A cybercrime perspective in wireless networks

Some Insights into interdisciplinary collaboration in the EU COST Action BEING-WISE

Martin Griesbacher

24.06.2025

HFDT Symposium



Behavioral Next Generation Wireless Networks for Cyber Security BEiNG-WISE - https://beingwise.eu

• EU COST Action: Interdisciplinary research network with 236 members in 41 countries

 Goal: to better understand human beings in wireless security systems and how to design usable security solutions









Behavioral Next Generation Wireless Networks for Cyber Security BEiNG-WISE - https://beingwise.eu

- EU COST Action: Interdisciplinary research network with 236 members in 41 countries
- Goal: to better understand human beings in wireless security systems and how to design usable security solutions
- 5 Working Groups:
 - 1. Cybersecurity in emerging wireless communication
 - 2. A cyber-crime perspective in Wireless Networks
 - 3. Optimal security approaches for wireless ystems and impact on the user4. Human Factors in Wireless Security

 - 5. Legal factors in Cybersecurity Wireless Systems: A Vertical Approach









Technologies/Application domains

Celullar Wireless Technologies (2/3/4/5/6G)

Wireless Local Area Networks (WLAN/Wi-Fi)

Cellular Wireless Technologies: 5G private letworks: Cellular communications + IoT + WLAN

Vehicular communications: ITS G5 (802.11p)

Vehicular communications: 5G

Short range communications in IoT (Bluetooth, zigbee)

Long range communications in IoT (LoRa, 5G)

Satellite communications

Other next generation wireless networks and systems

In general: wireless linking functionality/ component/stage/aspect between humans and digital technologies

cybercrime

illegal or harmful acts/events

which specifically exploit human vulnerabilities or directly target humans (human vectors)

acts of (cyber-)crime, terror, or war

acts of non-compliance

other unethical acts (e.g., market manipulation, disinformation campaigns, sabotage of attention, data collection practices, negligent security policies and policy making)

types of threat actors

individual actors

a) direct harmful actors (external and internal)
 b) indirect harmful actors (negligent or incompetent organisation members)

collective actors

a) direct harmful actors (e.g., criminal/terrorist networks, organized crime, states) b) indirect harmful actors

 b) indirect harmful actors (intermediaries, providers of malicious tools, data brokers, private and public organisations, law enforcement, states)

malicious artificial agents (algorithms, bots, AI)

attack(er) or event profiles

motivation and behaviours

(human vector) attack methods
-) social/human engineering
-) harassment, bullying
-) (hy)persuasion/disinformation
-) any other direct or indirect targeting/exploitation of human behaviours/aspects

attack tools/infrastructures

modus operandi

eco systems

cybercrime impact domains

human targets (victims)

targeting humans to harm human collectvies

human individuals (direct targets) end users, citizens, customers, minors, members of human collectives

human collectives (indirect targets) a) private entities

(companies, vendors and providers of wireless technologies, critical infrastructures) b) public entities (incl. law enforcement and national defense)

c) sociopolitical entities/institutions (society, nation, pillars of democracy, public discourse)

aspects of human individuals

vulnerability domains

a) behavioural patterns
 b) cognitive/perceptive aspects
 c) emotional aspects

integrity/harm domains

(significant violations of human dignity) a) physical b) mental

c) material d) social e) legal f) ethical

aspects of human collectives: organisations

vulnerability layers

"human

layers" as

targets =

human

vectors

① soft-/hardware

m physical

social

classified to legal

ethical

integrity/harm domains (digital assets)
a) data

b) financialc) knowledged) reputation

aspects of human collectives: sociopolitical

prevention techniques

security approach: countering/disruption/mitigation of attacks

cybersecurity compliance (regulations, policies, industry requirements, standards, certification)

enhancing/training cybersecurity competences (knowledge, skills, attitudes, agency)

calibrated defense/shielding based on cyber attack/victime profiles

security collaboration

training/awareness campaigns and tools for end users

law enforcement approach: threatening/punishing (potential) attackers

Cybersecurity frameworks

(ISO/IEC TS 27110:2021)

identify

(threat intelligence, risk assessment, cybersecurity economics, test suites, pentesting)

protect

(technical and organisational measures)

detect

(human- or technology-based threat/anomaly detection, ML/Al/LLM for defense/security, honeypots/honeynets

respond

recover



Technologies/Application domains

cybercrime

cybercrime impact domains

prevention techniques

Technologies/Application domains

Celullar Wireless Technologies (2/3/4/5/6G)

Wireless Local Area Networks (WLAN/Wi-Fi)

Cellular Wireless Technologies: 5G private Networks: Cellular communications + IoT + WLAN

