



Secure Networking

Dr. Douglas Maughan

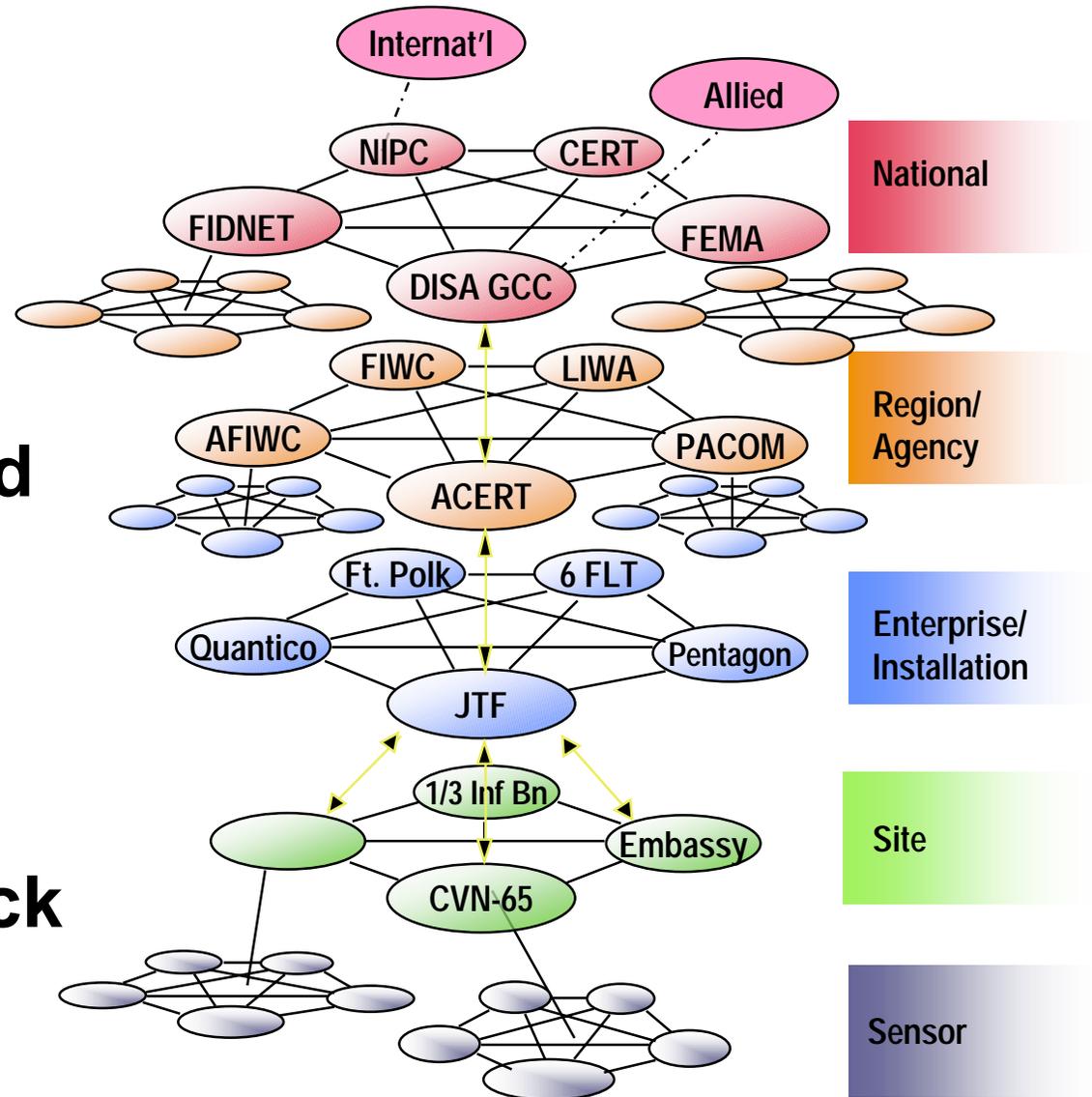
DARPA / ITO

dmaughan@darpa.mil



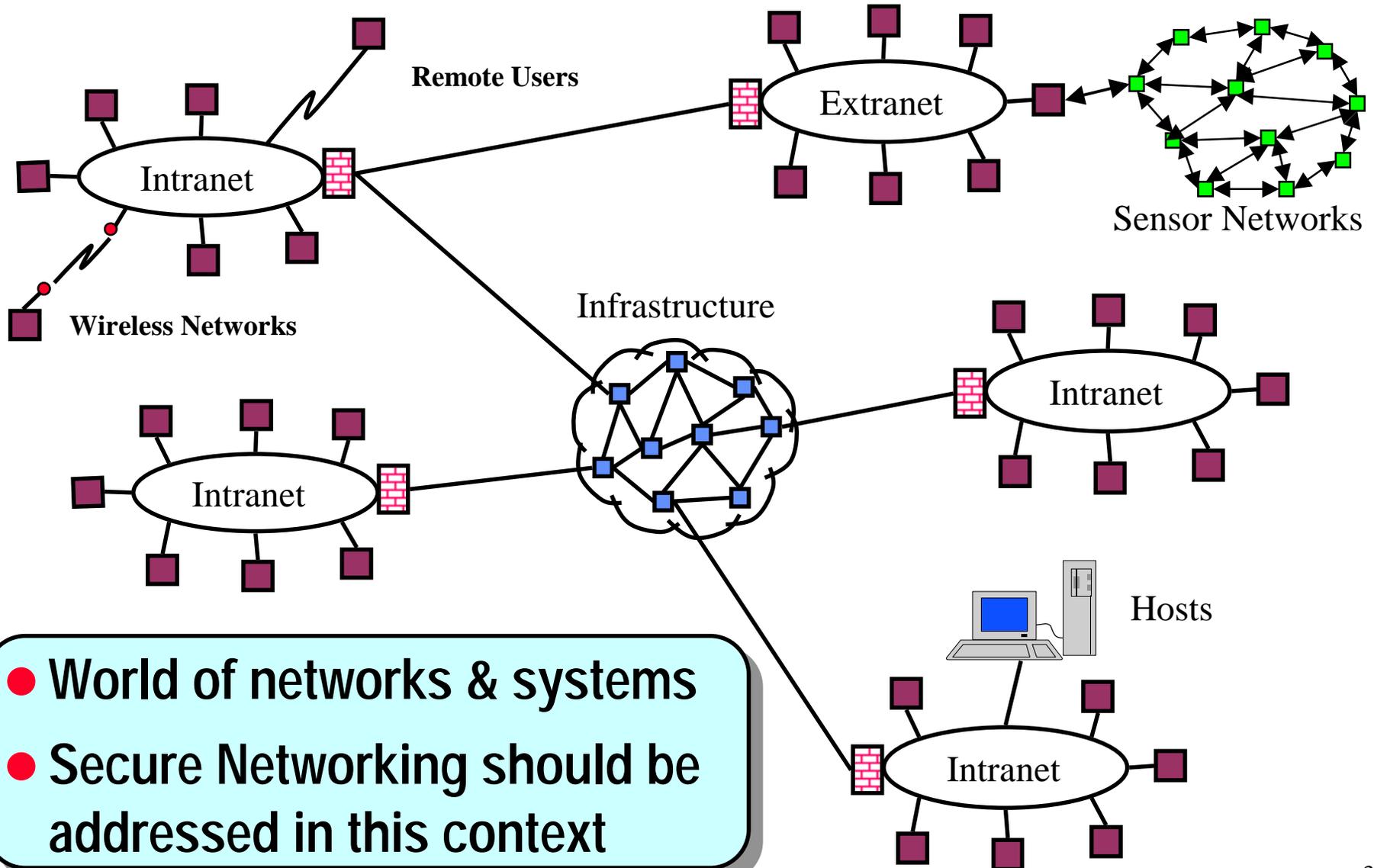
Network Reliance is Pervasive

- DoD depends on networking technology for information dominance at all levels of command hierarchy, BUT ...
- DoD networks are increasingly vulnerable to attack





