Representing a Human-Centric Cyberspace

Phoebe M Asquith[1,2*] and Phillip L Morgan[1,2]

[1] Airbus, The Quadrant, Celtic Springs Business Park, Newport, NP10 8FZ, UK
[2] School of Psychology, 70 Park Place, Cardiff University, Cardiff, CF10 3AT
{phillip.morgan.external, phoebe.p.asquith.external}@airbus.com

Abstract. There is a lack of consensus when using the term "cyberspace" [1]. Computers and network devices are prominent in definitions of cyberspace; less common is the essential and inclusion of human users. However, the human user is both implicitly integral to and actively part of the cyberspace.

Cyberspace is often conceptualized as three layers of interconnected networks: social, information and geospatial (physical) [2]. These represent an indirect human element within cyberspace. This is characteristic of related fields, such as cybersecurity, where human-centered research has been lagging behind technological aspects. A model that incorporates the human user in cyberspace is needed to direct future research and improve security and usability (navigation).

A new human-centric model of cyberspace is proposed (the HCCM), with the user as a physical and integral entity, together with recognition of the cognitive representation of cyberspace. It focuses on boundaries and transformation points between objects and spaces and offers a platform for future human-centric research in cybersecurity.

Keywords: Cybersecurity · Cyber security · Human user · Human Factors · Human-machine interaction

1 Introduction

Metaphors and analogies, such as "wild west" and "space", have been central to attempts to understand the global online computer network and its meaning for society and culture broadly [3]. The term "cyberspace" was first used by William Gibson in his book, Neuromancer [4], where he defined it as a "a consensual hallucination". Since then, although the term "cyberspace" is commonly used, there is a lack of consensus about its meaning and what it encapsulates [1] [5]. It is difficult to represent and model cyberspace, due to its associations across physical (e.g. computer hardware) and non-physical domains (e.g., 'information' or 'online' space).

Although computers and network devices are prominent in current common definitions, less common is the inclusion of human users. Cyberspace has been described

within dictionary[1] and literary sources with themes such as "communication", "virtual", "electronic", "network" and "computer" [5] [6] [7]. Kautz [8] identifies hardware and software as "universals" within cyberspace, and computers and computer networks as preconditions for cyberspace. We strongly assert that humans (e.g., system / computer / network users) are also preconditions for cyberspace: the human user is both implicitly integral to the creation of cyberspace and actively part of the cyberspace.

The presence of human-human connections and "communities" within the virtual space is widely acknowledged in research literature and common understanding [9]. Popular social media sites have billions of active users across the globe sharing information (for example Facebook, which had ~2.45 billion monthly active users in 2019 [10]). Information transferred from human cognitive and physical space into the digital realm has been conceptualized as an extension of the self within the virtual space [11] [12] [13]. Implications of human actions within cyberspace in law are becoming more widely discussed [14], and language (a human faculty) is mapped in cyberspace [15]. Models of risk within cybersecurity also include the interaction between humans and technology [16]. Despite this, the human user has not often been included within dynamic models of cyberspace. Crucially, a clearer model of the importance of the human user in cyberspace is needed, to direct future research and improve the security and usability (navigation) of cyberspace. A key aim of the current paper is to provide the structure of such a model, that we aim to develop further.

The "cyberspace" concept relies on a cognitive representation of a "space" within which information is shared. Human interactions with online devices provide a "window" into this virtual space. If humans are not integral to cyberspace:

a) The technology itself would not exist;
b) [Putting aside the human creation and development] All systems would need to be fully autonomous;
c) Large aspects of data movement would be neglected;
d) Signals would be reduced to binary connections with no "space" conceived.

Cyberspace has traditionally been modelled as having three layers of interconnected networks; geospace (physical), infospace (logical and virtual) and sociospace (social and political) [2] [1]. A cyber-physical system (CPS) facilitates the information communication across the three layers. The movement of information ultimately affects outcomes and decisions at sociospatial endpoints. For example, one model, based on cybernetics – "the scientific study of control and communication in the human and the machine" by Norbert Wiener [17], [18], identifies engineering [*geospace*] and software [*infospace*] aspects of machines in cyberspace, and, economic and socio-cultural aspects [*sociospace*] relating to human users [19]. These models represent, to some extent, a human end-point element to cyberspace, however it is an indirect role. Using models of cyberspace with individual and connected human users directly incorporated

[1] *Lexico dictionary* [32]: "The notional environment in which communication over computer networks occurs". *Collin's English Dictionary* [36]: "In computer technology, cyberspace refers to data banks and networks, considered as a place".

is crucial to help to guide research in human factors and socio-cultural aspects of cybersecurity, and beyond. For example, to embed improved cybersecurity practice within a staff culture, a multi-faceted and human-centric approach is needed [20] [21] [22].

