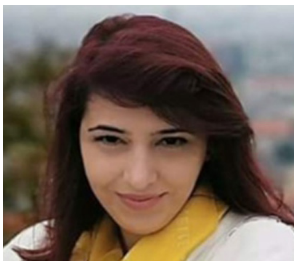

Carmen Elena CÎRNU
Editor in Chief
International Journal of
Cyber Diplomacy

EDITORIAL

We are proud to welcome you to the second edition of one of ICI's flagship products, the International Journal for Cyber Diplomacy. In this issue, we again have a strong international presence and a series of fascinating articles exploring different facets of the intersection between cyber and international issues. One such article I would like to draw your attention to is a report concerning a didactic tabletop exercise organized by the European Commission's Joint Research Centre with ICI Bucharest using the former's proprietary platform, Poseidon. This exercise, drawing together over 50 participants from 11 EU Member States, took place earlier in 2021 under the auspices of a pilot European course on critical infrastructure protection organized by the JRC with ICI Bucharest and the Digital Security Authority of Cyprus, under the aegis of the European Security and Defence College. The article underlines both the fascinating experience of the tabletop exercise, only partly diminished by having the debates take place entirely online, but also the role of international advanced education courses in fostering a European security culture that can then inform policy in areas that also include cybersecurity as a cross-cutting issue. The possibility of delivering quality submissions such as this one is what motivated the creation of the IJCD, and sustains our ambition of turning it into a tool to explore the various intricacies of the cyber diplomacy field (extending into cyber geopolitics), as well as a rallying point for a community of expertise that can then make its contribution to formulating solutions to these big problems affecting the international community.

The pandemic has brought cyber issues again to the fore of public consciousness, as the contraction of physically-mediated society brought with it an explosion in e-commerce, teleworking, online education and more. This vast transformation has brought with it an accelerated change in the security landscape and this has resulted in, among other issues, the need for states and other stakeholder entities to better coordinate in addressing collective action, the formulation of standards and best practices and the adoption of rules, norms and laws that govern behavior in cyberspace and which minimize the threat in a fragile environment.

It is still a subject of debate how this will be achieved. The main 'fashion' of our times is the multilateral approach, as inclusive as possible and based on trust enhancement measures that

should lower barriers to cooperation, should increase availability to contribute and sacrifice for collective security and decrease the rewards and the inclination to hostile behavior.
In practice, however, we see that the threat landscape is evolving faster than our capacity for governance in the multilateral sphere, which undermines its effectiveness. We still do not have acceptable and universal definitions for cyber-attacks, thresholds for being considered hostile action that invites legitimate retaliation, or the tools and procedures for credible attribution on the world stage. This 'lag in governance' is our greatest weakness and the most significant progress has been registered not at global levels, as has been the case in climate change governance, but at the level of alliances and supranational bodies. I refer here to the growing consensus within NATO regarding cyber attacks being a legitimate reason to invoke Article 5 for collective self-defense. I also refer to the developing cyber toolbox of the EU, including also sanctions.

While the future of cyber diplomacy is most definitely assured, its shape is not. While a global consensus on a rules-based order for the digital age would be the ideal, in practice we may discover that the alternative to an anarchic system is one in which blocs of nations agree on standards and then act to enforce them in order to promote stability. There are few walls left between economics, trade, regulation, security and defense in international relations, and allies or partners in one area will tend to develop varying levels of partnership in the others. The inability to develop a full relationship in all of these areas is a sure sign of systemic or geopolitical rivalries, and in this sense, cyber diplomacy becomes an indelible dimension of cooperation for would-be partners or, at the very least, for responsible stakeholders.

Join us in reading another issue of the International Journal for Cyber Diplomacy. It is with your assistance that we will manage to grow and to cultivate a stature befitting our chosen topic and our community of expert support.