INTRODUCTION TO CYBERPSYCHOLOGY

Briefing Paper

September 2024

GLOBAL
CYBERSECURITY
FORUM

About the Author

Prof. Dr. Mary Aiken
Pioneering the Field of Cyberpsychology

Professor Mary Aiken is a renowned cyberpsychologist, recognized globally for her pioneering work in the study of the impact of technology on human behavior.

Her research has significantly contributed to the discipline of cyberpsychology and has informed the establishment of the sub-discipline of forensic cyberpsychology. As one of the leading experts worldwide, Professor Aiken's contributions have not only advanced academic knowledge but also informed public policy in the development of safer and more secure online environments. Her book, The Cyber Effect (2016), is a seminal work in the field, offering a comprehensive overview of the effects of technology on individuals and society.

Beyond academia, Professor Aiken has played a critical role in shaping public policy around cyber safety and cybersecurity. She has advised various governments, law enforcement agencies, and international organizations on issues related to cybercrime, human factors in cybersecurity and AI, cyber safety, online harms, and youth protection online.

Professor Mary Aiken's work as a cyberpsychologist has been pivotal in advancing our understanding of the psychological effects of technology. Through her research, advocacy, and public engagement, she has highlighted the importance of addressing the challenges posed by the environment of Cyberspace and use of associated devices.

As technology continues to evolve, Professor Aiken's evidence-based insights will remain crucial for ensuring that our cyber future is secure, safe, sustainable, and aligned with human well-being. Her contributions have laid a strong foundation for the ongoing development of cyberpsychology as a critical 21st century science. Professor Aiken is a longstanding contributor to the Global Cybersecurity Forum.

Contents

Disclaimer

This document has been published by the Global Cybersecurity Forum (GCF) in collaboration with Knowledge Partners as part of their efforts to promote thought leadership in cybersecurity. While GCF and the knowledge partners have made every effort to ensure the accuracy and reliability of the information provided, neither party assumes any responsibility for errors, omissions, or inconsistencies in the content, nor for any consequences arising from its use or interpretation. The content is provided for general information purposes and may be subject to change without prior notice at the discretion of GCF.

Cyberpsychology is a rapidly evolving discipline which examines psychological aspects of human interactions with technology, and focuses on a wide range of research areas that include: Internet psychology; virtual environments; artificial intelligence; gaming; digital convergence; social media; and mobile and networking devices.[1] As the digital environment of Cyberspace becomes increasingly integral to daily life, understanding psychological implications is critical. The term 'cyberpsychology' was first coined in the late 1990s as the internet began to proliferate.[2] Initially, the focus was on understanding human behavior in virtual environments, such as online communities and multiplayer games. However, as technology has evolved, so has the scope of cyberpsychology, which now encompasses a wide range of areas that will be discussed in this paper.

1. The Origins of Cyber

Initially, 'cyber' referred to anything involving computers and the internet. The term 'Cyberspace' was popularized by science fiction author William Gibson in 1984.[3] Wiener, in the late 1940s, coined the term 'cybernetics,' derived from the Ancient Greek 'kybernētēs' which means pilot or governor (from kybernan to steer, govern).[4]

As the internet grew in the 1990s, cyber became a prefix for various activities and phenomena related to the online world, such as cybersurfing, and cyberculture. The term 'Cyberspace' came to represent the global information domain created by interconnected networks and the internet. The expansion of Cyberspace has led to the creation of numerous other cyber terms, including cybercrime, cybersecurity, and cyberattack.

The term cyber continues to evolve, especially as we enter an era dominated by virtual and augmented reality.

The concept of Cyberspace has also expanded to include the domain of war, as recognized in 2016 by the North Atlantic Treaty Organization (NATO), which formally declared Cyberspace as a distinct environment by defining it as a domain of operations alongside the traditional domains of land, sea, air, and space.[5] This marked a significant shift in its strategic approach to security, and to the premise of cyberwarfare.

In terms of Cyberspace operations, the domain is conceptualized as having three interrelated layers:[6] the physical network; the logical network; and the 'cyberpersona' layer, (which refers to us – the human component).

As technology progresses, it's likely that new cyber-related terminologies and concepts will continue to emerge, reflecting the increasing integration of digital and virtual experiences into everyday life.

