*European Journal of Risk Regulation* (2025), **16**, 466–468
doi:10.1017/err.2025.10026

CAMBRIDGE UNIVERSITY PRESS

PREFACE

# EU Cybersecurity Policies in Cyber-Physical Ecosystems: Challenges and Perspectives

Raffaella Brighi[1] and Giovanna Adinolfi[2]

[1]Department of Legal Studies, University of Bologna, Bologna, Italy and [2]Department of International, Legal and Historical-Political Studies, University of Milan, Milan, Italy
**Corresponding author:** Raffaella Brighi; Email: raffaella.brighi@unibo.it

## Abstract

After an introduction to the notions of cybersecurity and cybersecurity-related risks, this preface introduces four collected contributions on challenges and perspectives of EU cybersecurity policies in cyber-physical ecosystem.

**Keywords:** Cybercrime; cyber physical eco-systems; cybersecurity; EU cyber resilience act; facial recognition technologies

Cybersecurity is an integral part of citizens' lives. Not only are economic activities, but also the orderly functioning of societies and democracy at large, increasingly dependent on interconnected networks, information systems, and devices. The security of these digital technologies must be ensured not only for individuals to trust them but also to uphold human rights and fundamental freedoms. The widespread use of networks, information systems, and connected devices from the 1990s to the early 2000s led to an expansion of the "attack surface," which refers to the potential areas that malicious actors can target. Yet, the increasing deployment of cyber-physical systems (CPS) signifies a fundamental shift in the threat landscape.[1] CPS sit at the intersection of the physical and digital worlds, integrating components such as physical objects, software, and networks to control physical processes in real time. Through sensors and actuators, they gather environmental data, autonomously determine operational status and interact with other CPS.[2] Supported by 5G, cloud computing, and artificial intelligence, CPS technologies are transforming industry, agriculture, healthcare, transportation and public policies by increasing automation and autonomy. However, significant security challenges are emerging. On the one hand, CPS represent a new attack surface for cyber threats, as highlighted by ENISA, which predicts a rise in attacks by 2030.[3] The lack of specialised skills, misconfigurations, insufficient maintenance and inadequate support make these devices vulnerable. Attacks can exploit outdated devices or those with default settings to gain initial access, move laterally across networks, and compromise sensitive data. Against the

[1] See PG Chiara, *The Internet of Things and EU Law: Cybersecurity, Privacy and Data Protection Challenges* (Cham, Springer 2024).

[2] See A Rayes and S Salam, *Internet of Things from Hype to Reality: the Road to Digitization* (Cham, Springer 2022).

[3] ENISA, *Identifying Emerging Cyber Security Threats and Challenges for 2030* (2023), available at https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf.

© The Author(s), 2025. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/err.2025.10026 Published online by Cambridge University Press

background of today's "digital-physical"[4] environment, risk factors and threats go beyond the technical infrastructure networks, information systems and devices. Cyberattacks could also infringe individuals' fundamental rights, impair physical safety[5] and have critical consequences for the democratic process of a society.

On the other hand, CPSs coupled with AI-based surveillance technologies have become extremely attractive to profile consumers or predict their preferences and enhance law enforcement authorities' control and monitoring.

The massive collection of behavioral, health and connected device data exposes individuals to risks such as profiling and social engineering attacks. To ensure the secure and sustainable development of CPS, an integrated approach is needed that balances innovation, fundamental rights and advanced cybersecurity measures, preventing the misuse of technology and mitigating risks to users' and citizens' privacy and security.

Cyber threats are, therefore, on the rise, varied and sophisticated, and the changing geopolitical scenario has further intensified the scope of the risk: known challenges have returned to the fore, and new ones have emerged, such as the security of supply chains on which critical infrastructures often rely.

In the context of rising safety and cybersecurity risks due to the digitisation and datafication of society, this special issue seeks to highlight the various normative challenges – legal, ethical and social – that cybersecurity governance faces, with a particular focus on the European continent. Thus, in recent years, risk-based regulation[6] has predominantly been the model of governance adopted by the European Union since the publication of the Digital Single Market Strategy.[7] EU legislation in the fields of data, online content and artificial intelligence is informed by a risk-based approach, albeit with differences.[8] Recent EU legislation in the field of cybersecurity makes no exception to this regulatory trend.

