Towards a Theory of Cyberpower

Franklin Kramer, Stuart Starr, Larry Wentz, Eli Zimet
CTNSP, NDU
Dan Kuehl
IRMC, NDU

June, 2007

Agenda

- Context
- Goal, Objectives
- Framework
- Selected Observations
- Summary

“For Estonia and NATO, A New Kind of War”*

- What/When
  - Cyberspace attacks against Estonia (presumably by Russia)
  - Spring 2007
- Key Questions
  - Is this an “armed attack”?
  - Is the NATO alliance obliged to respond?
  - And if yes, how?

* Anne Applebaum, Washington Post, May 22, 2007

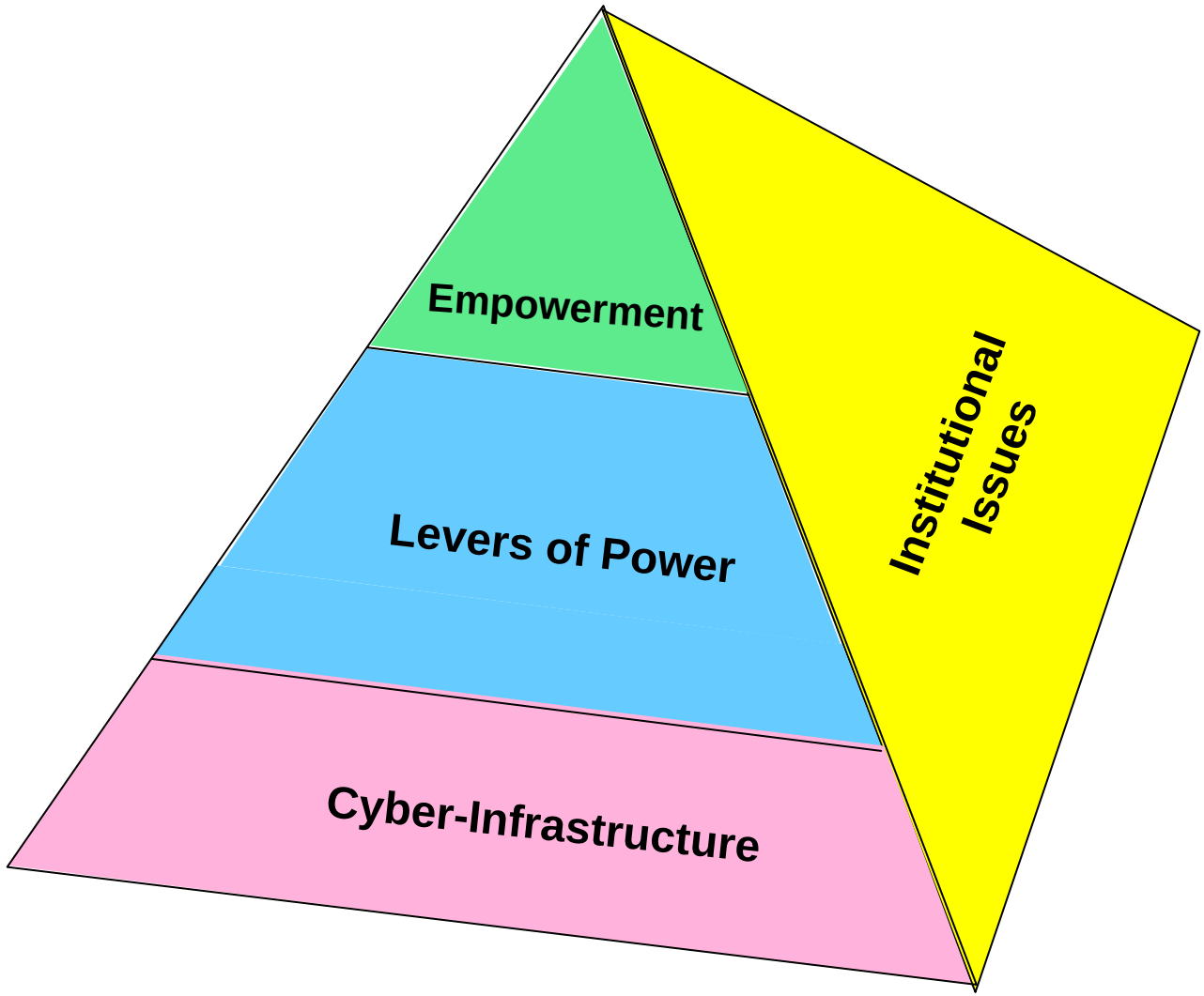
Goal

- "… there is a compelling need for a **comprehensive, robust and articulate cyber power theory** that describes, explains and predicts how our nation should best use cyber power in support of US national and security interests"
- "The theory should account for
  - The nation's increased use of and reliance upon national security, civil and commercial cyber capabilities
  - Other nations' and non-governmental actors' use of cyberspace
  - Direct challenges to the US's use of cyberspace
  - The changed and projected geo-strategic environment"

Objectives

- From a national security perspective, provide **frameworks** to structure cyberpower issues
- Identify and characterize major **cyberpower issues**
- Identify and explore **methods and tools** to perform policy analyses of cyberpower issues