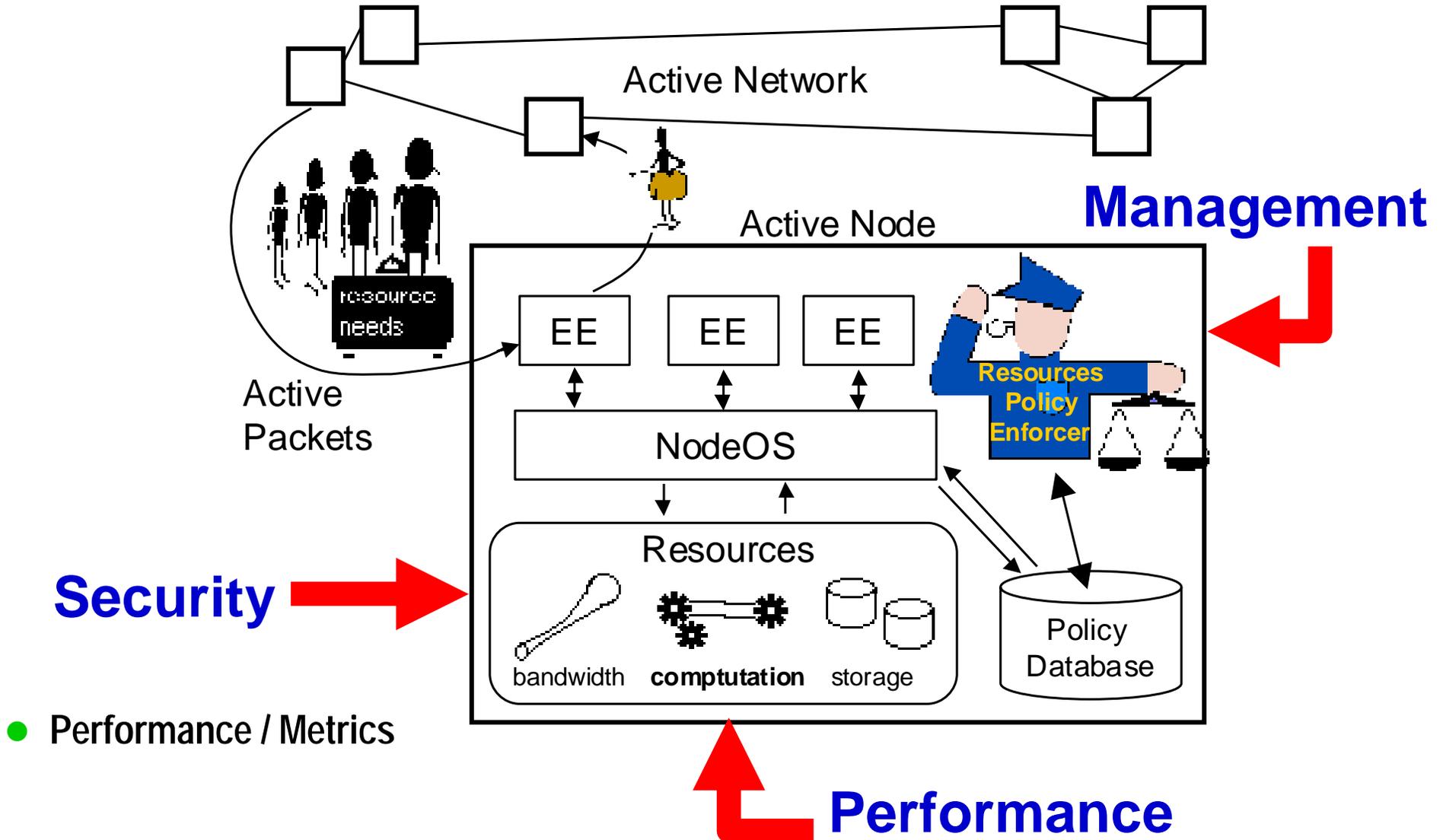
Networks and Systems Research Model



- World of networks & systems
- Secure Networking should be addressed in this context



