Journal of Posthumanism
2025
Volume: 5, No: 4, pp. 1302–1314
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i4.1242

Human Factors of Cybersecurity

DIAB M. AL-BADAYNEH[1], DARA D. AL-BADAYNEH[2], RABAB K. HASHISH[3]

Abstract

Human factors significantly impact cybersecurity, improving security efficiency or creating vulnerabilities for hackers. Employee behavior, decision-making, and communication can lead to security breaches. Human factors play a crucial role in cybersecurity, often overlooked compared to physical and technological safeguards. These factors are usually static, leading to a lack of assurance in their role in the cybersecurity chain. Recognizing and valuing the human element is essential for achieving or deteriorating security principles, addressing various types of cyberattacks, addressing challenges associated with human factors, safeguarding organizations from data breaches, maintaining reputation, and protecting financial security.The absence of interdisciplinary cooperation in the technology industry means products do not consider users' cognitive and emotional demands, especially in cybersecurity, where human factors and engineering concepts are primarily relied upon. This lack of criminological, sociological, and psychological expertise exacerbates human vulnerabilities, leading to products that fail to account for users' social, cognitive, and emotional needs, highlighting the need for a more comprehensive approach to human behavior. Research highlights the fallacy in relying on technological solutions to address human vulnerabilities in cybersecurity, highlighting the need for a more holistic approach that considers human behavior and performance.

Keywords: *Human Behavior, Cybersecurity, Cyber Risks, Human Factors, Impacts.*

Introduction

The connection between the physical and cyber worlds is functional and loosely coupled. All human activities have moved from physical space to cyberspace. New concepts, theories, and paradigms have emerged because of the new virtual comer. Online interaction often supplements offline F2F and social networks. From a cybersecurity perspective, human behavior can be seen as a cybernetic, closed system with social norms as a reference point for human behavior. AI has revolutionized policing by enabling autonomous systems to predict future events and adapt to new situations. This has increased interest in AI in various sectors, including healthcare, education, cybersecurity, and environmental protection. Law enforcement agencies, particularly in the EU, are embracing AI tools to make policing more efficient and cost-effective. However, concerns have been raised about the potential erosion of fundamental human rights due to its potential misuse. (Al-badayneh, 2025; Hardyns & Rummens, 2018).). Cybersecurity involves addressing human factors that can lead to breaches and implementing robust security measures to protect against these risks. Scholarly inquiry is crucial in understanding human elements in cybersecurity, as it significantly impacts the effectiveness of mitigative strategies against human-induced vulnerabilities, necessitating consensus among practitioners. (Al-Badayneh,

[1] Department of Security Studies, Graduate College, Police Academy, MOI, Qatar & IKCRJO, Jordan, ORCID 0000-0001-7416-6722
[2] Deanship of Development and Quality Assurance King Faisal University, KSA, 0000-0002-4526-6043
[3] Political Science Department University of Gothenburg Sweden, ORCID 0009-0006-7291-8373

2013). Cyberization uses communication and computer technologies to interconnect computers and devices, enhancing their practical utility and applications in transportation, finance, business management, education, telecommunications, and commerce. (Zhou, Delicato, Wang et al., 2020). Cybernetics is an interdisciplinary science that studies the control and information transmission processes in various systems, including machines, animals, and society. (Novikov, 2016, 7). It focuses on how digital, mechanical, or biological systems process information, respond to it, and evolve for better functioning. (von Foerster, 1962, 1979; von Glasersfeld, 1995; Wiener, 1965). Cybernetics is a multidisciplinary field that originated at the intersection of logic, mathematics, semiotics, biology, physiology, and sociology. It has applications in physics, engineering, management science, economics, sociology, and conceptual fields like philosophy and mathematics. The term "cybernetics" is not precise due to its multiple meanings, but it is described as a "notion" rather than a particular concept. (Alvarez & Ramírez-Correa, 2023).

Cyberization and Cyberspace

In the 1970s, popular science fiction television serials like The Cyborgs and The Six Million Dollar Man introduced the concept of cybernetics, which has evolved into various terms like cyberspace, cybermall, and cybercrime. This article explores its origins, meaning, principles, applications, and societal significance. Cyborgs are artificial beings with enhanced physical or mental faculties created by integrating organic life forms with technology, such as artificial limbs, organs, or chips. Cyborgs, a cybernetic organism, enhance human capabilities and have been significant figures in technology and culture since the 1960s. It combines individualism with control, eroding fixed categories between human and nonhuman. Recently, the cyborg has been used in social science and feminist theory to understand a non-coherent world filled with systematic inequalities, blurring the boundary between reality and fiction (Mingo, 2024; Kefalas, 2003; Warwick, 2012; Moser, 2001).

