A Gap Analysis of Visual and Functional Requirements in Cybersecurity Monitoring Tools

Christian Luidold, Thomas Schaberreiter
Faculty of Computer Science
University of Vienna
Vienna, Austria
email: christian.luidold@univie.ac.at, thomas.schaberreiter@univie.ac.at

***Abstract*—In order to access valuable indicator information in the field of cybersecurity, domain experts tend to use visualizations to quickly gain an overview of a given situation, even more so in the age of big data where initially following visual summaries tends to be more efficient before diving into raw data. For this purpose, researchers analyze the visual and functional requirements of systems to facilitate data exploration. In this paper, we conduct a trend analysis of latest research contributions presented in VizSec symposia in terms of visualization techniques and functional requirements. Additionally, an international and a currently ongoing national project, focusing on Local Public Administrations (LPAs) and Critical Infrastructures (CIs) are analyzed and compared to current state-of-the-art research in terms of requirements of real users in the field of CIs and LPAs. Particularly, a deficiency concerning the requirements of collaboration, enhanced situational awareness, multi-stakeholder involvement, and multi-stakeholder visualization were identified and are discussed in the context of the utilization of cybersecurity visualizations in their work environments.**

***Index Terms*—requirements analysis; collaboration; situational awareness; multi-stakeholder; visualization.**

I. INTRODUCTION

Monitoring tools are meant to provide users with processed data and, regarding human computer interaction, preferable visualizations of various granularities. Tools evolved in terms of functionality and monitored scope, trying to provide the best possible user experience in times of big data and dynamic environments. This is especially true in the field of cybersecurity, where in an environment of increasing complexity a continuous stream of potentially massive data needs to be automatically preprocessed and classified for increased human comprehension.

Despite the increased sophistication of cybersecurity monitoring tools, current state-of-the-art research mainly focuses on the concept of visualization for analyses and neglecting additional needs of users regarding collaboration, enhanced situational awareness, multi-stakeholder involvement, and multi-stakeholder visualization. These additional capabilities are especially valuable in the context of Critical Infrastructure Protection (CIP).

As the main point of monitoring tools focusing on dynamic environments lies in the provision of real-time data visualizations, the core work mostly focuses on which types of visualizations are used and how data can be interacted with in order for the user to facilitate a deeper understanding of the underlying data. In an organizational context, especially when dealing with CI, it might not be sufficient to determine the state of a given situation and provide assistance in terms of CI-related decision making on a purely technical level. The socio-technical and social dimension within an organization is a key factor for decision making: In order to implement a solution to a cybersecurity problem, it is often necessary to collaborate within the organization to decide on an appropriate course-of-action. The decision making process includes employees with different backgrounds on different levels of the organizational hierarchy. Yet the representation of the data describing the issues is geared towards employees with a technical background. In order to facilitate collaboration and informed decision making on all levels, data representations that are more suitable to employees without a technical background should be investigated as well.

This shows that data driven cybersecurity requires significant consideration regarding data provision and visualization for a wide range of stakeholders, e.g., technical personnel, managers, first responders, authorities, and the general public. Crucial information needs to be tailored to user groups according to their needs and ensuring irrelevant data is filtered out.

The main objective of this work is to analyze aspects of functionalities and visualization used in state-of-the-art research regarding cybersecurity monitoring tools, as well as comparing their potential for integration in existing workflow processes of LPAs and CIs. The central research questions addressed in this research paper are:

- What are current trends in state-of-the-art research for administrations and organizations in terms of visual and functional requirements?
- What are identified gaps between presented research contributions and the needs of organizations?

After this introduction, this paper continues with Section II describing the related work, providing mentions and evaluations from different domains (including CIP) regarding visualizations and similar trend analyses. Section III inspects core requirements analyzed in the context of the international research project CS-AWARE [1] in the field of cybersecurity for LPAs, and the currently ongoing national research project ODYSSEUS [2] aimed at creating a multi-layered risk model

 ISBN: 978-1-61208-821-1

in the CI sector. In Section IV, an additional analysis of state-of-the-art research of visualization and functional concepts in the domain of cybersecurity was conducted, followed by a comparison with findings from the previous section. Section VI provides a conclusion and outlook on future work.

II. Related Work

Concerning detection and analysis of cyber incidents, the human factor plays an essential role in the continuously evolving environment of cybersecurity. A variety of tools with different focus areas keep on emerging and all of them bring their own techniques and visualizations to address the specific problems at hand in that area.

According to D'Amico et al. [3], who conducted a survey on cyber operators in terms of cybersecurity visual presentations, the human factor is regarded as a critical part in assessing various situations and consequential decision making. The major issue being addressed is the fluctuant effectiveness of data visualization due to subjectivity, different levels of experience, as well as different goals of respective user groups. Their findings concerning visualizations concluded that visualizations are becoming increasingly more important than regular text-based analyses, although they should still be provided for deeper inspection. The greatest focus of the researchers with respect to the questions asked was whether hours worth of time and effort to learn discerning visualizations would pay off, to which 10 out of 15 participants agreed.