2. The Psychology of Cyberspace

Cyberspace refers to the virtual environments created by the internet, social media, online communities, and other digital platforms. Unlike the physical world, Cyberspace is characterized by its intangibility, anonymity, and boundless connectivity. These unique features significantly impact how individuals think, feel, connect, learn, work and behave online.

One of the key concepts in the psychology of Cyberspace is the Online Disinhibition Effect (ODE). First introduced by Professor John Suler, the acknowledged founder of the discipline of cyberpsychology, this term describes the phenomenon where individuals exhibit less restraint and behave more freely online than they would in face-to-face interactions (Suler, 2004).[7]

This disinhibition can manifest in both positive and negative ways. For instance, people may share more personal information, express themselves more openly, or engage in behaviors they would typically avoid in real life. On the other hand, disinhibition may also lead to negative outcomes such as cyber fraud, cyberbullying, hate speech, and other forms of online harm. Cyber effects such as online anonymity, convenience of use, easy accessibility, and disinhibition – along with minimization of status of authority online – are important variables associated with amplification and escalation of human behavior in cyber contexts.[8]

Is Cyberspace an actual place?

This question has been widely debated. And the answer is, yes. It is an actual space. As soon as we go online, we are taken to a different location in terms of awareness, emotions, responses and behaviors. The more time we spend in Cyberspace, the less time we are available in the physical world. Humans have evolved over centuries to utilize physical space, but Cyberspace is still a new environment to which humans have yet to evolve and adapt to. There is a symbiotic relationship between Cyberspace and the so-called real world, as Slane (2007) highlights: "Claims for the independence of Cyberspace are based on a false dichotomy, physical and virtual are not opposed; rather the virtual complicates the physical, and vice versa."[9]

"The more time we spend in Cyberspace, the less time we are available in the physical world. Humans have evolved over centuries to utilize physical space, but Cyberspace is still a new environment to which humans have yet to evolve and adapt to."

3. Application of Cyberpsychology

Cyberpsychology, the study of the impact of technology on humans, has significant applications across various industries and sectors.

As businesses increasingly operate in Cyberspace, understanding the psychological principles that inform and guide online behavior can enhance product design, marketing strategies, customer service, education and cybersecurity measures. By applying cyberpsychology, companies can improve user experiences, optimize employee and user well-being, and safeguard against cyber threats.

3.1 Healthcare

Cyberpsychology has profound implications for healthcare,[10] particularly in the areas of mental and physical health interventions and patient care. The rise of telemedicine and digital health tools such as video conferencing, has made it possible for patients to receive care remotely, which is especially beneficial in underserved populations and remote locations.

Telehealth has the potential to make healthcare more effective, convenient, organized, and available. However, these technologies also pose challenges in terms of maintaining the patient-provider relationship, ensuring the efficacy of care, and – importantly – securing health related data from cyberattacks.[11]

3.2 Education

In education, cyberpsychology informs the design of online learning environments and educational technologies.[12] Understanding how students interact with digital tools can lead to more effective teaching strategies and improved learning outcomes. For example, gamification and interactivity have been shown to increase student engagement and motivation.[13] Additionally, cyberpsychologists focus on the need for equitable access to educational technologies, aiming to ensure that students worldwide can benefit from online learning.

3.3 Industry and Commerce

User Experience (UX) and Interface Design: An important application of cyberpsychology in industry is in the design of user experiences (UX) and interfaces. By understanding how users think, feel, and behave in Cyberspace, companies can create more intuitive and engaging products.

For example, cyberpsychology research on cognitive load and attention span helps UX designers develop interfaces that minimize user frustration and enhance ease of use. Understanding the principles of visual perception and human-computer interaction allows designers to create interfaces that align with users' natural behaviors, leading to more satisfying and efficient user experiences (Norman, 2008).[14]

> **"By applying cyberpsychology, companies can improve user experiences, optimize employee well-being, and safeguard against cyber threats."**

Digital Marketing, e-Commerce and Consumer Behavior: The rise of e-commerce has revolutionized the way consumers interact with businesses, making shopping more accessible, convenient, and diverse. However, the success of e-commerce platforms is not solely based on the technology that drives them; it also depends heavily on understanding the psychological factors that influence consumer behavior online. Cyberpsychology is crucial in this regard, as understanding consumer behavior in online environments is key to crafting effective strategies. Insights into how users interact with social media platforms can inform targeted advertising, content creation, and brand management.

