Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

http://ecir.mit.edu/

A Research Collaboration of MIT and Harvard University

The Final Report

Version 1.2

Prepared by:

Nazli Choucri, Principal Investigator
Professor of Political Science
Massachusetts Institute of Technology

Cambridge, Mass. 2015

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

APPENDIX A-5

Report on

PERSPECTIVES on CYBERSECURITY

Annotated Table of Contents

Report on

PERSPECTIVES on CYBERSECURITY

`

Annotated of Table of Contents

1 Cybersecurity – Problems, Premises, Perspectives

Nazli Choucri and Chrisma Jackson

An introduction and comparative views of cyberspace

2 An Abbreviated Technical Perspective on Cybersecurity

Ben Z. Yan

Chapter 2 focuses on key technical issues. The purpose is to provide a "platform" that serves as foundations for understanding the technical functionalities essential for Internet operations and, by extensions, the potential targets for threat or damage. None of this issues addressed are contingent on a definition broader than the strictly technical features. Whatever is the definition of cybersecurity that assumed canonical status, it will most surely incorporate technical features.

3 The Conceptual Underpinning of Cyber Security Studies

Liu Yangyue

Chapter 3 introduces conceptual issues that will, increasingly, feature into the cybersecurity debates. It is about the conceptual underpinnings of cybersecurity from the perspective of security studies. Today it is near-impossible to talk of national security without reference to threats in and of the cyber domain. This condition, driven by today's imperatives, requires conceptual and analytical underpinnings if it is to assume a position of credibility in policy analysis or in broader theoretical contexts. Such is the challenge addressed in this chapter.

4 Cyberspace as the Domain of Content

Lyla Fisher

Chapter 4 focuses on cyberspace as a domain of content. By way of orientation, it differentiates between the ends and means of cyberspace so that policymakers can focus on the ends and experts can specialize in the means. This perspective has implications for emergent conceptions of cybersecurity given that it is the security of content that dominates

The next two chapters can be viewed as parallel analyses.

5 DoD Perspective on Cybersecurity

Glen Voltz

6 China's Perspective on Cyber Security

Liu Yangyue

.Chapter 5 is on cybersecurity seen by the US Department of Defense. Chapter 6 is on the China case. It is fair to say that these are far from mirror images of each other. Each reflects distinctive concerns. If there is a simple way of characterizing the US and the China perspective, it may be this: the US focuses on matters of process. China concentrates on features of structure. However unsatisfactory this distinction most surely is, nonetheless it captures some features of the differences between the two countries' conceptions of imperatives for cybersecurity.

The next two chapters can be viewed in parallel.

7 Pursuing Deterrence Internationally in Cyberspace

Chrisma Jackson

8 Is Deterrence Possible in Cyber Warfare?

Brooke Gier

Chapter 7 and Chapter 8 each take on the issue of deterrence in the cyber context. Is there a place for deterrence conventionally understood in the context of cybersecurity? Chapter 7 provides an initial mapping of the issues at hand. Labelled as a "discussion" of deterrence in the cyber era, this chapter outlines some of the major features or perhaps fault lines in debates and deliberations. Chapter 8 simply asks: "Is deterrence possible in cyber warfare?"

9 A Theoretical Framework for Analyzing Interactions between Contemporary Transnational Activism and Digital Communication

Vivian Peron

Chapter 9 provides a major shift in focus, idiom, orientation, methodology, and inference space. Puts forth a theoretical framework for analyzing interactions between transitional activism and digital communication. While the connection to cybersecurity may not be immediately obvious from this statement of focus, the fact remains that any cross border source of cyber threat is, by definition, transitional in the strict sense of the term. At the same time, transitional activism refers to a form of political activity that is organized across borders without reliance on the role of direction of the state

system. Inevitably, this chapter reminds us that, however tempting it might be, we cannot ascribe all incidents of cyber intrusion to state actors. But the motivations are multiple. Threats to cybersecurity in business and industry are likely come as much from other states than from competitors in the marketplace. But the responses by the state are different from those by business, private or public. The fact remains, however, the data are inconclusive about sources, motivations and so forth. What we are more confident about is the nature of the intrusion and, more often than not, the immediate impacts on the target.