Vehicular communications: ITS G5 (802.11p)

Vehicular communications: 5G

Short range communications in IoT (Bluetooth, zigbee)

Long range communications in IoT (LoRa, 5G)

Satellite communications

Other next generation wireless networks and systems

In general: wireless linking functionality/ component/stage/aspect between humans and digital technologies



cybercrime impact domains

human targets (victims)

targeting humans to harm human collectvies

human individuals (direct targets) end users, citizens, customers, minors, members of human collectives

human collectives (indirect targets)

a) private entities
(companies, vendors and providers of wireless technologies, critical infrastructures)
b) public entities
(incl. law enforcement and national defense)
c) sociopolitical entities/institutions
(society, nation, pillars of democracy, public discourse)

Human factors of cybersecurity based on European values and fundamental rights



Human factors of cybersecurity based on European values and fundamental rights



Cosmopolitan Harm Convention to "protect everywhere from avoidable suffering and distress"*

^{*} Linklater, A. (2001). Citizenship, Humanity, and Cosmopolitan Harm Conventions; International Political Science Review / Revue internationale de science politique, Vol. 22, No. 3, Transformation of International Relations: Between Change and Continuity. Transformations des relations internationales: entre rupture et continuité (Jul., 2001), pp. 261-277 (17 pages)



Human factors of cybersecurity based on European values and fundamental rights



Cosmopolitan Harm Convention to "protect everywhere from avoidable suffering and distress"*



harm caused by and through (next generation) wireless networks

^{*} Linklater, A. (2001). Citizenship, Humanity, and Cosmopolitan Harm Conventions; International Political Science Review / Revue internationale de science politique, Vol. 22, No. 3, Transformation of International Relations: Between Change and Continuity. Transformations des relations internationales: entre rupture et continuité (Jul., 2001), pp. 261-277 (17 pages)



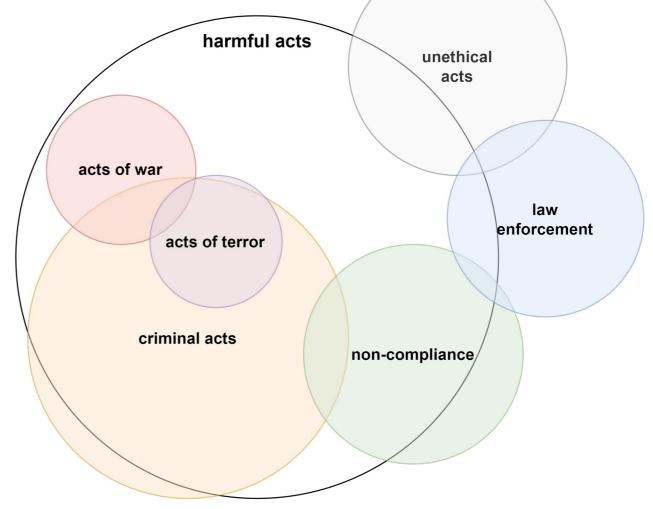
Human factors of cybersecurity based on European values and fundamental rights



Cosmopolitan Harm Convention to "protect everywhere from avoidable suffering and distress"*



harm caused by and through (next generation) wireless networks



^{*} Linklater, A. (2001). Citizenship, Humanity, and Cosmopolitan Harm Conventions; International Political Science Review / Revue internationale de science politique, Vol. 22, No. 3, Transformation of International Relations: Between Change and Continuity. Transformations des relations internationales: entre rupture et continuité (Jul., 2001), pp. 261-277 (17 pages)

