

Carmen Elena CÎRNU
Editor in Chief
International Journal of
Cyber Diplomacy

EDITORIAL

Welcome to the seventh volume of the International Journal of Cyber Diplomacy. This issue brings together contributors from universities, think tanks, defense institutions and our own research teams, writing from Romania, Malaysia, Slovenia, Germany and elsewhere. We thank our authors, reviewers and readers for helping ICI Bucharest build the IJCD into a place where policy practice and academic research can speak to each other, in support of the Center for Cyber Diplomacy and of our strategy of internationalization and networking.

From 10 to 12 March 2026, the Palace of Parliament hosted the Digital Innovation Summit Bucharest, organized by ICI Bucharest under the high patronage of the President of the Chamber of Deputies and the Government of Romania. It combined the ninth Critical Infrastructure Protection Forum, dedicated this year to dual-use technologies and artificial intelligence, with the fifth International Conference on Cyber Diplomacy and the second Blockchain Intelligence Forum on the final day. The panels addressed science diplomacy, international cooperation and regional conflicts, and we welcomed partners such as Azerbaijan's State Service for Special Communication and Information Security, with which we signed a memorandum of understanding in 2023.

The year also brought new institutions to cyber diplomacy. In New York, the Global Mechanism on ICT security, the permanent UN forum succeeding the open-ended working group, held its organizational session on 30 and 31 March and its first substantive plenary on 20 to 24 July, with thematic groups meeting in December. Given the geopolitical divisions behind its creation, the test will be whether states can turn an agreed framework of responsible behavior into practical cooperation. The UN Convention against Cybercrime, opened for signature in Hanoi in October 2025, has more than seventy-five signatories but only a handful of ratifications against the forty required, and it closes for signature on 31 December. Artificial intelligence now has a UN venue as well: the Global Dialogue on AI Governance met in Geneva on 6 and 7 July, days after the Independent International Scientific Panel on AI published its preliminary report.

Two developments closer to the subject of this issue deserve mention. The first is the Pall Mall Process, launched by the United Kingdom and France in 2024 to curb the proliferation and irresponsible use of commercial cyber intrusion capabilities. After a Code of Practice for States in 2025, guidelines for companies, drawn up after a consultation from November 2025 to January 2026, are expected to be finalized in November. The process is voluntary and has no enforcement mechanism, but it illustrates our view that cyber diplomacy is not the sole preserve of foreign ministries. The second is the European Commission's proposal of 20 January 2026 to revise the Cybersecurity Act, which would allow the EU to designate high-risk ICT suppliers and to restrict or phase out their products in critical sectors. Whatever form it takes, it shows cybersecurity regulation serving as an instrument of foreign economic policy, and countries that buy or sell the technologies concerned will follow it closely.

Closer to home, the war in Ukraine continues to shape the Black Sea and the eastern neighborhood. The NATO summit in Ankara on 7 and 8 July reaffirmed Article 5, described deterrence and defense as complemented by space and cyber capabilities, and recorded a pledge of 70 billion euros in support for Ukraine in 2026. The Republic of Moldova opened its first accession negotiating cluster with the European Union on 15 June and a second, on external relations, on 14 July, aiming to conclude negotiations by 2028. For Romania, which shares a language, a border and a growing digital agenda with Moldova and sits on the Alliance's Black Sea flank, these events bear directly on policy priorities, and several articles in this issue speak to them.

The contributions reflect this range. Two address information manipulation: one draws lessons for international cooperation and information resilience from hybrid conflicts in the Middle East, adding a regional case to our earlier comparative work on disinformation, and the other treats Malaysia as a node in the diffusion of foreign information manipulation and interference (FIMI) and in the defense against it.

Norms and sovereignty form a second group. One article asks how the norms developed for cyberspace can carry over to the governance of outer space, a theme that has followed this journal since its earlier issues, while colleagues from the Slovenian Ministry of Defence examine cyber diplomacy in an age of technological sovereignty, setting the UN normative framework beside the strategic approaches of the United States, the European Union and Japan.

Two articles focus on Romania and the Republic of Moldova. The first separates formal commitments from measurable outcomes in the emerging bilateral digital cooperation framework, in areas such as roaming, digital identity, cybersecurity cooperation and funding, and finds the current architecture meaningful but still fragmented. The second approaches self-sovereign identity as an instrument of cyber diplomacy, following the path from cyber resilience to digital trust between the two countries. Finally, an article on cyber diplomacy in NATO's evolving architecture presents Romania as a regional hub and a vector of resilience in the Black Sea, in light of the Ankara summit.

We hope you will keep reading and engaging with us and we invite you to publish your research with the IJCD and to join the next International Conference on Cyber Diplomacy.