Human–Computer Interaction considerations when developing cyber ranges

Lynsay A. Shepherd
Stefano De Paoli
Jim Conacher

This is the authors' accepted manuscript of a paper published in International Journal of Information Security and Cybercrime:

Shepherd, L.A., De Paoli, S. & Conacher, J. (2020) 'Human–Computer Interaction considerations when developing cyber ranges'. *International Journal of Information Security and Cybercrime*, 9(2): pp. 28-32. DOI: https://doi.org/10.19107/IJISC.2020.02.04

The final publication is available at www.ijisc.com

Human-Computer Interaction Considerations When Developing Cyber Ranges

Lynsay A. Shepherd[1][0000−0002−1082−1174], Stefano De Paoli[2][0000−0003−1120−4773], and Jim Conacher[1][0000−0002−5712−0148]

[1] School of Design and Informatics, Abertay University, Dundee, United Kingdom
[2] School of Business, Law and Social Sciences, Abertay University, Dundee, United Kingdom
{lynsay.shepherd, s.depaoli, j.conacher}@abertay.ac.uk

Abstract. Cyber-attacks are continuing to rise globally. It is therefore vital for organisations to develop the necessary skills to secure their assets and to protect critical national infrastructure. In this short paper, we outline human-computer interaction elements which should be considered when developing a cybersecurity training platform, in an effort to maintain levels of user engagement. We provide an overview of existing training platforms before covering specialist cyber ranges. Aspects of human-computer interaction are explored with regards to their relevance in the context of cyber ranges. We conclude with design suggestions when developing a cyber range platform.

Keywords: Cybersecurity · Security Awareness · Cyber Range · Human-Computer Interaction · Cybersecurity Education.

1 Introduction and Background

In the field of cybersecurity, there is a growing interest in the design, development, and deployment of training platforms such as cyber ranges which can supplement and improve security professionals' skills. In this short paper, we aim to present an overview of existing cybersecurity training platforms, alongside a brief discussion of Human-Computer Interaction (HCI) elements which should be considered when developing a specialised cyber range platform. We then offer guidance for improving and maintaining user engagement with these platforms through consideration of appropriate HCI techniques.

1.1 Human-Computer Interaction (HCI)

HCI is a broad field which initially focused on a combination of human factors engineering and cognitive science [3]. It continues to link in with interaction design, ergonomics, informatics, and psychology. HCI plays a vital role in cybersecurity (e.g. usable security). Though HCI is linked to a number of fields and communities, the overarching goal is the *"linkage of critical analysis of usability, broadly understood, with development of novel technology and applications"* [3].

1.2 Cybersecurity Training Platforms

Training platforms are directly connected with the learning experience of the user; therefore, the user interface plays an essential role in both supporting learning pathways and keeping the users aware of the underlying processes simulated by the training platform. Cybersecurity training platforms have been used in a number of domains. Examples of such training platforms include Immersive Labs Human Cyber Readiness Platform [12], and Secure Code Warrior [24]. Further examples can be found in Table 1.

1.3 Cyber Ranges

Cyber ranges can be defined as *"interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment"* [20], and are a specific type of training platform created for security professionals. They are typically composed of a virtual network environment and allow for the creation of simulated cyber-attack scenarios and incident response exercises. There is a growing need for training platforms such as cyber ranges. Owing to the sustained increase in cyber-attacks experienced by organizations around the World (particularly in the wake of the COVID-19 pandemic [15]), continually enhancing the cybersecurity resilience of such organizations is essential to ensure critical infrastructure remains protected.

Existing cyber ranges encompass a variety of areas, but they have generally been created for military, research and commercial purposes (Table 1). Cyber ranges are a developing area for research e.g. the European Commission's H2020 Digital Security programme has funded platforms such as FORESIGHT [9].

