M.A. (Name of the Course)

ROLE OF INTERNATIONAL AND REGIONAL ORGANISATIONS IN CYBER SECURITY: AN ASSESSMENT

By
Name of Student
Roll Number
Year: 2 Semester: IV

DISSERTATION PROPOSAL

Date

NALSAR UNIVERSITY OF LAW
HYDERABAD

INTRODUCTION:

Almost everyone recognizes the salience of cyberspace as a fact of daily life. Given its ubiquity, scale, and scope, cyberspace has become a fundamental feature of the world we live in and has created a new reality for almost everyone in the developed world and increasingly for people in in the developing world[1].

Cyberspace is a game changer in international relations, and new digital technologies and ways of communicating will have a considerable impact on security and strategic stability. Many of the central beliefs that underpinned international politics during the years of the Cold War have become increasingly irrelevant in the face of new types of economic competition, forms of conflicts, factors of power and international influence, new actors and a generally new global environment. The central reason for this is that the amount and speed of information shared globally between different actors has increased significantly, thus fundamentally changing how decisions are made in international politics.

The new nature of information communications has also created unprecedented opportunities for intentional deceit, and the dissemination of false information. The technologies that were supposed to raise the level of confidence and interdependence between actors have instead exacerbated mistrust in both domestic and international relations to a scale that would be impossible without this new technological infrastructure. Together—the ubiquitous spread of information technologies and the intensification of information sharing—should be understood as a new information era. It brings unquestionable benefits, but at the same time humanity faces a number of serious challenges. In particular, information security. Insecure information communication means that third-party actors could acquire unauthorized access to sensitive information, which could be for their often-nefarious purposes. This insecure communication infrastructure inevitably leads to a greater inability to remain competitive, maintain advantages and generally pursue political goals.

Legal scholarship about cybersecurity has focused on cyberspace as a new domain for warfare. As such, existing discussions have tended to concentrate on cyber "crime," cyber "espionage," cyber "attacks," and cyber "warfare" as willfully perpetrated, pre-meditated, and intentional actions. Furthermore, existing legal literature has focused almost exclusively on the legal obligations of, and possible sanctions against, states and non-state actors that orchestrated cyber attacks, and to a much

1 Nazli Choucri and Ors, "Institutions for Cyber Security: International Responses and Data Sharing Initiatives", Working Paper CISL# 2016-10, Massachusetts Institute of Technology Cambridge, Available at: http://web.mit.edu/smadnick/www/wp/2016-10.pdf; Accessed on: 08-04-2021

lesser extent on the responsibilities of states whose own cyber infrastructure has been used by another state or by non-state actors to carry out harmful cyber operations against a third state.

Over the better part of a decade, the convergence of four distinct but interconnected trends in international relations created demands for formal interventions involving governments and international coordination. First, Internet usage continued to rise, coupled with an expansion in forms of use. Second, many governments recognized that cyber vulnerabilities continued to threaten not only the security of their own networks, but also those of their citizens involved in routine activities on a daily basis. Third, a noted absence of coordinated industry response or of efforts to develop cooperative threat reduction strategies, reinforced an unambiguous gap-in-governance. Finally, a growing set of cyber incidents, large and small, signaled to governments the potential impact of their failure to address the emerging threats. In response to these trends, governments, in various ways, mobilized significant national and international resources toward the creation of a broad cyber security framework.

RESEARCH OBJECTIVE:

The objective of this paper is twofold: firstly, the research aims to analyse the cyber security setting globally and regionally; secondary it aims to signify the importance of Organisations, both governmental and non-governmental, and also propose suggestions to enhance cybersecurity co-operation among them.

STATEMENT OF PROBLEM:

While most of the literature is on concept of cyber security, threat perception, cyber crimes, there is very little literature on the role played by various players in the cybersecurity setting. It is the players in cybersecurity architecture that shaped the current setting. International and regional organisations play key role as they come second to the sovereign nations while enabling the cybersecurity.

