



Towards a (Preliminary) Theory of Cyberpower

Frank Kramer, Stuart Starr, Larry Wentz

Center for Technology and National Security Policy (CTNSP)

National Defense University (NDU)

June 17, 2008



Objective, Approach

- Objective
 - “... 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” (2006 QDR)
- Approach
 - Multiple workshops were convened to develop the chapters of a book
 - This was complemented by three efforts; we
 - Drew insights from observations of events, experiments, and trends
 - Built on prior national security methods, frameworks, theories, tools, data, and studies
 - Formulated and hypothesized new methods, frameworks, theories, and tools to deal with unexplained trends, issues



Why a Theory?

- A Theory of Cyberpower will serve to
 - Define
 - Categorize
 - Explain
 - Connect
 - Anticipate
- However, as a caveat, any preliminary theory of cyberpower will
 - **Not** be complete
 - Be, at least, somewhat **wrong**



Cyber Theory Challenges



- Timeframe: several decades
- Discipline: subsumes multiple disciplines (e.g., hard and soft sciences, professions), most of whom can not communicate effectively
- Definitions: most basic terms are still contentious
- Categorize: no agreed upon taxonomy
- Explain, anticipate
 - The field is changing exponentially (in the midst of “a tipping point”)
 - Little or no agreement on key frameworks
 - Ability to explain is limited, particularly for social science aspects
 - Reliable prediction is infeasible
- Connect: A holistic perspective has not yet been created



