FREEDOM FROM FEAR
MAGAZINE

THE NEW CRIMINAL CODE: DECIPHERING EMERGING THREATS IN CYBERSPACE

unicri
United Nations
Interregional Crime and Justice
Research Institute

GHENT
UNIVERSITY

CONTENTS

When code shapes crime: rethinking responsibility in the digital age

by Leif Villadsen
Acting Director of UNICRI

Foreword

Digital technologies are transforming the way societies function, communicate and protect themselves. At the same time, they are reshaping the nature of crime, creating new opportunities for harm while challenging existing legal, institutional and governance frameworks. Understanding emerging criminal threats in cyberspace has therefore become an essential priority for policymakers, practitioners and researchers alike.

Cyberspace is no longer simply a domain in which crime occurs; it is an environment that actively influences how criminal activities are organized, scaled and concealed. A wide range of digital technologies - from automated tools and data-driven systems to advanced online platforms - can enhance efficiency and connectivity, but they can also be exploited to lower barriers to entry, expand the reach of criminal networks and weaken traditional forms of oversight and accountability.

Criminal actors have demonstrated a notable capacity to adapt to these changes. Organized crime groups increasingly operate across digital and physical spaces, exploiting online infrastructures to facilitate cyber-enabled crime, fraud, illicit financial flows and other forms of transnational criminal activity. Terrorist actors similarly use digital en- vironments to disseminate propaganda, support recruiment and operate in decentralized ways that are more difficult to detect and disrupt. These dynamics highlight how emerging technologies are reshaping crime in cyberspace, often faster than regulatory and institutional responses can adapt.

At the heart of these challenges lies a fundamental tension between technological innovation and human responsibility. Digital systems, including those based on artificial intelligence, can process vast amounts of information and support decision-making, but they do not possess judgement, context or ethical awareness. Machine "reasoning" is based on mathematical models, statistical correlations and optimization towards predefined objectives. The risks associated with these developments extend beyond technical harm. Autonomous and semi-autonomous systems, whether deployed for security, surveillance or operational purposes, cannot make ethical judgements. A system may identify a threat or a target, but it cannot assess proportionality, intent or human dignity. When such technologies are misused or insufficiently governed, they risk eroding accountability, undermining trust and blurring the line between human decision-making and algorithmic action.

This is where human-trust solutions play a vital role. Keeping human beings meaningfully involved in decision-making processes, ensuring transparency and contestability of technological systems, and clearly defining responsibilities are essential elements of effective responses to cybercrime and online harms. Preserving digital trust is not only a technical objective, but a strategic and societal imperative.

UNICRI's work on cybercrime and online harms contributes to this effort by supporting States and stakeholders in strengthening prevention, enhancing criminal justice responses and promoting international cooperation in the digital space. Through research, capacity-building and policy-oriented initiatives, UNICRI seeks to address the evolving risks posed by cyber-enabled and cyber-dependent crime, while reinforcing respect for human rights and the rule of law.

This issue of F3 marks the first in a series dedicated to these themes. It explores the dynamics shaping the new criminal code of the digital era, shedding light on emerging criminal threats in cyberspace and on how technological change is reshaping criminal behaviour.

The issue gives voice to a diverse range of stakeholders, including young people, to reflect the many facets of the challenges posed by rapid tech- nological advancement for security and human rights, as well as the responses that are possible. It underscores that prevention and response must be inclusive and collaborative, involving all relevant actors - from governments and academia to the private sector and civil society.

By fostering informed dialogue and shared understanding, this issue aims to contribute to the collective effort to preserve digital trust and to promote an open, safe and secure digital era for all.