Cyber War and Peace Chapter Outlines

INTRODUCTION

PART ONE: CYBER-WHAT? UNDERSTANDING CYBERSECURITY AND INTERNET GOVERNANCE IN THE INFORMATION AGE

The book is structured into three parts. Part I is composed of the first two chapters. Chapter One introduces and defines key concepts such as "cyberspace," "property," "unmanaged commons," and the "global commons," as well as offering a primer on polycentric institutional analysis in the Internet governance context. Chapter Two describes comparative approaches to regulating cyberspace and managing cyber conflict juxtaposed against other global collective action problems.

CHAPTER ONE: GOVERNANCE AT THE FRONTIERS OF INTERNATIONAL RELATIONS: DEFINITIONS AND ASSUMPTIONS

INTRODUCTION
I. Key Definitions and Concepts
II. The Political Economy of International Spaces
III. Who Controls Cyberspace? Introducuing the 'Global Networked Pseudo Commons'
IV. Frameworks for Analyzing Global Common Pool Resources
CONCLUSION

The opening chapter is structured to provide an introduction to the governance of international spaces with a focus on cybersecurity and Internet governance by first exploring the application of commons principles to these unique environments. This examination begins by defining key concepts such as "commons," "pseudo commons," "public goods," "club goods," and "common-pool resources," before moving on to analyze commons governance through the lens of the economics, political science, and legal literatures. Specifically, the chapter discusses the applicability of law and economics concepts such as property rights, use rights, and transaction costs the traditional global commons (including the deep seabed, Antarctica, outer space, and the atmosphere) as well as to cyberspace. The political evolution of territorial sovereignty in these areas is also summarized—drawing from the work of Lawrence Lessig, Tim Wu, Jonathan Zittrain, and Joseph S. Nye, Jr., among others—with a particular emphasis on how cyberspace is distinct from other commons spaces and what that portends for management. Finally, the field of polycentric institutional analysis is introduced along with its application to cyberspace. It is the purview of Chapter One to provide an introduction to the primary characteristics for governing the managed and unmanaged global commons and how these concepts apply (and do not apply) to cyberspace. Chapter Two then discusses the array of global collective action problems stemming from these international spaces along with potential mitigation strategies, which sets the stage for the case studies in Part II.

CHAPTER TWO: MANAGING CYBER ATTACKS AS A GLOBAL COLLECTIVE ACTION PROBLEM

Chapter Two opens with a brief typology of cyber conflict encapsulating cybercrime, espionage, war, and terrorism, before discussing how and why these categories are breaking down in the Information Age and what comparative approaches to regulating cyberspace and managing cyber conflict exist as juxtaposed against other global collective action problems. There are three traditional management solutions to the overexploitation of common pool resources as predicted by the tragedy of the unmanaged commons scenario from which many collective action problems derive: privatization, nationalization, and common property legal regimes. This chapter introduces each of these concepts and reflects on the potential and limits of these approaches, including the ill-fated Common Heritage of Mankind (CHM) concept that was introduced to govern the deep seabed and Moon, as applied to cyberspace. The debate is then viewed through the lens of polycentric governance generally along with introducing a range of leading institutional design frameworks such as the Ostrom design principles, which are in turn applied to both atmospheric and Internet governance in Chapter Three.

PART TWO: SECURITY AND ENVIRONMENTAL THREATS FACING THE GLOBAL COMMONS: CASE STUDIES IN COMMONS MANAGEMENT AND THEIR APPLICATION TO CYBERSECURITY AND INTERNET GOVERNANCE

Part II of the book uses the foundation laid in Part I to analyze the outstanding governance challenges at the frontiers of international relations through the use of comparative case studies, highlighting applications to cybersecurity and Internet governance. Specifically, Chapter Three traces the development of both atmospheric and Internet governance—including coverage on the competing multi-stakeholder (public-private) and multilateral (state-centric) visions for cyberspace—to help identify governance best practices that could be cross-pollinated to help address both climate change and cyber attacks. Chapter Four focuses on the encroachment of continental shelves into the deep seabed using illustrative examples from the Arctic and South China Seas, which includes a significant cyber component given the expanding web of submarine cables in those areas.[1] Chapter Five then examines the current legal regime governing outer space and how resurgent national interests are challenging the peaceful use of the final frontier, including with regards to cyber attacks on satellite infrastructure.[2]

[1] *See, e.g.*, Paul Saffo, *Disrupting Undersea Cables: Cyberspace's Hidden Vulnerability*, ATLANTIC COUNCIL (Apr. 4, 2013), http://www.atlanticcouncil.org/blogs/new-atlanticist/disrupting-undersea-cables-cyberspaces-hidden-vulnerability.