Name	**Year**	**Description**	**Ref.**
US DoD Cyber Security Range	2009*	Cyber range, for military use.	[18]
ENISA Cyber Europe	2010	Training platform. Public/private sectors.	[8]
Secure Code Warrior	2015	Training platform targeting developers.	[24]
OutThink	2015	Training platform targeting organisations.	[21]
IBM Cyber Range	2016	Cyber range (commercial) for organisations.	[11]
Immersive Labs Human Cyber Readiness Platform	2017	Training platform targeting organisations.	[12]
AIT Cyber Range	2017	Cyber range (academic) targeting industry, research and government.	[1]
SecDevOps Cyber Range	2019	Cyber range (open-source, academic).	[23]
FORESIGHT	2019*	Cyber range linking aviation, smart grid and naval domains.	[9]
CyberEDU.ro	2020	Training platform for the wider infosec community.	[6]

Table 1: Summary of training platforms and cyber ranges (* indicates year development started).

2 Discussion

To ensure cyber ranges deliver an appropriate user experience in the context of an educational platform, we present design recommendations which aim to improve knowledge acquisition and maintain a high level of user engagement.

2.1 HCI and Cyber Ranges

Although human-computer interaction is a large field, there are some key areas which are appropriate in the context of the cyber ranges. This is not an exhaustive list of all applicable elements, but an overview of perhaps the most important aspects. The areas mentioned offer the possibility of keeping the user engaged in the context of a cybersecurity training platform.

User Interface (UI) The role of interface design in helping users learn has been explored in the context of e-learning. Work by Guralnick [10] highlights key factors in user interface design which aid the user. These include the layout of elements on-screen (to guide the users' eye to look at the relevant information), consideration of learner paths to help the user stay focused, and well-presented guidance on-screen to provide the user with feedback.

Crucially, if the UI is difficult to navigate, the user will become frustrated, and this will detract from the learning process. Existing cyber ranges such as the Kypo cyber range [4] considered the role of the UI, and have utilised a portal based on Liferay Portals [17] to ensure users of all abilities can interact with the system. Developers should consider building upon existing frameworks to provide a suitable UI for a cyber range.

Visualization Information visualization has proved successful in supporting learning [14]. Developers should consider deploying the use of user-centred design methods when creating visualisations in the cybersecurity domain [19]. Many examples of cybersecurity visualisations already exist, including Kaspersky Cyber Threat map [13] and the Talos Spam and Malware Map [25]. Such tools could be incorporated into a cyber range to help the user assess the impact of potential threats e.g. identifying the source of a DDOS attack.

Design Patterns Design patterns are design solutions to resolve common problems in software development. These can utilise theories of motivation [p3] [16] to create an engaging educational platform. Additionally, these patterns can be designed to be gameful, linking in with section 2.1 of this paper. Gameful design patterns can incorporate some of the elements which are used in gamification, such as badges and leaderboards. Gameful design patterns are particularly well-suited to applications with *"heavy simulation elements that the user should explore"* [p34] [16] - cyber ranges fall into this category.

Gamification Gamification involves the use of gaming mechanics in traditionally non-gaming environments [26]. Duolingo is a popular application which uses a combination of gamification elements such as learning paths, points, badges, scores, and leaderboards to help users learn new languages [7].

Gamification has been used in several cybersecurity training platforms and thus can be applied to cyber ranges. Existing cybersecurity work which has utilised gamification includes prototype mobile applications aimed at raising public security awareness [22]. Furthermore, it has also been suggested for use in cyber defence training [2], and used to tackle threats against critical national infrastructure [5]. Gamification will be deployed within FORESIGHT [9].

3 Conclusion

In this paper, we have provided an overview of existing cybersecurity training platforms, and have highlighted the developing field of cyber ranges. We have also outlined aspects of HCI which may help the end-user remain engaged with the platform, supporting learning and consolidating knowledge gained. We hope that developers of cyber ranges will take these elements of human-computer interaction into consideration, creating an engaging cybersecurity platform.

Acknowledgements

The authors would like to acknowledge the FORESIGHT project funded by the European Union's Horizon 2020 research and innovation programme (grant agreement: 833673), and the partners on the project.

