Old Framework, New World: Setting the Stage for the "New Normal" in International Relations. Major Challenges and Ever-Growing Opportunities for Development in Cyberdiplomacy

Monica GHEORGHIȚĂ
National Institute for Research and Development in Informatics - ICI Bucharest
monica.gheorghita@ici.ro

Abstract: The world is witnessing a fantastic acceleration of time and the Fourth Industrial Revolution. With all the tectonic plates shifting, we find ourselves caught in a technological progress that challenges the realms of nation-states to its core value systems and the bureaucratic hierarchies inherited from the last century. National boundaries or cultural hemispeheres are permeated like never before and we are just starting to become aware of the implications these multi-layered processes bring into our daily lives. It is high time for governments, private actors and civil society to join hands and reinvent the speed for the creation of new paradigms and a long-term, ideally concerted, human-centric vision at a moment where these technologies are becoming political and carrying strong values and the world is increasingly difficult to forecast. A new generation of diplomats is called upon to transform cyberdiplomacy into a key instrument of the XXI century. Just like in every other field of human interaction, transformational change lies ahead in diplomacy as well, shaped by those who possess the capacity to adapt, to create and to implement a worldwide vision. These "normative soldiers" of the new decade have a difficult task ahead, if one takes into consideration the already existing disruptions and the challenges faced by democratic processes and traditional political institutions. Through the first International Journal of Cyberdiplomacy, a global project en premiere, the Romanian Institute for Research and Development in Informatics – ICI Bucharest brings forward the proposal for a new pact of trust between governements, civil societies and the entrepreneurial ecosystems, one in which you, our contributors and our readers alike become the Demiurges of a new, interconnected World, leading to a more prosperous, safe and fair society of the XXI century.

Keywords: Information, Innovation, Strategic, New oil.

INTRODUCTION

The creation of cyberspace is one of the most significant heritages of the 20th century. The emergence of this new realm of global interactions is reshaping relations between States and poses one of the greatest challenges for national security worldwide. Collaborative efforts have been undertaken to establish new rules and common principles that have the potential to ease tensions and increase the predictability and stability of this omnipresent channel of communication.

Hans Morgenthau stated in his *Politics among Nations: The Struggle for Power and Peace*, that "a subtle diplomacy aiming not at the conquest of territory or at the control of economic life, but at the conquest and control of the minds of men" would be one of the most powerful "instruments for changing the power relation between nations" [Morgenthau, 1973].

Forty-five years later, Indian Prime Minister Narendra Modi shared the belief that "whoever acquires and controls" data will attain "hegemony." [Davos, 2018]

Cyberspace lacks leviathan and is anarchic and decentralized by design. [George Wren, MIT Cybersecurity Seminar, 2015]. Under multiple pressures of an inherent strategic competition in the Information Age, States, the main building blocks of the post-Westphalian international arena are shifting their behavior, with unpredictable consequences. The reasons behind these trends are manifold. Information is nowadays more important than at any previous point in history as a result of positive developments in new technologies. These breakthroughs have altered all the key features of information power: the influence over the political and economic landscape of other actors; the capacity to communicate rapidly and securely; the creation of sustainable economic growth and wealth and the capacity to have a competitive decision-making leverage over other players.

The mere characteristics of cyberspace shed light on the ways in which contemporary international relations theory, policy, and practice will be fundamentally reshaped in the near future. Among these features one can enumerate: *temporality* (replaces conventional temporality with near instantaneity), *physicality* (transcends constraints of geography and physical location), *permeation* (breaches boundaries and jurisdictions), *fluidity* (sustains alterations and reconfigurations), *participation* (reduces barriers to activism and political expression), *attribution* (obscures identities of actors and links to action), and *accountability* (bypasses mechanisms of responsibility). [Choucri, 2016]

More than ever, the ability to set up and protect, or disrupt, information flows plays a key role in world affairs. Globalization and the planetary proliferation of information and communication technologies have created a new ecosystem dominated by unimpeded interactions within and between networks of connected individuals, across national borders, time and space, potentially disturbing the familiar international order. Moreover, the multifaceted technologies and political processes that are converging have created a setting of unknown variables.

