Exploring a Diplomatic System of Cooperation in the Cyber Space through a Proposed Cyber Diplomacy Cooperation Framework

Natalia BELL, Alex MBAZIIRA
School Technology and Innovation,
Marymount University, Arlington, Virginia 22207, United States of America
nbell@marymount.edu, ambaziir@marymount.edu

Abstract

Cyberattacks are on the rise, and cyber weapons are the main tools used in modern warfare. All these occurrences are changing the nature of traditional diplomacy, contributing to developing new avenues for Cyber Diplomacy. The world's leading nations have realized the importance of establishing a diplomatic system of collaboration in the cyber sphere to facilitate bilateral relationships between nations and cooperation in cyberspace in already-established alliances such as NATO, the United Nations, and regional trade associations. Multiple studies have discussed and detailed the concept of "cyber diplomacy" and the diplomatic behavior associated with it; however, few of these analyses have sought to distinguish the "cyber diplomacy" concept from the more traditional and well-known concept of "diplomacy." The scope of this proposal is to create a Cyber Diplomacy Cooperation Framework which will bring together conventional elements of diplomacy and cutting-edge cybersecurity mechanisms. As cyber warfare concerns are growing, nations need a normative cyber diplomacy framework that can be adapted by countries to prevent cyber-crises and engage more nations in the discussion.

Index terms: cybersecurity, cyber diplomacy, framework

1. Background

In September 2022, the US Senate unanimously confirmed Mr. Nathaniel Fick to serve as the first-ever cyber ambassador-at-large for cyberspace and digital policy. Mr. Fick will run the newly established State Department’s Bureau of Cyberspace and Digital Policy. According to National Geographic (2022), records of diplomatic letters date back to the 14th century B.C. The novelty of the notion of "cyber diplomacy" relates to relationships in the digital environment as opposed to the physical space. As cyber-attacks continue to increase and cyber weapons transform modern warfare, all these events are transforming diplomacy by creating new avenues for Cyber Diplomacy (Halpern, 2019). For example, the Russian and Ukrainian conflict of 2022, which is involving both state and non-state actors participating as proxies in this hybrid war has rendered existing diplomatic tools ineffective and caused a need for a new framework of cyber diplomacy which can be effective in averting future cyber geopolitical crises (EU-Cyber Direct, 2022). Some of the key issues in modern cyber hybrid warfare which a cyber diplomacy framework needs to address include information operations, cyber-attacks, political manipulation, engagement of involved non-state actors, among others. There seems to be no agreeable term to define diplomatic tools and processes for cyberspace despite a growing need in national states to extend diplomacy to cyberspace. According to Diplo, a Swiss-Maltese nonprofit organization that focuses on capacity development in the area of digital

policy and Internet governance, the terms “cyber diplomacy” and “digital diplomacy” are often interchanged. Cyber diplomacy is associated with diplomatic efforts to address cyber security challenges while digital diplomacy is used to define the adoption of new tools in diplomatic practice, such as social media, websites, and online meeting platforms, as well as the implementation of digital foreign policy, including recent issues on the diplomatic agenda (diplomacy.edu). Furthermore, the State Department uses the terms “digital diplomacy” and “digital policy,” to refer to “responsible state behavior in cyberspace and advance policies that protect the integrity and security of the infrastructure of the Internet” (state.gov). While the European Commission widely uses the term “Digital Agenda" in its essential internet-related documentation, the Council of the European Union clearly articulates “Cyber Diplomacy” in its Outcome of Proceedings, “Council Conclusions on Cyber Diplomacy,” coming from the General Secretariat of the Council to the Delegations (consilium.europa.eu, 2015). Other adjectives and prefixes like "tech," "net," "virtual," and "e-" diplomacy are informally used; however, Diplo suggests that such trends appear to be confusing discussions and policies surrounding this topic (diplomacy.edu). Several studies have talked about and outlined the concept of "cyber diplomacy" and the diplomatic behavior that goes along with it, yet few of them have attempted to differentiate the “cyber diplomacy” notion from the more traditional and well-known concept of "diplomacy." As Attatfa et al. (2020) note, there is a considerable gap in the literature - a subject for future research.