Regarding the facilitation of decision making cited by Wagner et al. [4], one of the major issues lies in the fact that a diagnostic routine in a continuously evolving environment such as cybersecurity is virtually impossible. Generally, extensive domain knowledge is necessary to derive valid assumptions. Current trends show that instead of automating the process of decision making, the existing data has to be automatically analyzed and interactive visualizations as a basis for decision making need to be generated from those results. To facilitate comprehension, the output has to take the granularity of information into account. Despite the advantage of visualizing additional dimensions using 3D visualization techniques, a majority of tools and research contributions avoid their inclusion. Concerning the overall type of visualizations used, 24 out of 25 proposed systems support 2D visualizations, whereas only 4 out of 25 proposed systems either only support 3D visualizations or use it to complement their 2D visualizations.

Focusing on CI and CIP, Merabti et al. [5] explore major challenges regarding CIP, differentiating between system modelling, system of systems design (addressing the problem of a complex internal heterogeneous ecosystem), (cyber-) security, and crisis management. Concerning crisis management, the authors developed a tool facilitating the discovery of vulnerabilities and study cascade effects of crisis management processes. The user interface mainly relies on a 2.5D geographical map with a node-link diagram overlay.

Nukavarapu and Durbha [6] present a dynamic simulation model for real-time situational awareness for operational risk management in CIs during disasters. By employing a colored petri net visualizing data provided through a Geographic Information System (GIS) cascading effects can be simulated. The usage of the model aims to provide assistance regarding decision making and response planning for disaster response personnel. Although use case scenarios were provided regarding the motivation of the model's usage, there were no domain experts involved in the design or evaluation cycles.

Lee et al. [7] present a dynamic monitoring and analysis system incorporating multiple CI and GIS datasets. The system includes data processing and analysis capabilities regarding efficiency and vulnerabilities, as well as simulation of "what-if" scenarios in the context of CI incidents. The visualizations include node-link diagrams over geographical maps, line charts and textual representations. Follow-up work by Tabassum et al. [8] provides demonstration scenarios based on the previous work.

As part of communication and enhanced situational awareness analysis, Thom et al. [9] [10] conducted user interviews comprising of 29 domain experts from disaster response and CI management regarding the results of a social media analysis on a real world Twitter data set during the German flood 2013. While the results and the subsequent discussion with participating stakeholders provided various insights concerning data provision and data processing, e.g., included media support and classification, the domain experts stated fake news as a major concern.

Similarly, Mittelstädt et al. [11] introduce a visual analytics system for CIs with simulation features for cascading effects. The system facilitates enhanced situational awareness by analyzing Twitter messages linked to a given incident. The targeted users consist of various stakeholders from different domains, i.e., analytics experts and police, grouped into crisis managers, site commanders, or first responders. User evaluations and interviews conducted with domain experts from CIs and government provided positive feedback. A significant limitation stated during interviews was the aspect of fake news regarding analyzed Twitter messages.

Puuska et al. [12] present a CI simulation system focusing on the aspects of situational awareness and collaboration regarding data sharing. They conducted user interviews with domain experts and stakeholders from different CIs, mobile network operators, and rescue service providers (e.g. police force) resulting in a set of requirements covering collaboration, interoperability, multi-stakeholder needs, visualization, as well as general system requirements. The applied visualization techniques focus on node-link diagrams over a geographical map and line charts displaying the impact of natural disasters on CI.

III. Analysis of User Requirements in the CI and LPA Sectors

The following section analyzes requirements of nationally and internationally funded projects in the field of security, including the CS-AWARE project [1], and the currently ongoing ODYSSEUS project [2]. Special attention is given to

 ISBN: 978-1-61208-821-1

the concept of enhanced situational awareness to extend the regular scope.

A. Requirements Analysis in CS-AWARE

In the context of the CS-AWARE project [1], which focuses on the concepts of enhanced situational awareness and information sharing for LPAs, multiple end-user workshops organized in form of focus group interviews were conducted during the design cycles with cybersecurity and representatives from various LPA user groups (including executives, operations, and external stakeholders, i.e., the general public). During the evaluation cycles, a set of technical evaluations in form of user studies and UX interviews were conducted followed by the completion of questionnaires, if applicable.

1) User Requirements: The user requirements were acquired during the design cycle's workshops types with the project's end-user partners, the cities of Rome and Larissa. The workshops provided insights into internal processes, structure, and limitations of LPA operations. In the workshops, the domain experts reported their experience in form of stories in collaborative groups starting with individual experiences and afterwards broadening them by adding more details about the context, issues, and the outcome of events. Stories included various topics ranging from fake news to sharing potentially sensitive data through web conferencing tools. The involved user groups consisted of managers (n=5), system administrators (n=6), and local service users (n=2) in Rome, and manager (n=1), system administrators (n=3 + 1 unit manager) and local service users (n=2) in Larissa. The results of the workshops allowed to derive requirements based on each user groups objectives, including "reduction of time for threat understanding" and "more effective relation with service providers in handling cybersecurity", system artifacts, i.a., "report of information shared by other LPAs" and "weekly incident reports", and the desired behavior, i.a., "Regular communication with technical team and internal users" and "collaboratively discussing solutions", during the deployment of the system.

