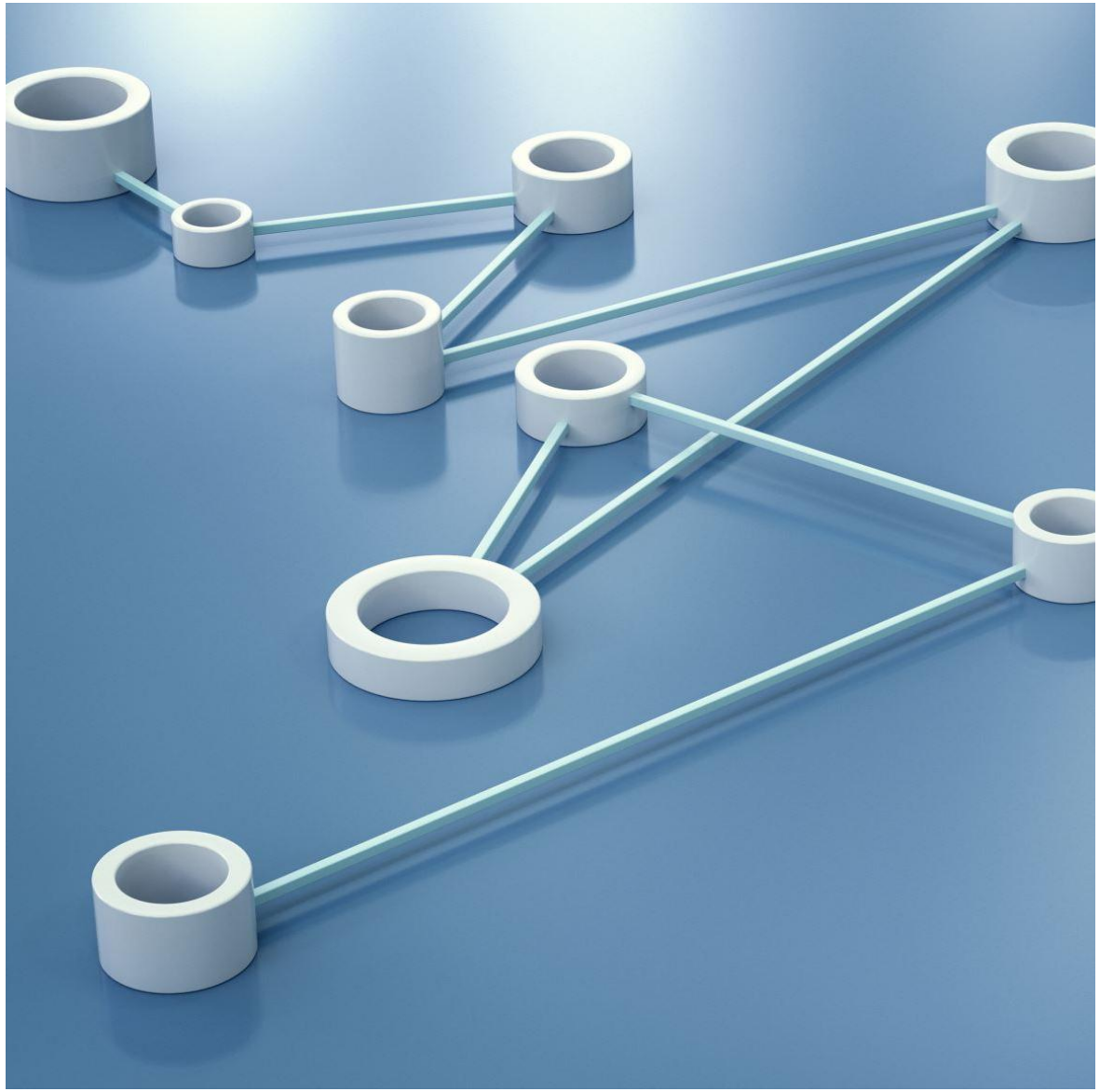
Cyberhealth: The Next Frontier of Cybersecurity

Cristina Andersson

Connect4Cyber 2026

Why Cyberhealth?

- Digital systems now shape behavior, wellbeing, and agency
- No shared definition but yet a massive societal impact
- Cybersecurity protects systems
- **Cyberhealth protects people inside those systems**



What Is Cyberhealth?

