Cyber diplomacy, strategic instrument in foreign affairs policy

Carmen Elena CÎRNU
National Institute for Research and Development in Informatics - ICI Bucharest
carmen.cirnu@ici.ro

Abstract: Cyber diplomacy is an emerging tool for states and other stakeholders to manage collective security risks and promote good governance in a world whose interdependencies lead to the propagation of risks, threats and vulnerabilities at a rapid pace and without regard for traditional boundaries and jurisdictions. This article presents the various facets of the emerging cyber diplomacy literature and details initiatives in this area. Overall, there is an understanding of its role in creating a more stable cyber environment, but there are significant hurdles to overcome, especially as they relate to trust and coordination.
Keywords: cybersecurity, Cyber diplomacy, internet governance, diplomatic strategies, deterrence

INTRODUCTION

Despite being a new subject, cyber-diplomacy has progressed rapidly at global level, in an effort to explain and outline the continuous attempts to provide solutions to an emergent type of struggle, particularly occurring in cyberspace. If the essential function of diplomacy is to create mutual profit by means of dialogue, then the essential function of cyber diplomacy is to create mutual profit by means of dialogue focused on cyber security topics. Barrinha and Renard (2017) envision even broader objectives of cyber diplomacy, regarding it as" an emerging international practice that is attempting to construct a cyber-international society, bridging the national interests of states with world society dynamics - the predominant realm in which cyberspace has evolved in the last four decades" [1].

More precisely, cyber diplomacy applies diplomatic instruments to solve issues pertaining to cyberspace. Essential matters such as the legislation prohibiting cybercrime, internet governance, cyber-attack response and the protection of critical infrastructure, require specific actions and strategies. In the recent years, the national economies were deeply affected by the new cyber technologies. This state of things has led to amendments of the diplomatic agenda, with cyber threats becoming the key priority. Cyber diplomacy entails a wide range of issues besides internet governance and cybersecurity, such as economic development and the military use of the internet.

CYBER DIPLOMACY AND DIGITAL DIPLOMACY

Often, the notion of cyber diplomacy is related to digital (electronic/computer) diplomacy. Superposing these notions generates lack of clarity regarding the relationship of diplomacy with the digital realm.

Using digital instruments/techniques in order to promote diplomatic objectives [2] is known as digital diplomacy (electronic/computer diplomacy). For clarity, digital diplomacy is to be regarded more as an instrument than a goal in its own right.

This instrument is dedicated both to governmental and non-governmental players. The diplomatic strategy consists of different tools and capabilities, influencing the development of policies and supporting diplomacy. There is a continuous need for developing adequate digital instruments with the purpose of implementing strategies in diplomacy, due to the fact that this issue requires a different type of approach than other fields, such as trade.

Diplomatic instruments and way of thinking are used by cyber diplomacy to solve issues related to cyberspace. Using digital instruments in the process of implementing diplomatic actions and using particular diplomatic techniques in order to address subjects related to cyberspace are separate but related operations.

Focusing solely on technical groups is not sufficient for sustaining digital security coalitions. This aspect was highlighted during the 30th CERT global reunion at Kuala Lumpur (June 2018) by Chris Painter, one of the elite cyber diplomats. The abilities and frame of mind required for the development and sustainability of these coalitions are fundamentally diplomatic. The drawing up of future-oriented diplomatic strategies may strengthen cyber security by encouraging cooperation among key stakeholders.

The following examples might illumine the relevance of diplomacy in the current geopolitical context, given that cyber security is a key priority for many governmental foreign policies:

• The Agreement among the Governments of the Shanghai Cooperation Organization (SCO) Member States on Cooperation in the Field of Ensuring International Information Security was signed by China and Russia. The SCO, founded in 2001 is a global organization aiming at facilitating the collaboration in different sectors (political, economic, military), particularly focusing on terrorism and related issues. The SCO member states are: China, Kyrgyzstan, Kazakhstan, Russia, Uzbekistan, India, Pakistan and Tajikistan;

• Four member states of the SCO addressed the polemical notion of `cyber sovereignty` in the Draft of International Code of Conduct for Information Security to the United Nations General Assembly (September 2011), succeeded by another draft in 2015. They argued for the necessity of regulating this notion because of its possible security threats. On the other hand, Western democratic countries expressed their concerns that a regulation of this sort would threaten the free human expression;

• An essential cyber security agreement was reached in 2015 between USA and China. The latter state was gravely concerned about Edward Snowden's unveiling of American cyber espionage actions. On the other part, China was accused by the US of digital espionage and cyber attacks. As several Chinese army officers were charged with digital espionage in May 2014, American President Obama pleaded for sanctions regarding intellectual theft against Chinese companies, just before a high-level meeting with President Xi Jinping. In this tensioned context, this agreement resulted in the output of cyber diplomacy related activity, which covered preliminary meetings and an extended meeting among officials from the two states.

