Carmen Elena CÎRNU
Editor in Chief
International Journal of
Cyber Diplomacy

EDITORIAL

I am very glad to welcome you to a new edition of the International Journal of Cyber Diplomacy. We have a very interesting line-up of articles, to match the interesting developments that are taking place worldwide.

2024 is shaping up to be a landmark year for democratic systems, with numerous legislative and executive elections, some countries such as Romania having more than one election at the same time. This is leading to anxieties about the security of electronic voting systems, electronic voter rolls as well as the impact of online disinformation, fake news, and algorithmic biases on the perceptions of the citizenry and the outcomes of democratic processes. These fit not just in a hybrid war context (or new generation warfare, 4th or 5th generation warfare depending on who you ask), but also is a result of systemic transformations that lead to emerging behaviors within the system outside of the control of deliberate state or non-state actors. On the positive side, we have citizens journalists and non-state development of key tools and amenities, such as fact-checking and awareness raising in cybersecurity. On the negative side, we have social media and search algorithms that enhance polarization to drive engagement, that are biased on issues and people in ways that disturb competition and persuasion in the public sphere, and can lead to out of control conspiracy theorizing or political enmity. Cyber Diplomacy becomes key as states and other entities try to address both deliberate and systemic issues with cross-border impact. States give and receive technical and logistical assistance to ensure fair elections and the perception of fair elections, they regulate (sometimes cajole, threaten and sanction) tech and social media companies oligopolies/ monopolies and they band together to build norms and regulatory frameworks that are stronger than individual state regulations. Ultimately, these are also in the interest of the systemic companies, which are, as a rule, interested in predictability and clarity in regulation and have chafed at contradictory pronouncements from political actors regarding systemic bias or political speech regulation. Look no further than the EU, but also efforts on the part of the OECD, the African Union and ASEAN to ensure electoral integrity.

The practice of Cyber Diplomacy, as it relates to these issues, is becoming more acute in the field of emerging digital technologies. We only have to consider the impact of quantum computing on the security of encryption for digital systems backing either digital voting or old-fashioned paper voting. We can also mention the potential of AI and especially generative AI in influence campaigns designed to polarize, manipulate, and confuse individuals, while drowning out authoritative sources and reducing public confidence in institutions that maintain coherence of values and perspectives within society. The various Cyber Diplomacy toolboxes enacted by the EU and other actors, including on specific issues such as 5G, will have to be joined by cyber diplomatic AI toolboxes encompassing regulations, norms, sanctions capacity but also the technical capabilities of identifying and attributing AI-based manipulation efforts, as well as assistance packages for affected partners. Some of these assistance tools themselves will be AI based, for instance to detect and delete in real-time AI messaging on political issues on social media, and terms and conditions of deployment will have to be negotiated.

We spoke about electoral bumper years, but this is just the latest in a line of opportunities to reflect on the challenges and opportunities that digitalization and cross-border interconnectivity have generated. It means that States and other stakeholders are "condemned to cooperate" to address the myriad issues that result from digitalization, whether related to systemic threats, crime, warfare, hybrid warfare, geopolitical competition, consumer, and citizens protection and more. We addressed many of these issues during the 4th International Conference on Cyber Diplomacy on "Safeguarding in the Digital Era: The Dialogues of Cyber Diplomacy" which took place on the 16th of April 2024 at the Palace of Parliament in Bucharest, Romania. For the first time, ICI Bucharest has included the conference in a larger format called Digital Innovation Summit Bucharest, which includes also the Critical Infrastructure Protection Forum, as well as business expos, hackathons, interministerial meetings, to drive home the interconnectedness promoted by digitalization. The event was a striking success, benefiting also from the partnership with the European Defence Agency among other relevant actors and stakeholders.

Lastly, as mentioned before, we have a great line-up of articles for this edition of the Journal. For the first time, we have contributions on the regulation of crypto-assets from a legal and financial perspective at European level, we have a material on the use of strategic foresight to enhance resilience, an analysis of cybersecurity for web technologies used in cyber diplomacy, overviews of cyber diplomacy in China and the Middle East, and more. We thank you for being with us and look forward to growing our community further.