Active Networks (ANETS)

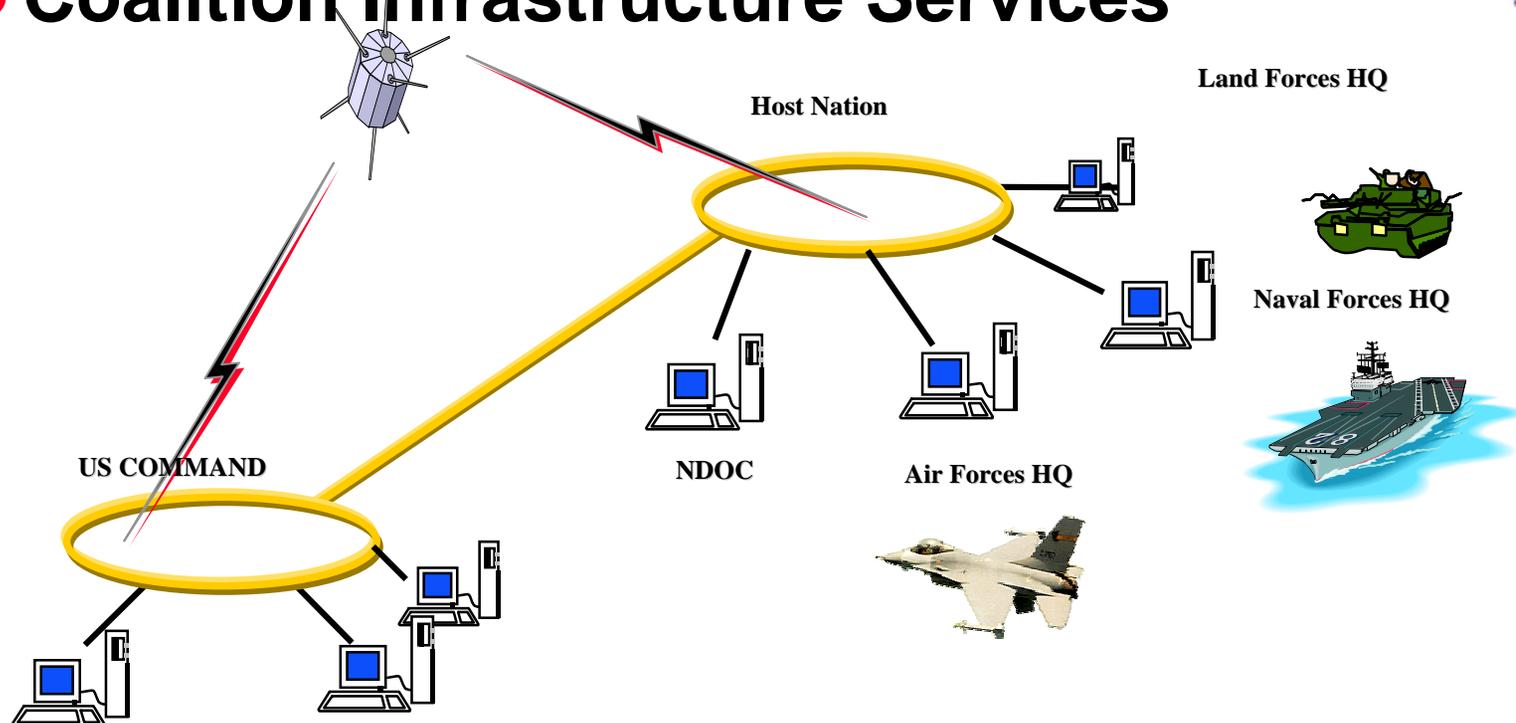




Dynamic Coalitions (DC)

Goal: Manage dynamic coalition formation and secure sharing by authorized members