We are increasingly using new vocabulary that reflects new behaviors, innovative ways to communicate and renewed threats to the security of states and individuals, groups and companies alike. It is a new reality or a "new normal" [Choucri, 2016], in a vital operational venue that brings new opportunities, new markets and new approaches for our collective view of rules of behavior, of international law and order. With data being "the new oil" [The Economist, 2017], investments continue to grow worldwide in search for innovative frameworks to promote economic development by facilitating the delivery of public goods and services to hard-to-reach communities across the globe, supporting education and generating constant job growth. Nevertheless, history has shown that the development of frontier technologies has always been inextricably tied to geopolitical disruptions and the continuation of this positive investment trend is, again, critically tied to security. A focus to create a secure cyber realm is more significant than ever, otherwise the full economic benefits that come with new technologies may not be attained.

On the other hand, there are signs of nations embarking on a cyber arms race, with investments in offensive capabilities that may trigger others to join in a spiral of cyber insecurity and the potential to inflict significant damage. It is therefore high time to act faster towards developing widely recognized norms and principles capable of shaping the behavior of actors in cyberspace. Geopolitics in the digital era will be marked by the influence of a plethora of actors, including large technology platforms, substate actors, nonstate actors, digitally-coagulated communities and even persuasive or merely vocal individuals. In the words of Samir Saran [2020], "the Westphalian state will soon co-exist and be implicated by the amorphous "cloud state", which exists beyond its geography. In this territory, domestic debates are not limited to citizens, and economic opportunities are dependent on the architecture of the cloud rather than trade regimes."

Another major challenge to traditional international relations is the fact that cyberspace, with its ubiquity and global dimension, is managed almost entirely by the private sector, found as such on the frontline of the information geopolitics. I agree with the inspired parralel used by Shaun Riordan [2019] - the existing strategy of depending on technical solutions against cyberattacks is the modern equivalent of the Maginot Line. We witness growing complexity in cyber management coupled with politicization. Public-private partnerships that support advanced technology development are, therefore, highly needed and a diplomatic approach may complement more security-focused approaches.

As revealed by an MIT study [2013], the expectation in the short run is that uneven patterns of cyber access will continue to reflect the distribution of power worldwide. In the long run, the global diffusion of cyber capabilities will expand political participation, enhance politicization of both idiom and action, and increase competition for influence and control over the management of cyberspace. These pressures will shape new ways of exerting power and leverage, create new structures and processes, and frame new demands for cyber norms, all of which will reflect the demography, capability, and values of the emergent cyber constituencies.

New institutions and mechanisms need to emerge to respond to a growing need for an *international digital forum*, to reunite the most powerful digital economies, both from the public and the private realms. It is notable that, while the institutional landscape is becoming increasingly dense, the coordination between them and the shared responses mechanisms lag far behind.

Promising efforts on the normative front are underway, within the United Nations (UN Group of Governmental Experts), the European Union and in other fora that have witnessed increasing numbers of international agreements that broaden these efforts, such as the Paris Call for Trust and Security in Cyberspace (November 2018), endorsed by more than 70 nations and 600 private sector companies, including Microsoft, Google and IBM. The outnumbering of State signatories by private sector organizations is a consistent expression of progress towards the creation of a multi-stakeholder environment that is quintessential to building strong norms in cyberspace.