Hai Zhuge has, for the past 10 years or so, been exploring the concept of a social-cyber-physical space and the future of a connected cyber-human world [23]. In a world with seamless cyber-human relationship, Zhuge envisaged the coming together of the Physical, Virtual and Mental [24], [25] [26]. The inclusion of 'Mental' here begins to allude to a vision of a cyberspace that can includes a cognitive element, to better direct human factors and psychological research in human-machine interaction.

The importance of human cognition in cyber-human interactions is also posited by Jinhua and colleagues [27], who describe cyberspace as a space parallel to traditional space, into which we project "simulations" of physical and social elements [28], [29], [30]. This is a useful concept, as it acknowledges humans as the creators of this projection, and places them as prerequisites to cyberspace. This is also key when directing research in the usability of systems and architecture.

A network model created by Hao et.al. [31] places humans as integral to activity within cyberspace and aims to help with analyzing threats in the cyberspace. The inclusion of humans is crucial to this process and with improving defence within cybersecurity; human error plays a major role in cyber-breaches [32] . This model begins to explore the importance of humans within the cyberspace, but does not fully address the interaction between humans and the physical or information space.

Each of these models has made important developments in conceptualizing a cyberspace that helps to guide research in the area. A new model of cyberspace is presented below, that brings together some of these ideas, to provide a more human-centric model. A network representation from the physical, cognitive and social human user, to the physical device and virtual spaces will help guide research in fields such as cybersecurity

2 A new model of cyberspace

Our new Human-Centric Cyberspace Model (HCCM) includes various novel concepts:

- The user as a physical and cognitive entity;
- The user as integral within cyberspace;
- The cognitive representation of cyberspace;
- A focus on boundaries and transformation of information between elements.

The new HCCM identifies humans, devices and systems as the key objects within cyberspace. Information is transferred between humans and systems through the use of devices that have hardware and software elements. Humans and systems are connected through a network of activity, which is dynamic and is driven by the goals of human users and architects. Within the HCCM, "cyberspace" is the cognitive representation of this activity space.

Human users exist in the physical space, interacting with physical devices. The physical human applies perceptual (e.g., seeing information, attending to information) and cog-

nitive (e.g., decision-making, judgment, reasoning) abilities that process the information presented via a device (e.g., the human-machine interface / HMI). "Social" or "cultural" aspects are also important manifestations within cyberspace: they are projections and representations created by human users, which are reliant on cognitive and perceptual processes (see **Fig 1**). Data transferred between systems is within the "infospatial" (not physical) space. The connected infospace is reliant on software, which in turn is reliant on hardware for function (see **Fig 1**).

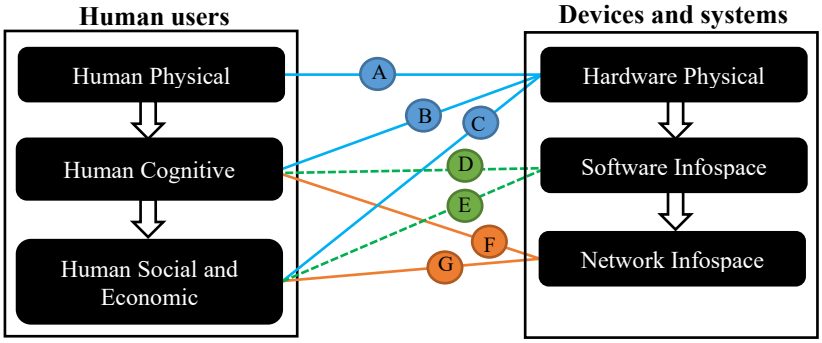

Fig 1. A human centered cyberspace model, to be used as a high-level tool to guide cyber research: see *Table 1* for suggested research areas based on connections.

Each of the levels in the human and machine aspects of cyberspace have important interactions across the human-system/machine boundaries (see **Fig 1**). Mapping these connections and boundaries can guide research concerning humans within cyberspace such as human-machine interaction and human-centered cybersecurity (see **Table *1***).

