On Digital Diplomacy. Key Issues

Mihai SEBE
European Studies Unit, European Institute of Romania, Bucharest, Romania
mihai.sebe@ier.gov.ro

Abstract

The current paper intends to be a foray into the aspects related to digital diplomacy. It presents the main working definitions and key legislative aspects as well as the Romanian case study, what have we done and what needs to be done.

Index terms: cyber diplomacy, digital diplomacy, digital foreign policy, e-diplomacy, terminology

1. Introduction

The impact of technology on our day-to-day activities has been debated thoroughly in the last years. If on the issues related to economy, industry, trade and so on there are a lot of studies and analyses one the impact on politics and general way of doing things in the public sector there are still under-researched areas. One such area is the impact of the technology on diplomacy and the current paper tries to provide a short tentative answer on the current state of affairs.

2. Key digital policy issues and terminological clarifications

The last couple of years have witnessed the linguistic expansion of the word „-cyber" or „-e" or „-digital" in various combinations, each of them sometimes more exotic than the other. However, several definitions stand up, each of them being more or less similar in form.

Thus, one first concept used is that of "e-diplomacy" seen as „the use of the web and ICT to help carry out diplomatic objectives" [1]. Another more extensive definition is that provided by Tutt (2013) of the "e-diplomacy" seen as: "the virtual conduct of public diplomacy, using digital information and communications technology (ICT), namely cyber-tools such as Social Media (Twitter, Facebook, Youtube, etc.), in order to communicate and to project a nation' s image into both the national and international public sphere." [2].

As for digital diplomacy, a more generic version is that from the MacMillan Dictionary (2018) „the use of the internet to achieve diplomatic goals" [3]. These definitions refer to the general use of digital tools by diplomats and foreign ministries and not a specific diplomatic policy *per se*.

Another concept that has appeared relates to the diplomacy of cyberspace that is defined as cyber-diplomacy. „Cyber-diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests concerning cyberspace. Such interests are generally identified in national cyberspace or cybersecurity strategies, which often include references to the diplomatic agenda. Predominant issues

on the cyber-diplomacy agenda include cybersecurity, cybercrime, confidence-building, internet freedom and internet governance." [4]

This definition is better suited for the purposes of this section as it relates to the European Union approach as expressly stated in the 2016 EU Global Strategy (EUGS), which expressly describes what it wants through cyber-diplomacy: "The EU will be a forward-looking cyber player, protecting our critical assets and values in the digital world, notably by promoting a free and secure global Internet. We will engage in cyber diplomacy and capacity building with our partners and seek agreements on responsible state behavior in cyberspace based on existing international law. We will support multilateral digital governance and a global cooperation framework on cybersecurity, respecting the free flow of information." [5]

In order to have this cyber capacity and confidence-building with partners, that are key for cyber-diplomacy, we need to have a series of building blocks referred by Lațici [6] from Pawlak's works [7]:

- Developing and building the resilience of institutions able to respond to and recover from cyber threats.
- Securing diplomatic commitments to uphold an open, free, and safe cyberspace.
- Promoting inclusive growth and the sustainable development of digital infrastructure; improving digital markets and securing a safe online economy.
- Developing cyber defence strategies to protect military networks, assets and defence institutions. [6]

Furthermore, OSCE has advanced into this territory of confidence-building measures that help cyber-diplomacy by issuing in 2016 a series of 16 recommendations through its Decision no. 1202 [8]. Cyber diplomacy is perceived at the EU level as a key toward de-escalation of conflicts because "only a long-term cyber diplomacy coordinated at the European level could help to bring about security in Europe and avoid conflict escalation." [9].