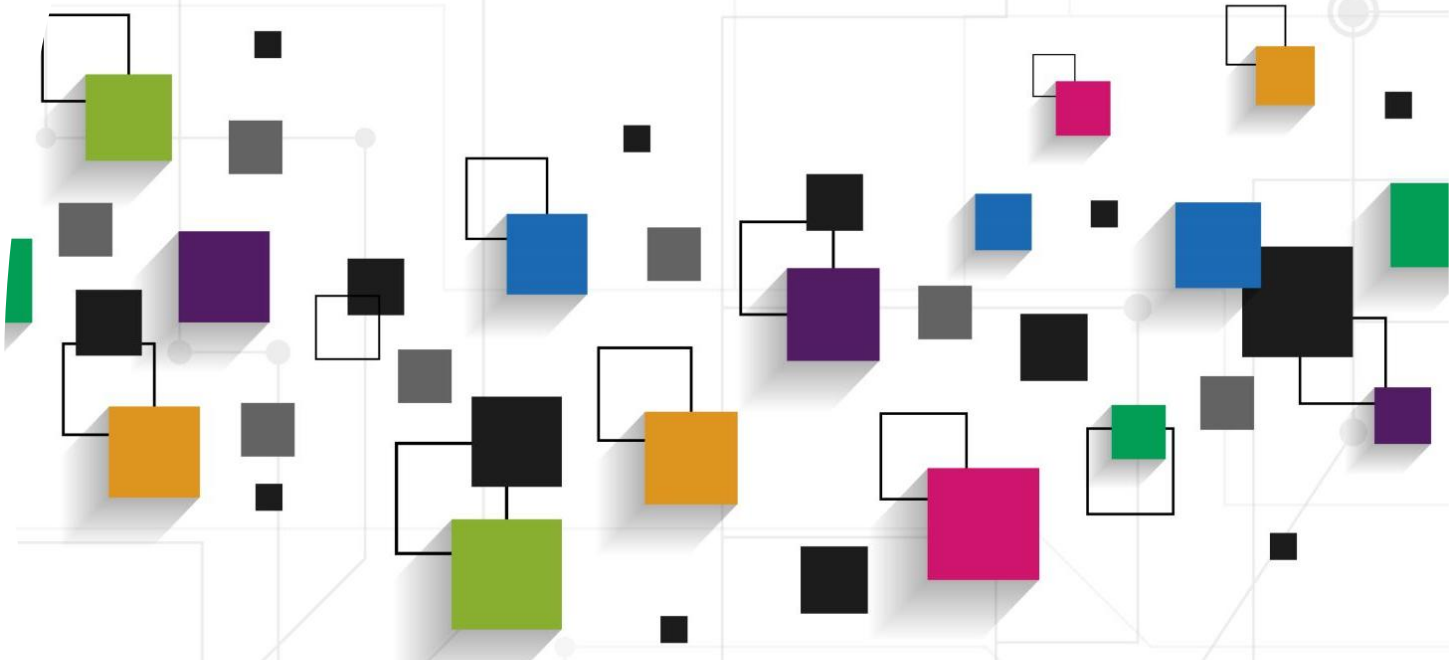
- The “health” of individuals and societies in digital environments

Interplay of:

- behavior-shaping technologies
- data ecosystems
- AI-driven decision-making
- Focus on **human agency, resilience, and autonomy**