2) Visual Requirements: Regarding the visual components used, the CS-AWARE system primarily focuses on tabular views and the provision of raw data. Used visualization techniques belong to the 2D display and geometrically transformed displays category, including a dartboard chart and a node-link diagram. The system focuses on textual representations of information and provides the users with a high degree of interaction including searching and filtering textual and visual representations, as well as zooming and panning the interface elements.

3) Functional Requirements: The main concepts of the CS-AWARE project are, i.a., collaboration and an extended aspect of situational awareness, as the latter focuses on the gathering of data from a multitude of external sources, as well as building a threat sharing community consisting of CS-AWARE users. Kupfersberger et al. [13] describe the information flow model of the CS-AWARE project providing an in-depth analysis regarding its functional requirements. One of the major requirements of the domain experts was the functionality of interoperability, specifically to seamlessly support the integration of the system into the existing work environment. This includes the sharing of findings between applications, i.e., data import / export and email notifications.

B. Requirement Analysis in ODYSSEUS

During the ODYSSEUS project [2], which focuses on the analysis of cascading effects between critical supply networks in cities, the domain experts from various CIs stated collaboration and enhanced situational awareness to be critical factors concerning the life cycle of threats.

While the core functionality of CIs (i.a., power supply or water supply) work independently from external networks and therefore generally remain unaffected by external outages, problems stated by the domain experts may arise from outside their field of activity, i.a., panic reactions from the population and fake news. These erroneously undermine public trust and pose a security risk for public administrations and the population. The identified requirements include:

1) Project Environment: The project environment consists of internal project partners encompassing research facilities, industry, and federal ministries. After creating a set of use case scenarios, multiple end-user workshops were conducted to evaluate the assumptions. The first workshop had the form of focus group interviews with domain experts from different CIs. After an initial assessment and adaptions of the use case scenarios, a set of subsequent workshops were conducted focusing on various domain experts regarding business continuity, and security from each CI involved.

2) Functional Requirements: In order to cope with potential problems, which is largely done in collaboration with other public administrations, a reliable flow of communication between these administrations and the CIs has been identified as essential.. In this regard, the requirement of information sharing is to be underlined, as it facilitates timely reactions of involved parties both in terms of communicating valuable information, and in terms of collaboration regarding mitigation actions and next steps.

Additional paths of information flows concerning information sharing facilitate enhanced situational awareness. While this constitutes a favorable advantage for CIP and other organizations, the domain experts stated the need for increased assessment of public resources regarding trustworthiness, duplicates, and accuracy in order to correctly assess the situation.

IV. Focus, Gaps of Major Trends Identified in Literature

In order to objectively evaluate the work presented in the Symposium on Visualization for Cyber Security (VizSec) during the years 2017 to 2019, a set of different categories were chosen ranging from visualization techniques to user involvement. Additionally, as not all papers focus on the demonstration of applications, general categories described by Liu et al. [14] were used for the classification of research contributions.

 ISBN: 978-1-61208-821-1

A. Dimensions Evaluated

The following subsection describes new dimensions evaluated in this paper, derived from or complementing existing categories.

1) Category of Contribution: Liu et al. [14] provide an analysis of submitted research in Information Visualization (InfoVis) concerning future trends, major goals, recent trends, and state-of-the-art approaches. The authors classify these works into four main categories: Empirical methodologies, Systems & Frameworks, Applications, and Interactions. In the context of this work the last category will be removed.

The category of contribution selects the main contribution type presented by the authors. If authors use an application to demonstrate their proposed model, then the contribution will be assigned to the empirical methodology category, despite also including an application.

2) Visualization techniques: Regarding visualization techniques, a subset of categories identified by Keim [15] and used by Wagner et al. [4] was selected consisting of: Standard 2D/3D Displays, Geometrically Transformed Displays, Iconic Displays, Dense Pixel Display, and Stacked Display. Additionally, as the VizSec specializes in the collaboration between academia, government, and industry, the following categories have been added or underlined form the list above:

- **Maps** as geographical visualizations. This category is part of the **Standard 2D/3D Displays** category, but due to the coverage of specific use cases, this subcategory will be treated separately.
- **Tabular View** as a textual representation of summarized or derived information, generally displayed as, but not limited to, tabs.
- **Raw Data** as supporting the display to raw data regarding the data source. This category is especially valuable to gain an in-depth understanding after an initial analysis in order to facilitate decision making.

Multiple categories can be selected due to a range of use cases applicable.

3) Interactivity and Mapping: The functionality of contributed applications is evaluated in part according to the presence of interaction and distortion techniques by Keim [15] and categorization by Wagner et al. [4]. The selected subset consists of different degrees of Interactivity, Filtering, and Dynamic or Static Mapping.

In addition to the categories listed in related work, we identified several additional categories relevant for interactivity and mapping, which is based on practical experience with user requirements from the CI and LPA field:

- **Interactivity Low** describes basic interactive features between the user and the application, e.g., viewing static visualizations.
- **Interactivity High** describes advanced interactive features between the user and the application, e.g., inspecting selections and applying filters.
- **Collaboration** as the functionality of collaboration between users using one application and external targets, or between multiple instances of the same application.
- **Customization** as the functionality to adapt the application view according to various parameters, i.a., color palette.