Table 1. Research areas identified using connections between elements of the HCCS.

	Description/Key Questions	Example research areas
A	Human users interacting with physical devices. How does design the of devices affect human usage?	Human-machine interaction; Human factors; Usability of hardware.
B	Humans processing information received on physical devices e.g. visualization techniques, nudges. How can hardware support decision-making and improve efficiency?	Human-machine interaction; Human factors; Usability; Decision-making.
C	Hardware availability across different cohorts. How does this technology support economic and social projections? How do technologies interact with multiple users across different cultures?	Inclusion; Technological advances.
D	Human interaction with software technologies. How does software support cognitive processes to achieve goals?	Cognition; Decision making.
E	Software availability across different cohorts. How does software support economic and social projections? How does interact with multiple users across different cultures and support shared goals?	Inclusion; Technological advances.

F	How does network architecture support human use and decision-making? How do humans represent a connected information space?	Cognition; Human-machine teaming; Decision-making.
G	How do connected networks support economic and social projections? How does a connected network interact with multiple users across different cultures and support shared goals?	Digital communications; Socio-economics; Policy and borders.

Each of the connections indicates an area of research that can be further broken down into research modules, inspiring topics and human factors guided research; an area that has been lagging behind a technological focus in areas such as cybersecurity. This model can aid with preventative management of cyber threats within a human-machine connected cyberspace by turning the risk of human error into an opportunity for research and improvement and by crucially including human-users in the planned solution [33].

Conclusion

Within the current paper, we highlight the lack of research and associated literature that models and considers humans as integral within cyberspace. Drawing upon some recent examples where humans have been considered to some extent [2] [19] [25] [27] [31] *and* through consideration of human physicality, cognitive abilities (e.g., perception, attention, thinking) and human social and economic factors, we have developed and present the first version of the HCCM. With humans included within conceptualizations of cyberspace, the model allows for important considerations to be recognized as areas for research investigation within the field of human-centric cybersecurity, and beyond. Next steps will involve further developing this high-level model to a more specific cyberspace concept and research guide.

Acknowledgments. Endeavr Wales for funding projects underpinning this work and Cardiff University for supporting this work.

References

[1] A. M. A. Kademi and A. Koltuksuz, “Formal Characterization of Cyberspace for Cyber Lexicon Development,” *ECCWS 2017 16th European Conference on Cyber Warfare and Security,* p. 200 (2017)

[2] J. Bayne, "Cyberspatial mechanics," *IEEE Transactions on Systems, Man, and Cybernetics, Part B ,* vol. 38, no. 3, pp. 629-644 (2008).

[3] R. Johnston, "Salvation or destruction: Metaphors of the Internet.," *First Monday,* vol. 14, no. 4 (2009).

[4] W. Gibson, Neuromancer, New York: Berkley Publishing group (1989).

[5] S. E. Madnick, N. Choucri, S. Camiña and W. L. Woon, "Tow(ards better understanding Cybersecurity: or are" Cyberspace" and" Cyber Space" the same?," *mit.edu* (2014).

[6] M. Mayer, L. Martino, P. Mazurier and G. Tzvetkova, "How would you define Cyberspace," *First Draft Pisa,* vol. 19 (2014).

[7] F. D. Kramer, S. H. Starr and L. K. Wentz, Cyberpower and national security., Nebraska: Potomac Books Inc. (2009).

[8] Kautz, 2010. https://www.slideshare.net/study4cyberwar/cyberspace-model. [Accessed 1 November 2019].

[9] H. Rheingold, The virtual community: Finding commection in a computerized world., Boston: Addison-Wesley Longman Publishing Co., Inc. (1993).

[10] J. Clement, "Facebook: number of monthly active users worldwide 2008-2019," Statista, 19 November 2019. [Online]. Available: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/. [Accessed 7 January 2020].

[11] M. McLuhan, Understanding media: The extensions of man., Cambridge, Massachusettes: MIT Press (1994).

[12] J. Zylinska, The cyborg experiments: The extensions of the body in the media age., London, UK: A & C Black (2002).

[13] A. &. C. D. Clark, "The extended mind.," *Analysis,* vol. 58, pp. 10-23, 1998.

[14] L. Lessig, "The zones of cyberspace.," *The Stanford Law Review,* vol. 48, p. 1403 (1995).

