Uncertainty and Risk: Investigating line graph aesthetic for enhanced cyber security awareness

*Note: Sub-titles are not captured in Xplore and should not be used

1st Pinney
dept. Cardiff school of technologies (of Aff.)
Cardiff Metropolitan University (of Aff.)
Cardiff, Wales
jpinney@cardiffmet.ac.uk

2nd Carroll
dept. Cardiff school of technologies (of Aff.)
Cardiff Metropolitan University (of Aff.)
Cardiff, Wales
fcarroll@cardiffmet.ac.uk

***Abstract*—Cybersecurity has never been more important than now (during/post COVID-19 pandemic). In 2020, we experienced a global shift to remote work and many businesses had to adopt new technologies to facilitate this remote operation. With this change, there was, not only, the increased risk of exposure to new types of cyber attacks but also, a lot of questions around how we should deal with these attacks. In particular, how do we present and visualise these new uncertainties and risks to ensure more heightened cyber security awareness. This paper focuses on the use of lines and in particular how the advancement in the aesthetic of the line could afford enhanced cyber security awareness. The results from a large study showed the influence of design element colour and design principle emphasis to portray intuitive visual warnings of uncertainty. Moreover, we found that the use of unanticipated colours paired with aesthetic qualities can afford a stronger impression of dangers and risks as opposed to those conventionally associated with danger. In terms of cyber security visualisations, these findings show that advanced line aesthetics have the power to nurture a heightened cyber security awareness. Furthermore, portraying the potential to encode further warnings and information into cyber security visualisations that employ the use of lines (i.e. force directed graphs).**

***Index Terms*—Visualisation, Cyber Security, Uncertainty, Risk**

I. Introduction

The COVID-19 pandemic has affected everyone and in terms of online security, designing for cyber security awareness has never been so important [1]. Indeed, it is a 'high-ranking national priority that is only likely to grow as we become more dependent on cyber systems' [2, p.770]. Frighteningly, it seems that in the pandemic, organisations are still less aware of the breaches and attacks that they are facing; this aligns with the fall in the proportion of organisations carrying out security monitoring and user monitoring in 2021 [3]. Without a doubt, the process of monitoring and understanding the threat landscape and then securing IT systems today still is a major challenge. The rapid growth and continued dependency on the cloud and the increasing security concerns associated with the delivery of cloud services has drawn many researchers to study cloud risks and risk assessments [4]. This paper focuses on the visualisation of these risks and uncertainties. In particular, the advancement of line aesthetics and how it can afford enhanced cyber security awareness. The following sections discuss why data visualisation is key to improving Cyber Security? It explores the visualisation of uncertainty in cyber security data and shares the main findings from a large study on peoples perceptions of the line aesthetics especially around danger and risk when modified through aesthetics.

Identify applicable funding agency here. If none, delete this.

II. Cyber Security Awareness and Data Visualisation

Data visualisation supports cybersecurity professionals in making sense of complex activities. It 'helps to comprehend and analyse large amounts of data, a fundamental necessity for network security due to the large volume of audits traces produced each day' [5, p.70]. The main consideration here is that it is not only the technical but also the human factors (i.e. human-centered issues in cyber operations) that need to be catered for in the visualisation to ensure a complete analysis of the network, the threat and/ or the situation.

According to Kasprzak et al. [6, p.1], security situational awareness is a crucial building block in order to estimate security level of systems and how 'to decide how to protect networked systems from cyber attacks'. This 'cyber situational awareness includes awareness of, e.g., any kind of suspicious/interesting activity taking place in cyberspace, where cyberspace includes any kind of computer network-related activity' [7, p.20]. However, the challenge lies not only in the detection, collection and analysis of suspicious/ interesting data but also how we visualise and share it. While many approaches have been designed and developed to investigate data analysis, data visualisation, data collection and management, the impact of Big Data exploration is still under-estimated [8]. For example, visualisation techniques are widely used to present information about the dynamics of network traffic, but they often still fail to represent the events in an understandable way [9]. As Zhou et al. [10, p339] highlight 'in reality they (security requirements) are every so often to be overlooked

due to the lack of expertise and technical approach to capture and model these requirements in an effective way'. Moreover, cyber security visualisations lack a thorough characterisation of the human-centred design problems and a critical analysis of the state-of-the-art solutions that exist for addressing these problems [11]. In general, human users can be easily overwhelmed by the high volume of Web data [12]. As a result, cyber security professionals need new and more effective ways to visualise cyber security data in order to provide a complete awareness and understanding of the cyber security landscape that they are working within. The need for 'embedding collaborative visualisation in cybersecurity systems are on the rise not only because intelligent visual data displays facilitate the highest possible situation awareness transmitted from the computer to the human but also as it provides the opportunity of collaboration with other experts in a timely manner' [13, p.1]. Despite these valuable innovations around how we might create new and novel visualisation experiences. This paper, particularly, is interested in the existing (and frequently used) line based graphs and how this could be further extended to afford more insightful visualisations around cyber security uncertainty and risk.

