Cyber-Diplomacy and Digital: Some Legal and Economic Aspects

Piergiorgio Valente (**Crowe Valente/Valente Associati GEB Partners; Link Campus University, Rome**) / **January 8, 2019**

For thousands of years the human species was constrained to limit its activities and creativity in the planetary space. Today, the Digital Revolution has opened a new space: the cyber-space, removing the limits once and for all.

Cyber-space is understood as a virtual world, a notional environment existing in and due to the network of telecommunication technologies. Although untouchable; it interacts with the physical world in the most dynamic manner with material consequences in the latter. The distinctive features of the cyberspace, deriving from its virtual nature, include:

1. the lack of physical borders and hence also of national frontiers;
2. the lack of distance or unification of physical space, meaning potential multiple presence of the event in any number of physical locations;
3. the nullification of time, since any event can happen in zero-time with a simple click and expanded impact;
4. anonymity or potential anonymity through the creation of profiles (even multiple ones) by the users.

Beyond doubt the cyber-space has invaded human life and is integral part of social interaction, economy and political activity, evidenced by new economic models, increased cultural interchange and worldwide impact of digitally expressed ideas. By-product of this development is that the cyber-space has become the new (battle-) field for cyber-attackers, cyber-defenders and cyber-diplomats. Cyber-attacks include any and all offensive actions having as target information systems, infrastructures, networks, devices etc. Since cyber-attacks can materially prejudice states' interests, cyber-defense tools are employed as response, for the purpose of protection.

On these premises **cyber-diplomacy** is the term coined to embrace diplomacy in the cyberspace, i.e. the use of diplomatic resources and the performance of diplomatic functions to secure national interests in the cyberspace. Cyber-diplomacy as such must be distinguished from so-called e-diplomacy, i.e. diplomacy performed through digital means, e.g. Facebook, Twitter etc. Relatively newborn, cyberspace constitutes modern generations' unknown to be conquered and ruled. Its nature, purely virtual and global, demands rules for cyberspace to perform its promise for sustainable growth for all.[1)] The drafting of these rules touches upon the various states' interests, sparking heated debates and inspiring cyber-diplomatic actions.

While rules are being drafted, question-marks on the framework keep multiplying, increasing pressure on national and international legislators and policy-makers. It is worth examining the actions being taken, since they preach to shape what is definitely an important space for the economy and the society and eventually to define the welfare of the future.

To begin with, the EU Member States have acknowledged the above in a series of actions. In 2014, the Council of the EU sought to outline a so-called **European Cyber Diplomacy Engagement**. It underlined the importance cyber-activities have gained for the economic development and the arising demand for measures to boost openness, connectivity and trust to ensure the competitiveness of the Digital Single Market. To the same end, the EU adopted in June 2017 a **common toolbox against cyber attacks** in order to enhance security online.

The same attitude is shared by various States around the world, taking unilateral or multilateral positions regarding cyber-attacks, their classification and the potential acceptable defenses. Illustrative example provides the **Talinn Manual**, including indications on the application of existing international law on cyber-operations in war and in peace as well as the **US International Strategy for Cyberspace**.

Although there is still no clear legal framework, there seems to be consent on the following:

1. the activity in the cyber-space and its expected growth rate in the near future compel the identification of clear rules;
2. taking into account the borderless character of the cyber-space, its legal framework may be effective if widely shared and implemented;
3. the cyber-space is integral part of the existing international reality and needs to fall under the existing international legislation;
4. the key question to be answered concerns the manner in which existing international law shall apply to cyber-activity.

The lack of clear rules in cyber-space implies uncertainty and hence increased risks.

As an example, firstly, under the curtain of uncertainty, conveniently anonymous subjects can use the cyber-space for criminal activities threatening social integrity. This was the key motive for the signature of the **Budapest Convention on Cybercrime** by 61 countries, recognizing that the "effective fight against cybercrime" requires international cooperation.

Secondly, focusing in the tax area, uncertainty as to the taxation of business activities in the cyber-space can have adverse implications for tax compliance. More specifically, the **2017 OECD/IMF Report on Tax Uncertainty** highlighted that tax uncertainty can incentivize business conduct that undermines tax legislation set by governments. In other words, unclear rules and inconsistent practices in taxation can encourage business towards tax avoidance. And beyond doubt the taxation of cyber-space is not clear at the present stage. Instead, the EU is continuing the heated debate on the 2018 Digital Tax Package, with ECOFIN failing to reach agreement in its **December 2018 meeting**; disagreement is also reflected in the **2018 OECD Interim Report on Tax Challenges of the Digital Economy**.

Thirdly, there is a clear risk that cyber-technology opportunities are exploited by States themselves in ways that cause harm to other States. This encompasses **State-backed cyber-attacks**, such as 2017 WannaCry ransomware as well as new aspects of harmful tax competition. Thus, the strong potential of blockchain technology has inspired targeted tax regimes in a number of small countries to attract blockchain-focused enterprises. It could signal the rise of **crypto-havens**, succeeding the heavily combatted tax havens' phenomenon and implying new routes for profit shifting. The lack of a coherent international (tax) framework could multiply the risk.

Most importantly, uncertainty cannot but compromise the potential of the cyber-economy. In lack of clear rules, digital integration is slowed down. Individual users do not trust the cyber-tools and tend to avoid undertaking major activities in the cyber-space.

To sum up, the cyber-space entails significant economic, social and political potential. It can lead to sustainable growth and shared welfare, if ruled appropriately or to the third world war, if not. Cooperation is of key relevance and the call is for States and international and supranational authorities to work together for humanity to make the most of the new tools.

Based on speech delivered in the context of a seminar on Cyber-diplomacy on 7 December 2018 at the Faculty of Political Studies and for the Superior European and Mediterranean Education "Jean Monnet" of the University "Luigi Vanvitelli".

References

1. ↑ Although hard to isolate and measure, the growth of digital economy is considered to exceed by far the growth of bricks-and-mortar economy during the last decade. *Cf.* International Monetary Fund, *Staff Report: Measuring the Digital Economy* (28 Feb. 2018).