Human TECHNOLOGY

ISSN: 1795-6889

https://ht.csr-pub.eu Volume 21(1), May 2025, 1-5

From the Editors-in-Chief

SENSE OF SECURITY IN THE DIGITAL AGE

Kristiina Korjonen-Kuusipuro
South-Eastern Finland University of Applied Sciences
Finland
ORCID 0000-0002-8528-0237

Adam Wojciechowski
Lodz University of Technology
Poland
ORCID 0000-0003-3786-7225

Abstract: In this Editorial, we discuss the sense of security that is one of human's basic needs and closely connected to human well-being. The sense of security among technology users is highlighted in turbulent times. Cybersecurity is a tool that technology developers, society and individuals can use to increase their sense of security.

Keywords: *sense of security, cyber security, vulnerability, technology users*

DOI: https://doi.org/10.14254/1795-6889.2025.21-1.0

NAVIGATING HUMAN VULNERABILITIES AND TECHNOLOGICAL TRUST

A sense of security constitutes a fundamental human need and is intimately tied to overall well-being. It encompasses both subjective feelings of safety and objective conditions that ensure protection from harm. Psychologically, it reflects confidence, peace of mind, and freedom from fear, while materially it relates to stable conditions that guarantee the satisfaction of basic needs and the assurance of a secure future. The sense of security is also inherently relational, closely connected to trust – whether in interpersonal relationships, societal institutions, or technological systems. (Murayama et al., 2009.)

Contemporary societies are increasingly marked by multiple, overlapping crises. The term polycrisis captures this convergence, describing how challenges such as climate change, ecological degradation, global conflict, forced migration, and pandemics intersect and exacerbate one another. These crises generate pervasive uncertainty and, in some cases, a dystopian atmosphere that erodes public optimism and trust in the future (Lawrence, 2024; Teixeira, 2024).

FRAGMENTATION OF SECURITY ACROSS GENERATIONS

In human-technology interaction research, the sense of security frequently emerges as a core concern. There is, for example, widespread distrust in social media and tech companies handling personal data, and the lack of control over data reduces trust and increases anxiety. In Finland, empirical studies focusing on different demographic groups illustrate how security perceptions vary. Among older adults, apprehension often centers on a lack of digital competence and fear of making irreversible mistakes – for instance, accidentally losing savings through online banking (Korjonen-Kuusipuro et al., 2020). Despite the availability of supportive technologies such as emergency alert devices and health monitoring systems, many older users feel overwhelmed and alienated by rapid technological changes. This perceived lack of control contributes to a diminished sense of agency and, by extension, a weakened sense of security.

Conversely, younger users are typically more adept at using digital tools but face other security-related challenges. Research highlights that Finnish youth are increasingly concerned about online bullying, digital surveillance, and breaches of personal data, and these concerns clearly affect their agency, ability to act. These issues reflect a societal fragmentation of security, where the boundaries between online and offline threats are blurred. While older adults may underestimate digital risks – believing themselves too "ordinary" to be targeted – young users are often more aware of the implications of digital visibility and take active measures to protect their privacy, sometimes to the extent of withdrawing from social media altogether. (Tuuva-Hongisto & Korjonen-Kuusipuro, 2025.)

THE VASTAAMO CASE: A TURNING POINT IN DIGITAL TRUST

Finland, often regarded as a leader in digital innovation and cybersecurity, was deeply shaken by the 2020 Vastaamo psychotherapy data breach. Hackers obtained and disseminated the personal and highly sensitive therapy records of over 33,000 clients, accompanied by ransom demands and individualized blackmail attempts. The psychological and emotional damage extended far beyond the direct victims to their families and communities, exposing the profound vulnerability of digital infrastructures (Ghanbari & Koskinen, 2024; Looi et al., 2025). The case not only revealed systemic weaknesses but also exemplified how quickly trust in digital systems can collapse.

The Vastaamo case exemplifies the strong ethical tensions that can emerge in digital environments, revealing both the extreme vulnerabilities of individuals and the capacity for collective response. While the incident demonstrated the profound cruelty of malicious cybercrime, it also mobilized an array of actors committed to restoring justice. Cybersecurity professionals, technology companies, and civic-minded individuals contributed to the investigation, assisting law enforcement in identifying and ultimately apprehending the perpetrator. Despite the successful conviction, the long-term psychological impact on victims and the broader erosion of trust in digital systems underscore the enduring consequences of such breaches.

TOWARD A SHARED RESPONSIBILITY

Cybersecurity has emerged as an essential component of digital literacy and responsible digital citizenship. The concept of cyber hygiene – encompassing practices such as using strong passwords, updating software regularly, and securing home networks – serves as a practical guide for individuals. However, emphasizing individual responsibility alone is insufficient.