4) User Involvement: The categories for user involvement differentiates between the level of expertise of people involved either in form of user interviews before or during the initial design processes, or user studies during the design or evaluation processes of the contributed research. The categorization follows adapted user types described by [16] and consists of:

- **No Users** describes a research contribution with no involved individuals during the design or evaluation cycles. Use case scenarios exemplifying the usage of the provided contribution without actual real user involvement also fall into this category.
- **Lay Users** are users without required domain knowledge.
- **Novices** are users with beginners knowledge of the domain, e.g., students in the required field.
- **Experts** are users with extensive domain knowledge generally working in the industry.

5) Included Content: The included content category provides an overview of all aspects involved comprising the individual research contributions as follows:

- **Tool, Prototype, etc.** describes the usage of a technical application either as the main contribution, or to support the main contribution.
- **Model, Approach, etc.** describes the usage of novel methods in order to tackle unique problem spaces through new visualization techniques.
- **User Study** describes the involvement of real domain experts for evaluation purposes.
- **User Story/ Interview** describes the involvement of real domain experts for the purpose of gathering information about the problem space being tackled.

B. Analysis of VizSec symposia 2017-2019

In the context of this work, we analyzed the years 2017 - 2019 of the VizSec symposia according to the categories described above. The VizSec symposium constitutes a forum of research contributions encompassing academia, government, and industry, which provides a meaningful insight into current trends. The results regarding relevant contributions might differ according to the authors intent. The outcome of the analysis is presented in Tables I to V, and are discussed in Section IV-B4 and Section V.

1) VizSec 2017: In terms of visualization techniques used, a majority of authors focus on simple 2D displays with additional techniques, if their usage would support the purpose of the work, i.a., dense pixel displays. Concerning interactivity, nearly every proposed tool includes a form of high interactivity characterized by the possibility to manipulate rendered visualizations, i.a., by applying filters, panning, or zooming.

A major gap identified of the VizSec 2017 papers is the functionality in terms of collaboration. Only two [17] [18]

 ISBN: 978-1-61208-821-1

out of ten papers addressed this topic, although Sethi and Wills [18] only conducted expert interviews resulting in those experts stating the need for collaboration without going into further detail on how to ensure this functionality, or proposing ways on the implementation. On the other hand, Franklin et al. [17] designed a prototype specifically supporting a collaborative process by implementing a shared space to ”brainstorm, share notes and hold [their] brains during interruption”.

2) VizSec 2018: All authors include a form of 2D displays as visualization techniques in their work with only Krokos et al. [19] additionally using 3D display visualization techniques. Apart from this aspect, nearly every author included another visualization technique in order to complement their work.

In terms of interactivity, seven out of nine papers proposing a tool or prototype implemented additional functionality for increased interactivity of the system.

Again, the major scientific gap identified in the VizSec 2018 papers is the aspect of collaboration, as none of the eleven papers discussed the importance of collaboration or incorporated collaborative functionality into their prototypes.

3) VizSec 2019: Every author with focus on a presented application included a form of 2D display into their research, with four out of seven authors including another visualization technique to complement their work.

The major gap identified in the VizSec 2019 papers is again the aspect of collaboration, as none of the eleven papers discussing or supporting the implementation of collaborative functionality. Ulmer et al. [20] discuss collaboration as part of future work.

4) Current Trends: In terms of evaluation techniques, Barkhuus et al. [21], is analyzing papers submitted to the CHI conference and found that those techniques commonly used in industry are generally unsuitable for academia as they are specifically designed to meet the needs of businesses. In terms of empirical evaluations, a strong shift in favor of qualitative evaluations was detected.

Staheli et al. [16] analyzed the research submitted to the IEEE VizSec symposia over a time period of ten years from 2004 - 2013. Their goal was to identify gaps in evaluation approaches regarding information visualization. Concerning the statement of Barkhuus et al. [21], the authors express that the research provided in VizSec papers are designed to be used in practical situations regarding real world use cases. The core findings in terms of trend analysis showed a rise regarding feature set utility, insight generation, and usability, while the aspect of collaboration was barely present (2 out of 119 research contributions).

Current trends in the context of VizSec research contributions show that a majority of submissions tend to focus on the presentation of novel applications or prototypes for visualization, as shown in Table I, while empirical methodologies (i.e. novel models or evaluations) fluctuate between years.

In contributions focusing on the presentation of applications or prototypes, or using them to visualize underlying models, a majority of research contributions use simple 2D charts as visualization technique, as depicted in Table II.

TABLE I. . RESEARCH CONTRIBUTIONS CLASSIFIED ACCORDING TO THE MAIN FOCUS OF THE CONTRIBUTION.

Category	VizSec 2017	VizSec 2018	VizSec 2019
Empirical methodology	[22]	[23], [24], [25], [26], [19], [27]	[28], [29], [30]
Systems and Frameworks			[31], [32]
Applications	[33], [34], [35], [36], [37], [38], [39], [17], [40]	[41], [42], [43], [44], [45]	[46], [47], [48], [20], [49], [50]

Additional provision of textual representations or access to raw data proves especially advantageous for domain experts in conducted evaluations. Visualization techniques using iconic displays or dense pixel displays tend to be part of empirical methodologies to underline alternative aspects of data, which consequently provides valuable input for further research.

