CyberCOP3D : Visualisation Collaborative et Immersive pour la cybersécurité

Alexandre Kabil

CyberCOP3D : Visualisation Collaborative et Immersive pour la cybersécurité

CyberCOP3D : Immersive Collaborative Visualization for Cyber Sécurity

Alexandre KABIL
IMT Atlantique
Technopôle Brest-Iroise CS 83818
29238, Plouzané, France
alexandre.kabil@imt-atlantique.fr

ABSTRACT

La visualisation de données en cybersécurité fait appel aux techniques de *Visual Analytics*. Ces techniques permettent entre autres de favoriser la *Situation Awareness*, via une *Common Operational Picture*. L'objectif de la thèse est de proposer un CyberCOP3D, à savoir un outil collaboratif immersif favorisant la *Cyber Situation Awareness*. Afin de nous appuyer sur un cadre réel, nous effectuerons une analyse de l'activité collaborative au sein de SOCs (*Security Operations Center*) et via un design centré utilisateur nous proposerons des profils de personas permettant de modéliser les besoins et pratiques des différents analystes.

CCS CONCEPTS

• **Human-centered computing** → **Visualization techniques**; *Virtual reality*; *Collaborative interaction*; • **Security and privacy** → *Network security*;

KEYWORDS

cyber security, collaborative visualization, common operational picture, human-computer interaction

RÉSUMÉ

Data Visualization in cybersecurity uses Visual Analytics techniques in order to enhance user's Situation Awareness through Common Operational Pictures. We propose in this paper a CyberCOP3D- an Immersive Collaborative COP- that will facilitate Cyber Situation Awareness. We will develop a model based on a collaborative activity analysis and a user-centered-design strategy, in order to define user's personas, according through needs and usages.

IHM '17 , August 28–September 1, 2017, Poitiers, France

MOTS-CLEFS

cybersécurité, visualisation collaborative, common operational picture interaction homme-machine

1 INTRODUCTION

La visualisation pour la cybersécurité est un domaine très vaste de par l'hétérogénéité des données à visualiser. De nombreuses solutions de visualisation se basent sur les principes du domaine de la *Visual Analytics* (VA), qui facilitent la prise de décision des cyberanalystes, via l'acquisition d'une *Cyber Situation Awareness* (CSA) [3, 4].

La CSA s'obtient via une visualisation et une compréhension d'une *Operational Picture* (OP), voire d'une *Common Operational Picture* (COP), qui sert entre autres de support à la prise de décision.

L'objectif de cette thèse est donc de proposer un CyberCOP3D, à savoir un outil collaboratif immersif favorisant la SA de cyberanalystes en leur proposant différentes interfaces contextuelles en fonction des données et des pratiques.

Afin de disposer d'un cas d'utilisation réel, nous allons effectuer une analyse de l'activité collaborative au sein d'un ou de plusieurs *Security Operations Centers* (SOCs) appartenant à des partenaires industriels de la cahire qui finance la thèse. Cette analyse de l'activité sera couplée à la définition de *personas* qui, via un design centré utilisateur, faciliteront l'élaboration de prototypes.

Dans une première partie, nous traiterons des besoins en visualisation pour la cybersécurité ainsi que de l'acquisition d'une *Cyber-Situation Awareness*. Nous expliciterons ensuite les objectifs de la thèse et les études que nous souhaitons mener dans les SOCs. Enfin, nous concluerons sur les perspectives attendues et les travaux en cours.

2 VISUALISATIONS POUR LA CYBERSÉCURITÉ

Il existe de nombreuses catégories de visualisations pour la cyber sécurité, qui peuvent selon Humphries *et al.* se découper en trois axes : le monitoring, l'analyse et le reporting [18]. Plusieurs revues de littérature les recensent, en considérant soit la sécurité des réseaux [12, 35], soit la visualisation d'évènements [26] ou la détection d'anomalies [47]. Plusieurs articles de positionnement de la communauté *Security Visualization* (*SecViz*) ont même vu le jour afin de proposer des axes de recherche et de cibler les challenges.