A. How to improve Cyber Security awareness?

In their paper, Grégoire et al. [14] raise fundamental questions pertaining to the integration of information and its presentation to the user. There are many ways for a cyber security professional to look at their data, however, in practice many organisations still depend on the tried and tested graph visualisations. For example, Tharani et al. [15] discuss how the visualisation of graphs can reflect the anomalies and patterns of fraudulent activities. The question perhaps is how effective these visualisations really are? As Maier et al. [16, p.1] note, data visualisation via dashboards can help the understanding of this cyber security data, however, 'it is not always straightforward due to difficulty for potential dashboard users to correctly interpret the displayed information'. Indeed, these dashboards can show simple counts, bar charts, line graphs and histograms of users and computers seen over time. However, are these visualisations as effective as they could be? In terms of cyber situational awareness, it should be about providing a deep insightful understanding of the cyber security situation. As Grégoire et al. [14, p.1] emphasise that 'situational awareness is essential for decision makers to efficiently manage their resources'. The authors of this paper ask, how can we do this (e.g. heighten cyber security awareness) with a line based graph?

III. Visualising Uncertainty in Data

Uncertainty is not a new concept and especially not when considering both physical and cyber. Generally visualising uncertainty can be categorised as a visualisation designer acknowledging and depicting data points as not a true representation and implementing methods to display the variations [17]. Similarly in the context of cyber security uncertainty is depicted as "imprecise and limited knowledge about attack possibilities" [18, p.52]. The authors classify the visualisation of uncertain information in both contexts (general visualisation and cyber security visualisation), as portraying an additional dimension to a visualisation to depict areas such as impreciseness, prediction and entirety of data sets. Similarly, research has shown the main causes of uncertainty can be a result of accuracy, precision, credibility, experimental and completeness [19] [20].

Visualising uncertain data can introduce a number of challenges such as that "uncertainty is naturally a challenge that all cyber-security managers face when they have to make decisions" [21]. Whilst this is not a surprise as uncertainty can influence thinking and emotions responses [22], we must also consider the method we use to depict the uncertainty as it may introduce further doubt or uncertainty to an already confusing decision process [23]. Often uncertainty is not visualised due to concerns surrounding the visualisation method, the concern of increasing complexity and the question of the necessity of depicting uncertain information. Furthermore, many existing methods of visualising uncertainty require a degree of background knowledge to interpret correctly [17]. More generally, research shows that people stimulate negative outcomes as a response to uncertainty [24]. With all this in mind, it raises the question of how can we create intuitive but effective visual depictions of uncertainty and risk that add value not complexity. In order to assess the requirements of depicting uncertainty, we must first explore the existing uncertainty and risks associated to cyber security and cyber awareness.