Cyberization is a process where various real things are connected to cyber existence. Emerging computing paradigms and information communication technologies, such as ubiquitous computing, social computing, and wearable technologies, are transforming the cyber world. The Internet of Things and cognitive cyber-physical systems transform how digital entities interact and communicate (Zhou, Delicato, Wang et al., 2020). Norbert Wiener defined cybernetics as “the study of control and communication in the animal and the machine” [248]. Cybernetics concerns concepts at the core of understanding complex systems, such as learning, cognition, adaptation, emergence, communication, and efficiency. One of the most well-known definitions is that of Wiener, who characterized cybernetics as being concerned with "control and communication in the animal and the machine."[Wiener, 1965] Another early definition is that of the Macy cybernetics conferences, where cybernetics was understood as the study of "circular causal and feedback mechanisms in biological and social systems."[von Foerster, H., Mead, M., & Teuber, 1951]. Ashby’s Law of Requisite Variety is known as The First Law of Cybernetics.

“The complexity of a control system must be equal to or greater than the complexity of the system it controls.” Heylighen1992, p. 10)

Cyberspace is a network of computing devices where electronic information is stored and communicated. A four-layer model captures its character, including the people who participate, the information stored and transformed, the logical building blocks supporting services, and the physical foundations supporting these elements. Cybersecurity refers to the human aspect of security, encompassing malicious actors and well-meaning individuals who interact with

technology, posing risks to organizations. This includes employees, suppliers, and third-party network access. The CIA's triad model, first mentioned in a NIST publication, focuses on confidentiality, integrity, and availability of information. It emphasizes trustworthiness and accuracy. (Andress, 2011).

Cybersecurity Insiders Report that 68% of organizations felt moderately to extremely vulnerable to insider threats in 2020. The World Health Organization highlights the increased cyberattacks during the COVID-19 pandemic, with healthcare organizations becoming targets. The Herjavec Group highlights society's growing vulnerability to cybersecurity threats. Unauthorized access and human factors are key factors in cybercriminals' attacks, where they steal credentials and infect systems with malware, making them more dangerous and challenging to detect. (Kadena & Gupi, 2021). Research on insider threats arising from dissatisfied employees or financial incentives poses a significant risk to information security. However, inadvertent insider threats caused by inadequate planning and attention to detail can also pose a threat (Hadlington, 2018). Orshesky (2023) and Kearney (2010) emphasize the significant role of human factors in ensuring the security and protection of systems.

Artificial intelligence focuses on creating computer systems that mimic human reasoning in rational knowledge domains. Ontologies structure subdomains, allowing for subtle use of knowledge. The human psyche contains potential elements memorized through inactive links, while artificial systems have dormant agents that must activate to reappear memorized facts. (Cardon, 2018). Computational intelligence techniques are crucial for cyberization, with recent advances in machine learning and AI focusing on algorithms and applications but less on the infrastructure of intelligent systems. (Zhou, Delicato, Wang, et al., 2020). AI can predict crime through the processing of large amounts of complex data, such as crime statistics and security footage. However, these systems must respect citizens' freedom, privacy, and not reproduce illegal activities or inequalities. This paper provides an overview of the different units and goals of AI applications in predictive policing, highlighting the challenges and opportunities of this technology in enhancing policing. (EUCPN, 2 02 2).

The Human Factors of Cybersecurity

The International Ergonomics Association (IEA, 2018) defines human factors as a scientific discipline analyzing human interactions and system elements. In the U.S., human factors are predominantly used, with three specializations: physical, cognitive, and organizational. Physical ergonomics focuses on tangible components, cognitive ergonomics explores mental processes, and organizational ergonomics optimizes organizational structures. (IEA, 2018). (Nobles, & Burrell, 2024). Human factors are crucial in understanding the interactions between humans, systems, and technology, aiming to optimize human well-being and system performance (Guastello, 2023). This field is essential in cybersecurity, as organizations face increasing cyber-attacks targeting human vulnerabilities. Human factors are crucial in assessing human behavior's role within contemporary technological systems' risk profiles (Reason, 1995). However, overreliance on technology can compromise human performance, potentially leading to a technology-induced cycle. Human factors are applied in high-stakes domains like aviation and nuclear power to improve system designs, reduce errors, and enhance efficiency (Nobles, 2022). Human factors in Cybersecurity are defined as the characteristics of an attacker, user, or defender, all of whom may contribute to or mitigate against cyber risk.(King et al., 2018). Human factors in cybersecurity refer to the impact of human behavior on cybersecurity systems, and the Human-Influenced Task-Oriented (HITOP) formalism is used for modeling human

decisions in security systems. (Noureddine et al., 2015). Human factors in cybersecurity refers to leveraging human factors principles to improve the integration between humans and systems, addressing human-related issues in data breaches and cyber-attacks (Nobles, Cunningham, & Robinson, 2022) Human factors in cybersecurity refer to the vulnerability of humans, such as persuasion and manipulation, which can be exploited through social engineering. (Rege, Williams, & Mendlein, 2019). Human Factors and Ergonomic Society (HFES), a global human factors professional organization, focuses on designing systems that optimize human well-being and performance by considering human factors. Their work involves understanding interactions between humans and system elements, utilizing theory, principles, data, and methods. (Nobles, & Burrell, 2024).

Human errors are a significant threat to security, often exploited by attackers. To mitigate these risks, organizations should implement continuous education, training programs, and robust security policies. Regular audits and enforcement mechanisms ensure compliance. Technological innovations like automation, user-friendly tools, and behavioral analytics can help identify potential threats and enhance operational efficiency, ultimately contributing to overall security (Thirupathi et al., 2024).

