Carmen Elena CÎRNU
Editor in Chief
International Journal of
Cyber Diplomacy

EDITORIAL

Welcome to ICI Bucharest's new publication, The International Journal of Cyber Diplomacy! For this journal, our aim is to bring together an eclectic group of contributors, from cyber experts to diplomats, military and law enforcement representatives and that it will contribute to the knowledge community that ICI has been building through its events, its partnerships and its publications. We are indebted to the members of our Advisory Board for their unwavering support and to our Editorial Board for their contributions in making this a successful first issue for our Journal. It is a publication which purposefully restricts itself to a certain topic, which may yet prove to be vast, rather than go the easy route of a topic which may accommodate any generality or pivot in accordance with fads and buzzwords.

There are a lot of buzzwords floating around the topic of cyber diplomacy, including digital diplomacy and data diplomacy, but by cyber diplomacy, the diplomatic activities between states, international institutions and even national institutions cross-border in order to handle cyber issues are envisioned. Our line-up reflects the inherent diversity of the concept. This first issue hosts articles on the legality of cyber warfare (and its regulation), on cyber sanctions, on a cooperation initiative for fighting transborder cyber crime and many more. Cyber acts not only as a medium for communication, coordination and integration of systems, but also as a binding agent for disparate systems in different sectors, different geographic areas and, just as importantly, different jurisdictions. Talk about cyber and, depending on your conversation partener, you may be talking about energy, or finance, about defence and security, or about privacy and consumer protection. There is no advanced or advancing nation which will not increase its degree of digitization of commerce, public administration, education or warfare, and there is no nation which will ever be secure and resilient without approaching the cyber issue with the utmost seriosity. Any who shirk this duty open themselves up not only to random accidents and cascading disruption, but also to deliberate threats with cyber as a means for coercion and subversion.

Cyber is the ultimate crosscutting issue and, in a globalised and globalising world, cyber diplomacy becomes as much of a necessity as science diplomacy, military diplomacy or cultural diplomacy, even moreso. And cyber diplomacy is not just the purview of diplomats, but also of experts in various field which find that their activity and security is increasingly

reliant on transborder cooperation through decision making, standard setting, information sharing and institutional constructivism. It means that diplomats have to be joined by critical infrastructure experts, by cyber experts, by public servants, military and law enforcement personnel and a host of other occupations categories impacted by cyber issues.

Cyber Diplomacy is not a proposal for a prospective instrument to settle cyber governance issues, but a reality. It is taking place at global levels and it is an emergent field which should be discussed and developed academically. For years, we have heard about states trying to negotiate cyber "ceasefires" regarding the proliferation and use of cyber weaponry as a means for hybrid warfare, given the vulnerability of systems and the potential for cascading disruptions in critical infrastructure systems (ex: cyber attacks against power plants). Even putative allies need cyber diplomacy to settle on a common position on an issue, such as the emerging consensus in NATO regarding the possibility of cyber attacks triggering Article 5 responses, or on the means through which sensitive information on attacks may be exchanged. Wherever there is discussion and a compromise to be made, you will find diplomacy. Whether it is the setting up of communications lines and information sharing for police work in transborder cyber activities, the sharing of information regarding attacks by cyber terrorists, rogue states and state agents, or the coordination of states believing in a rules-based order that safeguards a complex and interdependent international community, cyber diplomacy will be a natural part of it. This is because the trends are overwhelmingly in favor of an even deeper penetration of cyber into our daily lives, in the functioning of the economy and of states. With the Internet of Things adding trillions of networked sensors, with AI applications, driverless cars, many running on off-the-shelf components and software, as well as the commodification of malware, we see that the surface contact between the cyber realm and society is ever greater and the risks, vulnerabilities and threats more numerous.

In a multipolar world that is shrinking ever more because of advances in logistics and telecommunications, cyber diplomacy may become not just a tool for supporting decision making with regards to governance activities, but also a tool for a "modus vivendi" among an international community which is "condemned to cooperate" by the interdependencies which have accumulated and which care not for clashes of civilization, cultural enmity or historical resentment, but rhather for efficiency, growth, business continuity and quality of life.

It should also be said that this Journal arrives at an important moment for us as an organization. Its first venue of distribution will be our first course organized under the aegis of the European Security and Defence College of the European External Action Service – the pilot module for "Cyberdiplomacy – Tool for Strategic Security Policy" which will be attended by governmental officials, members of staff for intergovernmental and nongovernmental organizations and diplomats.

Ultimately, our publication efforts, courses and large scale events do not take place in a vacuum. They build off of each other to generate value for our knowledge community, to advance the issues of cyber security and critical infrastructure protection in Romania and to foster national and international partnerships that enhance security and create new opportunities for development and growth.

I hope you will find our efforts to be worthwhile and I look forward to the new opportunities for dialogue presented by the International Journal of Cyber Diplomacy.