[15] D. &. L. H. Ivkovic, "Multilingualism in cyberspace: Conceptualising the virtual linguistic landscape.," *International Journal of Multilingualism,* vol. 6, no. 1, pp. 17-36 (2009).

[16] C. Leuprecht, D. B. Skillicorn and V. E. Tait, "Beyond the Castle Model of cyber-risk and cyber-security.," vol. 33, no. 2, pp. 250-257 (2016).

[17] N. Wiener, Cybernetics or Control and Communication in the Animal and the Machine, Cambridge, Massachusetts: MIT Press (2019).

[18] P. R. Duffy, "Cybernetics," *The Journal of Business Communication ,* vol. 21, no. 1, pp. 33-41 (1984).

[19] T. Vinnakota, "A cybernetics paradigms framework for cyberspace: Key lens to cybersecurity.," *IEEE International Conference on Computational Intelligence and Cybernetics ,* pp. 85-91 (2013).

[20] M. S. A. M. &. N. J. R. Bada, "Cyber security awareness campaigns: Why do they fail to change behaviour?," *arXiv preprint arXiv:1901.02672 (*2019).

[21] R. &. V. N. J. .. Reid, " From information security to cyber security cultures.," *Information Security for South Africa IEEE,* pp. 1-7 (2014).

[22] A. M. K. S. S. C. S. R. Tonge, "Cyber security: challenges for society-literature review.," *IOSR J. of Computer Engineering,* vol. 2, no. 12, pp. 67-75 (2013).

[23] Zhuge, Multi-dimensional summarization in cyber-physical society., Burlington, Massachusettes: Morgan Kaufmann (2016).

[24] H. Zhuge and X. Shi, "Toward the eco-grid: a harmoniously evolved interconnection environment.," *Communications of the ACM,* vol. 47, no. 9, pp. 78-83 (2004).

[25] H. Zhuge, "Future interconnection environment.," *Computer,* vol. 38, no. 4, pp. 27-33 (2005).

[26] H. Zhuge, Future interconnection environment–dream, principle, challenge and practice. In International Conference on Web-Age Information Management, Berlin, Heidelberg: Springer (2004).

[27] L. Jinhua, H. Xu, X. Zhou, F. Lin and J. An, "Research of cyberspace architecture.," *International Conference on Cyberspace Technology (CCT 2013) ,* pp. 367-369 (2013).

[28] Zhuge, "arXiv," 2018. [Online]. Available: https://arxiv.org/abs/1805.00434. [Accessed 12 December 2019].

[29] R. A. Miller and D. T. Kuehl, "Cyberspace and the" First Battle" in 21st-century War.," *Defense Horizons,* vol. 68, no. 1 (2009).

[30] C. Czosseck and K. .. Geers, "Borders in cyberspace: can sovereignty adapt to the challenges of cyber security.," *The Virtual Battlefield: Perspectives on Cyber Warfare,* vol. 3, no. 88 (2009).

[31] Y. Hao, S. Guo, H. Zhao and Z. Chen, "Study on the modeling and analyzing of the role-based threats in the cyberspace.," *IEEE 2nd International Conference on Cloud Computing and Intelligence Systems,* vol. 3, pp. 1302-1306 (2012).

[32] I. Security, "ZXForce Threat Intelligence Index," IBM Corporation, Armonk, NY (2019).

[33] D. Tàbara, D. SAURí and R. Cerdan, "Forest fire risk management and public participation in changing socioenvironmental conditions: a case study in a Mediterranean region.," *Risk Analysis: AN INTERNATIONAL JOURNAL,* vol. 23, no. 2, pp. 249-260 (2003).

[34] "Lexico," [Online]. Available: https://www.lexico.com. [Accessed 3 December 2019].

[35] "Techopedia Dictionary," [Online]. Available: https://www.techopedia.com/dictionary. [Accessed 3 December 2019].

[36] "Merriam-Webster Dictionary," [Online]. Available: https://www.merriam-webster.com. [Accessed 3 December 2019].

[37] "Oxford Learner's Dictionary," [Online]. Available: https://www.oxfordlearnersdictionaries.com. [Accessed 3 December 2019].

[38] "Collin's English Dictionary," [Online]. Available: https://www.collinsdictionary.com/dictionary/english. [Accessed 3 December 2019].