THE ROLE OF CYBERDIPLOMACY IN BUILDING THE "PLATFORM PLANET": CONCEPTUAL CLARIFICATIONS

Against this background, how are States, accustomed to have monopoly over the affairs of citizens and resources, responding to the challenge of the "platform-ization of statecraft" [Saran, 2020]? What are the mechanisms of interactions they set up to capture this new powerful *Zeitgeist*? A large part of an ever-expanding literature and debate on the role of the "new diplomacy", or the "digital diplomacy" vs. "cyber diplomacy" has been generated by the adoption within governments at large and the ministries of foreign affairs around the world of digitally-based systems of content creation, transmission and storage usage the Internet, social media platforms, computers and a variety of wireless electronic devices. Typically conservative and resistant to change, with century-old traditions of conducting interstate relations, foreign ministries have been initially hesitant to embrace the unconventional. In recent times, this tendency has faded, with transformative effects worldwide, as one can witness a variety of new instruments and techniques used to support diplomatic activity, such as websites, blogs, RRS feeds, Twitter accounts, strategies of e-engagement et alia, that contribute to a deeper understanding of the sweeping changes that occur globally, where a variety of front-line issues are rooted in science and driven by technology. In an increasingly crowded infosphere, the 21st century diplomats have to master such techniques required to engage these issues. We played an almost desperate catch-up.

In the same vein, governments have used cyber venues to influence and to pursue their goals by affecting the security of their critics or detractors. It is a new approach that breaks down barriers and helps creating a kind of shared consciousness, a form of universal and collective intelligence. [Copeland, 2009] The consequences of these newly utilized instruments, products of globalization, are gradually unfolding. The WikiLeaks phenomenon is a good example to illustrate the double-edged value of technology, the risks and the implications associated with this case being deemed to endure long after the headlines have been forgotten. The State is not likely to accept, or even accommodate, such behavior. It remains a caveat, though, that the individual, alone or in groups, can significantly threaten established authority and weaponize information in unprecedented ways.

Moreover, States pursue the geopolitical gains that come from the expansion of their own technological systems and accompanying standards, by-products, rules and critical infrastructure protection. According to a Harvard Kennedy School study [2019], starting with 2015, the United States Department of Defense admitted that in order to preserve its global dominance, it needs to “rebuild bridges” with Silicon Valley and the tech sector. As a consequence, the Pentagon established new bases in U.S. tech hubs, focused on finding new avenues to leverage big data and AI-enabled technologies. As regards the People’s Republic of China’s case, the approach is even stronger. Under President Xi Jinping’s “civil-military fusion” thinking, all technologies acquired by the private and academic sectors, be they locally developed or imported, must be shared with the Chinese military.

One of the consequences generated by these competing behaviors is the growing division of the cyberspace and a low degree of interoperability between them. A struggle between “superpowers” in such an unconventional realm becomes therefore difficult to appease with the current instruments and mechanisms at hand. Different from previous iterations, a diverse team of stakeholders need to be engaged in order to adequately address the cyber realm.

Despite a growing corpus of writings on cyber-related issues in the study of international relations, a consolidated body of knowledge has yet to be set up. A cyber-inclusive view of international relations has become an imperative rather than a convenience.

Initially used interchangeably, the concepts of “digital diplomacy” and “cyberdiplomacy” have known necessary clarifications in recent literature. Melissen [2005] underlines “the evolution of diplomacy, namely the technological developments implicit in such terms as *cyber – diplomacy*, linking the impact of innovations in communications and information technology to foreign policy and diplomacy."

While *digital diplomacy* is instrumental in nature and includes merely the use of digital instruments for the promotion of diplomatic goals, *cyberdiplomacy* casts a light on the intersection of two realities, one belonging to a historically rooted institution dealing with the traditional conduct of international relations and the other "enabled by a constructed domain (*cyber*) as a new arena of human interaction with its own modalities, realities, and contentions" [Choucri, 2013], using the tools and mindsets specific to traditional diplomacy. It is about how to adapt or to reinvent diplomacy to have the suitable means for a hyperconnected world, by developing multi-stakeholder capabilities, and with the main task of building "an international community in cyberspace to which States and non-State actors will want to belong and consequently whose norms they will want to be seen to follow" [Riordan, 2019]. The core skills to support multi-level and heterogeneous coalitions needed for the development of a predictable and rules-based cyber realm are essentially diplomatic in nature.