Par exemple, Best, Endert & Kidwell ont proposé plusieurs points sur lesquels la SecViz doit se pencher, à savoir la grande quantité de données hétérogènes à traiter (trames et paquets réseau, historiques de connexion de routeurs, requêtes effectuées par des utilisateurs ou des bots, données souvent agrégées dans des *Security Information and Event Management system* ou SIEMs, qui traitent environ cinquante mille évènements de sécurité par seconde), la rapidité de transmission de l'information et donc de propagation des menaces et l'équilibre entre le temps passer à traiter un incident par rapport à son impact sur le système [5]. Gates & Engle soulignent quant à eux que l'esthétisme des interfaces pour la cybersécurité ne doit pas prendre le pas sur leur efficacité, et que cette efficacité doit pouvoir être évaluée [15]. La question de l'utilisation de la 3D est posée aussi bien en cybersécurité pour la détection d'anomalies [8] ou le monitoring du darknet [19] que dans d'autres domaines de la visualisation comme l'analyse de données spatialisées [10]. Les visualisations pour la cybersécurité s'appuient souvent sur des techniques d'*Information Visualization* (InfoVis) [16] ou de VA, comme *Percival* [1], afin de faciliter le travail des analystes et favoriser l'acquisition d'une *Cyber Situation Awareness* (CSA).

2.1 Visual Analytics

La VA consiste en l'utilisation couplée des compétences cognitives et visuelles d'un humain et d'une Intelligence Artificielle prétraitant les données afin de faciliter leur interprétation [39, 45]. Le recentrage des activités de la VA sur l'utilisateur [11] ainsi que le développement des technologies de réalité virtuelle ont permis entre autres l'émergence d'un nouveau champ d'application : l'*Immersive Analytics* [9, 17]. Bien que l'utilisation de la 3D et d'environnements immersifs en VA complexifie le développement d'applications par le manque de librairies graphiques adaptées [29] et par le besoin plus important en ressources informatiques [32], elle permet néanmoins de faciliter l'analyse de clusters [44], l'analyse de données volumétriques [22] ou la comparaison de jeux de données [6] en augmentant le nombre de dimensions affichées [14], en adaptant la vue au point de vue de l'utilisateur et en lui fournissant des métaphores de visualisation et d'interaction plus réalistes [32]. L'*Immersive Analytics* tout comme la VA permettent de favoriser la SA (*Situation Awareness*) des utilisateurs en leur proposant des vues facilitant la prise de décision et la compréhension de situations. Ces vues peuvent être contextualisées afin d'adapter le contenu aux besoins des analystes. Ainsi, nous pouvons présenter une vue globale aux utilisateurs sur une interface collaborative tout en leur proposant de s'immerger dans les données via des vues spécifiques s'ils souhaitent pousser leurs analyses.

2.2 Cyber Situation Awareness

La Cyber-SA est une adaptation aux domaines de la cybersécurité ou de la cyberdéfense militaire [2, 28] de modèles de SA existants. De nombreux articles de classification des modèles de CSA ont émergé, comme des revues de littérature [13], des articles de positionnement [30, 40] ou des articles se focalisant sur l'aspect cognitif [21] ou sur l'usabilité des modèles pour des centres de cybersécurité [31]. La CSA est décrite à chaque fois comme un processus holistique visant à regrouper et corréler différentes informations [42], à la fois interne à l'analyste (elle concerne ses raisonnements cognitifs) et externe (via l'utilisation d'algorithmes de fusion de données). Acquérir une SA ou CSA passe souvent par l'utilisation d'une *Operational Picture*, comme dans le modèle de prise de décision OODA (voir figure 1). Cette COP (aussi appelée *situational picture*) sert de support à la prise de décision et facilite la compréhension de la situation [24] à différents niveaux.

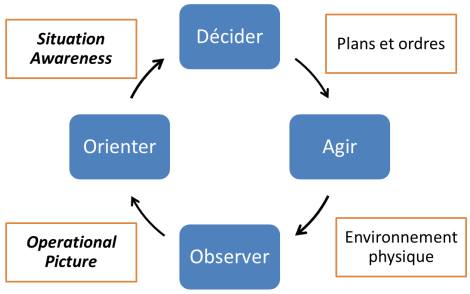

Figure 1: Cycle de prise de décision "Observ, Orient, Decide, Act", inspiré de [28].

Cette dernière peut aussi servir de support à une collaboration entre plusieurs humains, par le biais d'une *Shared Situational Awareness* [43, 46]. C'est sur cette acquisition collective de la SA que se concentre la thèse décrite ici.

3 CONCEPTION D'UN CYBER COP 3D

L'objectif de cette thèse est donc de proposer un **CyberCOP3D**, à savoir un outil collaboratif immersif favorisant la SA de cyberanalystes en leur proposant différentes interfaces contextuelles en fonctions des données et des pratiques. En proposant des vues hybrides 2D/3D, nous souhaitons ainsi améliorer certaines pratiques sans pour autant tout remplacer.