TABLE II. . RESEARCH CONTRIBUTIONS CLASSIFIED ACCORDING TO VISUALIZATION TECHNIQUES USED.

Category	VizSec 2017	VizSec 2018	VizSec 2019
2D Display	[33], [34], [37], [38], [39], [17], [40]	[23], [24], [41], [42], [43], [44], [25], [45], [26], [19], [27]	[46], [31], [28], [47], [48], [32], [20], [49], [50]
3D Display	[35]	[19]	[20]
Geometrically Transformed	[35], [36], [37], [39], [40]	[42], [44], [27]	[28], [32], [20], [49], [50]
Iconic Display		[25], [45]	
Dense Pixel Display			[29]
Stacked Display	[38], [39], [40]	[41], [42], [19]	[29], [48]
Maps	[39]	[42], [45], [32]	
Tabular View	[37], [38], [39], [17], [40]	[24], [41], [42], [44], [26],	[31], [48], [20], [49], [50]
Raw Data	[37], [38], [39], [17], [40]	[41], [43], [44], [45], [26]	[20]

As the main contribution of visualizations in cybersecurity is related to data exploration and insight creation, applications are bound to provide a high degree of interactivity - like the functionality of brushing and linking for the purpose of filtering data. The category Dynamic Mapping is especially relevant in this evaluation, as it constitutes an essential part of situational awareness. Detailed results are provided in Table III. The category of collaboration shows a significant gap in the cybersecurity ecosystem, despite a critical need for increased increased cooperation and collaboration between cybersecurity actors, as highlighted by the European cybersecurity strategy of 2013 [51] and the Network and Information Security (NIS) directive [52]. Although a few research contributions mention the aspect of collaboration as part of related work, it is generally not implemented by the presented conceptions.

Regarding user involvement in terms of interviews with domain experts and evaluation processes, the results seem to reflect the findings of Staheli et al. [16], as a majority of users in presented research contributions were domain experts vs. users with differing experience levels. Despite most contributions include tools or use case scenarios, about one third did not provide any end-user involvement (e.g. interviews

TABLE III. . RESEARCH CONTRIBUTIONS CLASSIFIED ACCORDING TO INTERACTIVITY AND MAPPING USED.

Category	VizSec 2017	VizSec 2018	VizSec 2019
No Interactivity			
Interactivity Low	[33], [34], [17]	[41],	
Interactivity High	[35], [36], [37], [38], [40]	[24], [42], [43], [44], [25], [45], [26], [19],	[46], [31], [47], [48], [32], [20], [49], [50]
Customization	[38]	[41], [47]	
Sorting/Filtering	[37], [38], [39], [17], [40]	[24], [41], [42], [43], [44], [45], [26], [19]	[46], [31], [47], [48], [32], [20], [49], [50]
Dynamic Mapping	[39], [17]	[19]	[47], [20], [50]
Static Mapping	[33], [34], [35], [36], [37], [38], [40]	[23], [24], [41], [42], [43], [44], [25], [45], [26]	[46], [31], [48], [32], [49]
Collaboration	[22], [17]		

or evaluations). The detailed evaluation results are shown in Table IV.

TABLE IV. . RESEARCH CONTRIBUTIONS CLASSIFIED ACCORDING TO USERS INVOLVED DURING DESIGN CYCLES OR USER STUDIES.

Category	VizSec 2017	VizSec 2018	VizSec 2019
No Users	[34], [35], [39], [40]	[24], [44], [26]	[31], [28], [29], [32], [30]
Lay Users		[25], [27]	[47]
Novices	[37], [38]	[45]	[46], [20], [50]
Experts	[33], [22], [36], [37], [38], [17]	[41], [42], [43], [19]	[47], [48], [20], [49]
Not disclosed		[23], [25]	

An overall analysis of the provided content of the research contributions includes either a tool or a user study to evaluate their findings. Initial user interviews provide the advantage of receiving in-depth experiences of domain experts on which research contributions can be build upon, despite opportunities for their implementation are often limited. A detailed table displaying the categorizations is provided in Table V.

TABLE V. . RESEARCH CONTRIBUTIONS LISTED ACCORDING TO PROVIDED CONTENT.

Category	VizSec 2017	VizSec 2018	VizSec 2019
Tools	[33], [34], [35], [36], [37], [38], [39], [17], [40]	[23], [24], [41], [42], [43], [44], [45], [26], [19]	[46], [31], [47], [48], [32], [20], [49], [50]
Algorithm/ Approach/ etc.	[34]	[23], [24]	[28], [29], [30]
User Study	[33], [22], [37], [38]	[23], [41], [42], [43], [25], [45], [19], [27]	[46], [47], [20], [49], [50]
User Story/ Interviews	[22], [36], [17]		[47], [48]

V. DISCUSSION OF IDENTIFIED GAPS

In the context of discussing gaps, the aspects of collaboration, enhanced situational awareness, multi-stakeholder involvement, and multi-stakeholder visualization are discussed, as we have identified a need for cybersecurity visualizations in this context from user feedback in the context of the two research projects presented in Section III.

The analysis shows that collaboration is rarely a factor in current state-of-the-art cybersecurity visualization research. The benefits of a collaborative approach include the facilitation of information sharing between CI stakeholders and government authorities during incidents and enhance mitigation and response actions, as shown by Puuska et al. [12], and in the context of CS-AWARE.

