

# DARPA Cyber Panel

Vipin Swarup

703-983-7625 • [swarup@mitre.org](mailto:swarup@mitre.org)

DARPA ATO





# Problem

- **Computer network defense (CND) systems possess:**
  - **Sensitive information about networks**
  - **Capabilities to control network elements**
- **CND systems are prime targets for attackers**



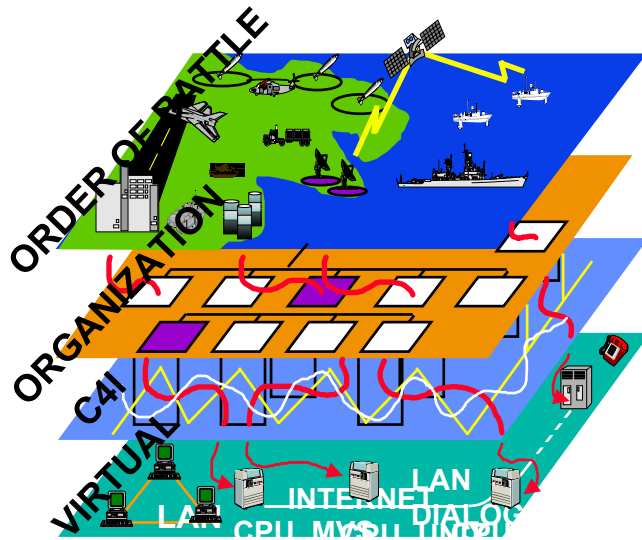
# Background

- **Survivability is the capability of a system to fulfill its mission in a timely manner, even in the presence of stresses**
  - **Stresses include attacks, failures, accidents, and abnormal loads**

# Objective

What Commanders need to know:

- Can I achieve my objective in this cyber environment?
- Will everyone get the orders if I send them now?
- Am I seeing an uncorrupted operational picture?



**DARPA Cyber Panel Objective:**  
Develop technologies that provide  
“big-board” view of system health  
and attack state

**Our Objective:** **Develop principles  
and requirements to enhance the  
survivability of Cyber Panel systems**

What we can tell them:

- Port scan on port 80
- Buffer overflow in sendmail

# Activities



- **Develop framework that applies “Defense-in-Depth” security principle to survivability**
- **Develop catalog of survivability goals and mechanisms**
- **Develop a survivability architecture for the protection and use of a Cyber Panel system**



