

Why should we use 3D Collaborative Virtual Environments for Cyber Security?

Alexandre Kabil, Thierry Duval, Nora Cuppens, Gérard Le Comte, Yoran Halgand, Christophe Ponchel

▶ **To cite this version:**

Alexandre Kabil, Thierry Duval, Nora Cuppens, Gérard Le Comte, Yoran Halgand, et al.. Why should we use 3D Collaborative Virtual Environments for Cyber Security?. 3DCVE 2018 : IEEE Fourth VR International Workshop on Collaborative Virtual Environments, Mar 2018, Reutlingen, Germany. 10.1109/3DCVE.2018.8637109 . hal-01770064

HAL Id: hal-01770064
https://hal.science/hal-01770064

Submitted on 18 Apr 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Why should we use 3D Collaborative Virtual Environments for Cyber Security?

Alexandre Kabil*
IMT Atlantique
Lab-STICC, UMR CNRS 6285

Thierry Duval†
IMT Atlantique
Lab-STICC, UMR CNRS 6285

Nora Cuppens‡
IMT Atlantique
Lab-STICC, UMR CNRS 6285

Gérard Le Comte§
Société Générale

Yoran Halgand¶
EDF

Christophe Ponchel‖
Airbus Defence and Space

ABSTRACT

Cyber Security data analysis is an important growing domain: more and more data visualization systems are offered to operators in order to improve their threat detection performances or facilitate suspect behaviors characterization. As today Cyber Security trend is to regroup employees in structures such as Security Operations Center (SOC) or Computer Emergency Response Team (CERT), collaborative approach seems to be relevant in this context. We think that 3D Collaborative Virtual Environments (3DCVE) can be used in order to improve users Cyber Situational Awareness, as they can allow them to have a better understanding of a cyber situation by mediating interactions towards them and also by providing different points of view of the same data, on different scales.

Index Terms: Human-centered computing—Human computer interaction (HCI)—Interaction paradigms—Collaborative interaction; Human-centered computing—Visualization—Visualization application domains—Visual analytics

1 CYBER DATA ANALYSIS AND VISUALIZATION

Cyber data analysis is a complex task due to the different dimensions of data that need to be analyzed and to the fact that cyber attacks are the combination of several layers of information (e.g. a scam email that executes a specific binary code into a pdf file in order to encrypt data). As more and more data are generated and collected on networks, analysts face a 'Needle in a Haystack' problem when they want to detect attacks and visualization tools helps them to detect discrepancies and to investigate [14]. Far from pop culture stereotypes, cyber operators use classical Command Line Interfaces (CLI) and Graphical User Interfaces (GUI) to detect incidents and cyber threats whereas other domains look at Natural User Interfaces (NUI) or even Immersive Analytics to improve users' analytics capabilities.

Thus, Cyber Security Visualizations face a paradox: they need to be simple enough in order to help analysts to understand what is going on on the network and they need to be precise enough to help them investigating incidents. That is why it exists specialized Cyber Security visualizations, such as Network Security [12], event visualization [10] or anomaly detection [13] tools.

Visual Analytics techniques help analysts to find anomalous behaviors, correlations or repetitive patterns [1]. A drawback of Visual Analytics solutions for Cyber Security is that they are very specific: they help cyber analysts to find one piece of evidence but when they want to get a 'Big picture', they need to use aggregating tools such as Security Information and Event Management (SIEM) systems. These systems are the backbone of Security Operations Centers (SOCs) but on the opposite of Visual Analytics solutions, they are neither interactive nor collaborative, and they need additional big data technologies such as the ELK Stack[1] (Elasticsearch, LogStash and Kibana tools) to help analysts to dig into data.

We think that we need to think beyond 2D canvases and aggregated dashboards: 3D collaborative data visualizations can help solving these problems by either separate views towards different analysts but letting them having a common ground, or proposing aggregated 3D interactive data representations that can give more information. 3D data visualizations can be effective if designed around users' point of view.