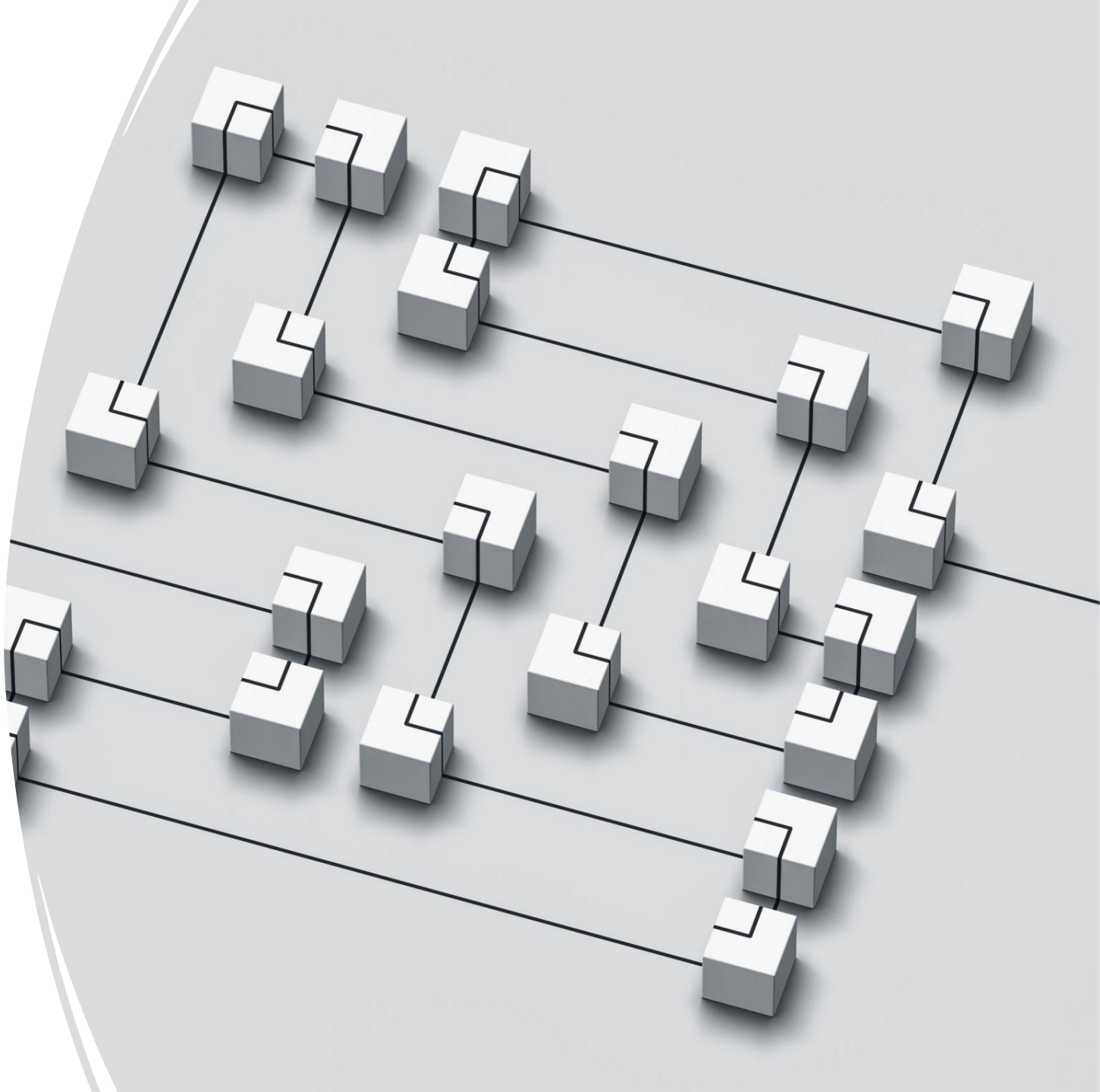
The Impact

- Wearables, apps, diagnostics, platforms influence daily choices
- Stress, trust, participation shaped by digital environments
- Weak cyberhealth → manipulation, polarization, vulnerability
- Strong cyberhealth → resilient citizens & resilient democracies



Governing Influence: The Diplomatic Challenge

- Behavioral data is a strategic resource
- Need for **influence transparency** in AI
- Cross-border interoperability & trust
- Agency-preserving design as a diplomatic priority
- Europe can lead with standards that protect autonomy



The Risk of Ignoring Cyberhealth

- - People become easier to influence and manipulate
- - Polarization deepens and trust erodes
- - Human agency shrinks in opaque digital environments
- - Wellbeing declines under cognitive overload and constant nudging
- - Societies become fragile without any attacking infrastructure
- - Behavioral data becomes a geopolitical vulnerability
- Corporate spying

What We Need to Build

Shared definitions and frameworks

Governance that aligns cybersecurity + public health + AI ethics

Tools that expand people's **circle of influence**

International cooperation on cyberhealth norms

Cybersecurity protects infrastructure. Cyberhealth protects us.

To build resilient societies in the age of AI, cyberhealth must become a strategic priority.

Thank you!