Framework

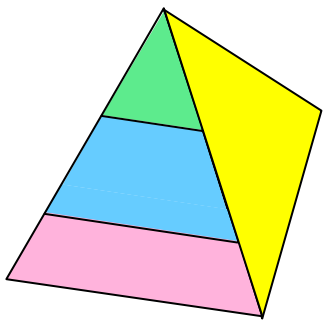

Empowerment
Levers of Power
Cyber-Infrastructure
Institutional Issues

Key Definitions

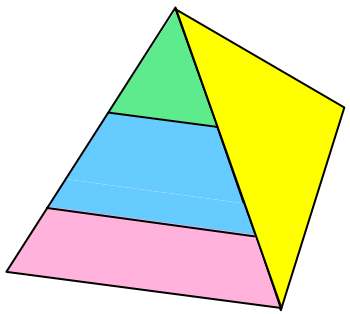
- "**Cyberspace** is an operational domain characterized by the use of electronics and the electronic spectrum to create, store, modify, and exchange information via networked and interconnected information systems and telematic infrastructures."
- " **Cyberpower** is the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power."
- "**Cyberstrategy** is the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power."

Key Activities: Cyber-Infrastructure

- Dan Kuehl, “Cyberspace, Cyberpower, Cyberstrategy”
- Eli Zimet, “Domains of Cyberspace”
- Ed Skoudis,
  - “Evolutionary Trends in Cyberspace”
  - “Security in Cyberspace”
- Marjorie Blumenthal, Dave Clark, “Revolutionary Trends in Cyberspace”
- Will O’Neil, “Critical Infrastructure Protection (CIP)”



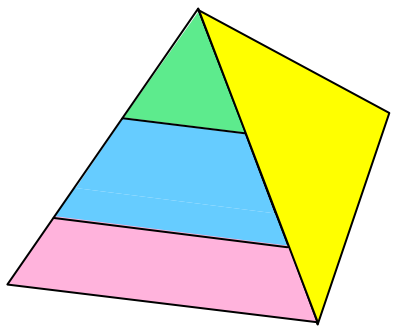
Key Activities: Levers of Power



- Greg Rattray,
  - "Principles of Cyberpower"
  - "Military Benefits & Risks in Cyberspace"
- Martin Libicki, "Military Applications of Cyberspace"
- Service perspectives on cyberspace
- Frank Kramer, Larry Wentz, "Influence Operations: Strategic and Operational Perspectives"
- Stuart Starr, "Influence Operations: Tactical Perspectives"

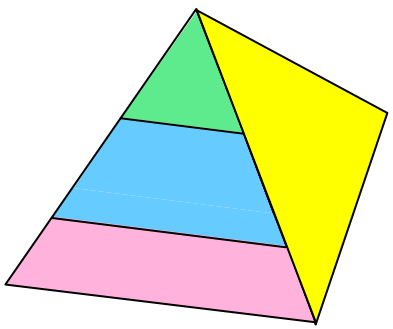
Key Activities: Empowerment

- Jarret Brachman, “Empowerment of Terrorists by Cyberspace”
- Eric Burton, Clay Wilson, “Empowerment of Transnational Criminals by Cyberspace”
- Tim Thomas, “Empowerment of Nation States by Cyberspace”
- Dick Kugler, “Deterrence in Cyberspace”



Key Activities: Institutional Issues

- Hal Kwalwasser, “Governance in Cyberspace”
- Tom Wingfield, “Legal Perspectives on Cyberspace”
- John McCarthy, “Institutional Aspects of CIP”
- Jim Kadtke, “Methods & Tools to Address Cyberpower Issues”



Military Opportunities & Risks in Cyberspace

Level	Opportunities	Risks
Strategic	• NCW-enabled • New “Center of Gravity” opportunities (e.g., deterrence; “virtual conflict”)	• Loss of technical advantage • Rapidly changing operating environment • Military dependence on key systems (e.g., GIG)
Operational	• Phasing of operations • Enhanced force structure mix (e.g., cheaper, more precise)	• Loss of advantage in operational pace
Tactical	• Discover and track adversaries using cyberspace	• New front for adversaries to build resources

We are assuming significant, unknown risk

Options to Address Military Cyberspace Issues

Strategic	Ensure resilience of supporting infrastructures
Operational	Plan to conduct operations against an adversary that is highly cyberwar-capable
Programs	Address cyberspace implications in the development process (e.g., Information Assurance)

Improve analytic capability

Summary (1 of 2)

- Cyber-Infrastructure
  - Cyberspace is a man-made environment that is experiencing
    - Exponential growth
    - Extraordinary diffusion of knowledge among stakeholders
  - The erosion of security in cyberspace is likely to adversely affect key levers of power
  - A new cyberspace architecture may be required to halt this erosion of security
- Levers of Power
  - The military must confront the implications of uncertain security to address unknown risks
  - Cyberspace has the potential to play an increasingly important role in stabilization and reconstruction operations (“I-Power”)

Summary (2 of 2)

- Empowerment
  - Changes in cyberspace have given rise to unintended consequences – it is making life more dangerous for information-enabled societies (e.g., enhanced power of terrorists, transnational criminals)
  - It is uncertain how near-peers (e.g., China, Russia) will exploit cyberpower
  - There is a need for “tailored deterrence” in cyberspace
- Institutional
  - Additional attention must be paid to key cyberspace issues (e.g., governance, legal, government-corporate responsibilities)
  - Research efforts are required to develop methods and tools to address cyberspace policy issues