[2] *See* Matt Burgess, *Hackers Targeting Satellites Could Cause 'Catastrophic' Damage*, WIRED (Apr. 26, 2016), http://www.wired.co.uk/article/satellites-vulnerable-hacking-chatham-house.

Chapter Three: On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Help Heal the Planet and Promote Cyber Peace

Introduction
- I. *The Imapct of Cyber-Enabled Technology, Resource Scarcity, and Multipolar Politics on Climate Change and Cyber Attacks*
- II. *An Introduction to Global Climate Change Law and Policy*
- III. *The Polycentric Internet Governance Ecosystem*
- IV. *Mitigating Climate Change and Cyber Attacks Through Polycentric Governance*

Conclusion

Although the atmosphere and cyberspace are distinct arenas, they share similar problems of overuse, difficulties of enforcement, and the associated challenges of collective inaction and free riders introduced in Part I. Moreover, "[m]illions of actors affect the global atmosphere[,]"[3] just as they do Internet governance. With weather patterns changing, global sea levels rising, and temperatures set to exceed 1.5 degrees Celsius by 2100, climate change is a problem affecting the entire world, but one in which benefits are dispersed and the harms are often concentrated. Similarly, much of the cost of cyber attacks is reportedly born by a relatively small number of nations even as others are becoming havens for cybercriminals.[4] This chapter tracks the evolution of the climate change regime discussing both top-down multilateral agreements (such as the UN Framework Convention on Climate Change) as well as bottom-up polycentric efforts with a particular focus from the 2009 Copenhagen Accord to the 2015 Paris Agreement. It then compares and contrasts these findings with the history of Internet governance from its birth in the late 1970s to the last major meetings in 2016. Finally, the potential of polycentric governance to mitigate the two global collective action problems of climate change and cyber attacks is assessed using a groundbreaking regime effectiveness study.

Chapter Four: Was Selden Right?: The Expansion of Closed Seas and its Consequences for Oceanic and Internet Governance

Introduction
- I. *The Impact of Cyber-Enabled Technology, Multipolar Politics, and Resource Scarcity on the Governance of Offshore Resources*
- II. *The Evolution of the Law of the Sea as Applied to the Governance of Offshore Resources*
- III. *Was Selden Right? Continental Shelf Claims and their Impact on the Deep Seabed Regime*
- IV. *From the Arctic to the South China Sea: Applying Polycentric Principles to Thaw Regional Hotspots and Protect the Poles*
- V. *Applying Lessons from Oceanic Governance to Internet Governance*

Conclusion

[3] Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 8 (World Bank Group, Policy Research Working Paper No. 5095, 2009), http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.

[4] *See* Rachael King, *Countries with the Most Cybercrime*, BLOOMBERG BUS. (2012), http://www.bloomberg.com/ss/09/07/0707_ceo_guide_security/1.htm [https://perma.cc/4H75-5GJ9] (noting that the United States, China, and Germany together comprise nearly 40 percent of global cybercrime).

This Chapter analyzes the shrinking high seas, which is due to the encroachment of continental shelf claims under the UN Convention on the Law of the Sea, and what that portends for the governance of regional hot spots such as the South China Sea and the Arctic, as well as the Internet due in part to the expanding web of submarine cables in these areas. The chapter begins by exploring how oceanic governance has been shaped by such forces as advancing technology (that in many cases has been accelerated by cyberspace), multipolar politics, and resource scarcity. It next investigates the evolution of the law of the sea from its Roman Law origins to the 1994 New York Amendments of the Third United Nations Convention on the Law of the Sea with special attention paid to the growth of the territorial seas. The chapter then analyzes the recent spate of continental shelf claims to Commission on the Limits of the Continental Shelf and their impact on the governance regimes applicable to offshore resources, using the Arctic, Antarctic, and South China Seas as illustrative examples. Finally, the chapter applies lessons, such as governance best practices in the form of minilateral norm building from the Arctic Council, to cyberspace.