3.1 Étude collaborative

Afin de disposer d'un cas d'utilisation réel, nous allons effectuer une analyse de l'activité collaborative [41] au sein de plusieurs SOCs (Security Operations Center) appartenant aux partenaires de la chaire Cyber CNI (cybersécurité des infrastructure nationales critiques) qui finance la thèse. Cette analyse permettra de dégager un modèle des pratiques collaboratives et servira de socle au prototypage de CyberCOP3D. Nous allons de plus nous baser sur un design centré utilisateur par le biais de la technique des *personas* afin d'analyser les besoins des différents acteurs du SOC et de leur fournir des profils d'utilisation adaptés [27].

3.1.1 Collaboration au sein d'un SOC. De ce que nous avons pu constater lors de visites préliminaires au sein de deux SOCs et d'après les recommandations de la MITRE [1] (institution américaine en charge de la cybersécurité), un SOC est un lieu dédié à la surveillance permanente d'un système informatique. Il est composé de trois niveaux d'analystes ayant des tâches différentes allant de la réponse immédiate à des incidents (niveaux 1 et 2) à l'investigation détaillée d'une attaque ou d'une vulnérabilité (niveaux 2 et 3), et de

1. https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-\cybersecurity-operations-center

responsables qui sont chargés de la communication d'informations avec les clients concernés par les incidents. Tous les personnels d'un SOC sont dans le même espace de travail où des écrans de contrôle sont présents afin de favoriser la coordination.

Nous souhaitons analyser les pratiques collaboratives dans les SOCs afin de déterminer quels sont les interactions entre les différents acteurs que nous pourrons modéliser et implémenter dans le CyberCOP 3D. Pour cela, une immersion de plusieurs jours avec les personnels nous permettra de récupérer des données quant à la coordination et la collaboration effective dans le SOC.

3.1.2 Pratiques au sein d'un SOC. Les analystes d'un SOC utilisent bon nombre d'outils de traitement de données en fonction des tâches qu'ils doivent effectuer. Leurs rôles étant prédéfinis par la structure même du SOC (analyste de niveau 1, 2 ou 3), la technique des *personas*, qui permet via un archétypage de mieux cibler les besoins et attentes de différents acteurs, nous parait pertinente quant à la caractérisation des pratiques individuelles dans un SOC. Cette technique a déja été utilisée en cybersécurité [27, 38] et a permis un prototypage de visualisations contextualisées, en fonction des différents rôles.

Nous proposerons aux personnels des SOCs des *personas* avec lesquelles ils pourront s'identifier. Ces *personas* nous permettront de définir des contextes d'utilisation et d'adapter les différentes vues du CyberCOP 3D.

3.2 Architecture du CyberCOP 3D

Nous allons développer une application multi-utilisateur fonctionnant à la fois sur support non-immersif (ordinateur de bureau classique), sur support immersif (casque de réalité virtuelle) et sur support tactile (table, tablette ou smartphone) (voir figure 2). Nous allons adapter l'interaction et la visualisation sur les différents dispositifs en fonction des rôles et contextes d'utilisation. Par exemple, un analyste pourra interagir avec un écran de monitoring sur son ordinateur tout en coopérant avec un autre analyste immergé dans les données. Ainsi, nous souhaitons non pas changer totalement les pratiques existantes, mais améliorer la CSA en fournissant des visualisations 2D ou 3D adaptées aux besoins. Nous pensons que cette méthode améliorera l'acceptabilité de notre solution par les utilisateurs car nous ne bouleverserons pas leurs pratiques : nous proposons une application additionnelle pouvant être utilisée ponctuellement, lors d'incidents nécessitant une coordination maximale par exemple. Les premiers retours auprès des personnels des SOC montrent qu'ils sont plutôt ouverts à de nouvelles propositions de solutions de visualisations pour la Cyber sécurité, et qu'ils sont curieux de pouvoir expérimenter des visualisations 3D et immersives.

4 CONCLUSION ET PERSPECTIVES

Nous souhaitons concevoir un CyberCOP 3D, un système collaboratif immersif pour les cyberanalystes. Nous allons étudier les pratiques collaboratives et individuelles au sein de SOCs de partenaires industriels pour disposer d'un cadre d'utilisation réel, pour définir des *personas* permettant de comprendre et de modéliser l'activité collaborative au sein d'un SOC. Ainsi, si nous pouvons définir des *personas* d'analystes de niveau 1, 2 ou 3 ou de décisionnaires, et si nous formalisons les actions permettant de traiter un incident de cybersécurité, nous aurons un scénario d'utilisation disponible.

