Beyond the binary: empowering youth as agents of change in cybersecurity and crime prevention

by **Per-Albin Johansson**

Global security and justice face a striking paradox. Despite youth crime's complex and profound societal repercussions,

> **"young people under the age of 24 (approximately 16% of the world's population[1]) remain largely excluded from decisions that will significantly shape their future."**

This disparity highlights a crucial need to shift the current approach from merely addressing youth crime as a challenge to actively engaging young people as key partners in reshaping crime prevention strategies.

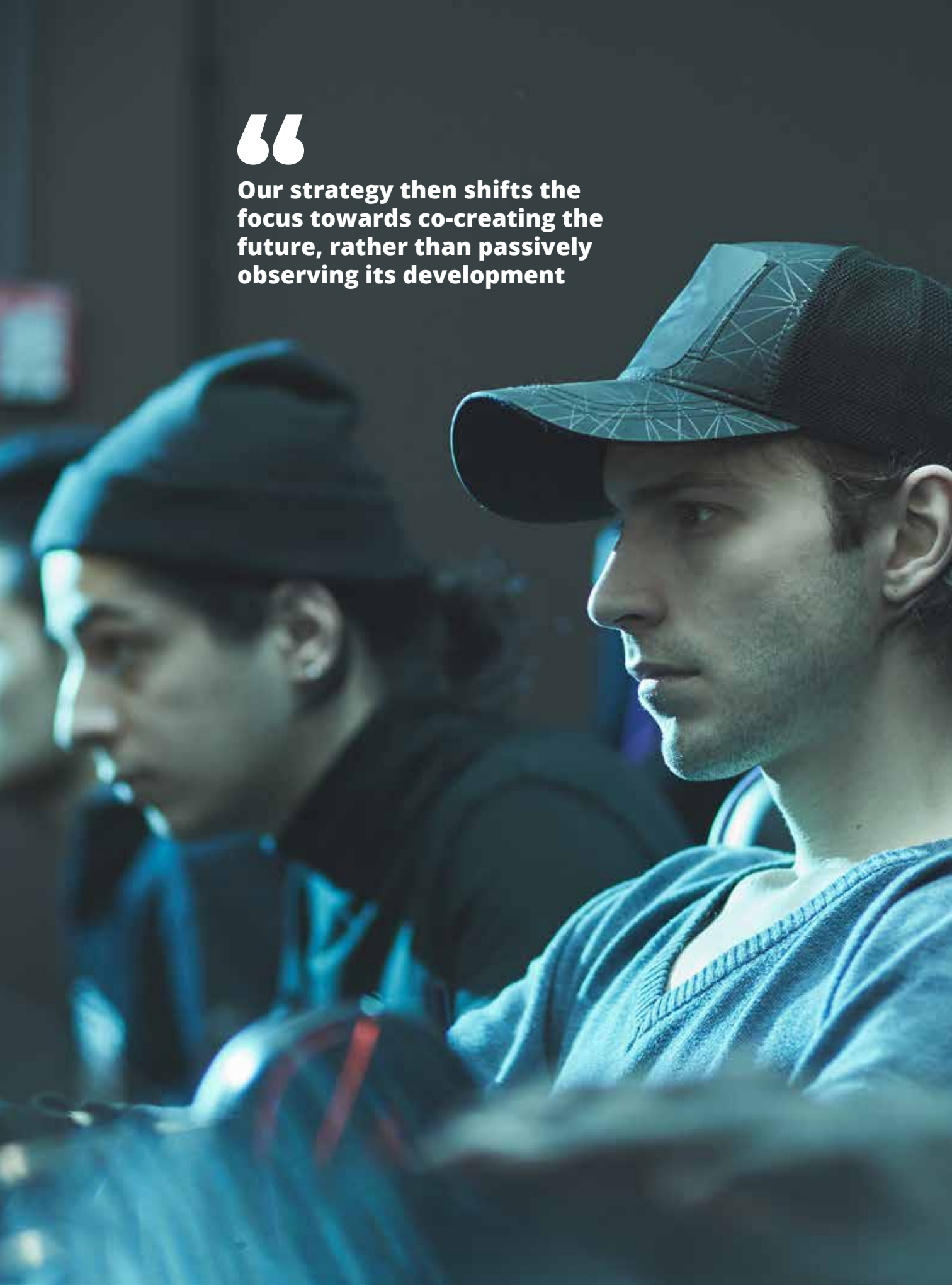
Simultaneously, it is evident that digital environments are emerging as one of the most prominent arenas of contemporary crime. This phenomenon extends far beyond traditional notions of offline criminal activity, encompassing a rapidly evolving spectrum of offences that occur online or are significantly facilitated by the Internet and related digital technologies. We are witnessing a fundamental reshaping of the criminal landscape, whereby cyber threats are not merely a specialized category but an increasingly pervasive element of modern criminality.

These 'digital and digitally mediated crimes' can broadly be categorized as cyber-dependent or cyber-enabled.[2] The first refers to offences that can only be committed using information and communication technologies (ICTs) or within the digital realm.

However — and more importantly concerning youth and adolescents — the second category comprises traditional crimes that are amplified, extended, or even made possible through the use of digital technologies. This category includes fraud, child sexual exploitation, illegal trade in

[1] United Nations, *World Youth Report 2020* (New York: Department of Economic and Social Affairs, 2020).

[2] European Parliamentary Research Service, *Cybercrime and Cybersecurity*, Briefing 760356 (Brussels: European Parliament, 2024).