Furthermore, understanding the psychological impact of personalization and customization in online shopping can help marketers create targeted experiences that resonate with individual consumers. This can lead to increased engagement, higher conversion rates, and stronger brand loyalty.

The lack of physical interaction in e-commerce makes it essential to understand the psychological processes that drive online shopping behavior, such as trust, risk perception, and the need for instant gratification. Trust is a fundamental element in e-commerce, where consumers must rely on digital cues to assess the credibility of a website or seller.

Cyberpsychology research has shown that factors such as website design, user reviews, perceived risk, ease of use, trust, and security indicators significantly impact consumer behavior.[15] Companies can also use insights from cyberpsychology research on decision-making processes to design user-friendly online shopping environments that reduce friction and enhance the customer journey.[16]

Employee Well-being and Productivity: In the workplace, especially in industries where remote work and digital collaboration tools are prevalent, cyberpsychology can help companies optimize employee well-being and productivity. Understanding the psychological effects of hybrid working arrangements, prolonged screen time, online communication, and digital multitasking can inform the design of healthier work environments.

Additionally, cyberpsychology can inform the design of digital tools that facilitate collaboration and reduce the cognitive burden on employees. For example, insights into how humans process information in virtual meetings can lead to the development of more intuitive video conferencing platforms, which can improve communication and reduce stress among remote workers.[17]

Organizational Cyberpsychology: An emerging area of research interest is the exploration of the intersection of human behavior, organizational dynamics, and technology. As organizations increasingly rely on digital platforms for communication, collaboration, and operations, there is a need to understand the psychological aspects of how individuals and groups interact with technology in the workplace. This research area draws on principles from psychology, information technology, and organizational studies to address the challenges and opportunities posed by the digital transformation of the workplace.

Future research in organizational cyberpsychology will likely focus on evaluating individual, group, and organizational dynamics mediated by technology, the challenges of integrating artificial intelligence in the workplace,[18] and the need to identify solutions to improve the well-being and performance of an organization and its employees.

4. Intersection of Cybersecurity, Cybercrime and Cyber Safety

The fields of cyberpsychology, cybersecurity, and cyber safety are deeply interconnected.

Understanding the psychological factors that influence online behavior can enhance cybersecurity measures and promote safer and more secure online environments. For example, by studying how individuals respond to cybercriminal social engineering attacks, cyber behavioral scientists can help to develop more effective training, education and awareness raising programs. Moreover, as digital technology continues to evolve, new challenges and opportunities will emerge at the intersection of these fields.

The advent and increasing adoption of technologies such as artificial intelligence and virtual reality presents new risks that require a multidisciplinary approach to address them effectively. For instance, the use of AI in cybersecurity has the potential to enhance threat detection and response, but it also raises ethical and bias concerns, along with the potential for misuse.

As a discipline, cyberpsychology can play a crucial role in understanding the human impact of these technologies and ensuring that they are used responsibly and effectively.

Cybercrime:
The most widely used classification system distinguishes between 'cyber-enabled' and 'cyber-dependent' crime. Cyber-dependent crimes are crimes that do not exist outside of Cyberspace, such as ransomware attacks and criminal hacking. Cyber-enabled crimes are traditional crimes that are now facilitated or have been made easier by technology.

Cyber enabled crimes range from white-collar crime to drug trafficking, online harassment to cyber fraud. However, a recent study by Phillips et al., (2022)[19] found that there is no single, clear, precise and universally accepted definition of cybercrime. This is problematic, as global classification variations could affect the measurement of and response to cybercriminal behaviors[20] and could impede international co-operation in tackling global cybercrime.

Cybercriminal Behavior:
One of the primary contributions of cyberpsychology to cybersecurity is understanding the behavior and motivations of cybercriminals.

According to Martineau et al., (2023), the approach to combatting cybercrime to date has been largely technology-centric (e.g., anti-virus, anti-spyware), despite the fact that cybercrimes are predominantly the result of human activities and based on human motives. Cybercriminals often exploit psychological vulnerabilities in their targets, such as trust, fear, and the tendency to comply with perceived authority.

For example, phishing attacks frequently rely on creating a sense of urgency or impersonating trusted entities to deceive victims into providing sensitive information.