The Global Commission on the Stability of Cyberspace identified a wide variety of cyber diplomacy initiatives beyond those of states (GCSC, 2017, p.52) [3], numbering almost a hundred and involving:

• Multilateral, regional, bilateral treaty initiatives;

• Unilateral initiatives meant to have an impact on the international plane;

• International organizations (UN bodies, specialized agency conferences, standards organizations);

• Intergovernmental declarations;

• Non-governmental organizations and academic institutions;

• Industry and sectoral organizations;

• Law enforcement agencies;

• And others.

CYBER DIPLOMACY OR CYBER DETERRENCE?

Another concept which is steadily gaining ground and could, in a way, be compared to diplomacy, is that of "cyber deterrence" which US policy thinkers have been exploring as a response to a "vast range of coercive activities directed against the United States and its allies" (Lewis, 2014) [4]. Such signaling needs to be persuasive with regards to intent and also as regards the capacity to inflict intolerable damage, which Lewis (2014) argued is not yet possible with cyber-attacks, although others (Davis, 2015) claim valid parallels between nuclear and cyber deterrence. MacKenzie (2017, p.11) [5] breaks cyber deterrence down into four basic components (deterrent declaration, penalty measures, credibility, and fear) and concludes that the United States, a leading cyber actor, fails to accomplish any of these preconditions for effective deterrence. In the end, deterrence is only "one element along a spectrum of influences" (Davis, 2015, p. 354) [6], some of which we will not have control over. Cyber diplomacy of the more benign type is one of the influences that lies within our grasp.

Van der Meer (2016, p. 102) [7] claims that defense and deterrence are likely more effective in the short term, but diplomacy will contribute the most to international security in the long term. He cites "cyber arms races" and "tit for tat" escalations as destabilizing factors, which can be mitigated by the confidence building of steady diplomatic overtures.

Libicki (2009, p. 7) [8] divided deterrence into two components - "deterrence by denial" which could be termed passive deterrence, and includes all attempts to secure ICT systems to prevent attacks and minimize impact, and "deterrence by punishment" or active deterrence, which is the credible threat of the use of offensive means to retaliate in case of an attack or to dissuade from aggressive actions. While we, generally, think of the latter when considering deterrence, the former is just as important to dissuade attack and should also be considered an element of cyber diplomacy, as perception management is considered part and parcel of diplomacy.

The success of cyber diplomacy hinges, as in all other diplomatic endeavors, on international norms and confidence building measures. Bilateral and multilateral confidence building measures act as "pressure valves" in the case of cyber conflict, for the safer release of tensions. These measures enhance "interstate cooperation, transparency and predictability, with the aim to reduce the risks of misperception, escalation, and conflict entailed by cyberthreats" (van der Meer, 2016, p. 103).

International norms are a form of social capital and are an intangible and crucial asset. Though it seems imprudent to praise them in a time of an unravelling of norms through the actions of revisionist actors, international security and stability would benefit from the organic development of norms restraining cyber aggression. They provide share understanding, which facilitate discussions of shared interests and negotiating or moving past divergent interests. Farrell (2015) [9] details three problems facing the establishment of new cyber norms and, therefore, the success of cyber-diplomacy. The various powers have different and even incompatible values relating to the protection of cyberspace. A perception of good faith is required, which is not so easy given the various revelations of widespread spying and influencing activities. Last, but not least, non-state actors (large companies, experts, activists, civil society groups) play a key role in the development of cyber norms and must be included in the process for there to be any hope of success.

THE NECESSITY OF COORDINATION IN CYBERSPACE - THE US RESPONSE

The Cyber Diplomacy Act (CDA) was integrated in a legislative thrust by the Foreign Affairs Committee of the House of Representatives, initially introduced in 2017. The CDA supports security at national level and promotes commercial interests (Limbago, 2017) [10].