2. Introduction

According to Attatfa et. al. (2020), cyber diplomacy began in 2007, a year that will always be recognized because of a large-scale cyberattack on Estonia. Since then, Europe has actively sought cyberspace security. In 2017, the European Council of the European Union agreed to develop a framework for a “joint EU diplomatic response to malicious cyber activities”: the cyber diplomacy toolbox (consilium.europa.eu, 2017). The Paris Call for Trust and Security in Cyberspace, launched at the 2018 Paris Peace Forum, has emerged as the multi-actor framework of reference for promoting core principles for the safety of cyberspace. NATO did not remain behind. In 2019, Jens Stoltenberg, NATO Secretary General, commented that “a serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all” (NATO, 2019). Due to the issue's importance, European countries started to make and use national cybersecurity strategies based on European institutions' cyber initiatives. The US also created several programs, such as the White House Office of the National Cyber Directorate, the 2021 President's Executive Order on Improving the Nation's Cybersecurity, the State and Local Government Cybersecurity Act of 2021, and agencies like the Cybersecurity and Infrastructure Security Agency, and, most recently, the State Department's Bureau of Cyberspace and Digital Policy and its first ambassador-at-large.

Alongside Europe and the United States, several other regions and countries have recognized the urgency to govern cyberspace. Moreover, the world’s great powers have come to recognize the need to establish a diplomatic system of collaboration in the cyber realm, to serve both individual countries' cooperation as well as through already established alliances such as NATO, the UN, etc.

This paper aims to introduce a Cyber Diplomacy Cooperation Framework that will incorporate traditional diplomacy and cooperation aspects as well as cybersecurity components in a novel manner. The objective is not to create a brand new framework but rather to adapt existing frameworks and extend them to address cybersecurity elements that have not been previously examined.

3. Proposed Cyber Diplomacy Cooperation Framework

The proposed Cyber Diplomacy Framework will follow the UN Sustainable Development Cooperation Framework's adapted key objectives:

1) Address national priorities and gaps in their pathway towards meeting their cybersecurity goals;
2) Must embody the spirit of partnership;
3) Collective promise to leave no one behind;
4) Responses to a countries' specific needs and realities;

To develop the framework, we will assess the short-comings of existing diplomatic tools in averting cyber warfare, which involves both state and non-state actors, information operations and political manipulation targeting civilians, loop-holes in international law exploited by aggressor nation-state and non-nation state actors to engage in cyberwar among others.

Traditional diplomacy covers various forms of cooperation, such as bilateral and multilateral agreements, regional pacts, international organizations that facilitate collaboration between nations, and strategic partnerships. Nonetheless, the emergence of cyber diplomacy requires the incorporation of new components. For example, addressing global cybercrime issues and fostering international cooperation for cyber security offense and defense are essential factors to consider. In addition, there is an increasing need to impose sanctions for criminal activities on a global scale, while the concept of cyber attribution has acquired significant importance in modern times, particularly in the context of cyber-attacks by foreign entities. Furthermore, creating new avenues for cybersecurity research and collaboration on a global scale could be a crucial element of the cyber diplomacy framework.

The US and NATO are ahead of most countries around the world on cyber-diplomacy. For example, the US House of Representatives recently passed the bill for Cyber Diplomacy Act of 2021, which is awaiting to be presented and passed by the Senate before being signed into law by the US President (McCaul, 2021). Given the resources and talent of the US and NATO in cybersecurity and information technology, the objective of our study is to develop a generalizable framework that can be adapted by countries desiring to develop cyber diplomacy programs.

The proposed Cyber Diplomacy Farmwork is based on three main pillars: Capacity Building, Cooperation and Trust. The Capacity Building refers to the process of countries working together to share resources, provide assistance to one another in the form of training and education, and provide technical assistance. The nations that participate in diplomatic cyber cooperation would pool their resources, provide one another with technological help, and collaborate on educational and training initiatives.

Cooperation is the second pillar, and it refers to the countries' willingness to build and adhere to a common agenda in terms of the many areas of cybersecurity. It also refers to the countries' willingness to develop various partnerships between governmental institutions, as well as private-public partnerships. In addition, the cybersecurity industry frequently depends on the community for the sharing of cyber threat intelligence as well as open-source intelligence regarding cyber dangers. Countries will coordinate their efforts to collaborate on a variety of fronts under the overarching concept of collaboration, including research and development.