Social engineering attacks are particularly effective because they exploit predictable human behaviors, rather than technical weaknesses in systems. The problem is compounded by the introduction of increasingly sophisticated technological attack vectors, such as cybercriminal use of synthetic images, videos, and audio, generated using deep learning and known as 'deepfakes.'[21]

By studying cybercriminal behavioral evolution and adaption tactics, cyberpsychologists can help to develop more effective training, awareness, intervention and deterrence programs. Understanding the modus operandi, motivation, behavioral profiles and evolution of cybercriminals can also assist law enforcement and cybersecurity professionals in anticipating and preventing attacks.

> **"Social engineering attacks are particularly effective because they exploit predictable human behaviors, rather than technical weaknesses in systems."**

Human Factors in Cybersecurity:
Cyberpsychology also plays a critical role in addressing the human factors that often contribute to cybersecurity vulnerabilities. The 'human factor' has long been recognized as being "the weakest and most obscure link in creating safe and secure Cyberspace" (Jeong et al., 2019 p. 338).[22] Studies have shown that a significant percentage of security breaches result from human error, such as using weak passwords, using unsecured personal devices for work or leaving devices unattended, or neglecting to update software. A recent industry study undertaken in conjunction with Stanford University found that approximately 88 percent of all data breaches are caused by an employee mistake.[23]

Many of these errors stem from cognitive biases and heuristics, which are mental shortcuts that people use to make decisions quickly.

For instance, the optimism bias – a tendency to overestimate the likelihood of positive events and underestimate the likelihood of negative events – can lead people to underestimate their personal risk of being targeted and compromised by cybercriminals. Additionality, employees are introducing technical short cuts into their work practices, for example the growth of Shadow IT and Shadow AI[24] software use within organizations, deployed without the knowledge of the IT or security group within the organization.

To mitigate these risks, cyber behavioral scientists advocate for the use of behavioral interventions that encourage better cybersecurity practices.

Cyberpsychology is a vital component of effective cybersecurity, offering insights into continuously evolving human habits, behaviors and cognitive processes that influence security outcomes.

Cyber Safety:
As the internet becomes increasingly integrated into our daily lives, the need for cyber safety initiatives and robust online safety technologies – commonly referred to as Safety Tech – has become more pressing than ever.

Safety Tech is informed by cyberpsychological principles and encompasses a wide range of tools and technologies designed to protect users from psychological risks, criminal dangers, and online harms. Recent reports have provided evidence of strong growth in the international Safety Tech sector.[25]

Safety Tech innovations provide technology solutions to technology-facilitated online harms and can assist in protecting people from the corrosive effects of misinformation, online harassment, discrimination, and extremism which increasingly threaten society. Safety Tech plays a crucial role in safeguarding users from various online threats by providing tools that detect, prevent, and respond to harmful and criminal activities.

These technologies include content filtering systems, parental control software, AI-driven moderation tools, and cyber fraud detection algorithms. Advances in machine learning and AI such as the development of 'Virtual Moderators'[26] have significantly improved the accuracy and efficiency of content filtering, enabling these systems to adapt to new threats in real time at scale.

Human oversight remains essential to address the nuances and complexities of online interactions that machines may not fully understand. A hybrid approach, combining automated tools with human moderation, is the most effective way to ensure online safety while maintaining accuracy.

Safety Tech operates at the nexus of cybersecurity and cyber safety. However, while cybersecurity primarily focuses on protecting data, systems and networks, cyber safety or Safety Tech focuses on protecting people. "It is critical that data, information, systems and networks are protected from cyber-attacks and are robust, resilient and secure. However, it is equally critical that the people who operate and use these systems are psychologically robust, resilient, safe and secure. Therefore, it is the combination of cybersecurity and Safety Tech that will deliver optimum protection." (Paladin, 2022, p 3).[27]

By addressing these challenges, Safety Tech can continue to evolve and provide robust protections that will make Cyberspace a safe and welcoming space for all.

> **"Human oversight remains essential to address the nuances and complexities of online interactions that machines may not fully understand."**

Forensic Cyberpsychology:
An evolving discipline intersecting psychology, digital forensics and criminal justice, forensic cyberpsychology investigates psychological aspects of cybercrime.

