

Structuring for Strategic Cyber Defense: A Cyber Manhattan Project Blueprint

O. Sami Saydjari

Cyber Defense Agency, LLC

10 December 2008

Under-space supporting societal fabric is as strategically important as space over head.

The Cyber Space Race is on!

National Strategic Threat

- **Threat**—Sovereignty is at risk
- **Planning**—**DARK ANGEL** (PCD)
 - \$500M, 3 years → Strategic Damage
- **Follow-on**—Congressional Commission for National Cyber Risk Assessment

A New Manhattan Project

- **Vision**—*overcome national strategic vulnerability ASAP*
- **Urgency**—*LC sleeper attacks likely, defenses will take years*
- **Priority**—*Adversary offense & U.S. dependency increasing*
- **Feasibility**—*Tech, Biz Case, Operation, Political, Timing*
- **Project Description**—*architecture, capabilities-driven*
- **Analogy Limits**—*Widget, secrecy, sustained*
- **Cyber Space Race**—*hard, pervasive, societal*

Strategic Cyber Capabilities

Desired End-States (OMW'07)

- **Continuity** of Critical Info Infra. Operations
 - resilience in face of strategic attack, recovery
- **Well-Defended Critical Assets**
 - make economically prohibitive to cause strategic damage
- **Local/Global Cyber Situation Awareness**
 - what's on, who's on, what's connected, traffic, threats
- **Confidentiality-Preserving Systems**
 - prevent unauthorized exfiltration of valued data
- **Extensible Systems Safely Embrace New Technology**
 - extend functionality safely and assuredly
- **Metrics-Based Quantifiable Security**
 - guiding light to progress

Organizing for Success

- The Right Organizing Model—DARPA, NASA
- The Right Start—Agile SPO orchestrating others
- The Right Place—Above the Fray
- The Right Clout—Presidential Backing
- The Right Authority—Power of the Purse
- The Right Leadership—Best of the Best, Diverse
- The Right Size—(Thermopylae) 300
- The Right Mission—Avoid Strategic Damage

A Way Forward

- **Use Architectural Principles**—stratify
- **Value and Prioritize**—protect critical, recovery
- **Validate**—testing to validate theory, strategies
- **Create Assured Trust**—authentication & attestation
- **Develop Human Capital**—workforce is key
- **Robust Standing Research**—create communities
- **Preparatory Deep Analysis**—assess “moves”

Conclusions

- Focus on Strategic Cyber Space
 - Avoid effort diffusion, being overwhelmed
 - Focus on “what can kill you”
- Stakes are High—*provide for common defense*
- Reengineering Cyber Space
 - Cyber territory is engineered and manufactured
 - Requires industry and market reengineering
- Strategic Uncertainty is not acceptable
 - Must understand gravity and nature
 - Ignorance represents a serious policy failure