Human factors play a significant role in cybersecurity threats, influencing people's interaction with information security and posing risks. Security technologies alone are not enough to protect organizations from cyberattacks. Human and organizational factors, such as external influences, human error, management, organization, performance and resource management, policy issues, technology, and training, can contribute to computer and information security vulnerabilities. Factors such as risky behavior, belief, lack of motivation, and inadequate use of technology can lead to vulnerabilities. To address these weaknesses, a practical and flexible human factors methodology must be integrated into development processes. Mobile devices' security solutions should focus more on users' behavior than technical problems (Badie & Lashkari, 2012; Tu et al., 2015). The human element is crucial in cybersecurity, as it helps identify and mitigate threats. Despite technological advancements like AI and machine learning, the human element remains essential. Human judgment and expertise are crucial in interpreting data, making nuanced decisions, and protecting our digital landscape.

According to behavioral science, social networking positively and negatively affects individuals and society. It facilitates communication, provides a sense of community, and offers support for those feeling isolated, but it also leads to addictive behavior and cyberbullying. Nudging is a behavioral science approach that influences people's decisions to lead to desired outcomes. In cyberpsychology, it can promote positive online behavior and prevent negative outcomes like cyberbullying and Internet addiction. Social investment, encouraging people to invest in their online relationships, can lead to increased well-being and reduced adverse outcomes, as demonstrated by studies on Facebook relationships. (Ayeni, Madugba, & Sanni, 2022). Cybercrime and cybersecurity are umbrella concepts encompassing traditional and newer crime forms. Networked technologies enhance cybercrime, while cybersecurity refers to policies and practices to protect data, networks, and systems from unauthorized access. National security institutions are increasingly involved in cybercrime control and prevention activities. The fields of cyber-criminology and cybersecurity need greater engagement and cross-fertilization, with cybercrime at one end and cybersecurity at the other. Cybercrime and cybersecurity are umbrella concepts encompassing traditional and newer crime forms. Networked technologies enhance cybercrime, while cybersecurity refers to policies and practices to protect data, networks, and systems from unauthorized access. National security institutions are increasingly involved in

cybercrime control and prevention activities. The fields of cyber-criminology and cybersecurity need greater engagement and cross-fertilization, with cybercrime at one end and cybersecurity at the other. (Dupont & Whelan, 2021).

Internet addiction involves salience, mood modification, tolerance, withdrawal symptoms, conflict, and relapse. It is like substance abuse and addiction, with withdrawal symptoms and tolerance being hallmarks (Griffiths (1999, p. 246-247) it is like DSM III. Marks (1990) shares similarities with substance abuse, including repeated urges, mounting tension, rapid switching off tension, gradual return of the urge, syndrome-specific cues, secondary conditioning, and strategies for relapse prevention. The urge to complete behavior and discomfort, if prevented, resemble craving and withdrawal symptoms of substance abusers (Sussman &Sussman, 2001). Human factors influence cybersecurity in the digital era. The increasing use of technology in various sectors exposes valuable information to potential breaches. The evolving nature of cyber threats highlights the importance of understanding these factors to prevent security incidents and data breaches. Further research is needed to explore behavioral science theories. Cognitive exploitation by malicious entities is a growing concern, highlighting the importance of human factors in cybersecurity. This has led to a shift in academic research towards a more nuanced understanding of human influences. Cognitive exploitation by malicious entities is a growing concern, highlighting the importance of human factors in cybersecurity. This has led to a shift in academic research towards a more nuanced understanding of human influences. It is important to recognize that human factors engineering is a scientific discipline established over 80 years ago (Nobles, 2022b) and originated from experimental psychological research in military aircraft. Human behavior plays a significant role in cybersecurity, with human error causing 90% of cyber breaches (CIEHF, 2022; Nobles, 2024, Al-Badayneh et al., 2020, Al-Badayneh et al, 2022).

Human error is a significant cause of cybersecurity issues, resulting from inadvertent actions or decisions that compromise security, leading to vulnerabilities or breaches. These errors can range from simple mistakes like not using a password to complex ones like improper configuring or falling into a security system. Psychological biases, such as overconfidence and docking, can also increase the likelihood of human error. Understanding these psychological factors is crucial for developing effective human-centered security strategies that manage and mitigate risks associated with human behavior in cybersecurity situations. A more human-centered approach requires incorporating psychosocial techniques into security strategies and policies. (Tambe-Jagtap, 2023).

Social engineering tactics exploit human psychology rather than technical vulnerabilities, accounting for 98% of all cyber-attacks. The Twitter cyber intrusion of July 2020 highlightsthe Achilles' heel of cybersecurity: human susceptibility. The future of cybersecurity lies in cultivating a culture of vigilance and education among the digital community. Organizations will adopt holistic cybersecurity frameworks that address technological vulnerabilities and the human propensity to trust. The NIST Cybersecurity Framework (CSF) and ISO/IEC 27001 are cutting-edge approaches to cybersecurity, emphasizing the synergy between technological measures and human factors. These frameworks emphasize integrating human insights and technological resilience to create a robust cybersecurity posture. (Abdi, 2024).