The discipline focuses on understanding the behaviors, motivations, and mental processes of individuals who engage in cybercriminal activities, as well as the psychological impact of these crimes on victims. As Cyberspace continues to expand, so too does the scope of cybercrimes, making forensic cyberpsychology an essential area of study for law enforcement, cybersecurity professionals, and psychologists.

A reference to the sub-discipline of forensic cyberpsychology first appeared in a 2014 Europol report, where it was argued that "the critical task for cyberpsychology as a discipline is to build up a body of established findings of how human beings experience technology, the critical task in forensic cyberpsychology is to focus on how criminal populations present in cyber environments" (Aiken & McMahon, 2014, p. 82).[28]

One of the largest cyberpsychology-informed cybercrime research projects to date has recently been completed, in which researchers investigated human and technical drivers of cybercrime (CC Driver, 2022).[29]

The findings informed an adapted model of the 'Theory of Planned Behaviour' (Aiken et al., 2024),[30] which focused on predicting youth intention to engage in criminal hacking, and incorporated a forensic cyberpsychology approach to cybercriminal behavioral profiling (Aiken et al., 2023).[31]

A key objective within this field is to understand the psychological profiles of cybercriminals, including their motivations, cognitive distortions, and behavioral patterns. Martineau et al., (2023)[32] recently published a systematic review of the cyber profiling literature. This work has made a significant contribution to advancing the knowledge base in the cyber behavioral sciences in terms of applying profiling techniques, frameworks, and methodologies to cybercrime.

Forensic cyberpsychology can play a critical role in digital forensics by providing insights into behavior and intent behind cybercrimes.

Understanding the psychological motivations of cybercriminals can aid in profiling suspects, predicting future offenses, and interpreting digital evidence. As cyber threats continue to evolve, the role of forensic cyberpsychology will be crucial in developing effective strategies for the prevention, investigation, and prosecution of cybercrimes.

However, as the field grows, it must also address the ethical challenges that arise from the intersection of psychology, criminology, technology, and the law.

5. The Future of Cyberpsychology

Cyberpsychology is a growing area of scientific interest. Areas predicted to be of significant interest going forward are:

AI and Algorithms

The study of the impact of AI and algorithms on human behavior will continue to be an important area of research and practice in cyberpsychology. The increasing use of AI in social media and other platforms to predict and influence user behavior raises questions about autonomy, manipulation, and ethical implications.

The increasing use of AI in cybercrime and cyberattacks is a cause for societal concern and will need to be addressed in a global context. The rise of generative AI, ChatGPT, chatbots and associated innovations represents a significant area of study within cyberpsychology. These technologies are increasingly being used in business, customer service, mental health apps, and even as companions for individuals seeking social interaction. However, the psychological impact of interacting with AI, particularly in terms of trust, empathy, and humanization of machines, is a complex issue that requires further study, guidance and oversight.

Operational Cyberpsychology

Spitaletta has undertaken important research and has been a pioneer in the area of 'operational cyberpsychology,' a field that "supports missions intended to project power in and through Cyberspace by leveraging and applying expertise in mental processes and behavior in the context of interaction amongst humans and machines" (2021, p.4).[33]

Building on this work, Lundie et al., (2024)[34] have conceptualized a research area that is broadly described as 'offensive cyberpsychology,' transitioning from national security and defense considerations to how organizations can not only defend their networks from cyberattacks but also effectively deploy active cyber defense protocols, and psychologically 'hack back.' Their landmark paper 'The Enterprise Strikes Back: Conceptualizing the HackBot - Reversing Social Engineering in the Cyber Defense Context' has generated much debate, discussion, and interest from industry stakeholders. Therefore, when applied to active cyber defense strategies, cyberpsychology can become a powerful tool in anticipating, identifying, mitigating and arguably deterring cyber threats.[35]

Active cyber defense involves proactive measures to detect, respond to, and neutralize cyber threats in real-time and at scale, often involving techniques such as deception, threat hunting, and automated responses. The integration of cyberpsychology into these strategies can enhance their effectiveness by aligning technical defenses with a deeper understanding of human behavior, specifically cyber attackers.

As cybersecurity increasingly relies on AI and machine learning to automate threat detection and response, incorporating cyberpsychological models into these systems can improve their effectiveness. This multi-faceted approach, the convergence of cyberpsychology and active cyber defense, represents a powerful alliance in the future fight against cyber threats.

