FREEDOM FROM FEAR
MAGAZINE

PROGRESS WITHOUT COMPASS

Rethinking crime, justice and rights in an algorithmic world

unicri
United Nations Interregional Crime and Justice Research Institute

GHENT UNIVERSITY

Contents

Between Daedalus and Icarus: Governing Risk in the Digital Labyrinth

by Leif Villadsen,
Acting Director of UNICRI

Today's global digital transformation is not merely technological; it is profoundly human, reshaping how we relate, decide, and understand the world. The myth of Daedalus and Icarus offers a compelling lens through which to interpret this moment. Daedalus, the father of Icarus, is both the architect of the labyrinth built to contain the Minotaur and the inventor of the wings designed to escape it. He embodies human ingenuity – the capacity to create systems of extraordinary sophistication to manage danger, but also the risk of becoming trapped within the very complexity we design. His role as a father adds a further layer of responsibility: he can provide tools and guidance, but cannot control how they are used. Icarus, by contrast, despite Daedalus' warning not to fly too close to the sun, represents the impulse to transcend limits, driven by ambition, possibility, and overconfidence. The closer humanity moves toward the metaphorical sun of limitless technological possibility, the more urgent become the questions of governance, ethics, and accountability. Together, Daedalus and Icarus capture a defining tension of our time – between creation and control, innovation and responsibility, freedom and risk.

This tension is not confined to myth. It is evident in modern history with the creation of the atomic bomb during the Manhattan Project – a turning point in human capability that demonstrated how scientific progress can outpace the frameworks needed to govern its consequences. Scientists, like Daedalus, harnessed extraordinary ingenuity to confront an existential threat, yet the power they unleashed raised enduring questions about responsibility, control, and the limits of human foresight.

Digital technologies are advancing at unprecedented speed, unlocking new opportunities for inclusion and development while simultaneously expanding the operational space for criminal actors. This dynamic reflects a fundamental asymmetry: technological capabilities grow exponentially, while societal understanding and institutional adaptation lag behind. As a result, threats – from opaque cybercriminal economies, growing overlaps among online harms and AI-enabled threats – are becoming more complex, less visible, and increasingly transnational, with impacts that extend beyond economic loss to affect trust, security, and fundamental rights.

At the same time, vulnerabilities are intensifying. Legal and regulatory frameworks remain largely confined within national borders, while cyber threats move seamlessly across them. Persistent challenges in attribution, accountability, and enforcement continue to expose structural gaps in the international legal architecture. Global efforts, including the new United Nations Convention against Cybercrime, mark important progress, but their effectiveness will depend on sustained political commitment and coordinated implementation.

This transformation is unfolding against a backdrop of escalating global tensions, persistent conflicts, and a visible erosion of multilateralism. As cooperation fragments, the capacity to address inherently transnational cyber threats is further constrained.

Addressing these challenges requires a balanced and comprehensive response. Strengthening normative frameworks is essential, but not sufficient. International cooperation must be deepened, and public–private partnerships reinforced, recognizing that much of the digital ecosystem lies beyond the direct reach of governments.

Young people stand at the centre of this transformation. They are among the most exposed to online harms, yet also among the most capable of shaping responses. As digital natives, they operate in environments defined by anonymity, algorithmic influence, and blurred boundaries between physical and virtual realities. Strengthening digital awareness, critical thinking, and behavioural understanding is therefore not only protective – it is strategic. Investing in digital literacy and positioning youth as active contributors to cybersecurity and crime prevention offers a pathway towards more sustainable solutions.

This issue of F3 brings together diverse perspectives that reflect the multifaceted nature of cyberspace today. From legal analysis to behavioural insights, from technological innovation to community-based initiatives, the contributions highlight both the complexity of the challenges and the breadth of responses required.

No single actor can address these challenges alone. A collective effort – grounded in shared responsibility, informed by knowledge, and guided by a commitment to justice and human rights – remains essential. Only through such an approach can technological progress serve not as a vector of harm, but as a foundation for safer and more equitable societies.

Yet, without clarity of direction, even collective efforts risk falling short. As depicted in The Parable of the Blind by Pieter Bruegel il Vecchio, a line of individuals advances across uncertain ground, each relying on the next, unaware of the risks ahead. It is a stark reminder that progress without vision does not merely fail – it amplifies vulnerability. Ensuring that awareness, responsibility, and cooperation guide our steps is therefore not optional, but essential to building safer, more just and resilient societies.