twins or CAVE systems, which are increasingly relevant in simulation-based cybersecurity applications. Their exclusion reflects limited coverage in the current body of ICSA literature but represents a promising direction for future research. Lastly, practical usability challenges, such as motion sickness, interface fatigue, and cognitive overload, are rarely discussed in the reviewed studies, despite their critical impact on the long-term viability and user experience of immersive systems. These human factors must be more thoroughly addressed to ensure that ICSA systems are not only effective but also accessible, comfortable, and operationally sustainable.

By acknowledging these limitations, we aim to improve transparency and support future research efforts that seek to expand methodological rigor, practical relevance, and inclusivity in the design and evaluation of immersive cyber situational awareness systems.

7. Conclusions

Immersive technologies are increasingly used to create cyber situational awareness through interactive visualizations for cybersecurity analysis, education, and training. Therefore, we have collected, investigated, and synthesized the body of knowledge on ICSA systems. In this survey, we have described 11 visualization techniques, nine interaction features, three levels of cyber situational awareness, and evaluation mechanisms for ICSA systems. Moreover, we have critically analyzed the research findings, which enables us to (i) propose a reference framework for designing and analyzing ICSA systems by mapping immersive visualization and interaction techniques to the different levels of ICSA; (ii) propose future research directions for advancing the state-of-the-art of ICSA systems; and (iii) highlight the industrial implications of ICSA systems.

This survey facilitates researchers and practitioners of ICSA systems in many ways. For researchers, we have identified several future research areas for advancing the state of the art on ICSA systems. For example, the projection phase of ICSA needs innovative

visualization and interaction techniques that help users in forecasting imminent cyber situations. Similarly, our survey highlights the need for large-scale user studies for providing tested and validated ICSA systems to end-users. For practitioners, this survey presents a framework that categorizes immersive visualization and interaction techniques according to the levels of ICSA. This facilitates practitioners in selecting suitable visualization and interaction techniques for designing and operating ICSA systems for specific purposes (e.g., perception). We hope this survey will provide researchers and practitioners with innovative ways and inspirations to use immersive technologies for cyber situational awareness.

Author Contributions: All authors contributed to the preparation of this paper. Conceptualization, H.A. and F.U.; methodology, H.A. and F.U.; validation, H.A., F.U. and R.J.; writing—original draft preparation, H.A.; writing—review and editing, F.U. and R.J.; supervision, F.U. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: Rehan Jafri was employed by Honeywell company. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Williams, C.M.; Chaturvedi, R.; Chakravarthy, K. Cybersecurity risks in a pandemic. *J. Med. Internet Res.* **2020**, *22*, e23692. [CrossRef] [PubMed]
2. Arogbodo, M. Impacts of the COVID-19 Pandemic on Online Security Behavior Within the UK Educational Industry. 2022. Available online: https://osf.io/preprints/psyarxiv/h5qgk_v1 (accessed on 12 July 2024)
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. [CrossRef]
4. Kuzior, A.; Tiutiunyk, I.; Zielińska, A.; Kelemen, R. Cybersecurity and cybercrime: Current trends and threats. *J. Int. Stud.* **2024**, *17*, 220. [CrossRef]
5. 2024 Data Breach Investigations Report. 2024. Available online: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf (accessed on 3 May 2025).
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. [CrossRef]
8. Endsley, M.R. Design and evaluation for situation awareness enhancement. *Proc. Hum. Factors Soc. Annu. Meet.* **1988**, *32*, 97–101. [CrossRef]
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. [CrossRef]
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. [CrossRef]
18. Abu Deeb, F. Enhancing Cybersecurity with Extended Reality: A Systematic Review. *J. Comput. Inf. Syst.* **2024**, 1–15. . [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
38. Alqahtani, H.; Kavakli-Thorne, M. Design and evaluation of an augmented reality game for cybersecurity awareness (cybar). *Information* **2020**, *11*, 121. [CrossRef]

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

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. [CrossRef]
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. [CrossRef]
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. [CrossRef] [PubMed]
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. [CrossRef]