The lack of understanding of human factors in cybersecurity is evident due to contradictory definitions. The operational definition focuses on adverse human behavior, while the scientific definition prioritizes system design to enhance human performance. (Nobles, 2022c; Nobles,

2022b; Nobles, 2019;). This knowledge disparity intensifies as academic publications often discuss negative security implications but fail to fully encompass the advantages of human factors as a scientific field (Jeong, Mihelcic, Oliver, & Rudolph, 2019; Mohammad, Hussin, & Husin, 2022; Rahman, Rohan, Pal, & Kanthamanon, 2021). While operational definitions focus on adverse human behavior, scientific definitions prioritize system design to enhance human performance and behavioral results. The lack of human factors specialists in cybersecurity intensifies knowledge disparity, necessitating thorough scientific and operational definitions to guide risk mitigation strategies and improve cybersecurity processes. (Jeong, Mihelcic, Oliver, & Rudolph, 2019; Mohammad, Hussin, & Husin, 2022; Rahman, Rohan, Pal, & Kanthamanon, 2021).

Human Cyber Risk

Human cyber risk encompasses potential risks in interactions, including potential cyber incidents. These risks can result from human behaviors like clicking on malicious links or providing sensitive information. These risks are challenging to predict and prevent, impacting digital and social interactions. Addressing these risks is crucial for preventing cyber threats. Human vulnerability, a weakness in cybersecurity, can lead to security breaches when exploited by cybercriminals. These threats exploit human behavior, highlighting the complexity of human vulnerabilities and the potential for cybercrime. Human errors at the security boundary pose significant risks to organizations, allowing cybercriminals to exploit this gateway. They exploit human factors of cybersecurity through phishing emails and social engineering attacks, allowing unauthorized access to the corporate network and exposing sensitive information. (Kost, 2024).

Research has shifted toward understanding human factors in cybersecurity (Jeong et al., 2019; Moustafa et al., 2021; Nobles, 2018). However, a knowledge gap exists in cybersecurity practice due to the lack of criminological, sociological, and psychological expertise from human factors practitioners, psychologists, cognitive scientists, and behavioral analysts (Nobles & Burrell, 2024; Nobles, Rangarajan & Burrell, 2025). Current literature characterizes human factors as the scientific field focused on comprehending and enhancing human interactions with systems (IEA, 2000), a term some practitioners call human **factors engineering**. Often disregarded in the cybersecurity chain, human aspects are vital to cybersecurity. They are frequently regarded as immobile, which makes their role uncertain. Despite their significance, human factors remain a significant source of vulnerability. Therefore, it is critical to acknowledge and appreciate their impact on upholding or undermining security standards. Furthermore, considering that human mistakes account for 70–80% of cyberattacks, corporations regard personnel as the most vulnerable component of cybersecurity, which is made worse by an excessive dependence on technological solutions. (Blau, Alhadeff, Stern, Stinson, & Wright, 2017; Meshkat, Miller, Hillsgrove, & King, 2020).According to research (Schneier, 2000), relying on technological methods to fix human flaws in cybersecurity is not a good idea. Instead, we need a more comprehensive approach that considers how people behave and perform. (Schneier, 2000, Nobles, 2022).

Psycho Cybernetics, a self-help book by **Maxwell Maltz**, offers a mechanical perspective on brain and body activity, empowering individuals to create a happier, more successful life.

“The science of Cybernetics does not tell us that “man” is a machine but that man has and uses a machine. Moreover, it tells us how that machine functions and how it can be used.(p.1)

Man's natural goal-striving nature leads to true success and happiness, as they complement and

enhance each other. (Maltz,2022)

Explaining Cybercriminal Behavior in Cyberspace

Routine Activity Theory. The Routine Activity Theory, proposed by Cohen and Felson in 1979, suggests that a crime must occur when there is a suitable target, a lack of a suitable guardian, and a motivated offender. This theory applies to cybercrime, as the opportunity for crime to occur is multiplied by the criminal's non-location-bound nature. **Bossler and Holt (2009)**confirmed the Routine Activity Theory in their publication, "On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities The theory can be used to inform cybercrime prevention and reduction strategies and make cybercrime less attractive to motivated cybercriminals. Routine Activity Theory applies to cybercrime regardless of the category, as opportunity is the root cause of crime. (Cox, Johnson, and Richards, 2009; Maras, 2017)

The rational choice theory. Cornish's rational choice theory suggests that people make decisions based on cost-benefit analysis, focusing on non-sociological factors. This approach helps social scientists understand human behavior and explains how decisions, whether wise or unwise, can be influenced by non-social factors. In cybercrime, electronic mechanisms like user IDs and surveillance cameras can serve as deterrents, providing a detailed analysis of criminal thought processes. (Cornish (1986).

Opportunity theory. The theory suggests that crime is influenced by opportunities arising from preventive measures, rather than the events that contribute to it. It posits that opportunities to commit crimes, regardless of physical property, are the root cause of crime. (Felson & Clarke, 1998).

Technology theory addresses cybercrime by designing solutions using cryptography, steganography, network protocols, and software engineering. Cybercrime thrives online due to the lack of selective message refusal mechanisms. Malicious hosts can send unwanted messages, exacerbated by the ubiquitous nature of the web. Routine activity theory is adapted for this study, as it captures philosophical assumptions and addresses the Achilles heel of web security. (Crocker, 1982).