Our strategy then shifts the focus towards co-creating the future, rather than passively observing its development

goods (drugs, weapons, etc.), and perhaps most critically, criminal recruitment.[3]

The increasingly blurred lines between the virtual and physical worlds contribute to the stark reality of escalating youth recruitment into criminal networks, a challenge that is particularly pressing in the Nordics.[4]

> **"Popular social and gaming-adjacent platforms, such as Roblox and TikTok, are increasingly used by criminal actors for recruitment purposes."**

The ease of access and anonymity these platforms afford allows recruiters to target and manipulate vulnerable adolescents. Through seemingly innocuous interactions, young people are subtly drawn into illicit activities. After instrumentalizing the individual for their purposes, those who orchestrated the initial crime disappear, leaving the new 'perpetrator' to carry out the illicit activities and, more importantly, face the consequences alone.

In parallel, the predominantly analogue legal and policy systems frequently lag behind arenas where crime increasingly risks creating lawless spaces: mainly in cyberspace.[5]

This evolving landscape reveals the profound inadequacy of many traditional legal constructs, particularly the foundational victim-perpetrator binary, to address modern criminal dynamics. Adolescents often oscillate between being targeted and being coerced into committing offences; consequently,

[3] Johansson, Per-Albin, "Northern Sprites: Gamifcation and Youth Recruitment in the Nordic Region, "*GNET Research*, 30 October 2024.

[4] Tollin, Katharina, Angerbrandt, Henrik and Jonsson, Anna, *Children and Youth in Criminal Networks: Network Entry, Offending, Conditions, and Network Exit,* Report 2023:13 (Stockholm: Swedish National Council for Crime Prevention, 2023).

[5] Europol, *Policing in an Online World* (The Hague: Europol, 2025).

> **"the lines between being an impressionable individual groomed and subsequently compelled into illicit acts are as blurred as those between the virtual and physical realities."**

Without clear and legitimate conceptualization, many young people are left in a legal and ethical limbo, where traditional definitions of culpability and victimhood offer little clarity or protection.

Youth caught up in episodes of violence, such as those observed in Sweden[6], are often placed in a precarious position and reductively categorized as either passive recipients of harm or singularly responsible perpetrators. This problematic framing highlights a critical inadequacy that is not merely a fallacy, but an opportunity to rethink our approach fundamentally. Rather than maintaining this dichotomy, we must champion a transformative method that recognizes and cultivates their potential as active agents of change before they become entangled in the cycle. Beyond their aforementioned and acknowledged vulnerabilities to cyber-dependent or cyber-enabled crimes, youth represent a powerful, often untapped, resource.[7]

Observations from contexts such as Sweden, as well as the Netherlands, indicate that the critical challenge in empowering youth as agents of change often lies not in their disinterest but in outdated communication strategies.[8]Adults frequently talk about young people, rather than with them, employing language, formats, and channels that fail to resonate. This oversight perpetuates the misconception that digital security is an inherently technical or frightening domain, leading to immediate disengagement. To truly connect with young

6 Europol, *Policing in an Online World* (The Hague: Europol, 2025).

7 United Nations Offce on Drugs and Crime (UNODC), Crime Prevention and Youth (Vienna: UNODC, n.d.).

8 Schiks, J.A.M., van 't Hoff-de Goede, Susanne and Leukfeldt, Rutger E., "An Alternative Intervention for Juvenile Hackers? A Qualitative Evaluation of the Hack_Right Intervention," Journal of Crime and Justice, vol. 47, no. 4 (2024): 492–510.

audiences, the discourse around digital safety must be reframed to align with their lived digital realities: encompassing social media interactions, online gaming, gamified environments, and, especially, peer relationships. This approach should therefore focus on demonstrating how proactive digital safety directly impacts their everyday lives. Practitioners should recognize that peer influence is a potent force among adolescents, accordingly, a powerful strategy emerges: cultivating a movement of digital role models on the very social and gaming-adjacent platforms where they spend much of their time.

This methodology is effectively realised by public-private partnerships like HackShield Future Cyber Heroes and its extensions, which engage youth through game mechanics in simulated and safe digital environments. Crucially, such an approach fosters their active agency.

> **"Selected participants, collaborating directly with both law enforcement and cybersecurity specialists, move beyond conventional learning to actively share their knowledge.[9]"**

Both in Sweden and the Netherlands, they act as intermediaries by conducting presentations for their classmates, leveraging peer influence to illustrate digital threats in a simple manner. Moreover, these young agents have gone on to facilitate crucial intergenerational knowledge transfer by subsequently advising seniors on online safety practices.

By supporting these youth-led voices through similarly integrated programs, it is possible to foster engagement and create a more relevant, accessible, and ultimately effective culture of cybersecurity awareness and resilience.

> **"The malevolent creativity of cybercrime necessitates equally creative responses, and neglecting the inherent agency of young people, with their innate understanding of online environments, is a critical gap that must be addressed."**

True progress hinges on recognizing youth not as passive subjects or singular perpetrators, but as indispensable agents of change. This engagement empowers them to not only protect themselves and their peers but also to defend acquaintances — such as vulnerable family members targeted by fraud or manipulation — from the growing impact of organized crime in digital environments. In essence, our strategy then shifts the focus towards co-creating the future, rather than passively observing its development.

[9] Spithoven, R., Leukfeldt, R., Misana-ter Huurne, E., van 't Hoff-de Goede, S., van Houten, Y., Bekkers, L., Foppen, E. and te Bos, J., *Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime* (The Hague: n.p., 2022).

About the Author

Per-Albin Johansson is an experienced conflict researcher and specialist in digital crime prevention who bridges the gap between complex academic theory and tangible, everyday security solutions. As the Safer Sweden Foundation's main expert on cyber-enabled crime, he utilises a multidisciplinary background in crisis management and conflict transformation to interpret the modern threat landscape. Whether researching online vulnerabilities or implementing agency-centred initiatives, Per-Albin is driven by the goal of eliminating the offender's opportunities for crime rather than restricting the victim's fundamental right to digital participation.