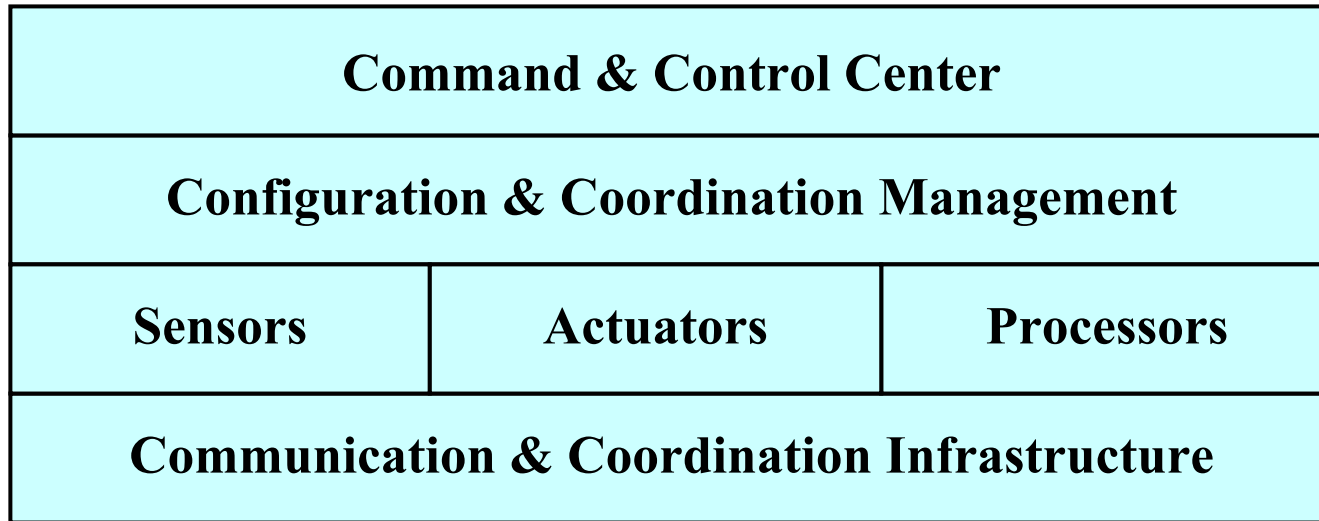
# Highlight



	<b>Stressor (e.g., attacker, war, time)</b>	<b>Stress (e.g., attack, load, accident, age)</b>	<b>Vulnerability (e.g., bug, exposure, fault)</b>	<b>Effect (e.g., failure, corruption, instability)</b>
<b>Prevent</b>	<p><i>Prevent stressors from forming</i></p> <p>Conventional mechanisms are all in the physical world E.g., deterrence</p>	<p><i>Prevent stresses on system</i></p> <p>Preemptive actions (CodeGreen) Deterrence (e.g., traceback) Deception (e.g., honeypots) Stealth (e.g., hide systems) Remote barriers</p>	<p><i>Prevent existence of vulnerabilities</i></p> <p>Security engineering (e.g., patches, firewall rules) Software engineering Adaptivity</p>	<p><i>Prevent effects from occurring</i></p> <p>Security Mask effects Localize effects (sandboxes) Bound effects (diversity)</p>
<b>Detect</b>	<p><i>Detect stressors</i></p> <p>Surveillance Intelligence</p>	<p><i>Detect stresses</i></p> <p>Remote monitoring Detect intrusions (e.g., IDS tools)</p>	<p><i>Detect vulnerabilities</i></p> <p>Scan system (vuln. scanners) Detect stresses (e.g., IDS tools)</p>	<p><i>Detect effects</i></p> <p>Monitor system state Situational awareness</p>
<b>Resist</b>	<p><i>Deter stressor actions</i></p> <p>Deterrence Psychological operations</p>	<p><i>Resist stress and minimize impact on mission</i></p> <p>Block attack paths Adapt defense mechanisms</p>	<p><i>Minimize impact of vulnerability on mission</i></p> <p>Prevent exploitation of vulnerability (e.g., preemptive attacks)</p>	<p><i>Minimize impact of effects on mission</i></p> <p>Predict effect (e.g., worm analysis) Localize effect (e.g., trust mgmt) Bound effect (e.g., diversity)</p>
<b>Tolerate</b>	<p><i>Tolerate stressor with capability to initiate various stresses (some possibly unknown)</i></p> <p>Fine-grained trust models</p>	<p><i>Withstand specific stresses or stress categories</i></p> <p>Intrusion tolerance Modify resource allocations Move functions</p>	<p><i>Sustain mission in presence of vulnerabilities</i></p> <p>Hide existence, location, and details of vulnerabilities (e.g., stealth, deception)</p>	<p><i>Sustain mission in presence of specific effects or classes of effects</i></p> <p>Degrade behavior gracefully Fault/intrusion tolerance Redundancy, dispersion</p>
<b>Recover</b>	<p><i>Recover from actions of a stressor</i></p> <p>Change protection level of defenses</p>	<p><i>Recover from stressed state</i></p> <p>Proactive security (e.g., change network topology)</p>	<p><i>Recover from exploitation of a vulnerability</i></p> <p>Reconfigure system security Alter monitoring characteristics</p>	<p><i>Recover from effects</i></p> <p>Reconfiguration Self-healing (e.g., restart system)</p>



# Highlight/Demonstration



- **Centralized server components**
- **Decentralized sensor, actuator, and processor networks**
- **Communication infrastructure**

# Impacts

- **Systematic foundation for developing survivability requirements and architectures for real-world systems**
- **New technologies needed to make computer network defense systems survivable**



# Future Plans

- Document “defense-in-depth” survivability framework
- Develop survivability requirements framework