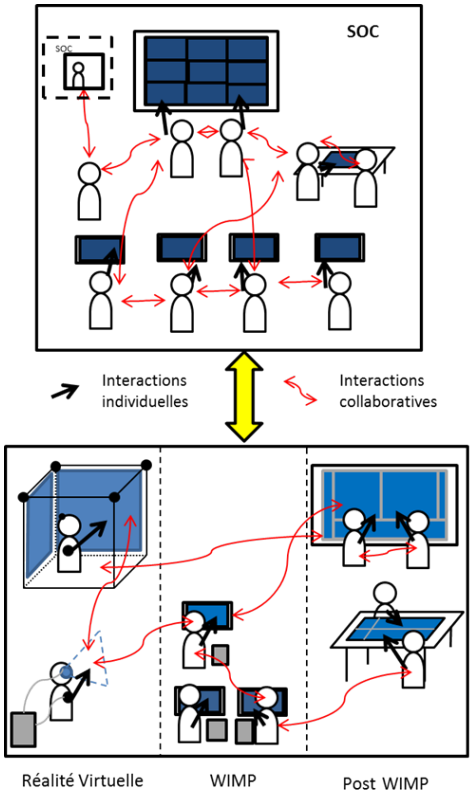

Figure 2: Schématisation du CyberCOP3D en bas, qui sera une transposition dans des environnements virtuels collaboratifs de l'activité au sein d'un SOC, en haut. L'interaction entre utilisateurs sera asymétrique et collaborative, favorisant ainsi la coopération et l'hybridation 2D/3D.

Le développement des prototypes se fera en parallèle des visites des SOCs. Afin de choisir l'architecture réseau la plus adaptée, nous effectuerons un état de l'art sur les applications immersives collaboratives. Nous utiliserons des données fournies par les partenaires de la thèse ou provenant de challenges de visualisation comme le challenge VAST afin de tester les prototypes au cours du développement. L'évaluation de solutions de visualisation pour la cybersécurité est encore aujourd'hui une question ouverte [37], et nous nous pencherons donc sur les travaux existants en évaluation de la SA [7, 25], de l'analyse de métriques de la VA [20, 23, 34] ou de l'activité collaborative [33, 36].

REMERCIEMENTS

Nous remercions EDF et la Société Générale, qui sont les partenaires industriels de la Chaire CyberCNI qui s'impliquent dans le suivi de cette thèse. La Chaire Cyber CNI de l'Institut Mines Télécom est portée par IMT Atlantique. Elle est soutenue par Airbus Defence and Space, Amossys, BNP Paribas, EDF, Nokia, Orange, La Poste et la Région Bretagne. Elle est reconnue dans le cadre du Pôle d'Excellence Cyber.

RÉFÉRENCES

[1] Marco Angelini, Nicolas Prigent, and Giuseppe Santucci. 2015. Percival : proactive and reactive attack and response assessment for cyber incidents using visual analytics. In *Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on*. IEEE, 1–8.

[2] Paul Barford, Marc Dacier, Thomas G Dietterich, Matt Fredrikson, Jon Giffin, Sushil Jajodia, Somesh Jha, Jason Li, Peng Liu, Peng Ning, and others. 2010. Cyber SA : Situational awareness for cyber defense. In *Cyber Situational Awareness*. Springer, 3–13.

[3] Tim Bass. 1999. Multisensor data fusion for next generation distributed intrusion detection systems. (1999).

[4] Tim Bass. 2000. Intrusion detection systems and multisensor data fusion. *Commun. ACM* 43, 4 (2000), 99–105.

[5] Daniel M Best, Alex Endert, and Daniel Kidwell. 2014. 7 key challenges for visualization in cyber network defense. In *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*. ACM, 33–40.

[6] Richard Brath. 2014. 3D InfoVis is here to stay : Deal with it. In *3DVis (3DVis), 2014 IEEE VIS International Workshop on*. IEEE, 25–31.

[7] Joel Brynielsson, Ulrik Franke, and Stefan Varga. 2016. Cyber Situational Awareness Testing. In *Combatting Cybercrime and Cyberterrorism*. Springer, 209–233.

