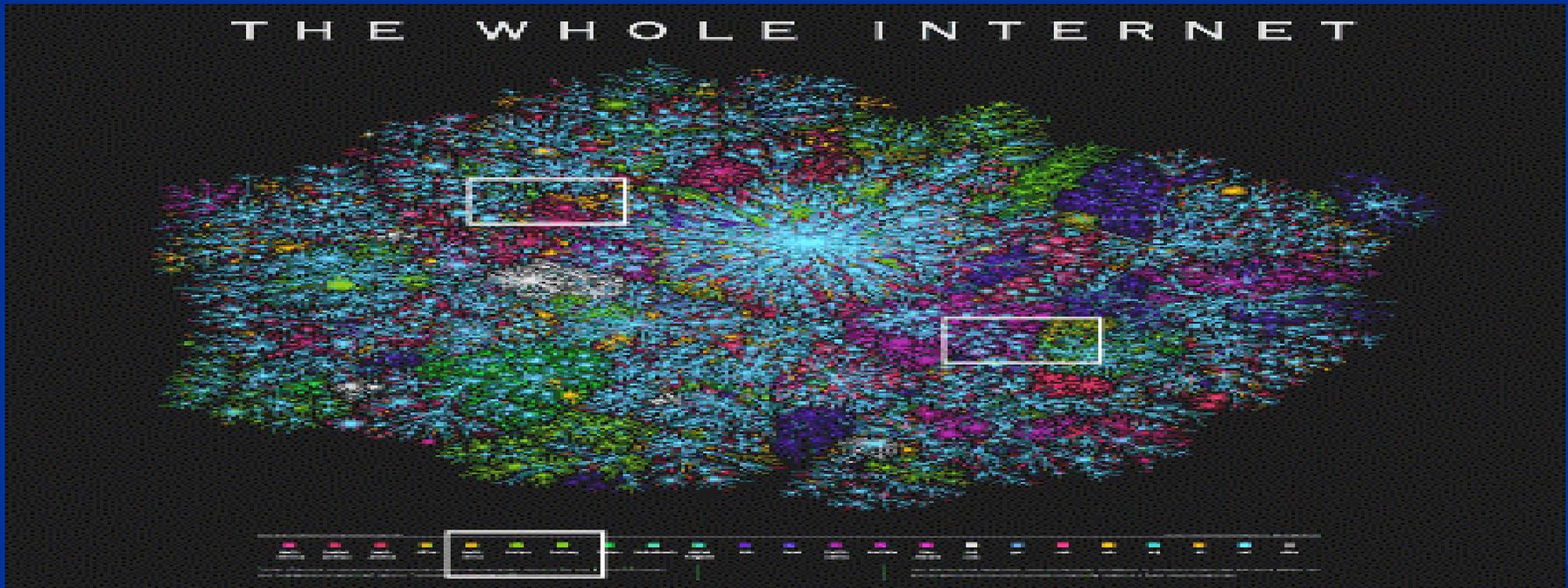


Wanted: a National Information Strategy for the Interconnected Age



Dr Dan Kuehl “kuehld@ndu.edu”

Information Resources Management College

National Defense University

“My Opinions...not the USG/DOD/NDU”



Thesis #1

“the battlespace”

- Information
 - Weapon - Tool - Process – Target ?
 - more than aid to “Blast - Heat - Fragmentation”
 - LTG Mike Hayden, DirNSA
- Synergy
 - human factors + information technology
- Information is now...
 - element of national power
 - operational environment/”battlespace”



Thesis #2

“the threat”

- Modern societies are increasingly vulnerable
 - Technologically/Economically
 - Infrastructures
 - telecommunications, energy, transportation, etc
 - Socially/Politically
 - Perception management, politics
 - “CNN Effect”, “strategic influence”, Al Jazeera, etc
- Employment/Protection requires BOTH technological capability AND political will



Thesis #3

“the partnership”

- The Department of Defense (or MOD), Federal Government, and the private sector share
 - Roles
 - Responsibilities
 - Capabilities

In protecting, leveraging, exploiting:

“national cyberspace” & information power



4 Fundamental Changes New Geostrategic Context

- **Cyberspace**: new operational realm/battlespace
 - Dominant in business, politics, warfare
- **Convergence**
 - Digital: 1110101110001010 = lingua franca
 - Information mediums (radio, TV, phone, etc)
- **Global Omnilinking**
 - Electronic digital connectivity of people, organizations, governments...globally & instantly
- **Critical Infrastructure Protection**
 - Opportunity...and vulnerability
 - Critical to advanced societies, but public/private links poorly understood
 - Roles and missions; what does “interagency” mean?