A Theory Will Serve to *Define...*

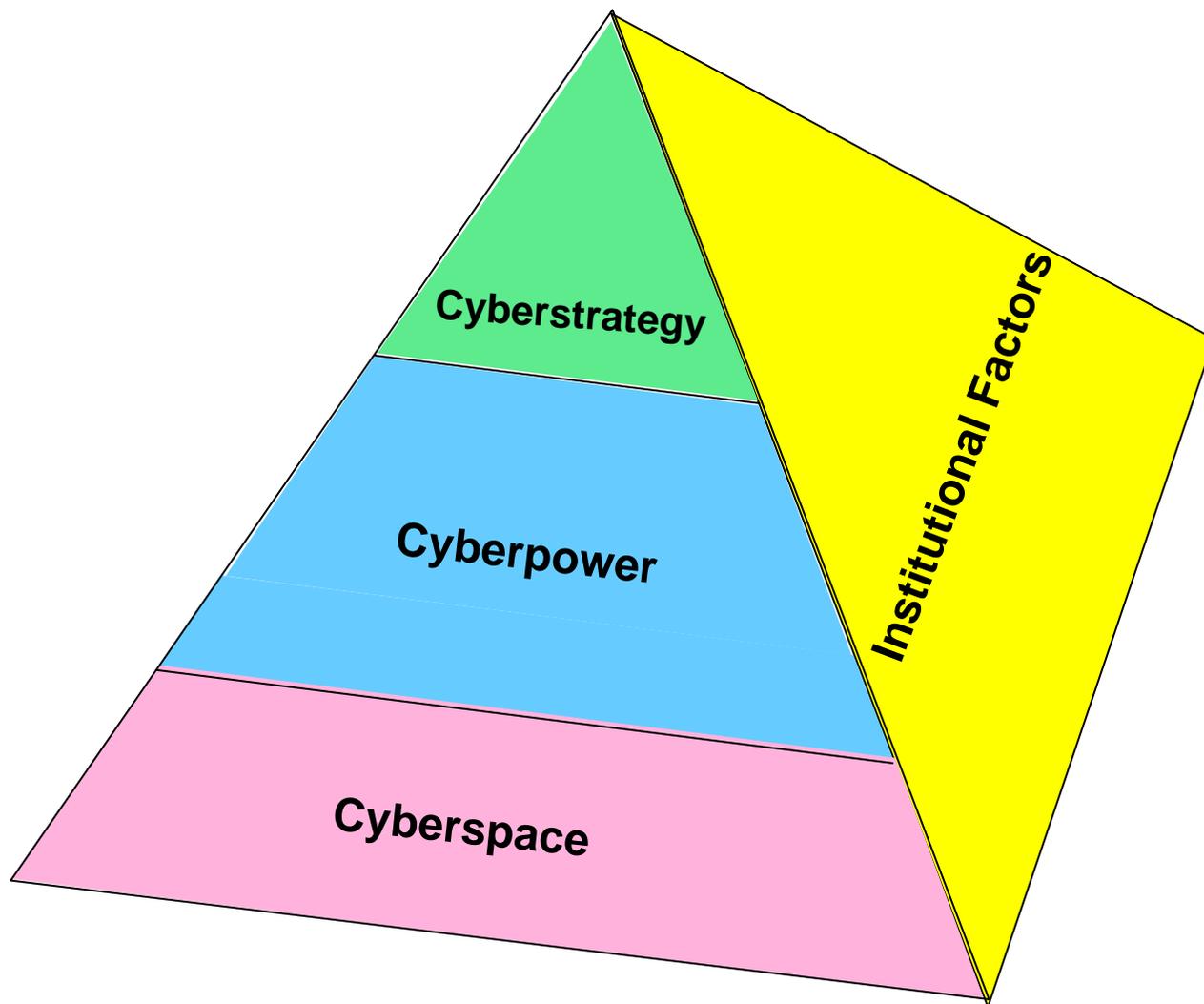


- Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and internetted information systems and their associated infrastructures.”
- **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