The final pillar that we propose to incorporate into this structure is Trust or confidence. The concept of transparency, which refers to being open and honest with cybersecurity policies, procedures, and operations, is one of the three factors that would be considered to come under the Trust pillar. Within the context of a cyber diplomacy cooperation environment, it is anticipated that the countries will construct and continue to maintain trust and confidence in each other's practices. The second part of the cyber diplomacy collaboration is the diplomatic engagement. Just as in conventional diplomacy, the diplomatic engagement in the cyber diplomacy cooperation would strive for appropriate conflict resolution methods and bilateral and multilateral dialogues regarding a variety of topics pertaining to cybersecurity. And last but not least is Accountability, which is the concept under which we propose shared sanctions norms to ensure proper attribution of cyber-attacks.

Fig. 1. Proposed Cyber Diplomacy Framework

4. Conclusion

As the cyber threat landscape continues to evolve and the attack surface continues to widen to integrate more globally interconnected devices over the Internet. There is a need for a normative cyber diplomacy framework that can be adapted by countries to avert cyber-crises and also involve more countries in dialogue as cyberwar continues to evolve. In this paper we proposed a Cyber Diplomacy Farmwork founded upon three pillars: Capacity Building, Cooperation, and Trust. The process of countries working together to share resources, providing aid to one another in the form of

training and education, and provide technical assistance is referred to as capacity building. Cooperation is the second pillar, and it refers to the countries' commitment to construct and adhere to a shared agenda in terms of the many areas of cybersecurity. Some examples of these areas include knowledge exchange in research and development, open-source intelligence and threat intelligence partnerships, and collaborative agendas. Trust, which includes dispute resolution, bilateral and multilateral discussion, transparency, and accountability, is the third and final pillar that we propose to add into this system.

Despite the fact that we are aware that this framework is capable of significant advancement, our primary objective was to present an exploratory viewpoint on a topic that is now under development. Furthermore, the intention behind this proposal is to make the topic accessible to possible recommendations, which will then be incorporated into subsequent works.

References

[1]. Attatfa A., Renaud K., and Paoli S., "Cyber Diplomacy: A Systematic Literature Review," Procedia Comput Sci. 2020;176:60-69. doi: 10.1016/j.procs.2020.08.007. Epub 2020 Oct 2. PMID: 33042293; PMCID: PMC7531992.

[2]. consilium.europa.eu (2015, February 11). Cyberattacks: The EU ready to respond with a range of measures, including sanctions. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[3]. consilium.europa.eu (2017, June 19). Council Conclusions on Cyber Diplomacy Retrieved from https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

[4]. diplomacy.edu. (2022). Digital diplomacy. Retrieved from www.diplomacy.edu: https://www.diplomacy.edu/topics/digital-diplomacy/

[5]. diplomacy.edu. (2022). FAQ about Diplomacy. Retrieved from https://www.diplomacy.edu/: https://www.diplomacy.edu/

[6]. europa.eu. (2022). Shaping Europe's digital future. Retrieved from https://digital-strategy.ec.europa.eu/en

[7]. National Geographic. (2022). Diplomacy. Retrieved from https://education.nationalgeographic.org/resource/diplomacy

[8]. NATO. (2019, August 29). Article by NATO Secretary General Jens Stoltenberg published in Prospect's new cyber resilience supplement. Retrieved from https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en

[9]. Paris Peace Forum. (2018). The Paris Call for Trust and Security in Cyberspace. Retrieved from https://parispeaceforum.org/en/initiatives/the-paris-call-for-trust-and-security-in-cyberspace/

[10]. state.gov. (2022). Bureau of Cyberspace and Digital Policy. Retrieved from https://www.state.gov/:https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/

[11]. EU-Cyber Direct. (2022). Is War in Ukraine the End of Cyber Diplomacy? » directions blog. https://directionsblog.eu/is-war-in-ukraine-the-end-of-cyber-diplomacy/

[12]. Halpern, S. (2019, July 18). How Cyber Weapons Are Changing the Landscape of Modern Warfare. The New Yorker. https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare

[13]. McCaul, M. T. (2021, April 22). Text - H.R.1251 - 117th Congress (2021-2022): Cyber Diplomacy Act of 2021 (2021/2022) [Legislation]. http://www.congress.gov/