> **"When applied to active cyber defense strategies, cyberpsychology can become a powerful tool in anticipating, identifying, mitigating and arguably deterring cyber threats."**

Cyber Leadership:
One of the most rapidly growing fields involving a wide range of disciplines such as computer science, cybersecurity, management, logistics, and cyberpsychology, 'cyber leadership' refers to the practice and discipline of leading organizations, teams, or initiatives in cyber contexts where technology, cybersecurity, resilience, and digital transformation are central to operations and strategy.[36]

It involves guiding and managing the technological aspects of an organization while ensuring that cybersecurity measures are robust and that digital strategies align with overall business objectives, including fostering emerging areas such as environmental, social, and governance (ESG) in cyber contexts.[37]

Cyber leaders are responsible for creating a culture of security awareness, driving innovation through technology, and navigating the complexities of cyber risks. Cyber leadership is increasingly critical as organizations across all sectors rely more heavily on digital technologies. The rise of cyber threats, the need for rapid digital transformation, and the growing importance of data and technology in business decision-making all contribute to the demand for strong cyber leaders.

We know a lot about identifying traits and qualities in real world leaders and mentoring and promoting them within organizations. However, there is a gap in our knowledge in terms of identifying potential cyber leaders, and this is where the cyber behavioral sciences can really add value.

Conclusion

This report has discussed the origins of the discipline of cyberpsychology along with the application of this science to a wide range of sectors and industries, from healthcare to education, and e-commerce to Safety Tech.

Constructs such as the environment of Cyberspace and the Online Disinhibition Effect have been discussed along with consideration of the intersection of cyberpsychology, cybersecurity, cybercrime and cyber safety.

As digital technology continues to evolve, so will the field of cyberpsychology. Areas of research interest going forward include AI and algorithms, operational and offensive cyberpsychology, and cyber leadership.

The continuously changing nature of Cyberspace in terms of virtual reality, GenAI, and the metaverse present ongoing challenges and opportunities for research and application.

Utilizing the science of cyberpsychology to understand the implications of ever-evolving technologies will be essential for fostering a safer and more secure Cyberspace and, in turn, safer and more secure cyber societies.

Endnotes

1. Connolly, I., Palmer, M., Barton, H. and Kirwan, G. (eds.) (2016). An introduction to cyberpsychology. Routledge Taylor & Francis Group.

2. Widman, J. (2018). The emergence of Cyberpsychology – Communications of the ACM. https://cacm.acm.org/news/the-emergence-of-cyberpsychology/#:~:text=Suhler%20said%20to%20his%20knowledge,and%20Social%20Networking%20in%202010.

3. Rothman, J. (2019). 'How William Gibson keeps his science fiction real,' The New Yorker, https://www.newyorker.com/magazine/2019/12/16/how-william-gibson-keeps-his-science-fiction-real.

4. Aiken, M. P. & Gawande, S. (2021). Nature, Structure and Science of Cyberspace: In S. Bhave (Ed.), Cyberpsychiatry Nagpur, India.

5. NATO. (2021). NATO Cyber Defence. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf

6. Department of Defense. (2018). Joint Publication 3-12: Cyberspace Operations. https://irp.fas.org/doddir/dod/jp3_12.pdf

7. Suler, J. (2004). 'The Online Disinhibition Effect', CyberPsychology & Behavior, 7(3), pp. 321–326.

8. Aiken, M. (2016). The Cyber Effect. https://www.maryaiken.com/the-cyber-effect

9. Slane, A. (2007). 'Review of Democracy, Social Space, and the Internet, by D. Saco', University of Toronto Law Journal, 57(1), pp. 81–104. http://www.jstor.org/stable/4491707.

10. New Jersey Institute of Technology .(2023). 'What is cyberpsychology and why is it important?', NJIT Admissions Blog.

11. Alder, S. (2024). 'Healthcare data breach statistics', HIPAA Journal.

12. Whitty, M.T. and Young, G. (eds.) (2016). Cyberpsychology: The study of individuals, society and digital technologies. Wiley.

13. Smiderle, R., Rigo, S.J., Marques, L.B., et al. (2020). The impact of gamification on students' learning, engagement and behavior based on their personality traits. Smart Learning Environments, 7(3).

14. Norman, K.L. (2008). Cyberpsychology: An introduction to human-computer interaction. Cambridge: Cambridge University Press.

