**Evolving Critical Infrastructure Cybersecurity Situational Awareness with Extended Reality and Spatial Computing**

Faced with ever-increasing data volumes, Security Operations Centers (SOCs) seek new solutions to make sense of the raw data and achieve a higher degree situational understanding. Finding these solutions is of paramount importance among critical infrastructures such as electric utilities, where combinatorial threats such as weather, vegetation management, and cyber actors create vast sums of information across disparate domains. This data deluge presents a singular challenge for these utilities, but also an unprecedented opportunity to fuse data and human intuition into a holistic understanding of the threats to the nation’s critical infrastructure in real time. Extended reality (augmented reality and virtual reality) and spatial computing (human interaction with a machine in which the machine manipulates references to real objects and spaces) is a new technology frontier that enables users to process and retain data 3-10 times faster than traditional methods, e.g., 2D data on a monitor [1,2]. **The successful mitigation of the risks associated with compromised grid equipment is predicated on the successful integration of extended reality and spatial computing into the workflow of security operations centers.**

The challenges of the 21st century demand that the security personnel of America’s critical infrastructure be able to fully grasp the true risk exposure of any activity, focusing on the alerts and workflows that are most important for rapid response and restoration of service. For example, Dr. Josiah Dykstra, a team technical director at the National Security Agency’s Laboratory for Telecommunication Sciences who leads the development a prototype of an augmented-reality system, stated that “cybersecurity workers in an operations center have a high cognitive workload, where information comes at them very fast and changes quickly. Our idea is, how can we help them manage this stress and help them with the mental demands of their work?”[3] By cross-sharing data between traditional Grid Operations and Security Operations, and then overlaying those data with geophysical and geo-tagged cyber asset information, the horizon of situational awareness for operators of both network domains expands and enables them to make better decisions faster.

An extended reality application that could assist in vulnerability impact modeling would be a game changing tool for the contextualizing risks and responding to incidents. Such risks include both IT and OT assets (as well as the dependencies on each), fault scenario identification, task processing, and prioritization queuing. Employees could immerse themselves in an extended-reality device to be transported to geophysical representations of the North American Bulk Electric System (BES). This representation can be inhabited by a group of analysts, themselves geographically disparate, working within the shared consensual visualization. Real-time information such as satellite imagery of vegetation on key interconnects could be represented alongside weather forecast data and the current state of critical IT and OT assets in the same path as that storm. Such a visualization would empower SOC and BES analysts, who typically monitor several applications within their own silos at once, to join together in a virtual representation of their shared reality to conquer the biggest threats.

The collaborative nature of extended reality can also mitigate the substantial cybersecurity skills gap, an estimated shortage of 359,236 infosec professionals in the workforce [4]. Talent, in whatever geography it can be found, can be brought together virtually. This feature removes the need to relocate highly skilled operators permanently or temporarily and, as a bonus, minimizes risks from future pandemics. While other teleconferencing and videoconferencing tools exist, only extended reality offers “presence”, where users feel as though they are actually together and experiencing activities, not just passively watching.

The promise of extended reality and spatial computing is clear, but to realize its potential, substantial investments must be enacted as soon as possible. The following features are most critical:

* Expanding options for the input of new data sources. Compatibility with a number of different data sources such as JavaScript Object Notation (JSON) is a logical next step, along with operations that allow the reading a remote file or data source, such API integration.
* Expanding the methods for the user to interact with the current and expanded data sources and to perform actions in real time on the data. Visualizations will incorporate these changes, and then dynamically reconfigure the graph to present the changes to the operator in real-time.
* Programmatic representation of the visualization based on algorithms or user feedback, through utilization metrics and preferences as saved by the user, to generate the most helpful data views, i.e. utilizing machine learning to highlight for users unusual clusterings and relevant, but possibly obfuscated, relationships
* Contextual styling for nodes and edges to allow additional options for data visualization (i.e., Skeuomorphic representations).
* Expanding the options for users to interact with the data representations, including node and edge-to-graph translation. This capability will allow the exposure of data contained within an individual node or edge for interaction graphically as opposed to text.

VR Ulysses website: <https://www.vrulysses.com/>

References

1. Bowman, D. & McMahan, R.P. (2007) “Virtual Reality: How much Immersion is Enough?” *IEEE Computer Society.* Vol. 40 Issue 7.

2. Hamilton, D. et al. (2021) Immersive virtual reality as a pedagogical tool in education: a systematic literature review of quantitative learning outcomes and experimental design. *J. Comput. Educ*. 8, 1-32.

3. <https://fedtechmagazine.com/article/2016/03/future-augmented-reality-and-cybersecurity>

4. (ISC)2 Global Workforce Study, 2020