Crime displacement theory. Crime displacement theory aims to reduce crime opportunities by moving crime from one location to another. This can involve geographic, temporal, target, tactical, and crime-type movements. It can be applied to combating cybercrime, with different outcomes such as positive, negative, neutral, even-handed, or attractive. Positive outcomes involve less severe damage, adverse outcomes involve more serious crimes, neutral outcomes involve the same seriousness, even-handed outcomes focus on repeated victimization, and attractive outcomes attract crime from other areas. (Felson and Clarke 1998).

The Space Transition Theory suggests that individuals with repressed criminal behavior in physical space may commit crimes in cyberspace due to their status and position. Identity flexibility, dissociative anonymity, and lack of deterrence factors in cyberspace provide offenders with the choice to commit cybercrime. Criminal behavior in cyberspace is likely to be imported to physical space, which may be exported to cyberspace. Intermittent ventures and the dynamic spatial-temporal nature of cyberspace provide opportunities for escape. Closed-society individuals are likelier to commit crimes in cyberspace than open-society people. (Jaishankar (2007).

Victim precipitation theory suggests that victims become targets for crime through confrontational or risky actions, passive presence in a criminogenic environment, or provocative behavior. Victims may knowingly act provocatively or display unknowingly motivating attributes and may be part of a group that threatens their political, social, and economic security. (Siegel, 2006). Victim precipitation theory suggests that sure victims make themselves targets for crime by engaging in confrontational or risky actions, being present in a location that provides a motivated offender with the opportunity to commit an offense, or engaging in provocative behavior in a criminogenic environment. (Siegel, 2006).

In conclusion, these theories provide valuable insights into the factors influencing criminal behavior and the strategies to combat cybercrime. However, the prevalence of cybercrime on the web and the lack of mechanisms for selective message refusal by hosts make it challenging to combat these issues effectively. All theories related to cybercrime. Rational choice theory posits that people make decisions based on cost-benefit analysis, while opportunity theory focuses on opportunities that emerge from preventive measures. Technology theory uses computer security theories to design and evolve authentication, verification, non-repudiation, and validation solutions.

Cyber Norms, Cyber Ethics, Cyber Deviance & Cyber Crimes

Since the late 1990s, the UN has been a hub for discussions on rules, norms, and principles for responsible state behavior in cyberspace. The Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG) and the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security presented their consensus reports in early 2021. These processes have inspired various sectors, including government, academia, civil society, and business. Cyber-normalization has affected the technical community in a less obvious and public way, but it fits into the larger picture of international law and relations. Disagreements on norms of state behavior are rooted in differences in values and principles related to internet governance, cybersecurity, and state and societal governance and sovereignty considerations. (Erskine and Carr 2016, Tech Accord 2021, Europol. 2020; Vincen et al., 2020)

Cyber ethics is a unique field that requires special attention due to the use of technologies within the cyber world. Students often judge right from wrong in real-world situations, making ethical decisions ranging from simple decisions to complex ones. Making and evaluating arguments is crucial in a modern world with diverse technological convergence. (Reznitskaya, 2002). The use of the internet in the virtual world has made it easier for children to identify right and wrong behavior. New technologies have made it possible for unsolicited commercial messages, digital photography, and access to sexually explicit materials. Schools, libraries, and parents need to take safeguards to prevent children from accessing inappropriate materials. Computer ethics should be considered due to the human tendency to view actions in the virtual world as less serious than real ones. (Vesna & Niveditha, 2012, p. 2). The Association for Computing Machinery's Code of Ethics and Professional Conduct (1993) emphasizes moral imperatives such as contributing to society, avoiding harm, being honest and fair, honoring property rights, providing proper credit, respecting privacy, and honoring confidentiality, similar to the 10 Commandments of Computer Ethics. (Vesna & Niveditha, 2012, p. 3).

Discussion

Technical controls often overlook the importance of human factors engineering in cybersecurity,

highlighting specific points where human interaction with technology introduces risks and potential failures. This lack of expertise can increase system complexity, cognitive overload, and weaken security posture (Nobles, Rangarajan, & Burrell, 2025). Human factors significantly influence security, impacting efficiency and vulnerability creation. Addressing these can protect organizations from data breaches, maintain reputation, and protect financial security. Human errors and mistakes are prevalent in cybersecurity, but human factors such as science, discipline, and profession are often overlooked. The human element, a costly vulnerability, is often overlooked in cybersecurity. Inconsistent definitions of human factors undermine efforts to address human-induced problems in cybersecurity literature. In-depth research is needed to understand the implications of inadequately defined human factors and their potential impact on cybersecurity measures. Addressing inconsistencies in human factors definitions is crucial for improving cybersecurity measures and fortifying defenses against human vulnerabilities. Human factors aim to mitigate errors, enhance productivity, and elevate safety and comfort standards. (Nobles, & Burrell, 2024).