15. Connolly, I., Palmer, M., Barton, H., & Kirwan, G. (2016). An Introduction to Cyberpsychology. New York: Routledge

16. Dewani, S., Presida, S. and Swatantra, G. (2024). 'The role of cyberpsychology in the context of digital marketing', Klabat Journal of Management, 5(1), pp. 72-89.

17. Butt, A. (2021). Cyberpsychology – The Challenges of Remote Working and Digital Wellbeing. Association for Business Psychology.

18. Wilkens, U. (2020). Artificial intelligence in the workplace – A double-edged sword. International Journal of Information and Learning Technology, 37(5), pp.253-265.

19. Phillips, K., Davidson, J.C., Farr, R.R., Burkhardt, C., Caneppele, S. and Aiken, M.P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. Forensic sciences, 2 F(2), pp.379-398.

20. McGuire, M. (2019). It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In: T.J. Holt and A.M. Bossler, eds. The human factor of cybercrime. London: Routledge, pp.3-28.

21. Sjouwerman, S. (2024). Council post: Deepfake phishing: The dangerous new face of cybercrime, Forbes. https://www.forbes.com/councils/forbestechcouncil/2024/01/23/deepfake-phishing-the-dangerous-new-face-of-cybercrime/

22. Jeong, J., Mihelcic, J., Oliver, G. and Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. In 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), Los Angeles, CA, USA, (pp. 338-345). IEEE.

23. Tessian. (2022). Why Do People Make Mistakes That Compromise Cybersecurity? https://f.hubspotusercontent20.net/hubfs/1670277/%5BCollateral%5D%20Tessian-Research-Reports/%5BTessian%20Research%5D%20Psychology%20of%20Human%20Error%202022.pdf

24. Maher, S. (2024). What is shadow AI and what can it do about it? Forbes. https://www.forbes.com/sites/delltechnologies/2023/10/31/what-is-shadow-ai-and-what-can-it-do-about-it/

25. Paladin, PUBLIC & Perspective Economics .(2023). The International State of Safety Tech 2023. https://view.publitas.com/public-1/international-state-of-safety-tech-report-2023/page/1

26. Unitary. (2024). https://www.unitary.ai/

27. Paladin Capital Group. (2022). Towards a Safer Nation: The United States 'Safety Tech' Market. https://www.prnewswire.com/news-releases/paladin-capital-issues-first-ever-report-on-emerging-billion-dollar-us-safety-tech-market-301459019.html

28. Aiken, M. P., & McMahon, C. (2014). The cyberpsychology of internet facilitated organised crime. Europol Organised Crime Threat Assessment Report (iOCTA).

29. CC-Driver. (2022). Project. https://www.ccdriver-h2020.com/project

30. Aiken, M.P., Davidson, J.C., Walrave, M., Ponnet, K.S., Phillips, K. and Farr, R.R. (2024). Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking. Forensic Sciences, 4(1), pp.24-41.

31. Aiken, M. P., Davidson, J. C., Kirichenko, A., & Markatos, E.P. (2023). Human Drivers of Cybercrime in E.P. Markatos (Ed.), Drivers, Trends, and Technology Evolution in Cybercrime (pp. 51-92). CC-Driver.

32. Martineau, M., Spiridon, E. and Aiken, M.P. (2023). 'Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature', Forensic Science, 3, pp. 452-477.

33. Spitaletta, J.A. (2021). Operational Cyberpsychology: Adapting a Special Operations Model for Cyber Operations. Johns Hopkins University Applied Physics Laboratory: Baltimore, MD, USA.

34. Lundie, M., Aiken, M.P., Amos-Binks, A., Lindke, K. & Janosek, J. (2024). The Enterprise Strikes Back: Conceptualizing the HackBot - Reversing Social Engineering in the Cyber Defense Context. Proceedings of the 57th Hawaii International Conference on System Sciences (HICSS).

35. Rich MS, & Aiken M.P. (2024). An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics. Forensic Sciences; Forensic Sciences, 4(1), pp. 110-151.

36. Cyber Resilience. (2024). 'Cyber Leadership Institute', Cyber Resilience. https://cyberresilience.com.au/cyber-leadership-institute/

37. KPMG .(2023). Cybersecurity in ESG. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2023/08/cybersecurity-in-esg.pdf

GLOBAL
CYBERSECURITY
FORUM