Cyber Diplomacy

The Next Challenging Geopolitics for Digital Bangladesh

Tawhidur Rahman, MCiiSM
CFIP, CCTA, CHFI, Lead Auditor, CCIP, CCII, Team Leader, BGD e-GOV, CIRT

Cyberspace reunites nearly three billion inhabitants worldwide, transforming its existence from the fief of a community of technical experts to a place of societal reflection and performance. Governments, armies, businesses and citizens need to grasp these cyber-realities, seemingly outside the traditional territory of geopolitics, but still mappable along the unchanging lines of human nature and behaviors.

Although it is a new topic, cyber-diplomacy has already advanced in leaps and bounds worldwide in an attempt to define and to summarize the efforts constantly made to solve a new type of conflict, namely those taking place in cyberspace. The primary role of diplomacy is to generate common advantage through dialogue, thus the primary role of cyber diplomacy would be to generate advantage through dialogue on cyber security issues. More concrete, a simple assumption would be that cyber diplomacy uses diplomatic tools to solve the problems that emerge in cyberspace.

Topics like internet governance, enforcement of law against cyber crime, response to malicious attacks arising in cyberspace, the protection of critical infrastructure, just to mention a few, are of utmost importance and require a dedicated agenda and concrete action. The last decade has seen emerging technologies impact national economic systems in virtual space. This has changed the diplomatic agenda, with cyber threats moving to the top and with many governments already acknowledging that ignoring cyber diplomacy is no longer an option for global dynamics. Both a confusion in terminology and a lack of common legislation when addressing the cyber diplomacy topic is observed, since beyond internet governance and cyber security, a range of topics, from military use of internet to economic growth, are also enclosed by cyber diplomacy.

Cyber diplomacy or digital diplomacy?

The concept of cyber diplomacy is often associated with digital diplomacy, electronic diplomacy or computer diplomacy. Overlapping use of these concepts raises confusion over the relationship between diplomacy and the digital world.

Digital (electronic or computer) diplomacy refers to the use of digital tools and techniques to advance diplomatic goals. If there is a need to avoid confusion, then we must properly define digital diplomacy: it is more of a tool than an end in itself. This tool can be used by state and non-state actors. The development of a diplomatic strategy includes a range of tools and techniques that also includes digital ones enhancing analysis, influencing key policies or policymaking, as well as supporting consular diplomacy. There is always a challenge, namely to develop dedicated digital tools to implement diplomatic strategies since there is a different approach to this issue than the one used to promote commerce and trade.

Cyber diplomacy is the use of diplomatic tools and diplomatic thinking to solve the problems from the cyberspace. The use of digital tools to promote broader diplomatic agendas and the use of diplomatic techniques and mentalities (or mental modes) to analyze and manage cyberspace problems are separate but linked activities. Cyberspace provides digital tools towards a more effective implementation of diplomatic strategies, generating at the same time a whole range of government-level measures and other issues that can benefit from the diplomat's techniques and mentality.

In order to sustain computer security coalitions, it is not enough to exclusively address technical teams. It is what top cyber diplomat Chris Painter stressed in June 2018 during the 30th CERT international meeting in Kuala Lumpur. The skills and mentalities necessary to build and sustain such coalitions are essentially diplomatic. The development of wider and forward-looking diplomatic strategies can enhance cyber security by promoting collaboration between governments, companies, and other key players.

In June 2009, China and Russia signed the Agreement among the Governments of the Shanghai Cooperation Organization (SCO) Member States on Cooperation in the Field of Ensuring International Information Security (Yekaterinburg Agreement). Established in ▸

2001, the SCO is an international organization composed of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Uzbekistan, India and Pakistan for the purpose of cooperation in the political, military and economic sectors, with a particular focus on extremism, separatism and terrorism;

In September 2011, four members of the SCO (including China and Russia) addressed a Draft of International Code of Conduct for Information Security to the United Nations General Assembly, followed by a new draft submitted in 2015, addressing the controversial global concept of "cyber sovereignty". The SCO strongly supported the regulation of this concept due to its potential threat to security, while Western democracies feared that such a regulation would be a threat to fundamental human rights, namely to the freedom of expression;