What it Adds Up To

- Global Economy
 - Dependent on interlinked networks
 - Information as critical as energy and capital
- Global Audience
 - Real-time 24-hour cycle
 - Waning controllability of information
- Global Society
 - Contact anyone, anywhere, anytime
- Strategic Impact: Diplomatic, Economic, Military



Information & National Power

- The **information component**
 - “Use of information content and technology as strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security”
 - Drs Dan Kuehl/Bob Neilson, Georgetown’s *NSSQ* 1999
 - President Ronald Reagan:
 - NSDD 130 (1984)
 - National Security Strategy (1987)



Information Environment

- **Physical: “Ether”/Cyberspace/”eSpace”**
 - Realm of electronic connectivity
 - Physical space
 - Future: increasingly dominant
 - business/economics, politics, warfare
- **Contextual: “influence/perception space”**
 - “Cognitive Space”
 - analogy: “political/economic environments”
 - Example: Serbian TV vs NATO cohesion 1999
 - If you lose the battle here, winning the other may not matter: see Mogadishu, 1993



IO Roadmap

SecDef 30 October 2003

- IO as a core military competency, on par with air-ground-maritime-special ops
 - We must dominate the information spectrum
- Core capabilities
 - EW, CNO, Psyop, Military Deception, Opsec
 - Why these five?
 - Immediate operational impact
 - Interdependent and require integration
 - Organize-Train-Equip implications
- Supporting/Related functions
 - Physical attack and security, IA, Counter-Intel, Public Affairs, Civil-Military Ops



Paradigm Kuehl

- **National Information Power**
 - **Broadest range of military, governmental and civilian capabilities; exploit the global information environment & dominate strategic context**
- **Information Operations**
 - **Wide range of military and governmental operations to protect and/or exploit the environment**
- **Information Warfare**
 - **Military offensive & defensive actions to control/exploit the environment**
- **C2W (information tech in war)**
 - - **blast, heat, fragmentation**

Dan Kuehl, "Joint Information Warfare"
NDU Press Strategic Forum #105
www.ndu.edu/inss



National Security Strategy

Last Clinton NSS, December 2000

- 3 Key pillars
 - Critical Infrastructure Protection (CIP)
 - Vital national interest, use force to defend
 - “Partnership” of public-private sectors
 - Information Warfare/Operations (IW/IO)
 - Lead to Network Centric Ops -- Transformation?
 - Public Diplomacy/International Public Information (PD/IPI).....”Softpower”, “Information Engagement”
 - “increasingly vital....transmit [our] message to people around the world” to “counter misinformation/incitement...mitigate conflict”



National Security Strategy

First Bush NSS, October 2002

- “Infrastructure”, “Information Ops”
 - 1 reference to each
- “Public Diplomacy/Information”
 - 3 references
- No sense of information as power or environment: no sense of its impact
- No coordination of Administration efforts
 - Diplomatically, militarily, economically
- Kuehl/Neilson “No Strategy for an Info Age” USNIP Sept 2003



Information Power...

Who's in Charge?



Diplomatic and Military...
Centralized and Hierarchical



Economic and Information...
Diffused and Shared





What's Lacking

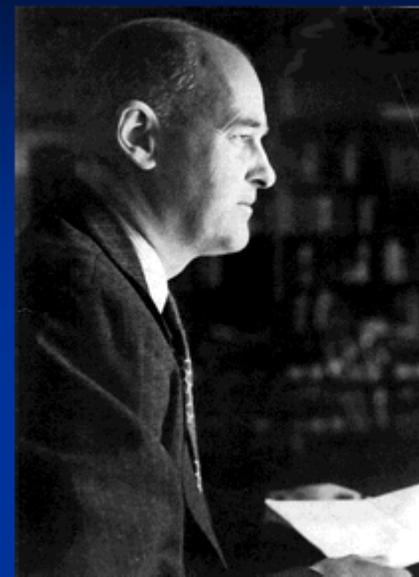
- Who and Where do we go for the COGs of Information Power?

- National Information Council?
- Who would be on it?