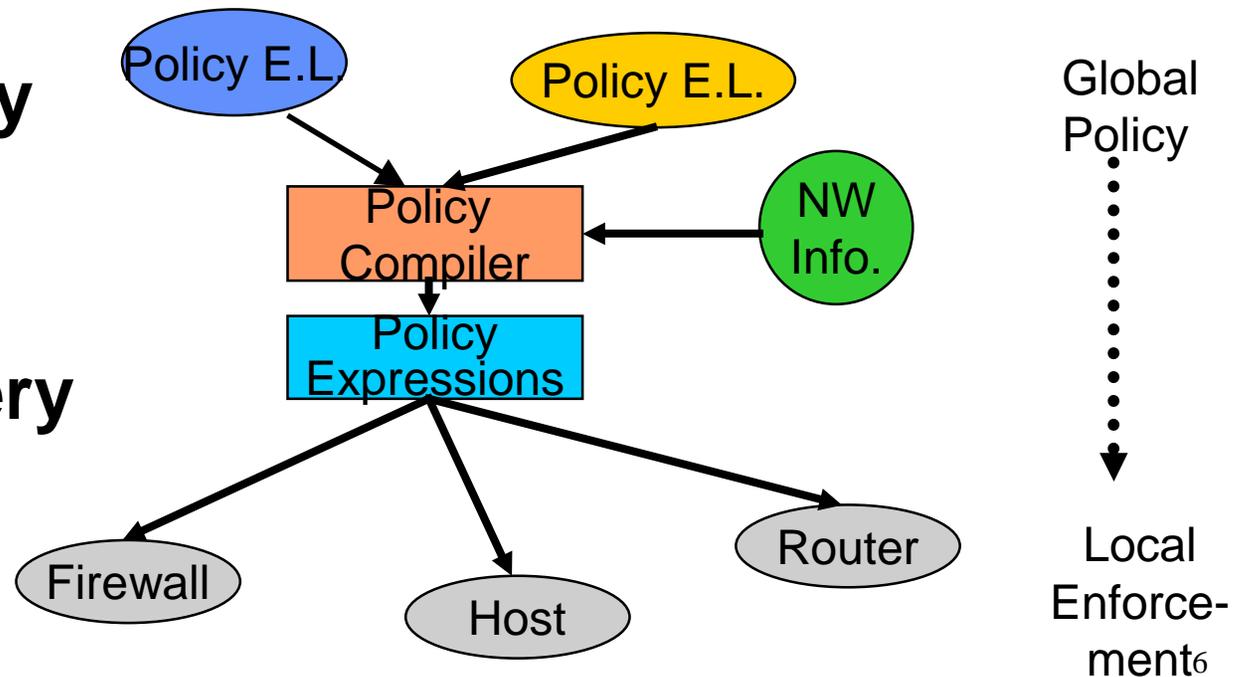
- **Multi-Dimensional Coalition Policies**
- **Secure Group Management**
- **Coalition Infrastructure Services**





Multi-Dimensional Coalition Policies (MDCP)

- Establish “standard” language for policy expression
- Capability to negotiate policies with potential coalition partners (implies multiple at same time)
- Dynamic policy management
 - ◆ Multi-game
- Policy discovery





Secure Group Management (SGM)



- New techniques for sender authentication
- Scalable distribution - group creation & re-key
- Leverage secure multicast standards work



Coalition Infrastructure Services (CIS)



