

W. P. CAREY

SCHOOL *of* BUSINESS

Exploitation of Information Technology in the Homeland Security Domain

Presented by: Dr. John N. Ellison

Generic Capabilities

- Intelligence Collection, Analysis and Dissemination
 - Organizational charters and missions
 - Rational resource allocation
- Intelligence Protocols and Exploitation
 - Data-base mining
 - Decision support

Generic Capabilities (continued)

- Dynamic C4IS&R Technology
 - Hardware, software, algorithms
 - Systems architecture and integration
- Organic – Self Organizing Networks
 - Real-time situational awareness
 - Adaptive operational support

Emergency Operations

- Integrated/Coordinated Planning
 - Federal-Allied Jurisdiction
 - State-Regional-Local Jurisdiction
- Crisis Management
 - Distributive indications and warning
 - Secure and integrated communication
- Consequence Management
 - Unified command and control structures
 - Prioritized first responder asset management – Federal, State and Local

Emergency Operations (continued)

- Reconstitution and Recovery
 - Damage surveillance
 - Resource allocation modeling
- Post-Event Evaluation
 - Performance data capture
 - Assessment algorithms

Some Key Concepts

- Asymmetric warfare strategy and doctrine
- Terrorist goals and objectives
- Terrorist organizations, networks and processes
- Vulnerability matrix – targets and value
- All source intelligence flow and fusion
- Discrete indications and warnings
- Preemptive defense and covert action
- Total situational awareness (TSA)

Some Key Concepts (2)

- Precision-unified response
- Network central operations
- Pre-attack:
 - Pre-emptive defense
 - Covert action
- Trans-attack:
 - Crisis management
 - Consequence management
- Post-attack
 - Reconstitution and recovery
 - Restoration and reconstruction

Information Technology and Cyber Warfare

- Offense
 - Dislocate enemy decision infrastructure
 - Disrupt communication systems
 - Corrupt data bases
 - Disintegrate networks
 - Decapitate command and control systems
 - Exploit deception and disinformation

Information Technology and Cyber Warfare

- Defense:
 - Harden command and control systems
 - Secure intelligence data
 - Build redundant and dynamic networks
 - Focus indications and warning (I and W)
 - Disseminate multisensor data products
 - Enhance vertical/horizontal interoperability