Human error is a significant factor in cyber incidents, often leading to unintentional mistakes or intentional breaches in digital systems. Despite the growing reliance on connected devices and digital systems, cybercriminals exploit technical and human vulnerabilities to gain unauthorized access to sensitive data. A human-centered approach to cybersecurity is needed, acknowledging the complex interplay between human behavior, organizational culture, and security technology. By understanding how people interact with security systems, their decision-making processes, and cognitive biases, organizations can develop more effective ways to reduce vulnerabilities and enhance safety. Human-focused interventions are crucial for effective cybersecurity, integrating technical and human elements. A holistic approach, combining training and awareness programs, can reduce human error in the short term. However, more research is needed to assess these improvements' long-term sustainability and feasibility. Traditional methods like phishing awareness training and password policies face user sensitivity and compliance challenges. Advanced techniques, like zero trust architecture and user behavior analytics, provide strong security but raise privacy concerns. A human-centered approach to cybersecurity can significantly reduce the impact of human error on cyber incidents. Combining continuous training, user behavior monitoring, and AI-powered object detection tools, this approach reduces financial burdens, strengthens technical security, and fosters a security culture. (Tambe-Jagtap, 2023).

This paper emphasizes the importance of human-centered cybersecurity, integrating technical capabilities with human needs to create systems that align with behavioral tendencies. (CIEHF (2022). Pollini et Al. (2022) and Nobles (2022) highlight the need for human factors professionals in cybersecurity teams to develop training, awareness programs, and interventions sensitive to human variability, reducing risks and fostering resilience. (Nobles, Rangarajan, & Burrell, 2025). Cybersecurity awareness is a challenging task for organizations to balance user needs with security. Human weaknesses can cause security issues, and organizations must cultivate a culture where positive security behaviors are valued. Employees face daily challenges related to information security, and security functions should be meaningful and minimally intrusive. Security policies should be comprehensible and easy to locate, and employees should be educated about the importance of security awareness. (Metalidoua, ea al., 2014).

Contreras (2022) highlights the lack of interdisciplinary collaboration in the technology sector, particularly in cybersecurity, where human factors engineering principles are heavily relied upon, resulting in products that fail to account for users' cognitive and emotional needs. This

lack of psychological expertise exacerbates human vulnerabilities, leading to products that fail to account for users' cognitive and emotional needs, highlighting the need for a more comprehensive approach to human behavior. Academic research is shifting towards a more nuanced understanding of human influences in cybersecurity, as cognitive exploitation by malicious entities is a growing concern. This shift is a testament to the importance of understanding human factors in cybersecurity. (Nobles, 2022b).

References

Al-Badayneh, D., (2025). Cybersecurity: Concepts, Applications & Cyber Social Threats (Arabic). Dar Alfikr, Amman. Jordan.

Al-Badayneh, D., (2013). Human Behavior: When and where virtual society meets physical society. European Journal of Science and Theology, February 2013, Vol.9, No.1, 105-110

Al-Badayneh, D. et.al., (2022). Cyberbullying Victimization, Strains and Delinquency in Qatar. European Journal of Science and Theology, December 2022, Vol.18, No.6, 37-45

Al-Badayneh, D. et al., (2020). Radical Thoughts: Fears About and Supporting ISIS Among Jordanian College Students. NATO and Meson University. NATO Science for Peace and Security Series book, 'From Territorial Defeat to Global ISIS: Lessons Learned,' is set to be published by IOS Press

Alvarez, J., Ramírez-Correa, P. (2023). A Brief Review of Systems, Cybernetics, and Complexity https://doi.org/10.1155/2023/8205320 Academic Editor: Saikou Diallo

Andress, J. (2011). 'Chapter 1 - What is Information Security?', in Andress, J. (ed.) The Basics of Information Security. Boston: Syngress, pp. 1–16. DOI: https://doi.org/10.1016/B978-1-59749- 653-7.00001-3.

Ayyad, W., Abu Al-Haija, & Al-Masri, K. (2024). Human Factors in Cybersecurity. Chapter 11. IGI Global.

Badie, N. and Lashkari, A. H. (2012) A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP,' Journal of Basic and Applied Scientific Research, 2(9), pp. 9331–9347.

Blau, A., Alhadeff, A., Stern, M., Stinson, S., & Wright, J. (2017) Deep thought a cybersecurity story, Ideas42© 2017.

Cardon, A. (2018) Beyond Artificial Intelligence: From Human Consciousness to Artificial Consciousness. ISTE Ltd and John Wiley & Sons, Inc.

Chartered Institute of Ergonomics & Human Factors (CIEHF). (2022). The role of human factors in delivering cyber security: An overview for cybersecurity decision-makers (White Paper). https:// ergonomics .org .uk/ resource/ the - role - of - human - factors - in - delivering - cyber - security.htm

Contreras, J. M. (2022, March 22). Why should tech products be designed alongside psychologists? https:// thedecisionlab .com/ insights/ technology/ why - techproducts - should - be - designed - alongside – psychologists

Dupont B., & Whelan C.(2021). Enhancing relationships between criminology and cybersecurity. Journal of Criminology 2021, Vol. 54(1) 76–92 https://www.researchgate.net/publication/350440828_Enhancing_relationships_between_criminology_and_cybersecurity#fullTextFileContent

Erskine, Toni, and Madeline Carr (2016). "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace." https://ict4peace.org/wp-content/uploads/2017/02/Carr-Beyond Quasi-Norms-in-Cyberspace.pdf.