References

1. AIT: Cyber range & training (2020), https://www.ait.ac.at/en/research-topics/cyber-security/cyber-range-training/ (Accessed 1 July 2020)
2. Amorim, J.A., Hendrix, M., Andler, S.F., Gustavsson, P.M.: Gamified training for cyber defence: Methods and automated tools for situation and threat assessment. In: NATO Modelling and Simulation Group (MSG) Annual Conference 2013 (MSG-111), 2013 (2013)
3. Carroll, J.M.: Human computer interaction (hci). In: The Encyclopedia of Human-Computer Interaction, 2nd Edition, chap. 2, pp. 21–62. The Interaction Design Foundation (2013)
4. Čeleda, P., Čegan, J., Vykopal, J., Tovarňák, D.: Kypo–a platform for cyber defence exercises. M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization (2015)
5. Cook, A., Smith, R., Maglaras, L., Janicke, H.: Using gamification to raise awareness of cyber threats to critical national infrastructure. In: 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR). BCS (2016)
6. CyberEDU: CTF Cyber Security Challenges Online Platform (2019), https://cyberedu.ro/ (Accessed 12 July 2020)

7. Duolingo: Duolingo (2020), https://www.duolingo.com/ (Accessed 1 July 2020)
8. ENISA: Cyber Europe 2020 (2020), https://www.cyber-europe.eu (Accessed 12 July 2020)
9. FORESIGHT: Foresight - advanced cyber-security simulation platform for preparedness training in aviation, naval and power-grid environments (2019), https://foresight-h2020.eu/ (Accessed 30 June 2020)
10. Guralnick, D.A.: User interface design for effective, engaging e-learning. In: Proceedings of the International Conference on E-learning. pp. 22–23. Citeseer (2006)
11. IBM: X-force command cyber tactical operations center (2020), https://www.ibm.com/security/services/managed-security-services/xforce-command-cyber-tactical-operations-center (Accessed 1 July 2020)
12. Immersive Labs: The human cyber readiness platform (2020), https://www.immersivelabs.com/product/benefits/equip-cyber-workforce (Accessed 1 July 2020)
13. Kaspersky: Cyber Threat Real-Time Map (2020), https://cybermap.kaspersky.com/ (Accessed 1 July 2020)
14. Klerkx, J., Verbert, K., Duval, E.: Enhancing learning with visualization techniques. In: Handbook of research on educational communications and technology, pp. 791–807. Springer (2014)
15. Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X.: Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. arXiv preprint arXiv:2006.11929 (2020)
16. Lewis, C.: Irresistible Apps: Motivational design patterns for apps, games, and web-based communities. Springer (2014)
17. Liferay: Liferay DXP for Portals (no date), https://www.liferay.com/download-features/l/portal (Accessed 1 July 2020)
18. Marines- The official website of the United States Marine Corps: DoD Cyber Security Range (2020), https://www.hqmc.marines.mil/doccsr/ (Accessed 1 July 2020)
19. McKenna, S., Staheli, D., Meyer, M.: Unlocking user-centered design methods for building cyber security visualizations. In: 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). pp. 1–8. IEEE (2015)
20. National Institute of Standards and Technology (NIST): Cyber ranges (2018), https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf (Accessed 30 June 2020)
21. OutThink: Cyber Security by CISOs, for CISOs (2020), https://outthink.io/ (Accessed 12 July 2020)
22. Scholefield, S., Shepherd, L.A.: Gamification techniques for raising cyber security awareness. In: Moallem, A. (ed.) HCI for Cybersecurity, Privacy and Trust. HCII 2019., Lecture Notes in Computer Science, vol. 11594, pp. 191–203. Springer, Cham (2019)
23. SecDevOps@Cuse: The Open-Source AWS Cyber Range (2019), https://github.com/secdevops-cuse/CyberRange (Accessed 12 July 2020)
24. Secure Code Warrior: Secure your Code, From the Start (2020), https://securecodewarrior.com/ (Accessed 12 July 2020)
25. Talos: Cyber Attack Map (2020), https://talosintelligence.com/fullpage_maps/pulse (Accessed 1 July 2020)
26. Tondello, G.F.: An introduction to gamification in human-computer interaction. XRDS: Crossroads, The ACM Magazine for Students **23**(1), 15–17 (2016)