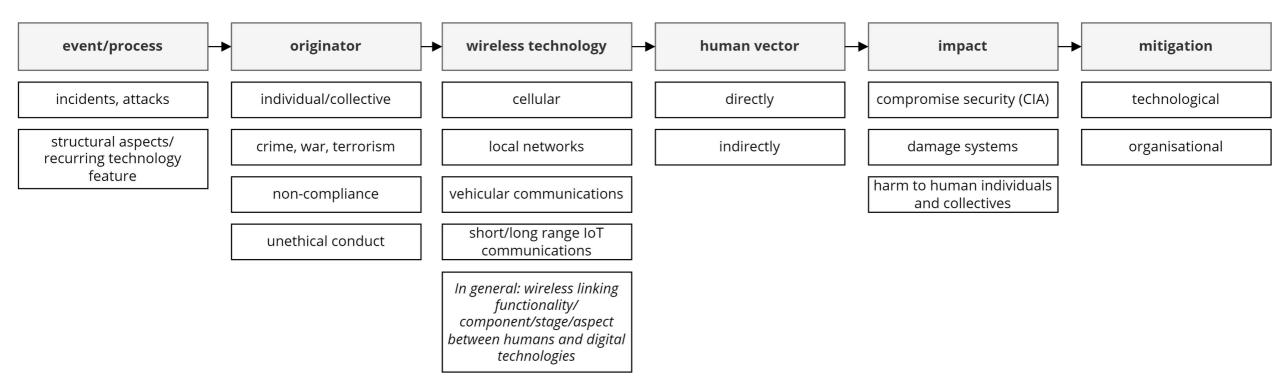


Focus of Working Group 2

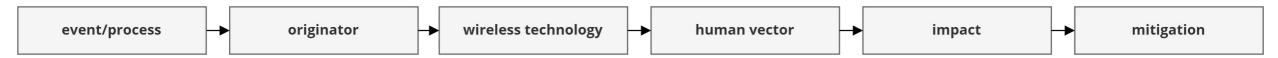
interdisciplinary perspectives (sociology, psychology, economics, media science, legal, (geo-)political, technological, ...) on ...

- a) events/processes,
- b) and their originators,
- c) which depend on the use of (new) wireless technologies,
- d) where human behaviours/aspects are directly or indirectly targeted/exploited
- e) to (significantly) compromise security/damage systems/harm human individuals and collectives
- f) and in technical and organisational measures to prevent those events/processes

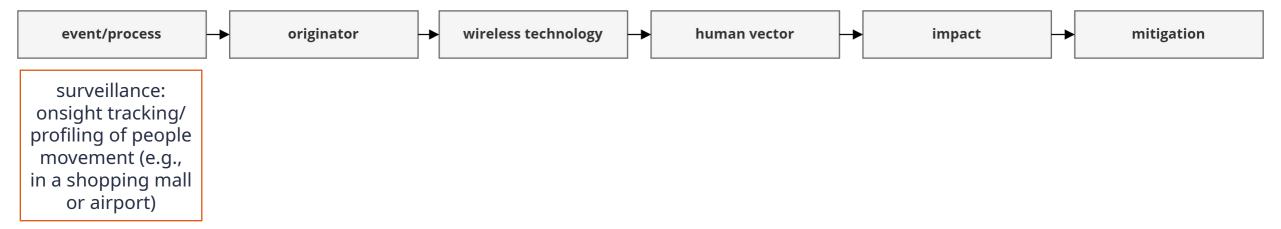
WG2 Interdisciplinary Research Heuristic