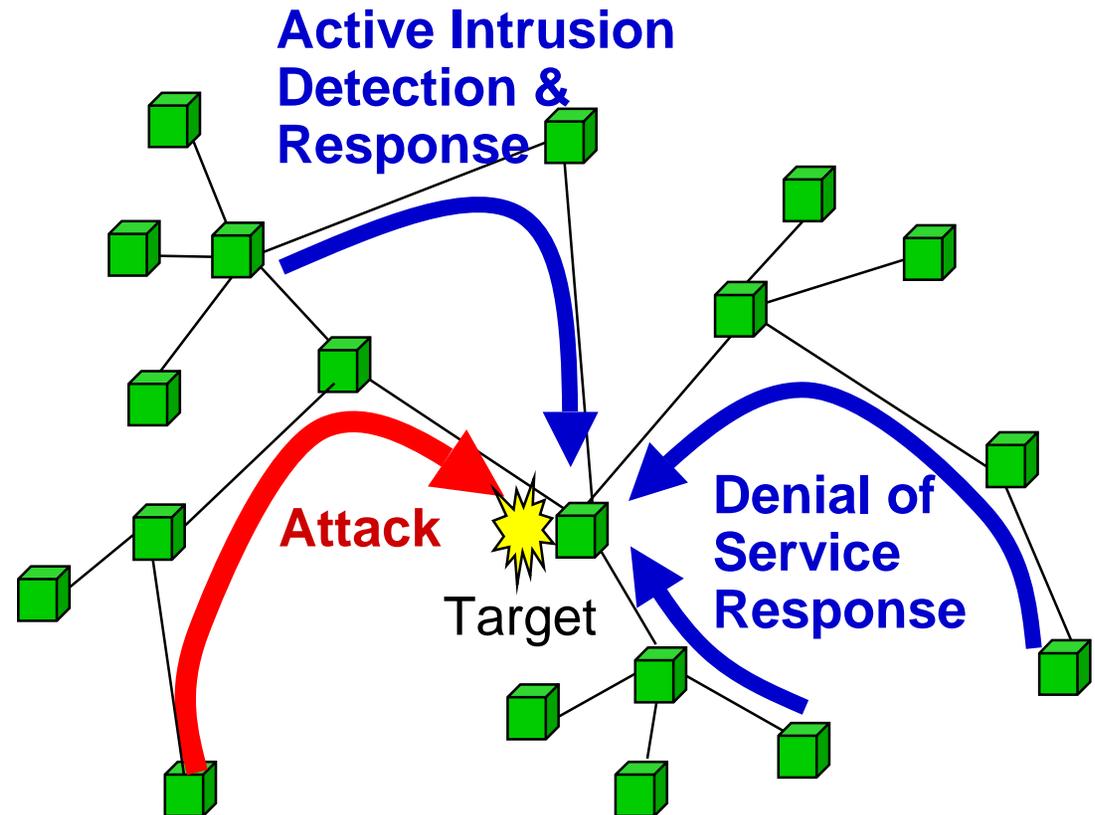
- **Scalable techniques for timely propagation of revocation information (e.g., compromised keys, expired certificates, etc.)**
- **Extend current technologies of cross-certification for rapid coalition deployment capabilities**
- **Secure identification/trust technologies (e.g., credentials)**



Fault Tolerant Networks (FTN)

Goal: Ensure continued network availability in the face of attack while containing attacker resources

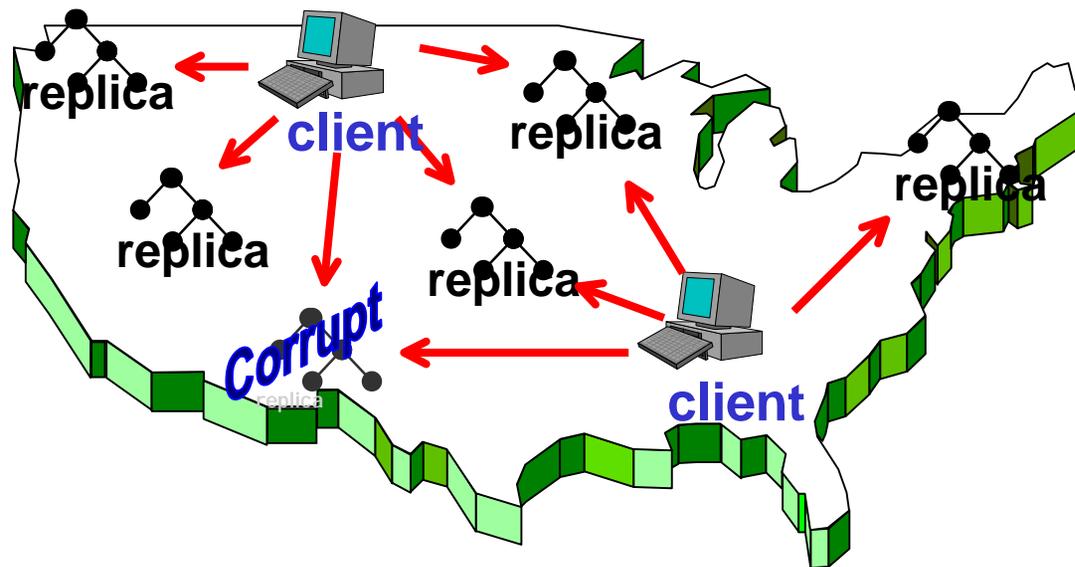
- **Fault-Tolerant Survivability**
- **Denying Denial-of-Service**
- **Active Network Response**