2 3D DATA VISUALIZATIONS

The question of whether using 2D or 3D visualizations for Information Visualization was already debated, for example during the 2014 IEEE 3DVis Workshop entitled "Does 3D really make sense for Data Visualization?", but even if there is now evidence that 3D representations are useful in some cases highlighted by Pirker and Gütl [11] or in the specific case of Volume data analysis by Laha et al. [9], we have not seen much 3D visualizations for Cyber Security, apart from the 2012 Daedalus-viz project developed by Inoue et al. [8] which is a still used darknet monitoring solution. We do agree with Cliquet et al. recent publication [4] on the fact that some arguments against 3D visualizations in the 2D versus 3D debate, which is twenty years old now, are not relevant anymore as technologies and usages have evolved:

- Head-tracking, which is now available on any HMDs, brings a real difference compared to static point of view, as it lets users naturally move around 3D elements, and gives them proper perspective and depth information. Its implementation can limit a lot data occlusion issues (which was a main argument against 3D Visualization), and can bring more insights on volumetric or spatial data.

- As we can now easily track users movements, natural interaction can offer a richer interaction vocabulary that can improve selection or navigation tasks. For example these tasks were complicated to do with a mouse and a keyboard when you had users trying to reach a specific node in a huge graph.

- Letting users waving hands to each other, pointing things with fingers or head-nodding in Virtual Environment was called 'Social VR' and this mutual awareness makes a lot of sense

*e-mail: alexandre.kabil@imt-atlantique.fr
†e-mail: thierry.duval@imt-atlantique.fr
‡e-mail: nora.cuppens@imt-atlantique.fr
§e-mail: Gerard.Le-Comte@socgen.com
¶e-mail: yoran.halgand@edf.fr
‖e-mail: christophe.ponchel@airbus.com

[1] https://www.elastic.co/webinars/introduction-elk-stack

while doing collective tasks; by knowing others gaze and interactions, you can improve their coordination and collaboration by letting them exchanging contextual information.

We are not saying that we should replace every existing 2D dashboard by a 3D interactive visualization: 2D charts are still powerful enough to compare statistical distributions or to show trends, but some actual solutions can combine both, as Virtualitics[2], which put users in a 3D environments where both 3D and 2D data representations are used. Immersive Analytics perspective goes in our direction by defending the fact that it is now possible to develop collaborative immersive data analysis solutions, as proposed by Chandler et al. and Hackathorn and Margolis [3, 7].

We are convinced that we should now re-think previous interactions and metaphors that were only theoretical due to a lack of computer graphical power or practical applications.

3 3D METAPHORS FOR CYBER SECURITY

Virtual Reality is not a recent research field, and some ideas and proposals that we consider currently innovations (VR Head-Mounted Displays for example) were developed years ago but technical limitations prevented them to be used by a large number of people. The CyberNet project for instance, developed by Gros et al. in the 2000 [6] was an ambitious one that aimed at providing different 3D metaphors for network management, such as the city metaphor: data are represented as buildings within a city, with different heights, numbers of windows and so on. The CyberNet project was abandoned but a brand new Cyber Security company, ProtectWise, uses also the City metaphor[3]. This example allows us to highlight the fact that besides science-fiction representations as Tron or Matrix, computer power allows us to implement ideas that were just theoretical until now.

Again, we are not saying that practices as network monitoring will change completely. We are just pointing that recent technologies allow us to rethink interaction and data visualization, as the Multiscale network Mixed-Reality visualization from Beitzel et al. [2] who propose to use a Microsoft HoloLens to analyse several layers of Network data. Collaborative approaches can take advantage of metaphoric representations as each user can have her/his proper way of interacting and visualizing data according to her/his practices and so far we have not seen any 3DCVE using these kinds of metaphors.

This is why we are currently working on an immersive collaborative system for Cyber Security called 3D CyberCOP (COP stands for Common Operational Picture): we propose a 3DCVE that can be fitted for collaborative Cyber Security investigation and reporting practices.

4 CONCLUSION

"Ways change, Stil. You have changed them yourself." Franck Herbert's Dune.

Cyber Security domain relies heavily on data analysis in order to face a growing number of cyber attacks that exploit now employees mistakes more than security flaws to compromise systems. Struggling against cyber threats is a more and more demanding task but we show that practices are still not harnessing yet the capabilities of 3D Collaborative Virtual Environments and Virtual Reality technologies.

