The New Emperors and their Global Kingdoms. Digital Capabilities, Business and Cyber Diplomacy

Monica GHEORGHIȚĂ
Former State Secretary for Global Affairs and Economic Relations, Ministry of Foreign Affairs
monica.gheorghita@ici.ro

The economic and health crisis caused by COVID 19 has disrupted the business systems of administrations and companies in the private and public sectors alike, forcing them to make a rapid shift to remote work. According to consultancy McKinsey, Europe is at 12% of its digital potential, while the US is at 18%. In the emerging markets, uptake will depend on the trajectory transformation takes: should countries play catch up with the developed world; create their own route to develop new and transformative technologies to increase competitiveness; or leverage the pandemic-induced acceleration of digitalization to leapfrog obsolete technologies and head straight to modern solutions, taking the so-called shortcuts to progress?

Past are the times where diplomacy was an activity undertaken by a select group of (mostly) white men elegantly discussing and negotiating the main issues in international politics in cocktail parties and at official receptions. It is not even just about relations between states. It now has to take into account "wider relationships and dialogues, involving such entities as regional and international organizations – be they intergovernmental or non-governmental – multinational firms, sub-national actors, advocacy networks, and influential individuals" [Jönsson & Langhorne, 2004]. The former British Ambassador Tom Fletcher observed, in relation to the latter group, that entrepreneurs such as Google's chairman Eric Schmidt have a "pulling power" that is hard to match for any state representative. They are, in his view, the "New Emperors". Diplomacy has also progressively extended to new policy areas over the years, entering uncharted political territories such as climate negotiations or, more recently, cyber issues.

Several incremental steps have been taken before they became recognized as a major foreign policy topic. Cyber issues were treated first as purely technical issues, then as external aspects of domestic policies. It was rather a "growing tide" of events, meetings, issues that required a diplomatic response. Diplomats eventually had to step in because cyber became a domain of diplomacy.

In direct connection with these evolutions, digital capabilities, as the very foundations of the cyber realm, have to keep up in order to reap the benefits of the soft and hard powers countries possess. Working as time and space "compressors", the online platforms have become quintessential tools for reaching a global audience. Keeping in mind the differences between digital and cyber diplomacy we dealt with in the first number of the IJCD, one observes that traditional means of information are replaced constantly with online channels, as people value more rapidity and accessibility to gain knowledge about various themes. In the same vein, these vehicles of data are increasingly influencing the perspectives and behaviors of people around the world. More and more obviously under the pressure of pandemics, state

actors use online platforms for hard and soft power reasons, on one hand to detect security threats, as digital capabilities prepare them to defend their resources against cyberattacks, or reach audiences for their cultural and trade contributions.

In addition, these capabilities are bringing a necessary revitalization to traditional diplomacy between state officials, as they allow for the efficient use of time during meetings and in communications with counterparts and teams in other (usually remote) countries without the need to physically travel.

One may argue that nothing replaces the value of face-to-face gatherings, nevertheless, now and in the near future, gradually, more countries will make use of cyberspace and allocate resources for these tools in the service of diplomacy and beyond, to take on the opportunities and the chance to allocate less resources for travel and accommodation and more for projects and faster decision-making. The big challenge remains for the diplomatic approach in cyberspace to bring together international/non-state actors in this community, hence the need to develop specific, tailor-made tools, regionally and under the auspices of the United Nations.

In the private sector, companies increasingly participate in international relations as significant non-state actors. If we look back in history, this has always been the case for major multinational companies. Since the XVIIth century, companies such as British East Indian have acted as sovereign entities. More recently, major energy companies have created their own "foreign ministries" and pursued their own policies, often separately from their national governments. The world has undergone stunning transformations since then and even smaller companies now are international, in terms of dependency on global supply chains. There is increased interest on their behalf to be able to analyze and predict what kind of non-commercial aspects may influence, in a positive or negative sense, their international operations and how can they alleviate the dangers that come with it. Moreover, the digital ecosystem we live in means that all companies are to some extent tech companies and every employee, not only the specialized departments, are responsible for cybersecurity. These entities must engage with cybersecurity, protecting their operations, data and customers, as they are subject to cyberwar, cyberespionage and cyber information war. If one pays careful attention to the type of reactions countries have had to relevant events, it becomes obvious that the lines of demarcation between public and private realms are increasingly blurred. For example, a cyberattack that took down the computing system of the Saudi Arabia's national oil (and the world's most valuable) company Aramco, wiping out data on three-quarters of the firm's PCs - documents, spreadsheets, e-mails, files, and replacing all of them with an image of a burning American flag, was attributed to Iran as a retaliatory response to the Stuxnet attack on its nuclear programme, in 2012. Another example shows that a number of the cyberattacks against the US, attributed to Chinese actors, have not been aimed at the government, but at the private sector suppliers of the Pentagon that are sometimes easier to penetrate and hold precious information about the American weapon designs.

In World Order, Henry Kissinger gives perhaps the clearest reasoning underpinning the rise of cyber-diplomacy, emphasizing that the absence of dialogue and diplomacy would be detrimental to the cyberspace, but also to the broader world order: "The road to a world order may be long and uncertain, but no meaningful progress can be made if one of the most pervasive elements of international life is excluded from serious dialogue. (…) Absent some

articulation of limits and agreement on mutual rules of restraint, a crisis situation is likely to arise, even unintentionally; the very concept of international order may be subject to mounting strains. [Kissinger, 2014]

As a consequence, an integrated approach with reinforced diplomatic strategies is needed to improve collaboration between governments and companies. Cybersecurity needs to be integrated into the core of the company's/public institution's functions. A diplomatic approach to these challenges would require the development of networks of influence and information among key stakeholders, both governmental and non-governmental, including academia, media and other companies. In a second step, building on these networks, it would create alliances among various stakeholders, in order to improve coordination between companies, as active participants in the decision-making process, and generate the appropriate responses to governmental measures, behaving to some extent, more like governments.

The public support in this regard is not negligeable, as well, and a long-term diplomatic engagement with the people is needed, using public and digital instruments at hand, raising awareness through smart power tools, in an ideally holistic and integrated manner to problems adopted by the diplomatic approach.

The prospects of international tensions resulting in more or less constant cyberwarfare are not insignificant, if one takes into consideration that what happens in cyberspace triggers retaliation (of economic, diplomatic or even military nature) in the physical space. The need for regulations and widely agreed norms of behaviour cannot remain unsettled for long. At the same time, the diplomatic services that want to remain relevant in the new world will require training in new, technical areas of expertise. The powerhouses of the future, be they in the private or public realm, will assume the truth of an intertwined role of both private and general interest, and will induce with strategic acumen the cult of education, work and saving, and the capacity to foresee the needs to achieve public goods.

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.