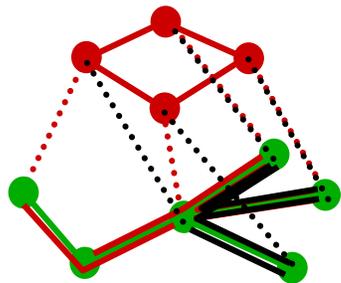
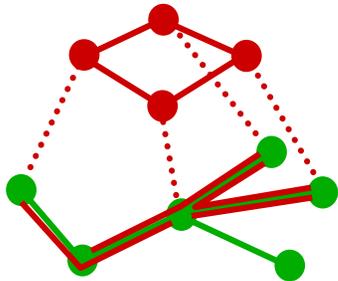
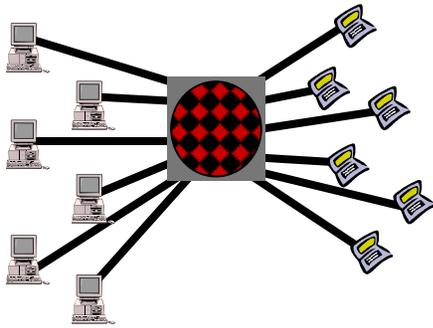
Fault-Tolerant Survivability (FTS)

- Replication and partitioning of network services; Redundancy of network resources
- Better understanding of network fault modeling
- Survivable virtual network overlays
- Create network self-healing capabilities





Denying Denial-of-Service (DDOS)

