



RDECOM



Cyber Security Research Panel

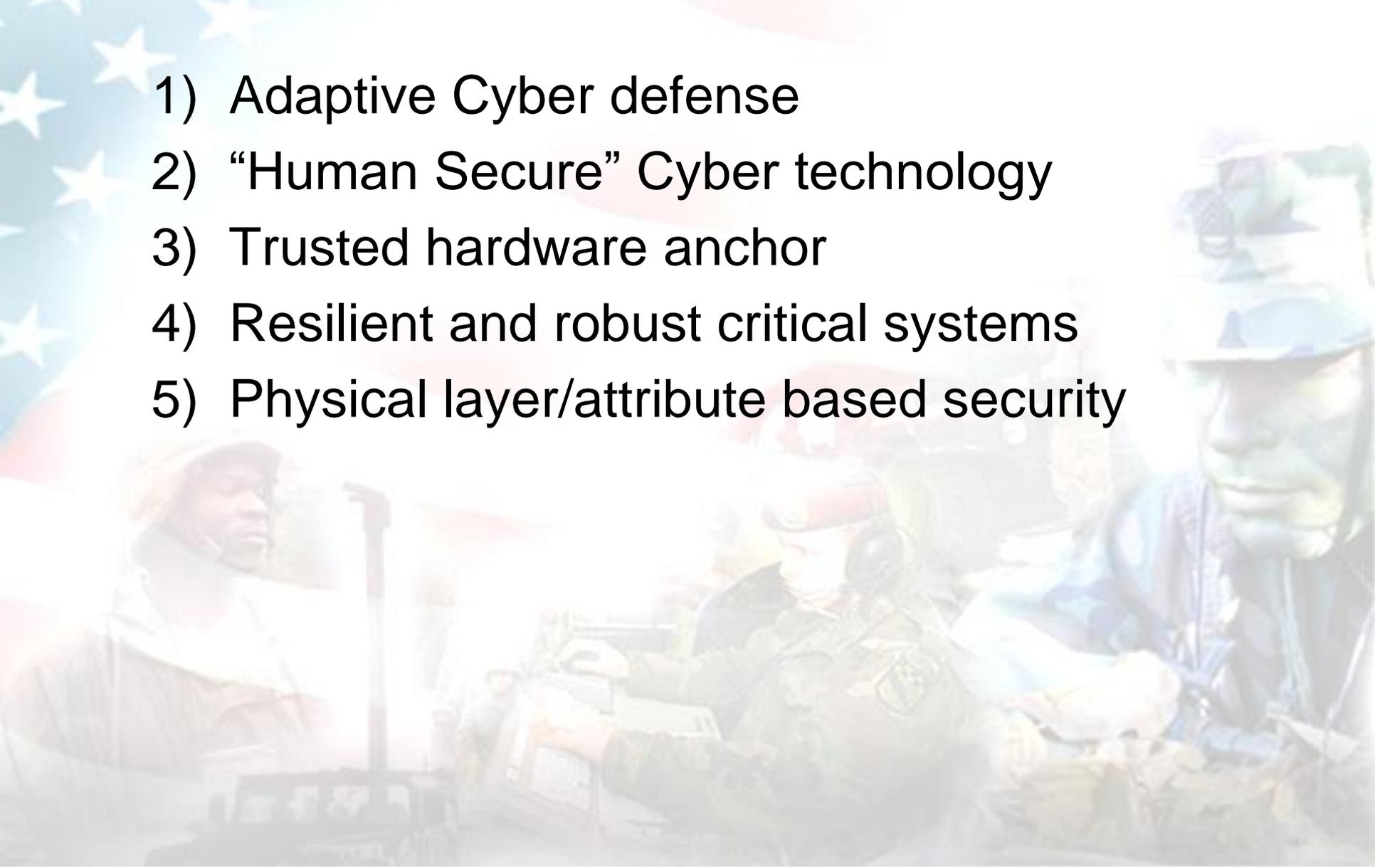


TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

Dr. Cliff Wang
Army Research Office

- 1) Human Behavior is the weakest link
- 2) Asymmetric Cyber Attack/defense
 - Static system vs. dynamic attacks
 - Long term reconnaissance vs. split second attacks
 - Large attack surfaces vs. need one vulnerability to succeed.
 - Large benign traffic vs. hidden attack traffic
- 3) Lack of cyber situation awareness

- 1) Adaptive Cyber defense
- 2) “Human Secure” Cyber technology
- 3) Trusted hardware anchor
- 4) Resilient and robust critical systems
- 5) Physical layer/attribute based security



ARO BAA web site:

<http://www.arl.army.mil/www/default.cfm?page=8>

Funding vehicle:

Single investigator program, MURI, STIR, DURIP etc

Funding process:

Informal white paper->proposal->Peer review->Award

Encourage special Workshop to explore new research thrust

- Adaptive cyber Defense
- Cyber security dynamics
- Hardware assurance
- Cyber Forensics/digital fingerprint
- Trusted Mobile computing and communication

- We leverages SBIR/STTR to make it happen
- Train students both as technology expert and business leaders.
- University should encourage entrepreneurship