A "strategy relating to United States international policy with regard to cyberspace" (Limbago, 2017) is necessary for the CDA, a strategical approach tackling rules, prevention

and associated policy instruments, and the suitability of existing legislation to cyberspace. The CDA has its roots in the increasing need of a plan for diminishing the prevalence of cyber malicious activities directed against the US. Prevention of and response to cyber-attacks require specific strategic approaches and doctrine. The proposed plan targets the creation of an Office of Cyber Issues and the establishment of an Ambassador for Cybersecurity. The latter would coordinate the US activities and strategies pertaining to cybersecurity (Limbago, 2017). The high-level cyber diplomat's role would be to prioritize the actions oriented towards prevention and response in cybersecurity, cooperating with external governmental authorities.

The act also tackles cooperation at a global level, with the goal of formulating US policies to assess and apply international rules in the cyber field. It should also be noted that the CDA takes into consideration the suitability of the Law of Armed Conflict in the cyber sphere and prevents attacks like those affecting critical infrastructures or corporate espionage, without directly referring to `cyber war`.

Efforts of the previous Presidential Administration were based on the assumption of an interconnected world in which it would no longer be possible for countries to individually create the security environment conducive to their safety and prosperity and would have to coordinate for collective action. The Obama-era International Strategy for Cyberspace (2011, p. 10) [11] placed an important emphasis on cyber diplomacy, and formulated key principles for it to be possible (sustaining basic liberties, respect for assets, valorizing confidentiality, prevention of criminal activity and right to self-defense).

The emerging norms of cybersecurity involve interchangeability at global level, firmness of network, secure access, multistakeholder governance and cybersecurity due diligence. The objective of cyber diplomacy from a national perspective is for the US to develop stimulants and collaborative problem solving for the global medium in which states cooperate and serve as reliable interested parties - admitting the inner value of a protected, open and trusted cyberspace. (International Strategy for Cyberspace, 2011, p. 11).

WHAT ABOUT THE EU?

The first European acts in the field of cyber diplomacy emerged at the beginning of the 1990s. In that period, the European Commission started to participate in the global discussions regarding the internet governance, succeeded by the founding of the Internet Corporation for Assigned Names and Numbers (ICANN). Notwithstanding, the strategic EU cyber security act from 2013 was a stepping stone in the evolution of cyber diplomacy, promoting a unitary international cyberspace policy. This represents one of its five main priorities that enunciates that the EU will look for ways to encourage freedom and openness of the Internet, supporting actions that develop standards of behavior and adapt existing international legislation to the cyber field. Moreover, the EU will seek to bridge the digital gap and contribute to the international actions to consolidate capacity in the field of cybersecurity (European Commission and High Representative, 2013) [12]. The EU envisioning of cyber diplomacy was based on five key priorities, as follows: promoting and defending fundamental rights in cyberspace, principles of behavior and adaptation of current international legislation in global security, internet governance, improving competitivity and wealth along with capacity development and consolidation. An additional priority regards cyber diplomacy, not as much in its goals but in its means. This sixth priority is related to the strategic cooperation with key stakeholders, as a result of its cross-sectional character and scope. (Council of the EU, 2015) [13].

To put it simply, the EU's approach moves into the direction of strengthening the interactions among the multitude of cyber actors, in compliance with its concern for cyber-related matters and with its wider actions to jointly involve different partners in a strategical way. Regarding cyber diplomacy, this specific approach has evolved reflecting the worldwide tendency as well as the evolution of the EU diplomatic dimension. However, on the EU's

diplomatic agenda cyber diplomacy issues are not yet the most noticeable element, the main orientation of the EU efforts being towards the enhancement of European abilities and the coordination of more actions.

THE CONTRIBUTION OF A CYBER DIPLOMACY TOOLBOX TO THE EU'S EFFORTS OF PROTECTING AGAINST CYBER-ATTACKS

The draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomatic Toolbox), endorsed in June 2017, focuses on delivering a harmonized common response at EU level to potential cyber-attacks.

Specific measures should be included in the diplomatic toolkit, under the EU Common Foreign and Security Policy (CFSP), that may help to protect against malicious cyber activities oriented against the EU Member States. It is still unclear what specific measures the toolbox will actually consist of, but it is known that, if needed, these measures can be `obstructive` and that the type of response would be relative to the extent, range, time-span, severity, complexity and effects of the cyber-attack.