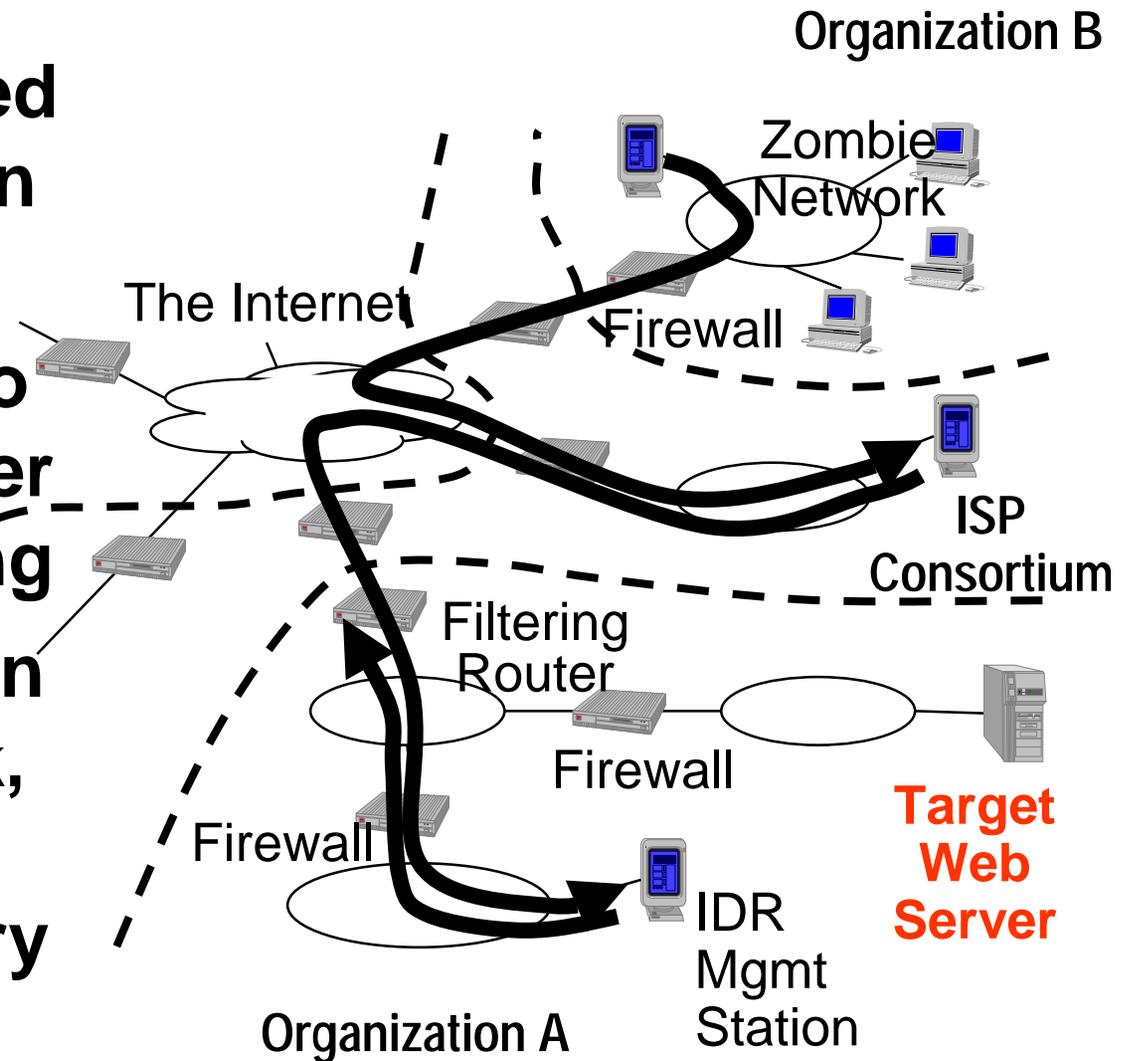


- **Develop market-based resource allocation strategies to limit resource consumption by attacker**
- **New communication protocols that execute based on incremental progress within trust chain**
- **Create accurate mechanisms for reliably attributing DoS attacks**
- **Harden current routing and naming infrastructure protocols against DoS attacks**



Active Network Response (ANR)

- Leverage advanced intrusion detection techniques
- Active networks to assist with attacker tracing and fencing
- Immediate reaction to real-time attack, limiting damage and begin recovery





Survivable Mobile Wireless Networking

Ensure future mobile, wireless networks are resistant to attacks via dynamic and adaptive configuration strategies

- **Develop capabilities for dynamic, survivable wireless network establishment**
- **Leverage wired information assurance solutions**
- **Create survivable key management capabilities to protect against compromise and enable rapid recovery and reconstitution**
- **Develop node adaptation strategies leveraging active networking**

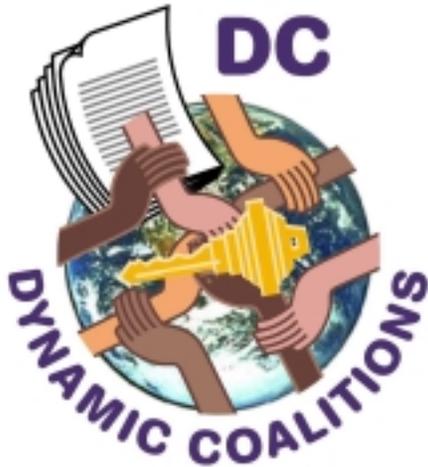


Summary / Conclusion

- **Networking technology is the cornerstone of DoD communication architectures of the future (e.g., JV 2010, JV 2020)**
- **Increasing environments of collaboration require technologies for secure sharing of data and resources**
- **Networks at all levels of command hierarchy must be resistant to attack and “operate through” those attacks which are successful**



Secure Networking



Dr. Douglas Maughan
DARPA / ITO
dmaughan@darpa.mil