- What do need from them?
What are we lacking?

- National Information Strategy
- Why don't we have one?
- **We need a strategic and conceptual foundation for how we can employ Information Power to support national security**

The "Long Telegram"



- 861.00/2 - 2246: Telegram
- *The Charge in the Soviet Union (Kennan) to the Secretary of State*
- SECRET
- Moscow, February 22, 1946--9 p.m. [Received February 22--3: 52 p.m.]
- 511. Answer to Dept's 284, Feb 3 [13] involves questions so intricate, so delicate, so strange to our form of thought, and so important to analysis of our international environment that I cannot compress answers into single brief message without yielding to what I feel would be dangerous degree of over-simplification. I hope, therefore, Dept will bear with me if I submit in answer to this question five parts, subjects of which will be roughly as follows:
 - (1) Basic features of post-war Soviet outlook.
 - (2) Background of this outlook
 - (3) Its projection in practical policy on official level.
 - (4) Its projection on unofficial level.
 - (5) Practical deductions from standpoint of US policy.



National Information Strategy (Suggested)

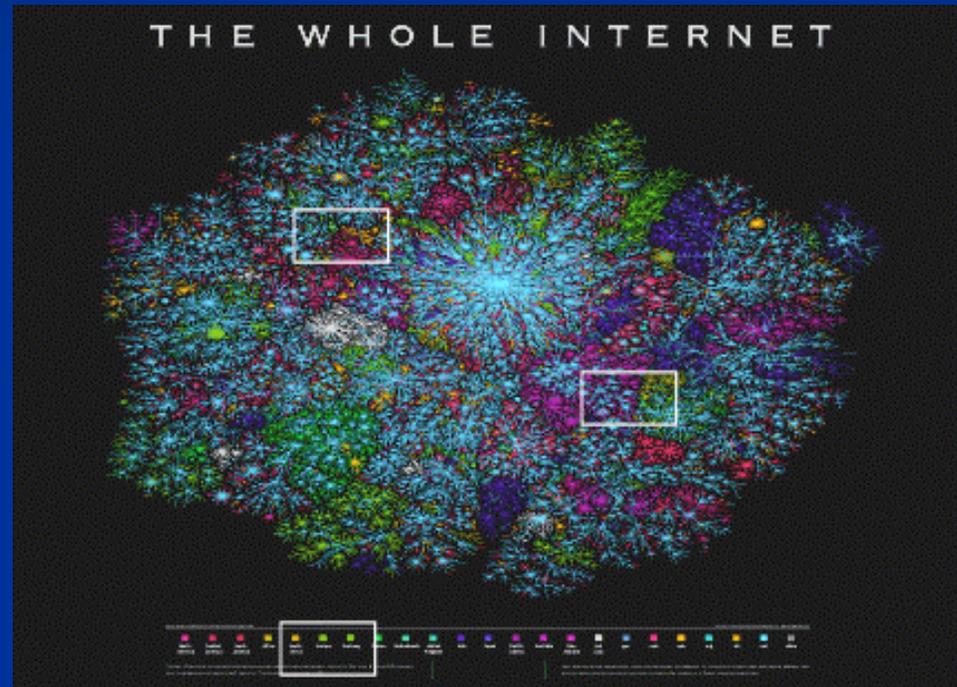
Build on '99/'00 National Security Strategies

- Partnerships
 - Need to build on PDD-63/HSPD-7 efforts...globally
 - Information Superiority
 - New American Way of War; JV2010/2020
 - Cyberspace and Information Operations...Net Centric Ops
 - The Economy
 - IT's decisive and dominant role...globally
 - Influence
 - Internet and TV in “global cognitive battlespace”
 - Essential operational medium for “War of Ideas”
- Dr Dan Kuehl, “Information Power & the National Security Strategy”, Cyberwar 3.0



What's Needed

- Information-age corollary to the “Long Telegram”
- New strategy is not “Containment”...it's **CONNECTIVITY!**
- Free flows of information can enhance
 - Democracy
 - Human rights
 - Economic development
 - Peace





Conclusion

The information environment and element of power:
critical to current/future military & national security
strategy

- Learn how to exploit and defend the information environment...or be defeated via it
- National security in the Interconnected Age requires new alliances and partnerships
 - In Defense, in the Government, in the World
- At least the future won't be dull and boring!



Q & A