Regarding enhanced situational awareness, the current state-of-the-art focuses on situational awareness within an organization rarely exceeding the boundaries of a given organization. A growing trend to CIP research can be observed in the context of evaluations of Twitter posts as analyzed by Thom et al. [9] [10] and Mittelstädt et al. [11]. The expectations of enhanced situational awareness incorporate the analysis of external data, i.a., social media or distinct information sharing communities, in order to gather more knowledge regarding active threats to facilitate responsive measures. Domain experts involved in CS-AWARE and ODYSSEUS stated an increased need for data analysis outside the organizational scope of LPAs and CIs.

Regarding multi-stakeholder involvement in the design and evaluation cycles of a project, the general trend in state-of-the-art analysis only incorporates the views of a single stakeholder group at most. Puuska et al. [12] and Mittelstädt et al. [11] incorporate views and processes of multiple user groups ranging from analysts to first responders. The expectations include an increased incident handling capability to account for multiple interdependent processes (i.a. supported incident handling & data sharing across departments and increased coordination with external organizations and authorities). During ODYSSEUS the need for the evaluation and adaption of created use case scenarios arose, after which different stakeholders were interviewed to gain insight into dependent processes including domain experts from CIs and LPAs.

Regarding multi-stakeholder visualizations, the current state of state-of-the-art research generally focuses on single use cases for technical personnel to alleviate readability of processed raw data. A majority of CIP related work provides visualizations encompassing at least technical user groups and facilitates coordination with other groups like, e.g., first responders, for which individual views need to be created. The expectations of incorporating multi-stakeholder visualization lies in the increased homogeneity of the ecosystem facilitating interoperability and collaboration. In the context of CS-AWARE, the need for accommodating different user groups (e.g. management, technical personnel) by representing data to suit their specific requirements was clearly expressed during the end-user workshops.

In order to meet those expectations, an initial assessment of involved stakeholder groups is essential, highlighting individual needs and desirable outcomes in terms of visual and functional requirements. Furthermore, the results may expose dependencies previously not taken into consideration. As a recommendation, we propose:

- Using workshops and user interviews during early stages of a project's life cycle to assess and define the desired outcomes for each user group. This includes the

 ISBN: 978-1-61208-821-1

assessment of what information is required by each user group, and how data needs to be represented to meet those requirements.

- Additionally, proposed systems need to take collaboration and coordination efforts between multiple user groups into account, including domain-independent stakeholders. Notably, the functionality of supporting data/information sharing provides stakeholders with the capability of efficient incorporation of a system into an existing environment.

VI. Conclusion and Future Work

In this work a gap analysis in the current state-of-the-art of cybersecurity related visualizations is presented. The requirements for cybersecurity visualizations of end users from the LPA and CI sectors are analyzed, based on results achieved during the two research projects CS-AWARE and ODYSSEUS. A gap analysis with respect to the requirements identified is conducted based on an in-dept analysis and categorization of the VizSec symposia from 2017-2019.

The findings show a gap between the state-of-the-art research and the extended requirements of LPAs and CIs specifically in the context of collaboration, enhanced situational awareness, multi-stakeholder involvement, and multi-stakeholder visualization. For each gap, we analyze the current trend, as well as expectations resulting from the implementation of these aspects. Finally, we propose recommendations aimed at increasing the efficiency of realization of projects including multiple domain-interdependent stakeholders.

Future work encompasses the evaluation of analyzed aspects and requirements to be included during the progress of the ODYSSEUS project, and providing a proof-of-concept implementation of cybersecurity related visualizations that take the aspects of cooperation/collaboration and optimization of visualizations for different user groups within the organization into account.

Acknowledgments

This work was partially funded by the Austrian FFG research program KIRAS in course of the project ODYSSEUS ("Simulation und Analyse kritischer Netzwerk-Infrastrukturen in Städten") under Grant No. 873539.

References

[1] "A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis CS-AWARE Project H2020 CORDIS European Commission," Sep 2020, [retrieved: September, 2020]. [Online]. Available: https://cordis.europa.eu/project/id/740723

[2] "Kiras - sicherheitsforschung," Aug 2020, retrieved: August, 2020]. [Online]. Available: https://www.kiras.at/en/financed-proposals/detail/d/odysseus-simulation-und-analyse-kritischer-netzwerk-infrastrukturen-in-staedten

[3] A. D'Amico, L. Buchanan, D. Kirkpatrick, and P. Walczak, "Cyber operator perspectives on security visualization," in *Advances in Human Factors in Cybersecurity*, D. Nicholson, Ed. Cham: Springer International Publishing, 2016, pp. 69–81.

[4] M. Wagner, F. Fischer, R. Luh, A. Haberson, A. Rind, D. A. Keim, and W. Aigner, "A survey of visualization systems for malware analysis," in *EuroVis*, 2015.

[5] M. Merabti, M. Kennedy, and W. Hurst, "Critical infrastructure protection: A 21st century challenge," in *2011 International Conference on Communications and Information Technology (ICCIT)*, 2011, pp. 1–6.