The 2015 USA-China agreement on cyber security represented an important step ahead since cyber security has been a critical issue in the relationship between the two countries: China has expressed grave concern over the Edward Snowden's revelations of the cyber espionage activities of America and its Five Eyes partners, while the US accused China of hacking and espionage activities. In May 2014, five Chinese military officers were accused of computer espionage and President Obama urged the imposition of sanctions against Chinese companies blamed for intellectual theft, just ahead of a meeting in Washington with President Xi Jinping. In this context, the result of the bilateral agreement was the output of the cyber diplomatic activity, including preparatory meetings and a four-day meeting between foreign affairs senior staffers of China and the US.

The US response to the need for harmonization in cyberspace

In November 2017, The Cyber Diplomacy Act (CDA) was included in a legislative push by the Foreign Affairs Committee of the House of Representatives, that was first introduced in September 2017. The act covers topics providing the foundation for the US to "work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure" in support of US national security and economic interests.

The Cyber Diplomacy Act requires a "strategy relating to United States international policy with regard to cyberspace", a strategy expected to address norms, deterrence and related policy tools, and the applicability of current international law to cyberspace. The act builds upon growing demand for a strategy to curtail cyber-attacks against the US. It has been noted the there is a lack of policy and strategy for deterrence and defending against and responding to cyberattacks and, accordingly, there is a need for a strategy and a doctrine regarding cyber-attacks.

The proposal aims to create an Office of Cyber Issues and to establish an Ambassador for Cybersecurity. The Ambassador for Cybersecurity would "lead all US engagement on issues pertaining to cybersecurity strategies, standards, and practices". The role of a high-ranking cyber diplomat would be to prioritize the efforts towards cyber-defense and response and to work with foreign governments.

Another topic addressed by CDA is global international cooperation with the aim to establish US policy to evaluate and implement global norms in cyberspace. It is worth mentioning also that the act considers the applicability of the Law of Armed Conflict to cyberspace and prohibits attacks such as those aimed at critical infrastructure or commercial espionage for corporate gains, without explicitly mentioning "cyber war".

What about the EU?

The EU's first acts of cyber diplomacy go back to the early 1990s, when the European Commission took part in the international debates on internet governance, followed by the establishment of the Internet Corporation for Assigned Names and Numbers (ICANN). Nevertheless, the 2013 EU cyber-security strategy represented a milestone in the development of the EU's cyber diplomacy, setting the promotion of an EU "coherent international cyberspace policy" as one of its five key priorities (European Commission and High Representative, 2013), stating that "the EU will seek to promote openness and freedom of the Internet, encourage efforts to develop norms of behavior and apply existing international laws in cyberspace. The EU will also work towards closing the digital divide and will actively participate in international efforts to build cybersecurity capacity". The vision for the EU's cyber diplomacy was based on the identification of five key priorities: the promotion and protection of human rights in cyberspace, norms of behavior and application of existing international law in the field of international security, ▸

internet governance, enhancing competitiveness and prosperity, as well as capacity-building and development. A sixth priority refers to cyber diplomacy, less to its objectives but more to its channels. It refers to "strategic engagement with key partners and international organizations" due to the "global cross-cutting nature, scope and reach" of cyber issues (Council of the EU, 2015).

This approach can be expressed in layman's terms as an intention to deepen the relationships with a number of key cyber actors, in line with both its growing interest for cyber issues and its broader efforts to engage strategically at the bilateral level with a number of partners. When referring to cyber diplomacy, the EU's approach has developed mirroring both a global trend and the development of the EU as a diplomatic actor. Still, cyber issues are not yet the most visible part of the EU's global diplomatic efforts, while most EU efforts are focusing on the need to increase European capabilities and coordinate more actions.