Source: Dan Kuehl, IRMC, NDU

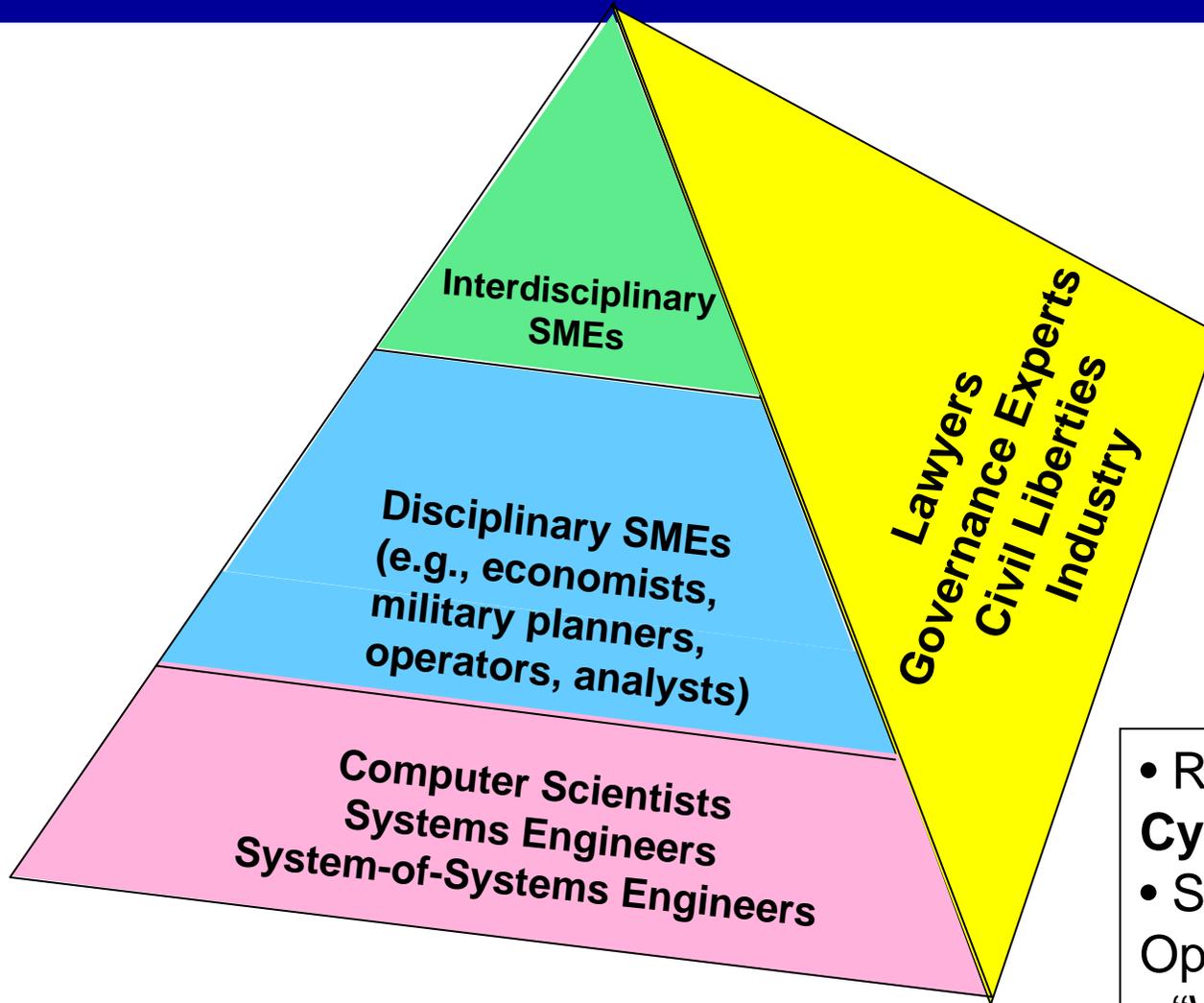


A Theory Will Serve to *Categorize* Areas





A Theory Will Serve to *Categorize* Intellectual Capital



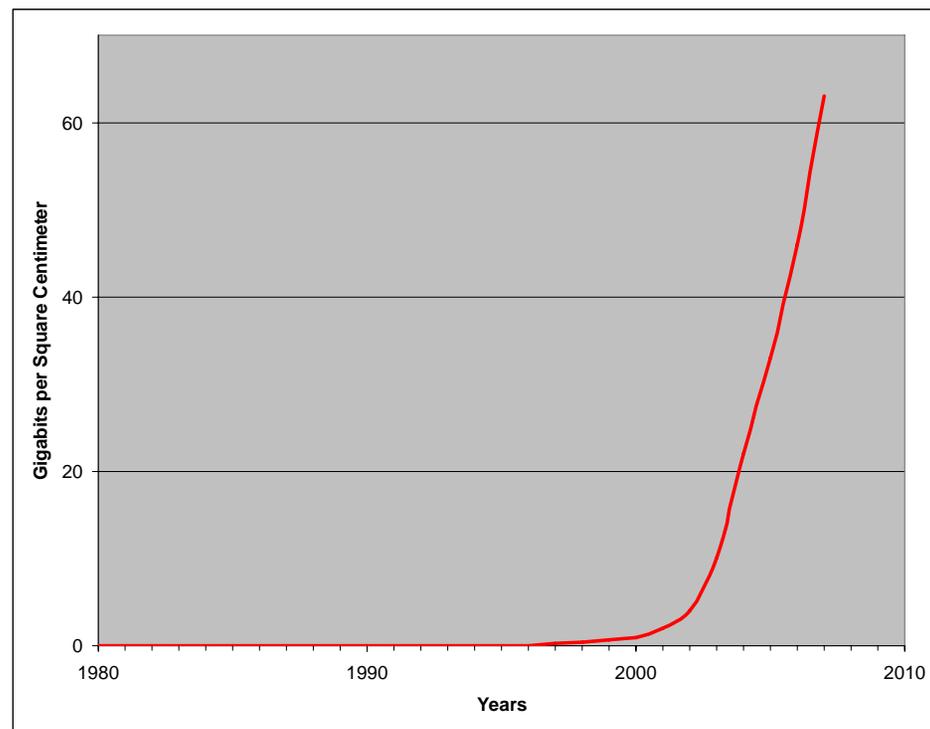
- Recipients:
Cyber Policy Makers
- Support:
Operations Analysts
- “Wild cards”: Futurists



A Theory Will Serve to *Explain*: Cyberspace (1 of 2)



- Cyberspace “rules of thumb”; e.g.,
 - Moore’s Law (e.g., design of micro-electronics)
 - Proliferation of IP addresses (in transitioning from IPv4 to IPv6)
 - Increase in hard drive capacity (2007 Nobel Prize in Physics)



Introduction of Giant-Magnetoresistance
Drives
(Gigabits/cm² vs. Time)



A Theory Will Serve to *Explain*: Cyberspace (2 of 2)