Cybersecurity must be understood as a collective endeavor involving individuals, technology providers, and governments. Despite increased public awareness, the roles and responsibilities within this triad remain ambiguously defined. Sociologist Norma Möllers (2021) poses critical questions about the intersection of digital infrastructure and national identity: What role does information infrastructure play in national belonging? How can states encourage civic engagement with such complex, often invisible systems? These questions are particularly pressing in an era where personal data is contested by global actors, from Western social media conglomerates to state-sponsored cyber operations.

The human dimension of cybersecurity must not be overlooked. Individuals are not anonymous "users", good or bad digital citizens as Möllers (2021) points out, but unique persons – children, parents, grandparents – each with varying degrees of knowledge, access, and risks. Policy solutions must therefore be inclusive, attuned to the specific vulnerabilities and needs of diverse populations. In this regard, governments carry a primary responsibility not only to protect digital infrastructure but also to engage meaningfully with citizens' lived realities. Whose voices are being heard in the design of secure digital systems? And who is left unheard? Who are silent voluntarily?

CONCLUSION

The Vastaamo incident stands as one of the most significant cybersecurity failures in mental healthcare globally, with severe repercussions for both individual well-being and public trust. It exemplifies the fragility of the sense of security in digital environments and the profound social costs of its breach. As societies become increasingly dependent on digital infrastructures, the challenge is not only technical but also ethical and societal: to build inclusive, resilient systems that recognize and respond to the complex ways in which technology mediates human security.

There is a call for a broader and deeper understanding of the sense of security among technology users. With this we do not refer only to the technological dimensions of cyber security but also to "the human", more profound need of the sense of security. There are people behind the cybersecurity; and it would be interesting to read their personal impressions of sense of security and safety – how the sense of security has influenced their career choice, for example. It is not an easy subject to deal with and some of the more technical security issues are understandably left under the smoke screen. But still, it would be interesting to see more research articles in Human Technology journal dealing with cybersecurity and sense of security in general.

REFERENCES

Bodo, B., Bene, M., and Boda, Z. (2025). False sense of security and a flurry of misplaced trust: the construction of trust in and by Facebook. *Information, Communication & Society*, 1–20. https://doi.org/10.1080/1369118X.2025.2482651

Ghanbari, H. and Koskinen, K. (2024). When data breach hits a psychotherapy clinic: The Vastaamo case. *Journal of Information Technology Teaching Cases* (0)0, 1-9. https://doi.org/10.1177/20438869241258235

Korjonen-Kuusipuro, K., Rasi-Heikkinen, P. Vuojärvi, H. Pihlainen, K., and Kärnä, E. (2022). (Eds.) *Ikääntyvät Digiyhteiskunnassa* (Older adults in Digital Society*)*. Gaudeamus. Helsinki.

Lawrence, M. (2024). Polycrisis in the Anthropocene: an invitation to contributions and debates. *Global Sustainability* 7, e5, 1–5. https://doi.org/ 10.1017/sus.2024.2

Looi JC, Allison S, Bastiampillai T, Maguire PA, Kisely S, Reutens S, and Looi RC. (2025). Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers. *Australasian Psychiatry* 33(1), 106–110. https://doi.org/10.1177/10398562241291340.

Murayama, Y., Hauser, C., Hikage, N., & Chakraborty, B. (2009). The Sense of Security and Trust. In M. Gupta & R. Sharman (Eds.), *Handbook of Research on Social and Organizational Liabilities in Information Security* (pp. 493-502). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-60566-132-2.ch029

Möllers, N. (2020). Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State. *Science, Technology, & Human Values*, 46(1), 112–138. https://doi-org.ezproxy.xamk.fi/10.1177/0162243920904436

Teixeira, C. (2024). *Youth, Protests and the Polycrisis. Unicef Innocenti*. Global Office of Research and Foresight.

Tuuva-Hongisto, S. & Korjonen-Kuusipuro, K. (Eds.) (2025). *Diginuoruus ja kasvavat erot*. (Digital Youth and Growing Inequalities). Nuorisotutkimusseura, Helsinki.

Authors' Note

All correspondence should be addressed to

Kristiina Korjonen-Kuusipuro
South-Eastern Finland University of Applied Sciences (Xamk)
Finland
kristiina.korjonen-kuusipuro@xamk.fi
ORCID 0000-0002-8528-0237

Adam Wojciechowski
Lodz University of Technology
Poland
adam.wojciechowski@p.lodz.pl
ORCID 0000-0003-3786-7225

Human Technology
ISSN 1795-6889
https://ht.csr-pub.eu