A. Risk and Uncertainty in Cyber Security

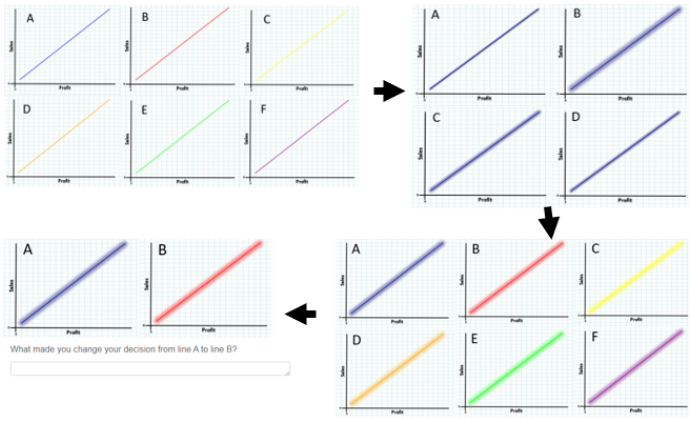
Firstly, we must be able to differentiate between uncertainty and risk. In the context of decision making a risk can be categorised as when outcomes and their probabilities are known, whilst uncertainty relates to situations when such information is not available [25]. In the context of cyber security, risks are presented more generally. A risk may be associated with situations/beings that may pose a threat to a businesses IT infrastructure. Moreover, cyber criminals, hackers, hacktivists and employee misuse can constitute to a cyber security risk [26]. Others have associated risk with not the proposed threat, but instead associating risk with the resulting impact in the occurrence of the threat [27]. In order to minimise the impact of risks in cyber security, many organisations conduct risk assessments. A risk assessment is an important part of business operations to identify, quantify and prioritise risks in accordance with a risk acceptance level [28]. As risk can be grouped dependant on the known probabilities, it provides the opportunity to continually asses and evaluate the threat a risk poses [29].In terms of cyber security, uncertainty can be an integral part of risk. In the following sections, we explore how we can visualise this uncertainty as a way to enhance cyber security awareness.

IV. Study

This study was conducted by Cardiff Metropolitan University between the 11th August 2021 until the 14th August

2021. The study was designed to evaluate how we can effectively render an aesthetic through the use of line, colour and emphasis to present a heightened impression of risk and uncertainty. The line graph was selected as it is a popular choice for temporal data sets [30]. Furthermore, research has displayed how the use of lines in real-time monitoring tools for cyber attacks have utilised lines [31]. The questionnaire was designed with a strong visual perspective to test a participant's response when presented with intuitive representations of uncertainty/ risk. During the time the questionnaire was live, there were one thousand one hundred and forty two fully completed responses gathered. Responses were gathered through an external third party company Dynata, who was used to distribute the questionnaire. Dynata's circulation of the questionnaire utilised a random sampling method in order to gather a diverse participant portfolio. The only restriction on the participant was the requirement to be over the age of eighteen. Any participant failing to meet this requirement was averted to an ending screen. Of those who completed the questionnaire there were 532 male, 604 female, 3 non-binary and 3 prefer not to say. The participants all resided in the United Kingdom

Fig. 1. Step-by-step process of participants path through a question section



The questionnaire was designed to take participants through a step-by-step process in which their answers would influence the subsequent questions. The example shown in Fig.1 displays a participant's journey through a particular set of questions. Firstly, the participant would be shown all colours (blue, red, yellow, orange, green, and purple) (using a 2pt line), the participant would then be asked to decide which coloured line emitted the most uncertainty. Once selected, the participant would then be presented with their chosen colour (for instance, blue), but now combined with the design principle emphasis to compose the aesthetic. There are four degrees of emphasis applied to the line 5pt, 8pt, 11pt and 18pt. Once again, the participant would be asked which line was most uncertain. When selected, the participant would then be presented back to all the colours but this time with the same degree of emphasis applied to all (for instance all with 18pt emphasis). This stage in the questioning was to test if the added aesthetic dimension influenced the participant to change their decision on which line was the most uncertain. If the participant changed their initial decision (for instance to red), they would then be prompted to explain their reasoning for switching. If the decision remained the same as original, they would then be asked why this colour with combined degree of emphasis portrayed the most uncertainty

V. Findings Discussion

The findings show that when participants were asked what colour was ranked as eliciting the most uncertainty, both yellow (22 percent of participants - 249 participants) and red (21.5 percent of participants - 246 participants) were ranked as the most uncertain colours. These were followed by blue (221 participants), green (167 participants), orange (130 participants) and lastly purple with 11 percent of participants (129 participants) ranking it as the least uncertain colour. On reviewing the initial rankings for the most uncertain colour, it was clear that no one colour stood out as taking the majority vote for being the most uncertain. However, when applying the design principle emphasis there were a clear shift in participants decisions. When participants were exposed to their selected colour with varying degrees of emphasis (5pt, 8pt, 11pt and 18pt), 57 percent selected the 18pt as the most uncertain, followed by 5pt with 24 percent and finally 8pt and 11pt with 9.5 percent each. Of the 495 participants selecting red and yellow as the most uncertain, 59 percent went on to select the colour with 18pt emphasis as the most uncertain.