Against the background of EU cybersecurity policy, in December 2020 the EU Commission and the EU High Representative for Foreign Affairs and Security Policy presented the third EU "Cybersecurity Strategy for the Digital Decade."[9] Cybersecurity is now a key, integrated component aligned with the European Digital Transition Plan,[10] the Recovery Plan,[11] and the European Security Strategy of July 2020.[12]

The Strategy contains proposals for legislative, investment and policy initiatives in three areas of EU action: (1) resilience, technological sovereignty and leadership; (2) developing operational capabilities for prevention, deterrence and response; and (3) promoting a global and open cyberspace.

[4] L Floridi, *The Online Manifesto: Being Human in a Hyper-Connected Era* (Cham, Springer Nature 2014).

[5] "Internet of Medical Things" (IoMT) is a prominent example of how cybersecurity is progressively taking into account safety considerations as cybersecurity technologies must ensure the integrity of life against cyberattacks.

[6] C Quelle, "Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach" (2018) 9 European Journal of Risk Regulation 509. See also R Baldwin, M Cave and M Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford, Oxford University Press 2012) 281.

[7] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe" COM(2015)192 final.

[8] G De Gregorio and P Dunn, "The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age" (2022) 59 Common Market Law Review 2, 476; PG Chiara and F Galli, "Normative Considerations on Impact Assessments in EU Digital Policy" (2024) 1 Medialaws 86.

[9] European Commission, *The EU's Cybersecurity Strategy for the Digital Decade* (JOIN2020) 18 final.

[10] European Commission, *Shaping EU's Digital Future* (2020), available at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_en#documents.

[11] European Commission, *Recovery Plan for Europe* (2020), available at https://commission.europa.eu/strategy-and-policy/recovery-plan-europe_en.

[12] European Commission, *European Security Union Strategy* (COM2020) 605 final.

https://doi.org/10.1017/err.2025.10026 Published online by Cambridge University Press

Against this background, this special issue aims to achieve twofold objectives. First, it seeks to examine the challenges presented by implementing the Commission's ambitious Strategy. Second, it aims to assess the implications of utilising new technologies for national security purposes.

To increase the level of cyber resilience and cybersecurity of the EU's public and private sectors, several actions have been promoted and will be tackled in the proposed contributions. In particular, two contributions will examine the legislative initiatives introduced by the European Union with the objective of preventing cyber-attacks. Pier Giorgio Chiara's article, entitled "Understanding the regulatory approach of the Cyber Resilience Act: protection of fundamental rights in disguise," will focus on the regulatory foundations and fundamental rights implications of the Cyber Resilience Act, which sets technical requirements for products with digital elements. In her article ("The Cyber Solidarity Act: framework and perspectives for the new EU-wide cybersecurity solidarity mechanism under the EU legal system"), Susanna Villani addresses the proposed Cyber Solidarity Act, which aims to enhance the detection of and preparedness for cyber threats across the EU.

A third selected contribution is based on the premise that the recent wave of EU regulations seems to neglect a traditional tool in the fight against cyber threats, namely criminal law. In "Cybersecurity and the Fight against Cybercrime: Partners or Competitors?" Laura Bartoli analyses the rationale behind this approach and the emergence of new trends and proposals aimed at facilitating the prosecution of cybercriminals.

The final contribution, by Giulia Gabrielli ("The use of facial recognition technologies in the context of peaceful protest: the risk of mass surveillance practices and the implications for the protection of human rights"), takes a human rights approach to examine the implications of the use of AI-based technologies by law enforcement authorities. Since the EU advances a vision of cyberspace founded on the rule of law, human rights and democratic values, it is imperative to ensure that the implementation of public security policies is aligned with States' obligations under human rights treaties.

The articles in this special issue are the first research outputs of the project "EcoCyber – Risk management for future cyber-physical ecosystems," within (Spoke 8 "Risk Management and Governance") the Italian project SERICS (SEcurity and RIghts in the CyberSpace, PE00000014) funded by the European Union – NextGenerationEU through the Italian Ministry of the University and Research National Recovery and Resilience Plan – Mission 4 Component 2, Investment 1.3.

**Cite this article:** R Brighi and G Adinolfi (2025). "EU Cybersecurity Policies in Cyber-Physical Ecosystems: Challenges and Perspectives". *European Journal of Risk Regulation* **16**, 466–468. https://doi.org/10.1017/err.2025.10026

https://doi.org/10.1017/err.2025.10026 Published online by Cambridge University Press