[6] N. Nukavarapu and S. Durbha, "Geo-visual analytics for healthcare critical infrastructure simulation model," in *2017 IEEE International Geoscience and Remote Sensing Symposium (IGARSS)*, 2017, pp. 6106–6109.

[7] S. Lee, L. Chen, S. Duan, S. Chinthavali, M. Shankar, and B. A. Prakash, "Urban-net: A network-based infrastructure monitoring and analysis system for emergency management and public safety," in *2016 IEEE International Conference on Big Data (Big Data)*, 2016, pp. 2600–2609.

[8] A. Tabassum, S. Chinthavali, S. Lee, L. Chen, and B. Prakash, "Urban-net : A system to understand and analyze critical infrastructure networks for emergency management," 2019.

[9] D. Thom, R. Krüger, T. Ertl, U. Bechstedt, A. Platz, J. Zisgen, and B. Volland, "Can twitter really save your life? a case study of visual social media analytics for situation awareness," in *2015 IEEE Pacific Visualization Symposium (PacificVis)*, 2015, pp. 183–190.

[10] D. Thom, R. Krüger, and T. Ertl, "Can twitter save lives? a broad-scale study on visual social media analytics for public safety," *IEEE Transactions on Visualization and Computer Graphics*, vol. 22, no. 7, pp. 1816–1829, 2016.

[11] S. Mittelstädt, X. Wang, T. Eaglin, D. Thom, D. Keim, W. Tolone, and W. Ribarsky, "An integrated in-situ approach to impacts from natural disasters on critical infrastructures," in *2015 48th Hawaii International Conference on System Sciences*, 2015, pp. 1118–1127.

[12] S. Puuska, S. Horsmanheimo, H. Kokkoniemi-Tarkkanen, P. Kuusela, L. Tuomimäki, and J. Vankka, "Integrated platform for critical infrastructure analysis and common operating picture solutions," in *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, 2017, pp. 1–6.

[13] V. Kupfersberger, T. Schaberreiter, and G. Quirchmayr, "Security-driven information flow modelling for component integration in complex environments," in *Proceedings of the 10th International Conference on Advances in Information Technology, IAIT 2018, Bangkok, Thailand, December 10-13, 2018*. ACM, 2018, pp. 19:1–19:8. [Online]. Available: https://doi.org/10.1145/3291280.3291797

[14] S. Liu, W. Cui, Y. Wu, and M. Liu, "A survey on information visualization: recent advances and challenges," *The Visual Computer*, vol. 30, no. 12, pp. 1373–1393, Dec 2014. [Online]. Available: https://doi.org/10.1007/s00371-013-0892-3

[15] D. A. Keim, "Information visualization and visual data mining," *IEEE transactions on Visualization and Computer Graphics*, vol. 8, no. 1, pp. 1–8, 2002.

[16] D. Staheli, T. Yu, R. J. Crouser, S. Damodaran, K. Nam, D. O'Gwynn, S. McKenna, and L. Harrison, "Visualization evaluation for cyber security: Trends and future directions," in *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*, ser. VizSec '14. New York, NY, USA: ACM, 2014, pp. 49–56. [Online]. Available: http://doi.acm.org/10.1145/2671491.2671492

[17] L. Franklin, M. Pirrung, L. Blaha, M. Dowling, and M. Feng, "Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2017, pp. 1–8.

[18] A. Sethi and G. Wills, "Expert-interviews led analysis of eevi — a model for effective visualization in cyber-security," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2017, pp. 1–8.

[19] E. Krokos, A. Rowden, K. Whitley, and A. Varshney, "Visual analytics for root dns data," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2018, pp. 1–8.

[20] A. Ulmer, D. Sessler, and J. Kohlhammer, "Netcapvis: Web-based progressive visual analytics for network packet captures," in *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 2019, pp. 1–10.

[21] L. Barkhuus and J. Rode, "From mice to men - 24 years of evaluation in chi," in *Proceedings of the SIGCHI Conference on human factors in computing systems*, ser. CHI '07. ACM, 2007.

[22] A. Sethi, F. Paci, and G. Wills, "Eevi - framework for evaluating the effectiveness of visualization in cyber-security," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec 2016, pp. 340–345.

[23] Y. Yang, J. Collomosse, A. K. Manohar, J. Briggs, and J. Steane, "Tapestry: Visualizing interwoven identities for trust provenance," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2018, pp. 1–4.

 ISBN: 978-1-61208-821-1

[24] R. Gove and L. Deason, "Visualizing automatically detected periodic network activity," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2018, pp. 1–8.

[25] D. L. Arendt, L. R. Franklin, F. Yang, B. R. Brisbois, and R. R. LaMothe, "Crush your data with vic2es then chissl away," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2018, pp. 1–8.

[26] B. C. M. Cappers, P. N. Meessen, S. Etalle, and J. J. van Wijk, "Eventpad: Rapid malware analysis and reverse engineering using visual analytics," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2018, pp. 1–8.

[27] J. Chou, C. Bryan, J. Li, and K. Ma, "An empirical study on perceptually masking privacy in graph visualizations," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2018, pp. 1–8.

[28] A. Dasgupta, R. Kosara, and M. Chen, "Guess me if you can: A visual uncertainty model for transparent evaluation of disclosure risks in privacy-preserving data visualization," in *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 08 2019.