In the EU, we consider cyberdiplomacy as "a set of diplomatic practices concerned with the broadly defined governance of cyberspace" [the working definition used by EUCyberDirect] and the main avenue for preserving and defending the open, free, secure and peaceful nature of cyberspace.

THE EUROPEAN UNION'S DIGITAL POLICY: CREATING THE INSTRUMENTS FOR TECH SOVEREIGNTY

The European Union and its Member States have constantly promoted an open, stable and secure cyberspace that respects human rights, fundamental freedoms and the rule of law. The EU's strength results from such a clear commitment towards cybersecurity as a pre-requisite for economic and social growth, in line with the United Nations Sustainable Development Goals.

The EU's cyberdiplomacy aims to strengthen resilience, build trust, prevent conflicts, protect human rights and freedoms and promote multilateralism through a variety of tools such as cyberdialogues with specific partner countries (among them US, Japan and Brasil); diplomatic demarches, statements and declarations; capacity building and technical assistance, targeted restrictive measures to deter and respond to cyber-attacks (since May 2019, including a ban on persons travelling to the EU, and an asset freeze on persons and entities; moreover EU persons and entities are forbidden from making funds available to those listed); engagement with civil society and the private sector.

In its political guidelines, the new Commission that has started the mandate in December 2019, set, *inter alia*, an ambitious plan for climate, *technology* and demography, fully aware of the constant need to address cross-cutting multifaceted issues raised by the cyber dimension, in order to promote EU political, economic and strategic interests and pursue engagement with key international actors.

The digital policy of the Commission focuses on ten priority areas: legislating on human and ethical implications (especially in the AI dimension, taking into consideration a global leadership role in the creation of these standards); data governance and a more balanced approach towards using big data, to the benefit of innovation, on one hand, and a strong core of ethical standards on the other; the adoption of a fairer system of taxation, given the inadequacy of the current legislation for business in the digital age; setting up a joint Cyber Unit in cybersecurity, with the initial purpose of information-sharing among member states; critical technology in emerging areas where the European Union may achieve sovereignty, i.e. the next-generation hyperscalers and investments in blockchain, quantum computing, algorithms and tools to allow data sharing and data usage; the development of common standards for 5G networks and content policy; the establishment of new rules for digital service providers; the improvement of digital literacy for both young people and adults (with the subsequent update of the EU's Action Plan for Digital Education); the digitalization of the EU Comission, by introducing new digital methods and digital diplomacy tools.

These priorities build upon the already existing infrastructures at the EU level, in both institutional (EU Agency for Cybersecurity – ENISA, the CSIRT & CERT EU network, the European Cybercrime Center, the European Judicial Cybercrime Network; EU Institute for Security Studies – EUISS; the Cyber Diplomacy Toolbox) and legislative terms (EU Cybersecurity Act; NIS Directive; General Data Protection Regulation – GDPR, a universally recognised instrument, providing new rules to give European citizens more control over their personal data; the Budapest Convention on Cybercrime; the Data Protection Police Directive; the EU Blueprint for Coordinated Response).

CONCLUSIVE REMARKS

The future of cyber-diplomacy can be envisaged at the juncture of two traditional dimensions of world politics: state sovereignty versus private authority, and international conflict versus cooperation. Cyberspace is no more separated from the real international relations of the 20th century and is now an integral part of the world stage we all share.

Deeply rooted in the cyber age and its rapidly changing configurations, the next decades will witness an even more rapid pace of technological development that has the pre-requisites to become central to the fabric of world politics, with a unique influence on the geopolitical landscape. Cyber escalation and proliferation will continue to affect our daily institutional and private lives.

