HUMANS IN THE CYBER LOOP: PERSPECTIVES ON SOCIAL CYBERSECURITY

Selim Mürsel Yavuz[*]
ORCID ID: 0000-0002-0545-9123

Edited by Dorota Domalewska, Aleksandra Gasztold, and Agnieszka Wrońska, *Humans in the Cyber Loop: Perspectives on Social Cybersecurity* (Leiden | Boston: Brill, 2025), Studies in Critical Social Sciences 317. ISBN 978-90-04-54989-0 (hb), 978-90-04-54990-6 (e-book). DOI: 10.1163/9789004549906.

Declaration[*]

Humans in the Cyber Loop makes a direct claim that many cybersecurity discussions quietly sidestep. Security is not only about protecting machines and networks. It is also about people and the social settings that shape what they notice, trust, and do online. Domalewska, Gasztold, and Wrońska approach cybersecurity as a socio-technical problem tied to community dynamics and to the political economy of platforms. That framing is hard to dismiss once you sit with it, because so many recent "cyber" harms travel through attention and trust, not only through technical compromise.

The authors build the book around the idea that humans are "in the cyber loop" as both vulnerability and resilience. People create openings for harm through ordinary behavior, limited attention, and familiar cognitive shortcuts. Yet people can also become the source of resilience when learning is shared and institutions design for safer routines. I kept thinking of a scene that plays out in almost any organization. Someone is racing to clear an inbox before a meeting. A message arrives that looks like it came from IT, uses plausible language, and offers a quick link "to verify." The login page looks normal. In a hurry, they comply. The error is human, but the surrounding conditions were designed to make the click feel reasonable.

This leads to the book's central contribution, the development of "social cybersecurity" as an analytic lens. Rather than separating cybercrime, cyber conflict, and disinformation from

[*] Presidency for Turks Abroad and Related Communities, PhD Student in International Relations at Social Sciences University of Ankara, Selimmurselyavuz@gmail.com.
[*] The author acknowledges the use of Gemini for proofreading and language editing purposes during the preparation of this manuscript. The final content was reviewed and approved by the author.

platform governance, the authors treat them as connected. Algorithmic curation, surveillance capitalism, and influencer markets sit alongside more conventional security threats because they shape influence and coordination at scale. The book also keeps psychosocial consequences in view, including hate speech, cyber aggression, and problematic internet use.

Conceptually, the early chapters are among the strongest parts of the volume. Drawing on Beskow and Carley's definition, the authors describe social cybersecurity as concerned with cyber-mediated changes in human behavior and socio-political outcomes, while also building the conditions for societal endurance under social cyber threats. This clarifies what is being added to the more familiar cybersecurity agenda. Traditional cybersecurity tends to focus on compromise, systems, and technical controls. Social cybersecurity draws attention to manipulation, influence, and marginalization. It is also explicitly interdisciplinary, and the authors are right to treat that as a requirement rather than a slogan.

The book's structure is pedagogical and cumulative. Across nine chapters it moves from definitions to cyber threats, then to information warfare and disinformation, algorithmic influence, platform political economy, influencer ecosystems, content overload and hate, and finally problematic internet use, before concluding with a synthetic "digital ecosystem" chapter. Chapters 1 to 3 trace a familiar arc from crime to warfare to information operations while keeping the human pathway central. Chapter 2 expands the taxonomy toward cyber war and hybrid warfare, stressing that hybrid operations span infrastructure attacks, social fragmentation, and narrative shaping. Chapter 3 then synthesizes psychological and network mechanisms of disinformation and uses Russia as an illustrative case of tightened media control after 2022.

Chapter 4, "The Power of Algorithms," is the analytic pivot because it makes influence tangible. The authors acknowledge that ranking and recommendation systems can broaden exposure under certain conditions. Still, their emphasis falls on the costs when curation hardens bias, suppresses content, or distorts public reality. They ground the discussion in controversies that will be familiar to many readers, including allegations that TikTok suppressed LGBTQ-supportive content in some contexts. The unsettling point is not only bias in a narrow sense. It is how easily "visibility" becomes a political variable, adjusted quietly and at scale.