CHAPTER FIVE: THE FINAL FRONTIER OF GOVERNANCE: DEFINING PROPERTY RIGHTS AND MANAGING WEAPONIZATION AND JUNK IN OUTER SPACE

INTRODUCTION

I. *The Impact of Cyber-Enabled Technology, Multipolar Politics, and Resource Scarcity on the Governance of Outer Space*

II. *The Evolution of Space Law*

III. *Property Rights and the National Regulation of Space*

IV. *Avoiding the Ultimate Tragedy of the Unmanaged Commons: Managing Space Weaponization, Junk, and Cyber Attacks through Sustainable Development*

CONCLUSION

Chapter Five examines the evolution of the legal regime governing outer space and how resurgent national interests are challenging the peaceful use of the final frontier, including with regards to cyber attacks on satellite infrastructure and their potential environmental and security effects. The Chapter begins by briefly investigating the impact of advancing technology (that in many cases has been accelerated by cyberspace), multipolar politics, and resource scarcity on space governance. It then discusses the evolution of space law from the Outer Space Treaty to the present, and analyzes the extent to which the governance structure of space is changing due to increasing national regulation and private activity, as well as to the expansion of Internet access and its associated demands. Next, this chapter examines whether the emerging space regime complex is mitigating the collective action problems of space weaponization and junk, and how the international community may do better using regime effectiveness findings from the literature on institutional analysis. Finally, as with Chapters 3 and 4, identified governance best practices, such as stemming from the International Code of Conduct for Outer Space Activities,[5] are applied to cybersecurity and Internet governance.

[5] *See, e.g.*, Micah Zenko, *A Code of Conduct for Outer Space*, COUNCIL ON FOREIGN REL. (2011), http://www.cfr.org/space/code-conduct-outer-space/p26556; Michael J. Listner, *The International Code of Conduct: Comments on Changes in the Latest Draft and Post-Mortem Thoughts*, SPACE REV. (Oct. 26, 2015), http://www.thespacereview.com/article/2851/1.

PART THREE: GOVERNING NEW FRONTIERS IN THE INFORMATION AGE

Part III of the book summarizes the lessons from Parts I and II, notably the potential for polycentric governance to promote cybersecurity with a special emphasis on the Internet of Things. This is accomplished in Chapter Six, which analyzes the results of the regime effectiveness studies from Part II, and discusses the promise and peril of polycentric regulation in cyberspace. Chapter Seven then suggests a path forward for promoting a positive cyber peace in the Information Age.

CHAPTER SIX: THE FUTURE OF INTERNATIONAL SPACES IN AN INTERCONNECTED WORLD

INTRODUCTION
I. *The Impact of Cyber-Enabled Technological Advancement, Resource Scarcity, and Multipolar Politics on Governance of Global Common Pool Resources*
II. *The Rise and Fall of the CHM Concept: Resurrecting the Purpose of the CHM for the Information Age*
III. *Regime Effectiveness in the Cyber Regime Complex*
CONCLUSION

This Chapter begins with a summary of the impact of cyber-enabled technological advancement, resource scarcity, and multipolar politics on explaining how and why strategies for mitigating global collective action problems are evolving, and what that means for cybersecurity and Internet governance going forward. It then discusses the rise and fall of the CHM concept, and the extent to which sustainable development principles are reinvigorating the central tenants of this concept and with it the sustainable use of global common pool resources. The chapter concludes with a global study of regime effectiveness across the new frontiers studied in Part II with a special emphasis on cyberspace.

CHAPTER SEVEN: A TWENTY-FIRST CENTURY VISION FOR CYBERSECURITY AND INTERNET GOVERNANCE

INTRODUCTION
I. *The Promise and Peril of Polycentric Governance in Cyberspace*
II. *Strategies for Securing the Internet of Everything*
III. *Operationalizing a Positive Cyber Peace*
CONCLUSION

Chapter Seven analyzes the promise and peril of polycentric governance in the Information Age, focusing on the changing role of the United Nations in a multipolar world by using examples from the Part II case studies. Distributed governance best practices identified throughout the study are then applied to promoting a global culture of cybersecurity, particularly with regards to securing the Internet of (Broken) Things, and vulnerable critical infrastructure. The book concludes by suggesting a polycentric path forward for reinvigorating the governance of international spaces in the twenty-first century in a way that avoids tragedies of the unmanaged commons scenarios. Only through such a multi-disciplinary, multi-sector, multi-stakeholder partnership might meaningful progress be made toward engendering sustainable models of Internet governance and an equitable cyber peace.