Fig. 2. Word-cloud participants red vs yellow 18pt emphasis

Fig.2 displays the most common key words participants expressed when asked why the red or yellow colour with 18pt emphasis was the most uncertain. It is apparent that those who selected red very much focused on feelings of risk and uncertainty, as expected from existing research that red can be used as a danger cue in communication [30]. Whilst those participants who expressed the yellow as most uncertain indicated it was more because of it's visual appearance. Whilst red is commonly associated with uncertainty, risk and danger, the yellow line was intrinsically evoking an uncertain impression from its 'indistinguishable' and 'faint' appearance. Interestingly, when exploring the red line with the lowest level of emphasis (5pt), 100 percent of participant's comments still only associated the uncertainty with the red colour. Whilst the yellow at 5pt emphasis had comments that strongly expressed that the uncertainty was caused by a weak and faintly presented line.

VI. Conclusions

This research has shown us that aesthetic rendering of uncertainty through colour and dimensions could play an important role for the presentation of cyber security uncertainties and risks. In this study we documented the influence of line graph colours with the design principle emphasis to elicit an aesthetic response. By evaluating the responses from test participants, we can determine that certain combinations of colour and emphasis trigger feelings of danger and risk more than others. As anticipated, we have seen that the colour red continues to provoke thoughts and feelings of danger and fear. Nevertheless, we have also uncovered how perceptions of colours such as yellow could be used to influence participants feelings around risk and uncertainty when combined with the aesthetic dimension emphasis. As we can see from fig.2, the colour yellow has afforded thoughts and feelings such as: "indistinguishable", "vagueness" and "unclear". By exploring different combinations of colour and emphasis, the study has unearthed this new aesthetic arrangement which may be used independently and/ or alongside the traditional red, orange, green visual encodings of colour to afford risk and uncertainty. Indeed, it has demonstrated that the depiction of uncertain data can be extended further through the strategic combination of certain design elements and principles. In detail, the combination of colour and emphasis can provide further avenues to enrich warnings but ultimately increase our ability to promote intuitive cyber security awareness. In doing so, it has highlighted how we can aesthetically render graphic depictions of uncertainty in cyber security to ensure a heightened and more widespread awareness of possible dangers and risk.

VII. Future work

Going forth, we feel there may be more opportunities for the aesthetic to strengthen the understanding of uncertainty visualisation in the cyber security field. This study is part of a bigger research project which is exploring the aesthetic depictions of uncertainty in a general sense.. The authors feel there is an opportunity to further evaluate uncertain data specifically in the context of cyber security. For instance, further expanding on the findings described in this study with a specific user-task analysis (such as visual warnings and fore directed graphs). By focusing on cyber security data, the authors will be able to understand if the same combinations of colour and emphasis elicit similar responses when considering a new context/scenario. Furthermore, currently in development is an interactive framework to support visualisation designers design for uncertainty in their data. This could hold potential for further cyber security awareness research. For example, the combination of textured lines with aesthetic qualities (i.e., movement and scale), showing a broken line over time could be explored to present connections that are lost or suspicious.

VIII. Acknowledgment

Supported by Knowledge Economy Skills Scholarships 2 (KESS2) which is an All Wales higher-level skills initiative led by Bangor University on behalf of the HE sectors in Wales. It is part-funded by the Welsh Government's European Social Fund (ESF) competitiveness programme for East Wales.