[29] S. O'Shaughnessy, "Image-based malware classification: A space filling curve approach," in *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 10 2019.

[30] M. Varga, C. Winkelholz, and S. Träber-Burdin, "An exploration of cyber symbology," in *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 2019, pp. 1–5.

[31] B. Laughlin, C. Collins, K. Sankaranarayanan, and K. El-Khatib, "A visual analytics framework for adversarial text generation," *arXiv*, Sep 2019. [Online]. Available: https://arxiv.org/abs/1909.11202

[32] S. Subramanian, P. Pushparaj, Z. Liu, and A.-d. Lu, "Explainable visualization of collaborative vandal behaviors in wikipedia," in *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 08 2019.

[33] M. Angelini, S. Lenti, and G. Santucci, "Crumbs: A cyber security framework browser," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2017, pp. 1–8.

[34] A. P. Norton and Y. Qi, "Adversarial-playground: A visualization suite showing how adversarial examples fool deep learning," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2017, pp. 1–4.

[35] L. Leichtnam, Totel, N. Prigent, and L. Mé, "Starlord: Linked security data exploration in a 3d graph," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2017, pp. 1–4.

[36] H. Kim, S. Ko, D. S. Kim, and H. K. Kim, "Firewall ruleset visualization analysis tool based on segmentation," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2017, pp. 1–8.

[37] G. R. Santhanam, B. Holland, S. Kothari, and J. Mathews, "Interactive visualization toolbox to detect sophisticated android malware," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2017, pp. 1–8.

[38] R. Romero-Gomez, Y. Nadji, and M. Antonakakis, "Towards designing effective visualizations for dns-based network threat analysis," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2017, pp. 1–8.

[39] M. Angelini, L. Aniello, S. Lenti, G. Santucci, and D. Ucci, "The goods, the bads and the uglies: Supporting decisions in malware detection through visual analytics," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2017, pp. 1–8.

[40] R. Theron, R. Magán-Carrión, J. Camacho, and G. M. Fernndez, "Network-wide intrusion detection supported by multivariate analysis and interactive visualization," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2017, pp. 1–8.

[41] A. Sopan, M. Berninger, M. Mulakaluri, and R. Katakam, "Building a machine learning model for the soc, by the input from the soc, and analyzing it for the soc," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2018, pp. 1–8.

[42] S. Chen, S. Chen, N. Andrienko, G. Andrienko, P. H. Nguyen, C. Turkay, O. Thonnard, and X. Yuan, "User behavior map: Visual exploration for cyber security session data," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2018, pp. 1–4.

[43] M. Angelini, G. Blasilli, P. Borrello, E. Coppa, D. C. D'Elia, S. Ferracci, S. Lenti, and G. Santucci, "Ropmate: Visually assisting the creation of rop-based exploits," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2018, pp. 1–8.

[44] G. Bakirtzis, B. J. Simon, C. H. Fleming, and C. R. Elks, "Looking for a black cat in a dark room: Security visualization for cyber-physical system design and analysis," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2018, pp. 1–8.

[45] A. Ulmer, M. Schufrin, D. Sessler, and J. Kohlhammer, "Visual-interactive identification of anomalous ip-block behavior using geo-ip data," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Oct 2018, pp. 1–8.

[46] J. Torres, E. Veas, and C. Catania, "A study on labeling network hostile behavior with intelligent interactive tools," in *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 2019, iEEE Symposium on Visualization for Cyber Security, VIZSEC ; Conference date: 20-10-2019 Through 25-10-2019. [Online]. Available: http://ieeevis.org/year/2019/welcome

[47] A.-P. Lohfink, S. Duque Antón, H. D. Schotten, H. Leitte, and C. Garth, "Security in process: Visually supported triage analysis in industrial process data," in *Proceedings of the IEEE Symposium on Visualization for Cyber Security 2019. IEEE Symposium on Visualization for Cyber Security (VizSec-2019), October 20-25, Vancouver, British Columbia, Canada*, IEEE. IEEE, 2019.

[48] M. Angelini, G. Blasilli, L. Borzacchiello, E. Coppa, D. C. D'Elia, C. Demetrescu, S. Lenti, S. Nicchi, and G. Santucci, "Symnav: Visually assisting symbolic execution," in *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 10 2019.

[49] B. Fouss, D. M. Ross, A. B. Wollaber, and S. R. Gomez, "Punyvis: A visual analytics approach for identifying homograph phishing attacks," in *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 2019, pp. 1–10.

[50] R. Ošlejšek, V. Rusňák, K. Burská, V. Švábenský, and J. Vykopal, "Visual feedback for players of multi-level capture the flag games: Field usability study," in *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 2019, pp. 1–11.

[51] "Eu cybersecurity plan to protect open internet and online freedom and opportunity - cyber security strategy and proposal for a directive - shaping europe's digital future - european commission," Mar 2020, [retrieved: September, 2020]. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[52] E. P. Council of the European Union, "Directive (eu) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union," *Publications Office of the European Union*, Jul 2016. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/d2912aca-4d75-11e6-89bd-01aa75ed71a1/language-en

 ISBN: 978-1-61208-821-1