HYPOTHESIS:

It is hypothesised that the International and regional organisations play important role in enabling and enhancing cybersecurity.

RESEARCH QUESTIONS:

The principle research questions are - 1. What is the current cybersecurity setting globally and regionally?; 2. What is the need of Organisations in maintaining peace and security?; 3. What is role played by the Organisations in enhancing and enabling cybersecurity?

To address these questions, the research will analyse the following critical Issues:

1. How did the evolution of International and regional organisations take place?
2. What is cybersecurity?
3. What is the need of cyber security?
4. What are the various International Organisations working in the domain cybersecurity?
5. How do the International Organisations play key role in enhancing and enabling cybersecurity?
6. What is the status of regional organisations in America, Europe and South Asia in cybersecurity architecture?
7. What are the laws covering such organisations and what are the principles binding the states in co-operation among them?

RESEARCH METHODOLOGY:

The research will be predominantly desk-based. The researcher will employ empirical research and vastly depend on the descriptive analytical method to answer the above questions. This research is aimed at analytically examining the existing situation, challenges and determine the possible reforms and strategies to overcome the issues.

As stated earlier, the research is predominantly library-based and where practicable , data may be drawn from the publications and presentations by the experts and policy experts and strategists. The researcher will mostly rely on government policies, speeches by eminent personalities, journal articles, online sources, monographs, scholarly writings, conference materials and text books, reports and publications in attempting the research questions.

SCOPE OF RESEARCH:

With the evolution of technology, the risk to protect it has also increased. As the cyberspace is dual-use in nature, and has strategic standing, it is important to protect the same. The interdependent of states has increased with the increase in cross-border threats and crimes. This interdependence and co-operation is assisted by the Organisations, both International and Regional. Therefore it is important to note the relevance and importance of the same.

LITERATURE REVIEW:

Institutions for Cyber Security: International Responses and Data Sharing Initiatives by Nazli Choucri, Stuart Madnick, Priscilla Koepke: This paper seeks to provide an initial baseline, for representing and tracking institutional responses to a rapidly changing international landscape, real as well as virtual. This paper argues that the current institutional landscape managing security issues in the cyber domain has developed in major ways, but that it is still "under construction." They also expect institutions for cyber security to support and reinforce the contributions of information technology to the development process. The authors begin with (a) highlights of international institutional theory and an empirical "census" of the institutions-in-place for cyber security, and then turn to (b) key imperatives of information technology-development linkages and the various cyber processes that enhance developmental processes, (c) major institutional responses to cyber threats and cybercrime as well select international and national policy postures and so critical for industrial countries and increasingly for developing states as well, and (d) the salience of new mechanisms designed specifically in response to cyber threats.

Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents by Oren Gross: This paper analysis the cyber threats, and obligations and responsibilities of the attacked states, which are directly affected by the cyber incidents.

RESEARCH PLAN:

The researcher will achieve the objective by analysing the literature through the following chapters -

1. Introduction

This chapter introduces the topic and also highlight the aim, scope and purpose of research.

2. Concept and evolution of International Organisations

This chapter analyses the evolution of International organisations.

3. Importance of Regional Organisations

It deals with the history and importance of regional organisations.

4. Concept of Security and Cyber Security

This chapter analysis the concept of security and cyber security.

5. International Institutions relating to Cyber Security

This chapter highlights various International institutions working in the domain of cybersecurity.

6. Role of Cyber-related Organisations in maintaining Cyber Security

This chapter analyses the role and importance of Organisations in maintaining cyber security.

7. Laws governing International cyber security co-operation

This part analyses and highlights various laws and policies governing the organisations and cyber co-operation among states.

8. Cyber security setting in South Asia, America and Europe

This chapter analyses the cyber security setting in south Asia, America and Europe.

9. Cyber Security setting in India

This part analyses the role of India in global cybersecurity.

10. Conclusion

This chapter contains the suggestions and conclusion made through the analysis and research.