3. Between tradition and innovation

Given the limited space of this section I would focus briefly on the cyber-partnerships that the EU has. It all starts from what Tikk (2020) sees as the fundamental "European conviction that states' actions in cyberspace as in any other domain, must be guided and governed by international law" [10]. For that purpose special attention is given to the development of the cyber aspects related to the EU partners. As such many of the EU strategic partnerships have developed also a cyber-dialogue component that, according to Renard (2018), varies depending on the countries in question. "(…) the EU's cyber partnerships aim not only for bilateral cooperation but also for 'reflexive' results (whereby the EU aim to develop its cyber and diplomatic agency) and 'structural' results (whereby bilateral partnerships aim to strengthen the multilateral fabric and global internet governance)" [11].

A similar topic was discussed with the African Union and is mentioned in the February 2020 Joint Communique: "They also stressed the critical role of cybersecurity and trust in the digital age and agreed to focus on and enhance capacity in privacy and data protection." [12]. A similar topic was mentioned in the August 2019 ASEAN-EU Statement on Cybersecurity Cooperation who "underscore our commitment to promote an open, secure, stable, accessible and peaceful information and communication technology (ICT) environment, consistent with applicable international and domestic laws. We intend to strengthen our cooperation on cyber issues." [13].

One still complicated issue is the future cyber cooperation with the United Kingdom following Brexit. Although UK is one of the top countries in the world as regards the issues of cybersecurity

there are still aspects that are unclear. However, one important positive aspect is that the 2020 Political declaration setting out the framework for the future relationship between the European Union and the United Kingdom mentioned the need for a strong dialogue in this area. "The United Kingdom and the Union will establish a cyber dialogue to promote cooperation and identify opportunities for future cooperation as new threats, opportunities and partnerships emerge" [14]

4. Developing an active cyber diplomacy and a digital foreign policy. Case studies

At the EU level, one document that stands apart is the 2015 Council Conclusions on Cyber Diplomacy which stipulates that the EU and the Member States should have a "coherent international cyberspace policy that promotes EU political, economic and strategic interests and continue to engage with key international partners and organizations as well as with civil society and the private sector" [15]. The document then goes on and provides a series of key recommendations that should be implemented by the Member States.

This would be further supplemented in October 2017 by a series of implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities. These guidelines can be divided in:

- Preventive measures: Cyber confidence and capacity building abroad, awareness-raising activities of EU cyber policies.
- Cooperative measures: Political and thematic dialogues or EU diplomatic démarches.
- Stability measures: Official statements by EU leadership, Council conclusions, diplomatic engagements in international forums and démarches.
- Restrictive measures (sanctions): Travel bans, arms embargos, freezing of assets [16].

EU support for Member States' lawful responses should they fall victim to a cyber act: including in the case of invoking the EU's mutual assistance clause, Article 42 (7) TEU and the solidarity clause, Article 222 TFEU. NATO Allies can also invoke Article 5 [6].

As regards Romania we need to use the same distinction from the beginning of the section. For the "e-diplomacy" aspects we need to mention a series of projects in the consular area that envisaged to create an integrated digital system of travel documents management (E-PASS), an electronic portal for obtaining visas (E-VIZA), a travel app of the MFA and so on. [17] [18]

Concerning the proper cyber-diplomacy actions, Romania has been a constant supporter of all of the EU measures taken in area related to cyber-security or cyber-diplomacy and has been in line with the EU decisions. The active involvement of Romania was duly noticed by the other Member States and in December 2020 Bucharest was chosen to host the European Cybersecurity Competence Center, described as "a future hub to distribute EU and national funding for cybersecurity research projects across the bloc" [19].

The Romanian MFA is in charge of the cyber diplomacy and coordinates from the political level the issues related to cybersecurity [20]. Also, it is active at the UN, NATO and OSCE level on issues linked to the cyber domain [21].

One of the most recent diplomatic interventions of Romania in cyber affairs is the April 2021 statement of support toward the United States in condemning the cyber-attacks on SolarWinds Orion platform, which also reaffirms Romania's position on regulating the cyberspace: "The Romanian MFA reaffirms its commitment to continue cooperating at international level in order to prevent such disrupting activities, by promoting an international framework for responsible state behavior in the cyberspace, based on the implementation of international law." [22].