Together with other attempts, the toolkit highlights the relevance of the Member States generating a common unitary diplomatic reaction directed against potential cyber-attacks, harmonized diplomatic responses being regarded as enhancing the security at EU level. The toolkit leaves room for questions, resembling more a declaration of intents than a strict regulator.

One element of restrictive measures are cyber sanctions. Moret and Pawlak (2017) [14] define five elements of a successful EU cyber sanctions regime, in theory, which add up to a critique of the weaknesses of the EU decision making and implementing process:

• Sanctions should be paired with other policy instruments and be well positioned within the context of the EU foreign strategy;

• The EU must have a clear vision of the sanctions and whether they are meant to coerce behavior, constrain options or signal EU resoluteness against aggression, the later of which has the most chances of success in an empirical study;

• The third element is shared situational awareness, which Moret and Pawlak (2017) translate into information sharing, but could just as easily be interpreted as a matter of similar threat perception, which de Spiegeleire and Korteweg (2006) [15] identified as an important element of sustainability of collective action within alliances;

• Sanctions also require the cooperation of the private sector and of other non-state and non-political actors, who lend their support and their expertise to the process;

• The unintended economic and political consequences must also be taken into account.

Bendiek (2018) [16] details five types of measure which are available to the EU under its cyber diplomacy toolbox - preventative, cooperative, stabilizing and restrictive, as well as the lawful responses for self-defense on the part of Member States. Export controls also feature prominently in its cyber diplomacy efforts. Ultimately, "the EU has opted for a non-military cyber-security policy. This helps resist the temptation to respond to threats in cyberspace immediately. Instead, the EU privileges political measures as part of the CFSP, so as to make its mark as a force for peace. This approach should be understood as a clear political signal by its partners and competitors worldwide" (Bendiek, 2018, p. 8).

A WAY AHEAD

Efforts have been made both by the US and the EU towards a common and comprehensive approach for cyber diplomacy to contribute to conflict prevention, the mitigation of cybersecurity threats and to greater stability in international relations. It is expected that cyber security would reduce threats, promote diplomatic negotiation, and limit the potential aggressive behaviors. Nevertheless, until cyber diplomacy is actively implemented actions, the results of this approach and its goals cannot be properly assessed.

Other countries may also play their part in

cyber diplomacy, not just through centralized initiatives or through bilateral formats, but also through networks of institutions developing organically based increasing contacts and ties. For instance, the National Institute for Research and Development in Informatics in Bucharest, Romania, is in the process of launching a Cyber Diplomacy Initiative which leverages its network of institutional partners and contacts, as well as existing initiatives (the European Center for Excellence for Blockchain etc.) in order to contribute, at policy level, to cyber diplomatic efforts.

Finally, we should not discount another aspect of the emerging cyber diplomacy paradigm - its ability to support a new strategy of influence as a variant of "mass diplomacy" (Pahlavi, 2003) [17], wherein the issues of preventive security and spearheading economic interests are also joined by a strengthening of political influence.

References

[1] https://www.tandfonline.com/doi/abs/10.1080/23340460.2017.1414924 sau aici http://www. egmontinstitute.be/content/uploads/2018/01/Barrinha-Renard-Cyberdiplomacy_GlobalAffairs. pdf? Type =pdf
[2] https://www.diplomacy.edu/e-diplomacy
[3] https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf
[4] https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/141117_Lewis.pdf with details: https://www.csis.org/analysis/deterrence-cyber-age
[5] https://media.defense.gov/2017/nov/20/2001846608/-1/-1/0/cpp_0004_mckenzie_cyber_ deterrence. pdf
[6] http://nyujilp.org/wp-content/uploads/2015/11/NYI203.pdf
[7] https://www.clingendael.org/sites/default/files/pdfs/book_securing-cyberspace-chapter_July2016.pdf
[8] https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
[9] https://www.cfr.org/report/promoting-norms-cyberspace
[10] https://www.endgame.com/blog/technical-blog/cyber-diplomacy-act-what-it-why-it-matters
[11] https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyber space.pdf
[12] https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
[13] http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf
[14] https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf
[15] https://www.nato.int/docu/review/2006/Invokation-Article-5/Future_NATOs/EN/index.htm
[16] https://www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf
[17] https://www.researchgate.net/publication/228739617_Cyber-Diplomacy_A_New_ Strategy_ of_ Influence