References

[1] F. Carroll, P. Legg, and B. Bonkel, "The visual design of network data to enhance cyber security awareness of the everyday internet user," 2020.
[2] A. Vieane, G. Funke, R. Gutzwiller, V. Mancuso, B. Sawyer, and C. Wickens, "Addressing human factors gaps in cyber defense," 2016.
[3] E. Johns, "Cyber security breaches survey 2021: Statistical release," 2021.
[4] S. New, A. Martin, and O. Akinrolabu, "Cyber supply chain risks in cloud computing – bridging the risk assessment gap," *Open Journal of Cloud Computing*, vol. 5, 2017.
[5] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "An evaluation framework for network security visualizations," *Computers and Security*, vol. 84, 2019.
[6] W. Kasprzak, W. Szynkiewicz, M. Stefaczyk, W. Dudek, M. Wagierek, D. Seredyski, M. Figat, and C. Zieliski, "Agent-based approach to the design of a multimodal interface for cyber-security event visualisation control," *Bulletin of the Polish Academy of Sciences: Technical Sciences*, vol. 68, 2020.
[7] U. Franke and J. Brynielsson, "Cyber situational awareness - a systematic review of the literature," *Computers and Security*, vol. 46, pp. 18–31, 2014.
[8] A. Bagozi, D. Bianchini, V. D. Antonellis, A. Marini, and D. Ragazzi, "Summarisation and relevance evaluation techniques for big data exploration: The smart factory case study," vol. 10253 LNCS, 2017.
[9] M. Debashi and P. Vickers, "Interactive sonification of network traffic to support cyber security situational awareness," 2018.
[10] B. Zhou, C. Maines, S. Tang, and Q. Shi, "A framework for the visualisation of cyber security requirements and its application in bpmn," 2018.
[11] A. Dasgupta, D. L. Arendt, L. R. Franklin, P. C. Wong, and K. A. Cook, "Human factors in streaming data analysis: Challenges and opportunities for information visualization," *Computer Graphics Forum*, vol. 37, 2018.
[12] T. T. Nguyên, "Debunking misinformation on the web: Detection, validation, and visualisation," 2019.
[13] S. Mihindu and F. Khosrow-Shahi, "Collaborative visualisation embedded cost-efficient, virtualised cyber security operations centre," vol. 2020-September, 2020.
[14] M. Grégoire, "Visualisation for network situational awareness in computer network defence," *Visualisation and the Common Operational Picture*, 2005.
[15] J. S. Tharani, E. Y. A. Charles, Z. Hou, M. Palaniswami, and V. Muthukkumarasamy, "Graph based visualisation techniques for analysis of blockchain transactions," vol. 2021-October, 2021.
[16] J. Maier, A. Padmos, M. S. Bargh, and W. Wörndl, "Influence of mental models on the design of cyber security dashboards," vol. 3, 2017.
[17] C. O.Wilke, *Fundamentals of Data Visualization*. O'Reilly Media, 2019.
[18] S. Jajodia, P. Liu, V. Swarup, and C. Wang, "Cyber situational awareness: Issues and research," *Advances in Information Security*, vol. 46, pp. 51–68, 2010.
[19] P. Levontin, J. L. Walton, L. Aufegger, and M. J. Barons, *Visualising Uncertainty : A short introduction*, 2020, no. January.
[20] J. Chung and S. Wark, "Visualising Uncertainty for Decision Support," p. 49, 2016.
[21] A. Fielder, S. König, E. Panaousis, S. Schauer, and S. Rass, "Risk assessment uncertainties in cybersecurity investments," *Games*, vol. 9, no. 2, pp. 1–14, 2018.
[22] A. Danczak and A. Lea, "The psychology of uncertainty in difficult decisions," vol. 10, no. 8, pp. 466–472, 2017.
[23] L. Padilla, M. Kay, and J. Hullman, "Uncertainty Visualizations," *Journal of Cognitive Engineering and Decision Making*, vol. 6, no. 1, pp. 30–56, 2020.
[24] E. C. Anderson, R. N. Carleton, M. Diefenbach, P. K. J. Han, and E. C. Anderson, "The Relationship Between Uncertainty and Affect," vol. 10, no. November, 2019.
[25] K. Park and A. Shapira, "Risk and Uncertainty," in *The Palgrave Encylopedia of Strategic Management*, M. Augier and D. Teece, Eds. London: Palgrave Macmillan, 2017.

[26] NCSC, "CYBER SECURITY AND RISK MANAGEMENT An Executive level responsibility Cyberspace poses risks as well as opportunities," National Cyber Security Centre, United Kingdom, Tech. Rep., 2013.
[27] CSA, "GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE," Cyber Security Agency, Singapore, Tech. Rep. December, 2019.
[28] I. Kuzminykh, B. Ghita, V. Sokolov, and T. Bakhshi, "Information Security Risk Assessment," pp. 602–617, 2021.
[29] Z. Baig and S. Zeadally, "Cyber-security risk assessment framework for critical infrastructures," vol. 25, no. 1, pp. 121–129, 2015.
[30] W. Javed, S. Member, B. Mcdonnel, S. Member, and N. Elmqvist, "Graphical Perception of Multiple Time Series," *IEEE Trans Vis Comput Graph*, vol. 16, no. November, pp. 927–934, 2010.
[31] M. Baykara, U. Gurturk, and R. Das, "An overview of monitoring tools for real-time cyber- attacks," in *6th International Symposium on Digital Forensic and Security (ISDFS)*, no. August, 2018, pp. 1–7.