Erskine, Toni, and Madeline Carr. 2016. "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace." https://ict4peace.org/wp-content/uploads/2017/02/Carr-Beyond Quasi-Norms-in-Cyberspace.pdf.

EUCPN (2 02 2). Ar t if icial int elligence and predict ive policing: r isks and challenges. Brussels: EUCPN. https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf

Europol. (2020). “New Report Finds that Criminals Leverage AI for Malicious Use – And it’s Not Just Deep Fakes.” https://www.europol.europa.eu/newsroom/news/new-report-finds-criminalsleverage- ai-for-malicious-use-%E2%80%93-and-it%E2%80%99s-not-just-deep-fakes .

Hadlington L., (2018). Employees attitude towards cyber security and risky online behaviors: An empirical assessment in the United Kingdom. International Journal of Cyber Criminology International Journal of Cyber Criminology. DOI: 10.5281/zenodo.1467909 https://www.researchgate.net/publication/329250919_Employees_attitude_towards_cyber_security_and_risky_online_behaviours_An_empirical_assessment_in_the_United_Kingdom

Hardyns W., & Rummens, A., (2018). Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges, European J ournal on Criminal Policy and Research 24:3 (2018), 201-18, https://www.ojp.gov/pdffiles1/nij/230414.pdf

Heylighen F. (1992): "Principles of Systems and Cybernetics: an evolutionary perspective", in: Cybernetics and Systems '92, R. Trappl (ed.), (World Science, Singapore), p. 3-10.

International Ergonomics Association (IEA). (2000) Definition of human factors. http//www.iea.cc/whats/.

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019, December). Towards an improved understanding of human factors in cybersecurity. In 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC) (pp. 338–345). IEEE. DOI: 10.1109/CIC48465.2019.00047

Kadena E., & Gupi, M. (2021) Human Factors In Cybersecurity: Risks And Impacts. DOI: 10.37458/ssj.2.2.3

Kearney, P. (2010). Security: The Human Factor. Cambridgeshire: IT Governance Publishing.

Kefalas, A. G., (2003). Cybernetics in Encyclopedia of Information Systems, Pp. 365-378. https://doi.org/10.1016/B0-12-227240-4/00024-1 . Elsevier Science (USA).

King, Z., Henshel, D., Flora, L., Cains, M., Hoffman, B., & Sample, C. (2018). Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment. Frontiers in Psychology, 9. https://doi.org/10.3389/fpsyg.2018.00039

Kost E., (2024). Human Factors in Cybersecurity in 2025 https://www.upguard.com/blog/human-factors-in-cybersecurity#:~:text=Human%20cyber%20risk%20refers%20to,internal%20information%20to%20unauthorized%20persons .

Kulikova, A., (2021) Cyber norms: technical extensions and technological challenges, Journal of Cyber Policy, 6:3, 340-359, DOI:10.1080/23738871.2021.2020316. https://doi.org/10.1080/23738871.2021.2020316

Law, J., Moser, I., (2001). Cyborg in International Encyclopedia of the Social & Behavioral Sciences.

Maltz M., (2022) Psycho-Cybernetics: A New Way To Get More Living Out of Life. Profile https://www.meaningfulhq.com/psycho-cybernetics-by-maxwell-maltz.html

Meshkat, L., Miller, R. L., Hillsgrove, C., & King, J. (2020, January). Behavior modeling for Cybersecurity, In 2020 Annual Reliability and Maintainability Symposium (RAMS)1–7, IEEE.

Metalidoua, E., Marinagic, C., Trivellasc, P. Eberhagen, N., Skourlasd, C., & Giannakopoulosa, G., (2014) The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioral Sciences 147 (2014) 424 – 428 https://www.researchgate.net/publication/275544268_The_Human_Factor_of_Information_Security_Unintentional_Damage_Perspective

Mingo H., (2024). Emerging Vulnerabilities in Cyberspace: Analyzing Organizational Behaviors and Complexities. RAIS Conference Proceedings, November 21-22, 2024. 143-152