This was followed months later by a new statement condemning the malicious cyber activities against Microsoft Exchange Server and the cyber campaign conducted by APT40 Group. It once more reiterates the Romanian principles regarding cyberspace: "Romania expresses its concern regarding any form of hostility and irresponsible behavior in cyberspace. Romania also reaffirms its firm commitment and involvement in supporting European and international enhanced efforts to prevent, discourage, deter and respond to such destabilizing actions, in accordance with the international framework for responsible state behavior in cyberspace, based on the application of international law.

Promoting and protecting the global, open, free, stable and secure cyberspace as well as the protection of intellectual property represents a major objective in sustaining the economic, society and security development at the international level, with respect for democratic values and rules-based order." [23].

A special mention should be given to the first Romanian Presidency of the Council of the European Union (1 January - 30 June 2019) where we can mention that "thanks to RO PRES, the Council of the EU set up a framework that would allow for the first time the EU to impose sanctions on individuals or entities responsible for cyber-attacks" [24].

Later on these initial ideas and initiatives took a new life as they were synthetized and given an official form in the new Romania's Cybernetic Security Strategy 2022 – 2027. In order to consolidate Romania's role worldwide, Romania want to have a worldwide engagement toward "promoting the notion of a global, open, stable and secure cyberspace, where human rights, fundamental freedoms and the rule of law are fully applied." Moreover this document provides a first, official definition of what cyber-diplomacy is: "diplomatic action aimed at promoting, supporting, defending and protecting, through international dialogue and cooperation with partner countries and international organizations, a global, open, free, stable and secure cyberspace, in which human rights, fundamental freedoms and the state fully applies to social welfare, economic growth, prosperity and the integrity of a free and democratic society and contributes to conflict prevention, mitigation of cyber security threats and greater stability in international relations". This ambitious plan in the area of cyber-diplomacy meant to consolidate Romania's standing in the international digital arena will imply for 2023 the creation of a high level diplomatic representation position [25].

5. Conclusion

In the end of this preliminary expose on cyber-diplomacy one thing is clear - the cyberspace has become a major part of the international relations and the majority of states have adopted cyber strategies and dedicated resources and staff to pursue their objectives in the cyber space. Cyber-diplomacy is only going to get more and more present in the day-to-day diplomatic activity as a cyber-international society is building up. What makes it so special is that it is a sector in a permanent construction as the technical realities and the day-to-day social dynamics are on a constant move.

Cyber-diplomacy role should be to strive to build confidence between the actors in the cyber space from an aggressive, strategic lead action toward a more peaceful co-existence defined by rules and norms: "in practical terms, at the moment the cyber-world still needs work to ensure adherence to international law and norms of responsible behavior - otherwise it's pure anarchy" [4].

In this author opinion, given the above mentioned information, we are now going beyond seeing the cyber-diplomacy as just a theoretical exercise or as a concept analyzed by academics alone. Cyber-diplomacy is now a day to day reality that goes beyond the sole institutions responsible with the classical diplomacy. It is becoming a collaborative activity that requires a whole-of-society approach and new ways of doing things and of communicating them. In the cyber-area we are all becoming in

a way cyber-citizens / cyber-diplomats responsible of our own actions and promoting a safe space, where the human rights and the liberties of all must be respected. Cyber-diplomacy is no longer a theoretical construct but a daily reality.

References

[1] Fergus Hanson (March 2012), Revolution @State: The Spread of Ediplomacy, Lowy Institute for International Policy, https://www.brookings.edu/wp-content/uploads/2016/06/03_ediplomacy_hanson.pdf.

[2] Tutt, Alexander (2013). E-Diplomacy Capacities within the EU-27: Small States and Social Media [Master's Thesis]: https://www.grin.com/document/274032.

[3] MacMillan Dictionary (2018). Digidiplomacy: https://www.macmillandictionary.com/dictionary/british/digiplomacy.

[4] Barrinha, André & Thomas Renard (2017) Cyber-diplomacy: the making of an international society in the digital age, Global Affairs, 3:4-5, 353-364, DOI: 10.1080/23340460.2017.1414924.

