Relevance and Importance of Cyber Diplomacy for Developing Countries

Gamini Gunawardane[1*] and Karen Jone[2]

California, USA[1]

University of South Africa, South Africa. [2]

*ggunawardane@fullerton.edu

Abstract - Modern societies, economies, and critical infrastructures of every country and organization are largely dependent on computer networks and information. The exponential growth of the Internet and its use by various emerging technologies such as social media, cloud computing, and smartphone technology has led to significant growth of cyber-attack incidents often with disastrous consequences. Forbes magazine reported that global cyber security crime in 2017 cost an estimated 1 trillion US dollars which are expected to increase to 6 trillion US dollars by 2021. Individual countries' efforts to ensure cyber security have been in existence for many years but it is difficult for national laws and policies to address global cyber security problems sufficiently. Therefore, experts have recommended Cyber Diplomacy as a way of combating global cyber threats. This paper addresses the current status of cyber diplomacy at the global level; cyber diplomacy policies and practices in developing/small countries; the relevance and importance of cyber diplomacy to developing/small countries, and cyber diplomacy models and practices suitable for such countries. Our analysis and conclusion are based on a comprehensive survey of the literature (journal articles, conference proceedings, and industry publications), industry and consultant white papers, expert opinion papers, and bilateral and multilateral agreements. Our Preliminary findings indicate that there is a need for cyber security at the global level and hence the value of cyber diplomacy even in developing countries. In cyber diplomacy, small states show a preference for engaging in dialogues among multilateral organizations with varying policies dependent on domestic conditions.

Keywords: Cyber security. Cyber diplomacy. Developing countries

I. Introduction

Modern societies, economies, and critical infrastructures of every country and organization are largely dependent on computer networks and information. The exponential growth of the Internet and its use by various emerging technologies such as social media, cloud computing, and smartphone technology has led to significant growth of cyber-attack incidents often with disastrous consequences. Common tools used by these attackers include malware, ransomware, phishing, SQL injection, cross-site scripting, service denial, MITM attacks, and session hijackings. Forbes magazine reported that global cyber security crime in 2017 cost an estimated 1 trillion US dollars which is expected to increase to 6 trillion US dollars by 2021. These global cyber-attacks are driven by financial and political motives.

The increasing threats in cyberspace have triggered discussions on the best strategies for combating these threats and safeguarding data and information stored in electronic platforms. This field is called Cyber Security. Individual countries' efforts to ensure cyber security have been in existence for many years. In the early days, individual country efforts to ensure cyber security were implemented in financial and health care institutions in some countries. A good example is the United States of America (USA). In the USA, The Health Insurance Portability and Accountability Act (HIPAA) of 1996 established national standards to protect individuals' medical records and other individually identifiable health information ("protected health information"). Similarly, in the USA, The Gramm-Leach-Bliley Act (1999) requires financial institutions to safeguard customer-sensitive financial data.

However, in recent times, the need to understand cyber security strategies at the international level has been recognized. Modern cyberspace involves multiple countries, making it difficult for national laws and policies, which differ by country, to address the problem sufficiently. Therefore, experts have recommended several strategies, including diplomacy, as a way of combating cyber threats. This field known as *Cyber Diplomacy* leads to cyber security agreements between two countries (bilateral) or multiple countries (multilateral). Diplomacy is the attempt to adjust conflicting interests of countries (referred to as "States" in international relations) by negotiation and compromise. Such negotiations result in understandings (such as Memorandum of Understandings or MOUs) and formal agreements. Cyber Diplomacy, therefore, is the evolution of diplomatic activities to tackle cyber security issues in the modern digital age.

In international relations and diplomacy, developing countries are sometimes referred to as "small countries" or "small states". In this paper, we will use these three terms interchangeably. Small states are an integral and important part of the international order. About two-thirds of United Nations members fall into this category. They operate in the same broad political and economic environment as all other states. In their foreign policy, they pursue the same objectives of security, prosperity, and well-being of their citizens. Cyber security at the international level is a concern for small countries/states as well. Therefore, attention has been paid in recent times, to the importance of small states also engaging in cyber diplomacy.

There is a wide body of theories and knowledge on how foreign policy and relations, and diplomacy in general, apply to small states. It is generally assumed that because of the different international contexts in which small and large states operate, their foreign policies will reflect different sets of constraints. Therefore, it is reasonable to assume that the objectives and conduct of cyber diplomacy in developing or small states will be different from the general international level cyber diplomacy objectives and practices.

II. Materials and Methods

Research questions this paper will address are: (1) What is the current status of cyber diplomacy at the global level? (2) What is the current status of cyber diplomacy policies and practices in developing/small countries? (3) What is the relevance and importance of cyber diplomacy to developing/small countries, and what cyber diplomacy policies, models and practices should such countries adopt?

Our analysis of, and conclusion on, these research questions will be based on a comprehensive survey of the literature (journals articles, conference proceedings, and industry publications), industry and consultant white papers, expert opinion papers, bi-lateral and multilateral MOUs and agreements, and legal reviews related to cyber diplomacy.

III. Results and Discussion

Our Preliminary findings include the following:

(1) There is a strong understanding across the world that governments and industries must work together to tackle cyber security at the global level.

(2) There seems to be a consensus that early warning of new threats is vital, and that continuous monitoring has emerged as the principal viable approach for dealing with cyber security on a global scale. This shows the value in cyber diplomacy at the global level to build global coalitions.

(3) A handful of bilateral and multi-lateral cyber security agreements are in place. These include a cyber security treaty between China and Russia, an African Union treaty ("African Union Convention on Cyber Security and Personal Data Protection."), the Shanghai Cooperation Organization Security,", NATO's "Enhanced Cyber Defense Policy", and The United States and China MOU on timely responses to malicious cyber activities.

There is evidence that developing countries are also subject to international-level cyber security threats. This is due to a lack of surveillance capabilities, unsecured networks, a lack of cyber regulations, and a shortage of ICT security knowledge and capabilities.

(5) Cyber diplomacy is an inevitable tool for less-capable states in the twenty-first century.

(6) In cyber diplomacy, small states show a preference for engaging in dialogues among multilateral organizations because they reduce the power asymmetry between states, decrease the transaction costs of diplomacy, and impose constraints on large states. Small state security policies vary widely depending on domestic and international conditions.

References

[1] Attatfa, A., Renaud, K. and Paoli, S.D. "Cyber Diplomacy: A Systematic Literature Review. Procedia Computer Science," 176, p. 60-69, 2020.

[2] Barrinha, A., Renard, T., Cyber-diplomacy: the making of an International Society in the digital age. Global Affairs 3, p. 353–364, 2017.

[3] Holmes, A., and Simon J. R., "Global diplomacy: theories, types, and models," Boulder, Colorado: Westview Press, 2016.

[4] Van der Meer, S., "Enhancing international cyber security: A key role for diplomacy. Security and Human Rights" 26, p. 193–205, 2015.