Mohammad, T., Hussin, N. A. M., & Husin, M. H. (2022). Online safety awareness and human factors: An application of the theory of human ecology, Technology in Society, 68, 101823.
Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behavior in improving cyber security management. Frontiers in Psychology, 12, 561011. DOI: 10.3389/fpsyg.2021.561011 PMID: 34220596
Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. HOLISTICA–Journal of Business and Public Administration, 9(3), 71–88. DOI: 10.2478/hjbpa- 2018- 0024
Nobles, C. (2019) Establishing human factors programs to mitigate blind spots in cybersecurity, MWAIS 2019 Proceedings, 22.
Nobles, C. (2022a). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. HOLISTICA–Journal of Business and Public Administration, 13(1), 49–72. DOI: 10.2478/hjbpa- 2022-0003
Nobles, C. (2022b) The Dunning-Kruger Effect around human factors in cybersecurity, Top Cyber News Magazine. https://www.linkedin.com/company/topcybernews/.
Nobles, C. (2022b, March) The Dunning-Kruger Effect around human factors in cybersecurity, Top Cyber News Magazine. https://www.linkedin.com/company/topcybernews/.
Nobles, C. (2022c) Stress, burnout, and security fatigue in cybersecurity: A human factors problem, HOLISTICA–Journal of Business and Public Administration, 13(1), 49-72.
Nobles, C. (2023). Human Factors in Cybersecurity: Academia's Missed Opportunity. Proceedings of the Eighteenth Midwest Association for Information Systems Conference, Saint Paul, Minnesota, May 19-20, 2023
Nobles, C., & Burrell, D. (2024). Exploring the variability of human factors definitions in cybersecurity literature. MWAIS 2024 Proceedings. 28. https:// aisel .aisnet .org/ mwais2024/ 28
Nobles, C., Cunningham, M., & Robinson, N. (2022).Straight From the Human Factors Professionals' Mouth: The Need to Teach Human Factors in Cybersecurity. Proceedings of the 23rd Annual Conference on Information Technology Education. https://doi.org/10.1145/3537674.3555782.Science of Security. https://doi.org/10.1145/2746194.2746215.
Nobles, C., Rangarajan, A., & Burrell, D. (2025). Human Factors Engineering- as- a- Service in Cybersecurity. Chapter 14, DOI: 10.4018/979-8-3693-6437-6.ch014
Noureddine, M., Keefe, K., Sanders, W., & Bashir, M. (2015). Quantitative security metrics with humans in the loop. Proceedings of the 2015 Symposium and Bootcamp on the loop. https://www.researchgate.net/publication/300725723_Quantitative_security_metrics_with_human_in_the_loop
Novikov D.A. (2016). Cybernetics: From Past to Future. Heidelberg: Springer, p.107 ISBN 978-3319273969, 3319273965
Orshesky, C. (2003). Beyond technology - The human factor in business systems. Journal of Business Strategy, 24, 4, 43-47.
Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition Technology and Work, 24(2), 371–390. DOI: 10.1007/s10111- 021- 00683- y PMID: 34149309
Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021, June) Human factors in cybersecurity: A scoping review, In The 12th International Conference on Advances in Information Technology (pp. 1-11).
Rege, A., Williams, K., & Mendlein, A. (2019). An experiential learning cybersecurity project for multiple STEM undergraduates. 2019 IEEE Integrated STEM Education Conference (ISEC), 169-176. https://doi.org/10.1109/ISECon.2019.8882112.
Schneier, B. (2000) Semantic attacks: The third wave of network attack, Crypto-Gram Newsletter, 14.
Tambe-Jagtap, S. (2023) Human-Centric Cybersecurity: Understanding and Mitigating the Role of Human

Error in Cyber Incidents. SHIFRA Vol. (2023), 2023, pp 53–59. ISSN: 3078-3186.

Tech Accord (2021) Paris Call for Trust and Security in Cyberspace: Six Working Groups Launched to Advance Global Cybersecurity.https://cybertechaccord.org/paris-call-for-trust-and-security-incyberspace-six-working-groups-launched-to-advance-global-cybersecurity/

Thirupathi L., Bhaskar Ch, V., Vasundara, B., Gugulothu, R., Sundaragiri, D., & Pulyala, R. (2025). Understanding and Addressing Human Factors in Cybersecurity Vulnerabilities. Chapter 2. Pp 12-15IGI Global

Tu, Z. et al. (2015) Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination', Information & Management, 52. DOI: 10.1016/j.im.2015.03.002.

Vesna, J & Nivedith, D. (2012). Ethics in cyberspace- a philosophical approach. International Journal of Advancements in Research & Technology, Volume 1, Issue 3, August 2012 1 ISSN 2278-7763 Copyright © 2012 SciResPub. IJOAR T

Vincent, B., Davison, N., Goussac, N. & Carlsson, M., (2020). Limits on Autonomy in Weapon Systems. https://www.icrc.org/en/document/limits-autonomous-weapons.

von Foerster, H., (1962) Self-Organizing Systems and their Environments. In: Yovits and Cameron, eds. Self-Organization. New York: Pergamon Press, 31-50.

von Foerster, H., (1979). Cybernetics of Cybernetics. In: Krippendorff, K.,ed. Communication and Control. New York: Gordon and Breach, 5-8.

von Glasersfeld, E. (1995). A Constructivist Approach to Teaching. In L. P. Steffe, & J. Gale (Eds.), Constructivism in Education (pp. 3-15). Hillsdale: Erlbaum. http://www.vonglasersfeld.com/172

Warwick, K., (2012). Cyborgs. Pp. Pages 699-704 in Encyclopedia of Applied Ethics (Second Edition). Academic Press. San Diego.

Wiener, Norbert (1965). Cybernetics: Or Control and Communication in the Animal and the Machine. Cambridge, Massachusetts: MIT Press.

Zhou, X., Delicato, F.C., Wang, K.IK. et al. (2020). Smart computing and cyber technology for cyberization. World Wide Web 23, 1089–1100 (2020). https://doi.org/10.1007/s11280-019-00773-y https://link.springer.com/article/10.1007/s11280-019-00773-y#:~:text=Cyberization%20refers%20to%20using%20communication,according%20to%20certain%20network%20protocols .