The EU's attempt to defend against Cyber-Attacks with the help of a Cyber Diplomacy Toolbox

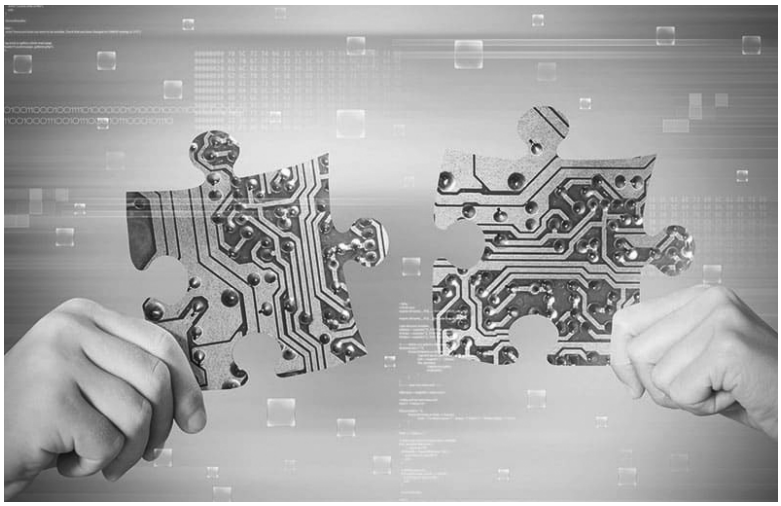
Adopted in June 2017, the draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomatic Toolbox) aims to provide a way of coordinating a collective response of EU Member States to malicious cyber activities at the EU level.

The toolbox should include diplomatic measures within the EU Common Foreign and Security Policy (CFSP) which could be used against malicious operations directed against Member States in cyberspace. However, it is still not clear of what kind of measures this toolkit will include in practice, but it does say that the measures can be, if necessary, "restrictive" and that the response would be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity.

Along with other efforts, the toolbox stresses the importance of EU Member States unifying their diplomatic response against malicious cyber activities, the common diplomatic efforts being seen as a way to strengthen the security of European countries. However, despite being a clear step ahead, the toolbox leaves a lot of open questions, being more of a manifesto than a provider of actionable norms.

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. Cyber diplomacy is expected to encourage cooperation also through diplomatic negotiation, to improve the mitigation of threats, or to moderate the behavior of potential aggressors, but until it is put into action it will be difficult to estimate the degree of influence of this approach in terms of reaching the proposed goals.



Conclusion

Diplomacy as a major instrument between states in the world is facing a new phase. The new phase shows that diplomacy is not only the art to negotiate and protect one's interest or to promote the influence in international affairs. Cyber diplomacy has strong international implications that require international commitment and collaboration and along with appropriate defense capabilities, cyber diplomacy development and diplomatic strategies designed to outline the present security environment. Cyber diplomacy is also fundamental for confidence building measures between countries in a region.At the international level, there is already acknowledgement that cyber threats are one of global security issue as many of the high-scale businesses and administrations are run on cyber space hence the cyber space is very fragile to be destructed by viruses created by hackers. Hand in hand with that argument, North Asia, Europe and North America have recognized the diplomatic opportunity to shape cyber policy elements of international security present through devoting hefty budgets and resources towards it. Cyber-security defined as a complex reality with many dimensions. Responding to the cyber challenge requires a good understanding of this complex issue.

"Bangladesh's growing stakes and interest in engaging in cyber diplomacy as a foreign policy.Bangladesh reiterates her commitment to contribute to making cyberspace – the new frontier in our common heritage of mankind – more inclusive, secure and resilient."

Bangladesh's growing stakes and interest in engaging in cyber diplomacy as a foreign policy.Bangladesh reiterates her commitment to contribute to making cyberspace – the new frontier in our common heritage of mankind – more inclusive, secure and resilient. We wish to work together with all concerned to address the existing gaps in international norms to guide cyber security and safeguard measures." The challenges before countries like Bangladesh in the face of organized cybercrimes and attacks. The awareness building work being done in collaboration with the civil society and private sector to preserve the right to privacy and freedom of expression in the cyberspace within an enabling legal framework ■