



Mission, System, Information, Cyber Assurance

**Daryl R. Hild, PhD
Associate Department Head
G021, AF & COCOM Security**

Cyberspace

- A new warfighting domain
 - The traditional domains: Land, Sea, Aero (air, space)
- A unique AOR
 - All other AORs operate, execute missions, through cyberspace
 - Completely man-made: so an opportunity to re-engineer it?
 - Borderless: “There is no ‘there’ [in cyberspace]”
 - Donald Proctor
 - A key front in today’s irregular conflicts
 - US warfighter is no longer network enabled; he/she is network dependent



The Confluence of Space & Cyberspace



- Space is increasingly being contested
 - By nation states
- Cyberspace is increasingly being contested
 - By nation states, terrorists, organized crime, individuals
- Space and Cyberspace are entangled
 - Capabilities in both are:
 - Information technology based
 - Provide asymmetrical advantages – offensively and defensively
 - Lucrative targets – to military, finance, transportation, telecommunications, ...



National Security Perspectives



- **Director of National Intelligence Dennis Blair**
 - We face nation states, terrorist networks, organized criminal groups, individuals, and other cyber actors with varying combinations of access, technical sophistication and intent
 - Many have the capabilities to target elements of the U.S. information infrastructure for intelligence collection, intellectual property theft, or disruption

- **Quadrennial Defense Review, February 2010**
 - DoD is investing in and developing the latest technologies to enable our forces to operate in cyberspace under a wide range of conditions, including in contested and degraded environments
 - DoD can no longer afford to [treat] ... its information technologies and networks as simply benign infrastructure that facilitates their work

Architecting NSS Ground Systems

- **Attractive target for affecting space and cyberspace missions and capabilities**
- **Assurance challenges**
 - **Mission Assurance:** How to achieve mission resiliency? How to enable operating in, and through, contested environments?
 - **System Assurance:** How to build trusted systems? How to sustain trustworthy systems?
 - **Information Assurance:** How to assert confidentiality, integrity, and availability when constructing IT-based systems and missions?



Cyber, Identity & Information Assurance (CIIA)

Developed by DASD(CIIA)

Last Updated: January 14, 2010

Send questions/suggestions to iatac@dtic.mil