[8] Besnik Camaj and Etienne Petremand. 2015. Detecting networks anomalies and attacks using 3D visualization. (2015).

[9] Tom Chandler, Maxime Cordeil, Tobias Czauderna, Tim Dwyer, Jaroslaw Glowacki, Cagatay Goncu, Matthias Klapperstueck, Karsten Klein, Kim Marriott, Falk Schreiber, and others. 2015. Immersive analytics. In *Big Data Visual Analytics (BDVA), 2015*. IEEE, 1–8.

[10] Steve Dübel, Martin Röhlig, Heidrun Schumann, and Matthias Trapp. 2014. 2D and 3D presentation of spatial data : a systematic review. In *3DVis (3DVis), 2014 IEEE VIS International Workshop on*. IEEE, 11–18.

[11] Alex Endert, M Shahriar Hossain, Naren Ramakrishnan, Chris North, Patrick Fiaux, and Christopher Andrews. 2014. The human is the loop : new directions for visual analytics. *Journal of intelligent information systems* 43, 3 (2014), 411–435.

[12] Keith Fligg and Genevieve Max. 2012. Network security visualization. *IEEE Network Special Issue on Recent Developments in Network Intrusion Detection* (2012).

[13] Ulrik Franke and Joel Brynielsson. 2014. Cyber situational awareness–a systematic review of the literature. *Computers & Security* 46 (2014), 18–31.

[14] Rubén Jesús García-Hernández, Christoph Anthes, Markus Wiedemann, and Dieter Kranzlmüller. 2016. Perspectives for using virtual reality to extend visual data mining in information visualization. In *Aerospace Conference, 2016 IEEE*. IEEE, 1–11.

[15] Carrie Gates and Sophie Engle. 2013. Reflecting on visualization for cyber security. In *Intelligence and Security Informatics (ISI), 2013 IEEE International Conference on*. IEEE, 275–277.

[16] Vinicius Tavares Guimaraes, Carla Maria Dal Sasso Freitas, Ramin Sadre, Liane Margarida Rockenbach Tarouco, and Lisandro Zambenedetti Granville. 2016. A survey on information visualization for network and service management. *IEEE Communications Surveys & Tutorials* 18, 1 (2016), 285–323.

[17] Richard Hackathorn and Todd Margolis. 2016. Immersive Analytics : Building Virtual Data Worlds for Collaborative Decision Support. (2016).

[18] Christopher Humphries, Nicolas Prigent, Christophe Bidan, and Frédéric Majorczyk. 2014. Catégorisation par objectifs de la visualisation pour la sécurité. In *CESAR*.

[19] Daisuke Inoue, Masashi Eto, Koei Suzuki, Mio Suzuki, and Koji Nakao. 2012. 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*. ACM, 72–79.

[20] Tobias Isenberg, Petra Isenberg, Jian Chen, Michael Sedlmair, and Torsten Möller. 2013. A systematic review on the practice of evaluating visualization. *IEEE Transactions on Visualization and Computer Graphics* 19, 12 (2013), 2818–2827.

[21] Mieczyslaw M Kokar and Mica R Endsley. 2012. Situation awareness and cognitive modeling. *IEEE Intelligent Systems* 27, 3 (2012), 91–96.

[22] Bireswar Laha, Kriti Sensharma, James D Schiffbauer, and Doug A Bowman. 2012. Effects of immersion on visual analysis of volume data. *IEEE Transactions on Visualization and Computer Graphics* 18, 4 (2012), 597–606.

[23] John T Langton and Alex Baker. 2013. Information visualization metrics and methods for cyber security evaluation. In *Intelligence and Security Informatics (ISI), 2013 IEEE International Conference on*. IEEE, 292–294.

[24] Vincent Lenders, Axel Tanner, and Albert Blarer. 2015. Gaining an Edge in Cyberspace with Advanced Situational Awareness. *IEEE Security & Privacy* 13, 2 (2015), 65–74.

[25] Ashish Malviya, Glenn A Fink, Landon Sego, and Barbara Endicott-Popovsky. 2011. Situational awareness as a measure of performance in cyber security collaborative work. In *Information Technology : New Generations (ITNG), 2011 Eighth International Conference on*. IEEE, 937–942.

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

[27] Sean McKenna, Diane Staheli, and Miriah Meyer. 2015. Unlocking user-centered design methods for building cyber security visualizations. In *Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on*. IEEE, 1–8.