- Strawman “principles of conflict”
 - The offensive has the advantage; e.g.,
 - “Target rich” environment (difficult for defense to prioritize, defend selected targets)
 - Challenges of attribution
 - If cyberspace is to be more resistant to attack, it may require a new architecture that has “designed in” security
 - It will be a challenge to transition from the current legacy system to a more secure objective system



A Theory Will Serve to *Explain*: Cyberpower



- “Rules of Thumb” for Cyberpower
 - Regard “Metcalfe’s Law” as a myth (i.e., “value” varies as N^2)
- Selected observations on military effectiveness
 - Studies of prior military theories (e.g., Mahan and Sea Power) have served to identify
 - Key factors of cyberpower
 - The need for risk assessments
 - In net-centric operations (NCO), the network helps, but it is not clear in what way
 - “I-Power” can be the basis for enhanced performance in Stability and Humanitarian Assistance/Disaster Relief (HA/DR) operations
- Selected observations on Information operations
 - Based on operational objectives, there is a need for changes in Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, and Facilities (DOTMLPF)
 - “New media” have the potential to revolutionize strategic communication



A Theory Will Serve to *Explain*: Cyberstrategy



- The “low end” users (e.g., individuals, hacktivists, terrorists, trans-national criminals) have enhanced their power considerably through recent cyberspace trends
- Potential near-peer adversaries are aggressively exploring options to exploit attributes of cyberspace (e.g., exfiltration of data; implementation of innovative cyber strategems)
- In light of the 2007 attack against Estonia, NATO is rethinking its cyber policy (e.g., Bucharest communique, creation of a Cyber Defense Management Authority)
- A theory of “cyber-deterrence” is beginning to emerge, drawing on all levers of power



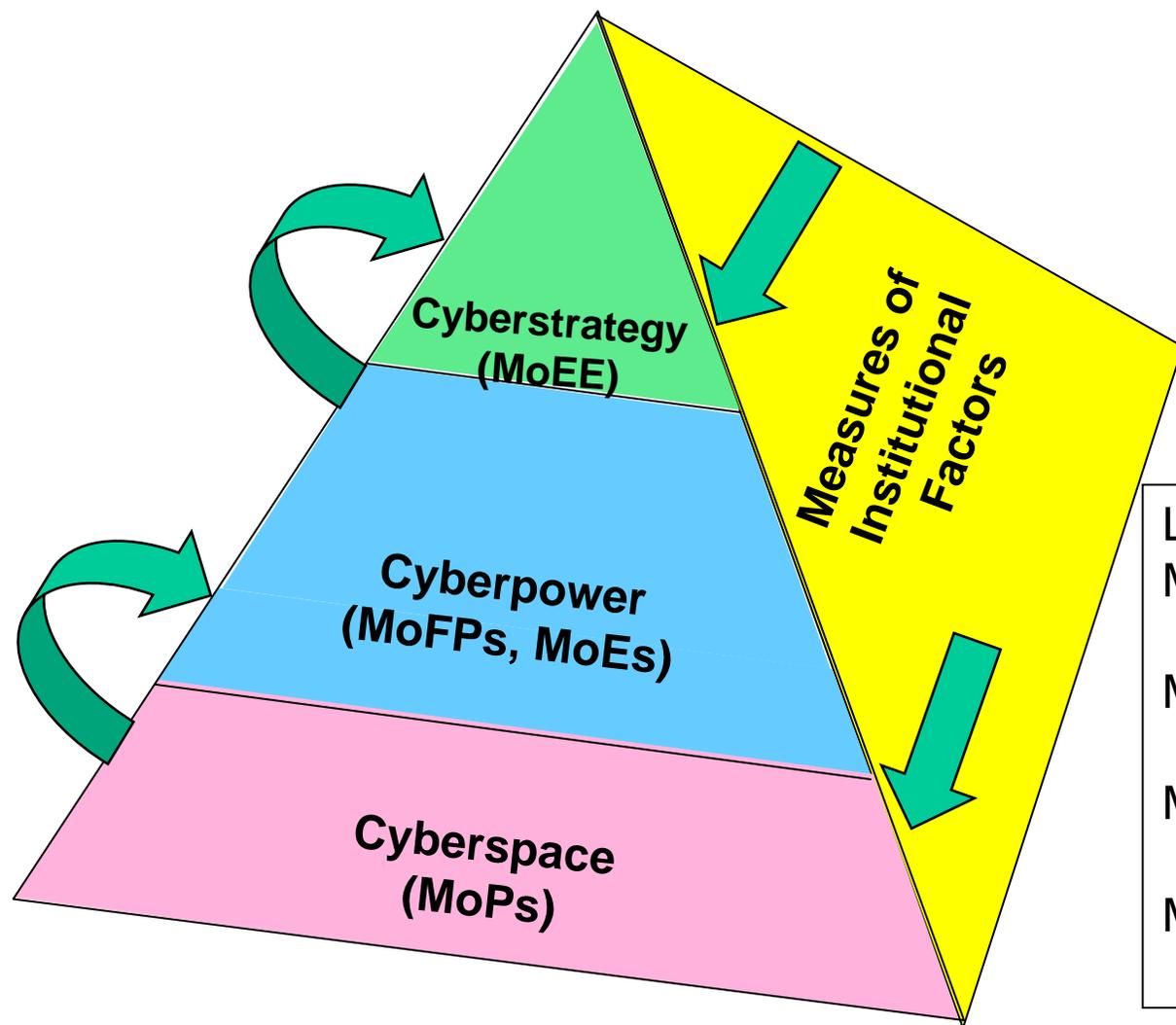
A Theory Will Serve to *Explain*: Institutional Factors