We think that this is due partly to the fact that analysts are not aware of the recent changes in 3D Data Visualization brought by new Virtual Reality devices. Moreover, these devices coupled with years of experience of 3D CVE scientists can now put previous theories into action, as we show with 3D virtual Cities for data analysis. We explained how these devices can change the way we interact with data, and we have highlighted why we think that 3D CVE could be used for raising users Cyber Situational Awareness (CSA) [5]. Finding ways of representing data in a fancy 3D visualization is not enough and we should give users the possibility to collaborate within the same Virtual Environment to interact naturally with data and to train on realistic Cyber situations.

[2]https://www.virtualitics.com/

[3]https://www.inc.com/kevin-j-ryan/protectwise-futuristic-cybersecurity-startup.html

ACKNOWLEDGMENTS

This work was supported by the Cyber CNI Chair of Institute Mines Télécom, which is held by IMT Atlantique and supported by Airbus Defence and Space, Amossys, EDF, Orange, La Poste, Nokia, Société Générale and the Regional Council of Brittany. It has been acknowledged by the Center of excellence in Cyber Security.

REFERENCES

[1] M. Angelini, N. Prigent, and G. Santucci. Percival: proactive and reactive attack and response assessment for cyber incidents using visual analytics. In *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*, pp. 1–8, Oct 2015. doi: 10.1109/VIZSEC.2015.7312764

[2] S. Beitzel, J. Dykstra, P. Toliver, and J. Youzwak. Exploring 3d cybersecurity visualization with the microsoft hololens. In *International Conference on Applied Human Factors and Ergonomics*, pp. 197–207. Springer, 2017.

[3] T. Chandler, M. Cordeil, T. Czauderna, T. Dwyer, J. Glowacki, C. Goncu, M. Klapperstueck, K. Klein, K. Marriott, F. Schreiber, et al. Immersive analytics. In *Big Data Visual Analytics (BDVA), 2015*, pp. 1–8. IEEE, 2015.

[4] G. Cliquet, M. Perreira, F. Picarougne, Y. Prié, and T. Vigier. Towards hmd-based immersive analytics. In *Immersive analytics Workshop, IEEE VIS 2017*. Phoenix, United States, Oct. 2017.

[5] U. Franke and J. Brynielsson. Cyber situational awareness–a systematic review of the literature. *Computers & Security*, 46:18–31, 2014.

[6] P. Gros, P. Abel, R. Dos Santos, D. Loisel, N. Trichaud, and J. Paris. Experimenting service-oriented 3d metaphors for managing networks using virtual reality. In *Laval Virtual–Virtual Reality International Conference*, May 2000.

[7] R. Hackathorn and T. Margolis. Immersive analytics: Building virtual data worlds for collaborative decision support. In *2016 Workshop on Immersive Analytics (IA)*, pp. 44–47, March 2016. doi: 10.1109/IMMERSIVE.2016.7932382

[8] D. Inoue, M. Eto, K. Suzuki, M. Suzuki, and K. Nakao. Daedalus-viz: Novel real-time 3d visualization for darknet monitoring-based alert system. In *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, VizSec '12, pp. 72–79. ACM, New York, NY, USA, 2012. doi: 10.1145/2379690.2379700

[9] B. Laha, K. Sensharma, J. D. Schiffbauer, and D. A. Bowman. Effects of immersion on visual analysis of volume data. *IEEE Transactions on Visualization and Computer Graphics*, 18(4):597–606, April 2012. doi: 10.1109/TVCG.2012.42

[10] G. Markowsky and L. Markowsky. Visualizing cybersecurity events. In *Proceedings of the International Conference on Security and Management (SAM)*, p. 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2013.

[11] J. Pirker and C. Gütl. Virtual worlds for 3d visualizations. In *11th international conference on intelligent environments (Workshop)*, pp. 265–272, 2015.

[12] H. Shiravi, A. Shiravi, and A. A. Ghorbani. A survey of visualization systems for network security. *IEEE Transactions on visualization and computer graphics*, 18(8):1313–1329, 2012.

[13] T. Zhang, X. Wang, Z. Li, F. Guo, Y. Ma, and W. Chen. A survey of network anomaly visualization. *Science China Information Sciences*, 60(12):121101, 2017.

[14] C. Zhong, J. Yen, P. Liu, R. F. Erbacher, C. Garneau, and B. Chen. *Studying Analysts' Data Triage Operations in Cyber Defense Situational Analysis*, chap. 2, pp. 128–169. Springer International Publishing, Cham, 2017. doi: 10.1007/978-3-319-61152-5_6