[28] Wim Mees and Thibault Debatty. 2015. An attempt at defining cyberdefense situation awareness in the context of command & control. In *Military Communications and Information Systems (ICMCIS), 2015 International Conference on*. IEEE, 1–9.

[29] Patrick O'Leary, Sankhesh Jhaveri, Aashish Chaudhary, William Sherman, Ken Martin, David Lonie, Eric Whiting, James Money, and Sandy McKenzie. 2017. Enhancements to VTK enabling scientific visualization in immersive environments. In *Virtual Reality (VR), 2017 IEEE*. IEEE, 186–194.

[30] Cyril Onwubiko. 2016. Understanding Cyber Situation Awareness. (2016).

[31] Timea Pahi, Maria Leitner, and Florian Skopik. 2017. Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers. (2017).

[32] Johanna Pirker and Christian Gütl. 2015. Virtual Worlds for 3D Visualizations.. In *Intelligent Environments (Workshops)*. 265–272.

[33] Jean Scholtz and Alex Endert. 2014. User-centered design guidelines for collaborative software for intelligence analysis. In *Collaboration Technologies and Systems (CTS), 2014 International Conference on*. IEEE, 478–482.

[34] Aneesha Sethi, Federica Paci, and Gary Wills. 2016. EEVi–Framework for Evaluating the Effectiveness of Visualization in cyber-security. (2016).

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

[36] Anderson Gregório Marques Soares, Carlos Gustavo Resque dos Santos, Sandro De Paula Mendonça, Nikolas Jorge Santiago Carneiro, Brunelli Pinto Miranda, Tiago Davi Oliveira de Araújo, Alexandre Abreu de Freitas, Jefferson Magalhães de Morais, and Bianchi Serique Meiguins. 2016. A Review of Ways and Strategies on How to Collaborate in Information Visualization Applications. In *Information Visualisation (IV), 2016 20th International Conference*. IEEE, 81–87.

[37] Diane Staheli, Tamara Yu, R Jordan Crouser, Suresh Damodaran, Kevin Nam, David O'Gwynn, Sean McKenna, and Lane Harrison. 2014. Visualization evaluation for cyber security : Trends and future directions. In *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*. ACM, 49–56.

[38] Jennifer Stoll, Dave McColgin, M Gregory, V Crow, and W Keith Edwards. 2008. Adapting personas for use in security visualization design. In *VizSEC 2007*. Springer, 39–52.

[39] Guo-Dao Sun, Ying-Cai Wu, Rong-Hua Liang, and Shi-Xia Liu. 2013. A survey of visual analytics techniques and applications : State-of-the-art research and future challenges. *Journal of Computer Science and Technology* 28, 5 (2013), 852–867.

[40] George P Tadda and John S Salerno. 2010. Overview of cyber situation awareness. In *Cyber situational awareness*. Springer, 15–35.

[41] Takeshi Takahashi, Youki Kadobayashi, and Koji Nakao. 2011. Toward global cybersecurity collaboration : Cybersecurity operation activity model. In *Kaleidoscope 2011 : The Fully Networked Human ?-Innovations for Future Networks and Services (K-2011), Proceedings of ITU*. IEEE, 1–8.

[42] Huaglory Tianfield. 2016. Cyber Security Situational Awareness. In *Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on*. IEEE, 782–787.

[43] Michael Tyworth, Nicklaus A Giacobe, Vincent Mancuso, and Christopher Dancy. 2012. The distributed nature of cyber situation awareness. In *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2012 IEEE International Multi-Disciplinary Conference on*. IEEE, 174–178.

[44] Bing Wang and Klaus Mueller. 2014. Does 3D really make sense for visual cluster analysis ? yes !. In *3DVis (3DVis), 2014 IEEE VIS International Workshop on*. IEEE, 37–44.

[45] Xu-Meng Wang, Tian-Ye Zhang, Yu-Xin Ma, Jing Xia, and Wei Chen. 2016. A Survey of Visual Analytic Pipelines. *Journal of Computer Science and Technology* 31, 4 (2016), 787–804.

[46] Jeroen Wolbers and Kees Boersma. 2013. The common operational picture as collective sensemaking. *Journal of Contingencies and Crisis Management* 21, 4 (2013), 186–199.

[47] Tianye Zhang, Xumeng Wang, Zongzhuang Li, Fangzhou Guo, Yuxin Ma, and Wei Chen. 2017. A survey of network anomaly visualization. *Science China Information Sciences* 60, 12 (2017), 121101.