[5] A Global Strategy for the European Union's Foreign and Security Policy (2016): https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

[6] Lațici, Tania (2020). Understanding the EU's approach to cyber diplomacy and cyber defence. European Parliament: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937EN.pdf .

[7] Pawlak, Patryk (2018). Operational Guidance for the EU's international cooperation on cyber capacity building, European Union Institute for Security Studies: https://op.europa.eu/en/publication-detail/-/publication/508a8d73-a426-11e8-99ee-01aa75ed71a1/language-en/format-PDF/source-117729241.

[8] Decision no. 1202 OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies (2016). OSCE: https://www.osce.org/files/f/documents/d/a/227281.pdf.

[9] Bendiek, Annegret (2018). The EU as a Force for Peace in International Cyber Diplomacy. SWP, Berlin, Germany: https://www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf.

[10] Tikk, Eneken (2020). International Law in Cyberspace: Mind the gap: https://eucyberdirect.eu/content_research/international-law-in-cyberspace-mind-the-gap/.

[11] Renard, Thomas (2018): EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain, European Politics and Society, DOI: 10.1080/2374 5118.2018.1430720.

[12] 10th African Union Commission - European Commission Meeting - Joint Communique (29 February 2020): https://ec.europa.eu/commission/presscorner/detail/en/statement_20_365.

[13] ASEAN-EU Statement on Cybersecurity Cooperation (2019): https://asean.org/storage/2019/08/ASEAN-EU-Statement-on-Cybersecurity-Cooperation-FINAL.pdf.

[14] Political declaration setting out the framework for the future relationship between the European Union and the United Kingdom (2020/C 34/01): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2020.034.01.0001.01.ENG.

[15] Council Conclusions on Cyber Diplomacy (February 2015): https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

[16] Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (2017), https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf.

[17] Ministry of Foreign Affairs of Romania (2021a). Proiecte în domeniul consular [Projects in the consular area]: https://mae.ro/node/29926.

[18] Ministry of Foreign Affairs of Romania (2021b). Proiecte din fonduri europene [Projects from European funds]: https://mae.ro/node/35750.

[19] Cerulus, Laurens, Leonie Cater & Vincent Manancourt (in press) (2020). Bucharest to host new EU cyber research hub. Politico: https://www.politico.eu/article/bucharest-to-host-eus-new-cyber-research-hub/.

[20] Ministry of Foreign Affairs of Romania (2021c). Rolul MAE în domeniul securităţii cibernetice pe plan naţional [The MFA role in the area of cyber security on the national arena]: https://mae.ro/node/28366.

[21] Ministry of Foreign Affairs of Romania (2021d). Problematica securităţii cibernetice în cadrul organizaţiilor internaţionale şi implicarea României ca membru al acestora [The question of cyber security within the framework of the international organizations and Romania's involvement in its capacity as a member]: https://mae.ro/node/28369.

[22] Ministry of Foreign Affairs of Romania (2021e). The Romanian Ministry of Foreign Affairs joins the United States in condemning the cyber-attacks on SolarWinds Orion platform: https://mae.ro/en/node/55404.

[23] Ministry of Foreign Affairs of Romania (2021f). The Romanian Ministry of Foreign Affairs joins the international demarches of condemning the malicious cyber activities against Microsoft Exchange Server and the cyber campaign conducted by APT40 Group: https://mae.ro/node/56228.

[24] The Romanian Presidency of the Council of the European Union. Results, 2019, https://www.romania2019.eu/wp-content/uploads/2017/11/Brosura-200x210-bilant-ENG.pdf.

[25] The Romanian Government, Decision no. 1321 of 30 December 2021 concerning the approval of Romania's Cybernetic Security Strategy for the period 2022 – 2027, and also of the Action Plan for the implementation of Romania's Cybernetic Security Strategy, for the period 2022 – 2027, https://legislatie.just.ro/Public/DetaliiDocumentAfis/250128.