BIBLIOGRAPHY

- Benoliel, Daniel. (2015). Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study. North Carolina Journal of Law & Technology, Vol. 16(3).
- Carr, Madeline. (2016). Public-private partnerships in national cyber-security strategies. International Affairs, Vol. 92(1), 43-62.
- ENISA. (2014). An Evaluation Framework for National Cyber Security Strategies .
- Henschke, Adam and Shannon Brandt Ford. (2017). Cybersecurity, trustworthiness and resilient systems: guiding values for policy. Journal of Cyber Policy, Vol. 2(1), 82-95.
- Internet Society. (2016). Internet Governance - Why the Multistakeholder Approach Works .
- ITU. (2018). A Guide to Developing A National Cybersecurity Strategy .
- Lindstrom, Gustav and Eric Luiijf. (2012). Political Aims & Policy Methods. In Alexander Klimburg (Ed.). National Cyber Security Framework Manual (pp. 44-65). NATO CCD COE Publication, Tallinn.

- Morgus, Robert and Justin Sherman. (2018). The Idealized Internet vs. Internet Realities: Analytical Framework for Assessing the Freedom, Openness, Interoperability, Security, and Resiliency of the Global Internet (Version 1.0).
- Newhouse, William, Stephanie Keith, Benjamin Scribner, and Greg Witte. (2017). National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. NIST Special Publication 800-181.
- Reich, Pauline, Pravin Anand, Vaishal Mittal, Ayushi Kiran, Anna Maria Osula, and Stuart Weinstein (2014). Internet governance: International law and global order in cyberspace. In Manfred Steger, Paul Battersby, and Joseph Siracusa. (eds.). The SAGE Handbook of Globalization (pp. 592-620), Sage.
- Seger, Alexander. (2012). Cybercrime strategies. Global Project on Cybercrime.
- Whitmore, Andrew, Namjoo Choi and Anna Arzrumtsyan. (2009). One Size Fits All? On the Feasibility of International Internet Governance. Journal of Information Technology & Politics, Vol. 6:1, 4-11.
- Azmi, Riza, Willam Tibben, and Khin Than Win. (2018). Review of cybersecurity frameworks: context and shared conceptsv. Journal of Cyber Policy, Vol. 3(2), 258-283.
- Finnemore, Marth and Hollis, Duncan. (2016). Constructing Norms for Global Cybersecurity. American Journal of International Law, 110(3), pp. 425-479.
- Jardine, Eric. (2018). Mind the denominator: towards a more effective measurement system for cybersecurity. Journal of Cyber Policy, Vol. 3(1), 116-139.
- Lacy, Mark and Daniel Prince. (2018). Securitization and the global politics of cybersecurity. Global Discourse: An Interdisciplinary Journal of Current Affairs and Applied Contemporary Thought, Vol. 8(1), 100-115.
- Malone, Eloise F. and Michael J. Malone. (2013). The 'wicked problem' of cybersecurity policy: analysis of United States and Canadian policy response. Canadian Foreign Policy Journal, Vol. 19(2), 158-177.
- Sexton, Mark. (2016). U.K. cybersecurity strategy and active cyber defence - issues and risks. Journal of Cyber Policy, Vol. 1(2), 222-224.
- Scott J. Shackelford and Amanda N. Craig. (2014). Beyond the New Digital Divide: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity. Stanford Journal of International Law, Vol. 50(1), 119-184.

- Shackelford, Scott J. and Andraz Kastelic. (2016). Toward a State-Centric Cyber Peace: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity. N.Y.U. Journal of Legislation and Public Policy, Vol. 119, 895-984.
- Thomas, Timothy. (2014). Creating Cyber Strategists: Escaping the 'DIME' Mnemonic. Defence Studies, Vol. 14(4), 370-393.
- Van der Berg, Bibi and Esther Keymolen. (2017). Regulating security on the Internet: control versus trust. International Review of Law, Computers & Technology, Vol. 31(2), 158-177.