What keeps this chapter from becoming a simple critique is the authors' contrasting case. Estonia is presented as a governance model in which AI-enabled public services and the #KrattAI initiative are framed as public-good deployment, with human oversight positioned as a final layer of accountability. The point is not that Estonia has solved automation. It is that objectives and incentives matter. Systems built for engagement and monetization invite one set of outcomes. Systems built for public service, coupled with oversight that is at least visible to the public, invite a different set of outcomes.

Chapters 5 to 7 widen the focus to the socio-economic systems that scale social cyber threats. Chapter 5 treats digital marketing as a paradox. Personalization can feel empowering, yet it is often built on surveillance and behavioral steering. The authors draw on the language of surveillance capitalism and describe "hypernudges" as subtle ways platforms shape choices. Chapter 6 turns to influencer ecosystems and, in the discussion of "kidfluencers," highlights both the strain of persistent visibility and the weak protections around labor and privacy when content is produced in identifiable home settings. Chapter 7 connects content abundance to overload, hate speech, and cyber aggression, and it calls for multidisciplinary counter-hate strategies. The thread remains consistent. When incentives reward outrage and speed, the information environment becomes easier to weaponize.

Chapter 8 shifts to "digital dependency," and it changes the book's tone in a useful way. The authors outline symptoms such as loss of control, tolerance-like escalation, and withdrawal analogues. They stress that full abstinence is unrealistic, so the practical goal is balanced use framed as "conscious computing." They also summarize research on brain structure and function associated with addictive patterns and treat these findings as security-relevant insofar as they affect impulse control and decision-making. For security studies readers, this chapter expands what vulnerability can mean. It is not only weak passwords or unpatched systems. It can also be fatigue, compulsive checking, and attention fragmentation that make manipulation easier and self-control harder.

The concluding chapter consolidates an ecosystemic view through a socio-ecological approach that places the human being at the center of the digital ecosystem. Attention markets, micro-targeting, automated decision-making, and surveillance-based personalization are treated as forces shaping perceptions, relationships, and democratic stability. The authors also resist technological determinism. Manipulation and power-seeking predate Web 2.0.

Platforms amplify and accelerate those dynamics, which is precisely why governance and resilience still matter.

As an academic contribution, *Humans in the Cyber Loop* succeeds most as synthesis and orientation. Its chief strength lies in integrating multiple levels of analysis, from cognition and dependency to platform governance and hybrid conflict, supported by accessible cases and examples. For teaching and for interdisciplinary conversations, that coherence is valuable. The main limitation is the same breadth that makes the book readable and usable. Because the authors aim to provide representative examples rather than sustained case studies, the analysis sometimes reads as a well-organized tour. Readers looking for operationalization will find fewer concrete measures and research designs than the definition of social cybersecurity might suggest.

Two final points are worth noting. First, the book's normative stance is explicit and generally well defended, especially where it criticizes moderation practices that hide vulnerable users rather than confronting harassment. Still, the policy discussion could go further by treating regulatory tradeoffs more systematically, including transparency versus security, moderation versus speech, and privacy versus personalization. Second, the authors disclose using AI tools, including ChatGPT, Paperpal, Grammarly, and DeepL, followed by human proofreading. In a book about human agency inside algorithmic systems, that disclosure is quietly instructive.

Overall, *Humans in the Cyber Loop* is a timely entry point into social cybersecurity as both an interdisciplinary research area and a policy-relevant lens on contemporary digital threats. Its greatest utility is as a framework builder. It helps readers see that disinformation, algorithmic curation, surveillance economies, influencer-driven persuasion, and digital dependency are not separate problems. They interact within a single ecosystem, and that interaction is where security debates now need to live.