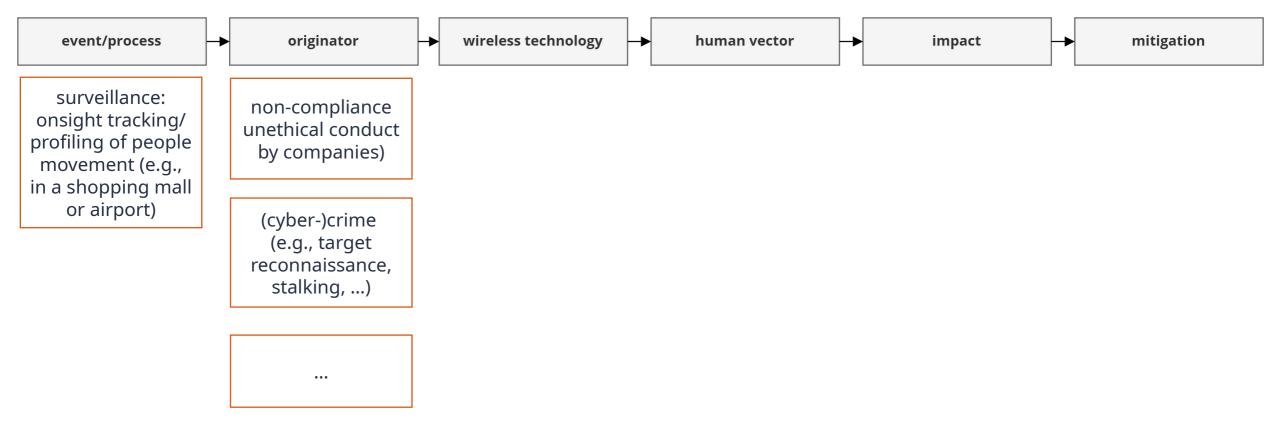




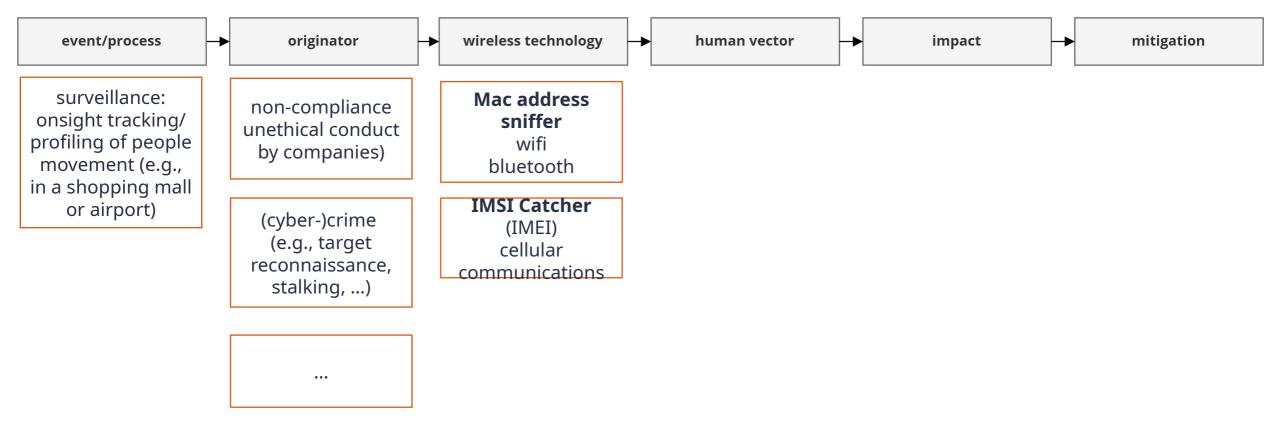








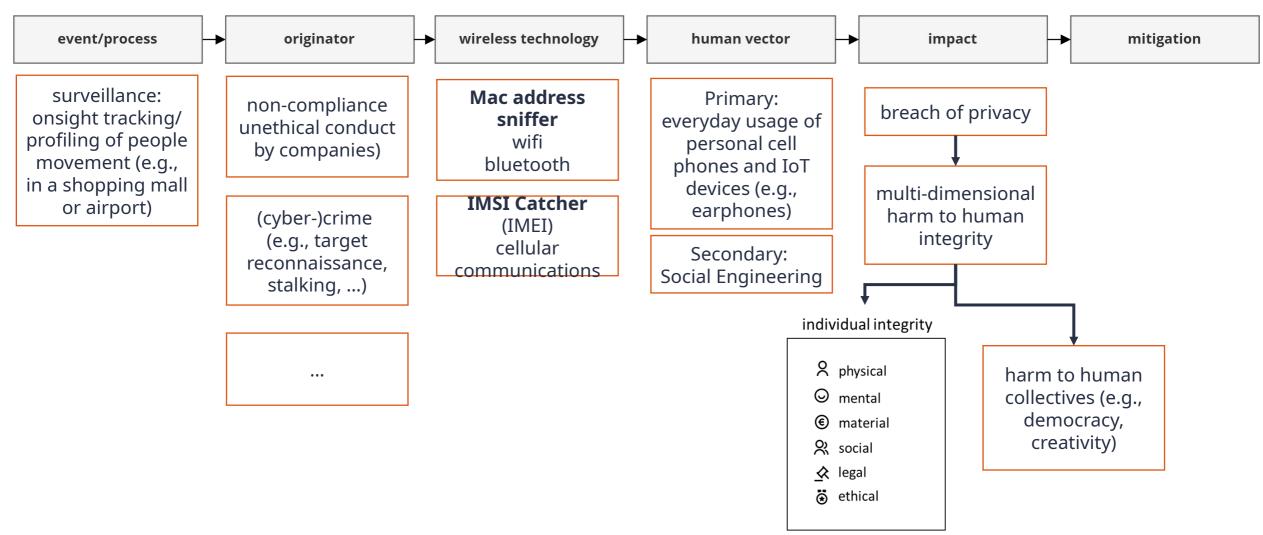






wireless technology event/process originator mitigation human vector impact surveillance: Mac address Primary: non-compliance onsight tracking/ sniffer everyday usage of unethical conduct profiling of people wifi personal cell by companies) movement (e.g., bluetooth phones and IoT in a shopping mall devices (e.g., **IMSI Catcher** or airport) earphones) (cyber-)crime (IMEI) (e.g., target cellular Secondary: reconnaissance, communications Social Engineering stalking, ...)







Vielen Dank!

Kontaktinformationen

Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH

Concorde Business Park F 2320 Schwechat Austria, Europa

Firmenbuch: FN 280353i Landesgericht Korneuburg

UID: ATU62886416

www.rise-world.com welcome@rise-world.com