- Given the complexity of the governance mechanisms, one should seek *influence* over cyberspace vice *governance*
- The legal community has barely addressed the key cyber issues that must be resolved during the next decade; e.g.,
 - What is an act of (cyber)war?
 - What is an appropriate response to a “cyber attack”?
- There is a need for a framework and enhanced dialogue between champions of civil liberties and proponents of enhanced cyber security to establish an adequate balance
- Guidance and procedures are required to address the issue of sharing of cyber information between the USG and industry



A Theory Will Serve to *Connect*



Legend:

MoPs: Measures of Performance

MoFPs: Measures of Functional Performance

MoEs: Measures of Effectiveness

MoEE: Measures of Entity Empowerment



A Theory Will Serve to *Anticipate*: Cyber Research Challenges

Area	Research Areas
Cyberspace	<ul style="list-style-type: none">• Perform technology projections to identify key breakthroughs• Explore options to enhance attribution• Develop techniques to protect essential data from exfiltration, corruption• Formulate an objective network architecture that is more secure, and identify options to transition to it
Cyberpower	<ul style="list-style-type: none">• Extend analyses to other levers of power (e.g., diplomatic, economic)• Perform risk assessments to address cyber-dependence• Quantify the Blue-Red information duel
Cyberstrategy	<ul style="list-style-type: none">• Conduct research on "tailored deterrence"• Identify S&T to enhance strategic communication• Explore options to address cyber espionage
Institutional Factors	<ul style="list-style-type: none">• Perform research on cyber influence; legal frameworks; balance between security and civil liberties
Cyber Assessment	<ul style="list-style-type: none">• Develop analytical methods, tools, data, and intellectual capital to assess cyber issues



A Theory of Cyberpower: Residual Challenges



Area	Assessment	Residual Challenges
Define	Green-Amber	<ul style="list-style-type: none">• Rationalize key definitions (e.g., cyber; domain; information operations)
Categorize	Green-Amber	<ul style="list-style-type: none">• Develop a family of frameworks to address various policy issues
Explain	Green-Amber	<ul style="list-style-type: none">• Address a variety of topics that have not been treated in the book (e.g., civil liberties; diplomatic, economic issues)
Connect	Red	<ul style="list-style-type: none">• Develop appropriate Measures of Merit (MoMs) and explore their linkages
Anticipate	Red-Amber	<ul style="list-style-type: none">• Improve assessments of highly non-linear trends



Summary

- The CTNSP Team has
 - Developed a preliminary theory of cyberpower
 - Generated a book on the subject that consists of approximately thirty chapters
 - Identified many key cyber policy issues and formulated preliminary recommendations
- However,
 - Considerable effort is required to enhance the evolving theory of cyber
 - Many of the key policy issues require additional analyses