The immediate imperative for theory, policy and practice is to analyze and converge on concepts, rules and mechanisms that can best address the challenges posed by the new realities. The cyberdiplomats will need to play versatile, proteic roles, the main part when called upon to do so, by their own governments that need to take the lead and coordinate the process, and secondary/complementary roles, adding upon the security and technical measures that will prevent the cyberspace to become, in the apt words of Shaun Riordan, "a Hobbesian world of perpetual war of all against all". Together, they are already working for the establishment of a core set of norms, rules and regulations similar to public international law for the physical space, i.e. "not perfect, but with just sufficient incentive to keep barbarity at bay".

We are currently on testing grounds and it is up to us, government and private sector representatives alike to prove that we have the capacity to offer durable solutions and to build solid XXI century norms, rules and regulations for the cyber realm.

REFERENCE LIST

CHERTOFF, M., 2020, Establishing Norms in Cyberspace, available at: https://americas.chathamhouse.org/article/the-paris-call-and-establishing-norms-in-cyberspace/

CHOUCRI, N., 2012, Cyberpolitics in International Relations, Cambridge, MA: MIT Press

CHOUCRI, N., 2016, Emerging Trends in Cyberspace: Dimension and Dillemas. In Williams, P. & Fidder, D. (eds), Cyberspace: Malevolent actors, criminal opportunities and strategic competition. Carlisle, PA: Strategc Studies Institute and U.S. Army War College Press

COOPER, A.F., 2013, The Changing Nature of Diplomacy, in: Andrew F. COOPER, Jorge HEINE, and Ramesh THAKUR, (eds.), 2013, The Oxford Handbook of Modern Diplomacy, Oxford University Press

COPELAND, D., 2013, Digital Technology, in: Andrew F. COOPER, Jorge HEINE, and Ramesh THAKUR, The Oxford Handbook of Modern Diplomacy, Oxford University Press

MELISSEN, J., 2013. Public Diplomacy, in: Andrew F. COOPER, Jorge HEINE, and Ramesh THAKUR, (eds.), 2013, The Oxford Handbook of Modern Diplomacy, Oxford University Press

MELISSEN, J., 2012. Public Diplomacy, in: P. KERR and G. WISEMAN, (eds.), Diplomacy in a Globalizing World, Oxford University Press

NYE, J. S., 2010. Cyber Power. Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010, [online], available at: <http://tinyurl.com/33nhlrv>

RIORDAN, S., 2019, Cyberdiplomacy: Managing Security and Governance Online, Polity Press

ROSENBACH, E., MANSTED, K., 2019, The Geopolitics of Information, Harvard Kennedy School, Belfer Center for Science and International Affairs

SARAN, S., 2020, Navigating the Digitisation of Geopolitics, available at www.orfonline.org/expert-speak/navigating-the-digitalisation-of-geopolitics-60612/?amp

"Data is Real Wealth: PM Modi in Davos," Business Standard, January 23, 2018, https://www.business-standard.com/article/news-ani/data-is-real-wealth-pm-modi-in-davos-118012300923_1. html

MONICA GHEORGHIȚĂ

PhD, is a career diplomat, former State Secretary for Global Affairs in the Romanian Ministry of Foreign Affairs (January 2017-November 2019). During her tenure, she was the MFA Special Representative for Afghanistan and the Romanian National Coordinator of the China – Central and Eastern European countries ("16+1"/"17+1") format of cooperation. Previously, she served as director for Asia Pacific, adviser to the Minister of Foreign Affairs and expert in the Chancellery of the Prime Minister.

A graduate of the University of Bucharest/Law (2003) and of the Institute of Business Law and International Cooperation Nicolae Titulescu-Henri Capitant of the same University, Mrs.Gheorghita was the first Romanian diplomat admitted to the Oxford University Foreign Service Programme (2006-2007). In 2012, she earned a PhD in Military Sciences and Intelligence from the National Intelligence Academy/Romania. During 2014-2015 she did post-doctoral studies at the World Economy Institute/the Romanian Academy, with a thesis on the "16+1" cooperation mechanism.