U.S. AIR FORCE

USSF

AFRL

CYBER SURVIVABILITY TECHNICAL SHOWCASE

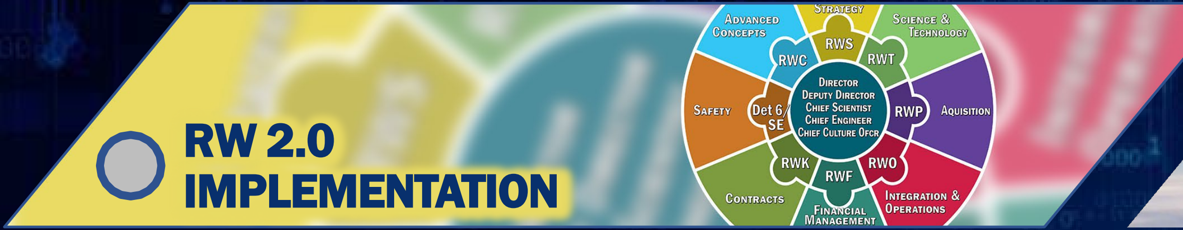
Juanita Riley | DI Technical Showcase

MUNITIONS DIRECTORATE | 30 March 2023

Juanita.Riley.2@us.af.mil

- **Technical Directorate:** One of nine Technology Directorates comprising the Air Force Research Laboratory
- **Location:** Northwest Florida - Eglin Air Force Base
- **Mission:** Discover, develop, integrate, demonstrate, and transition conventional air- launched weapons technologies, enabling the Department of the Air Force to dominate across all domains

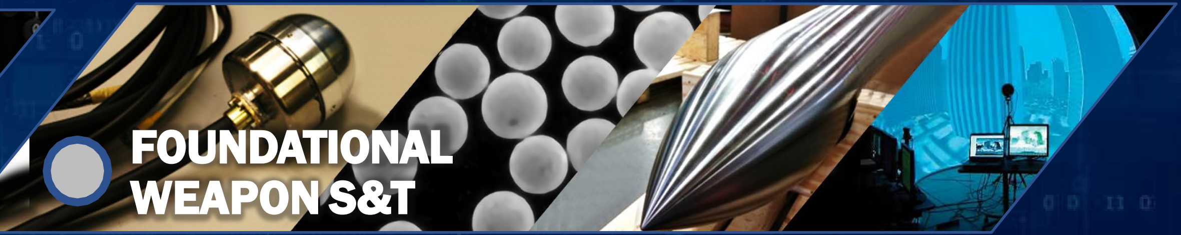
2023 Priority Areas for Munitions Directorate



RW 2.0 IMPLEMENTATION

COUNTERAIR

DIGITAL MATERIEL MANAGEMENT



FOUNDATIONAL WEAPON S&T

NETWORKED, COLLABORATIVE, AUTONOMOUS (NCA) WEAPONS

AIRBASE DEFENSE

COUNTERMARITIME

S&T ENABLERS FOR NDO, SOF, AND SPACE

Cyber Survivability

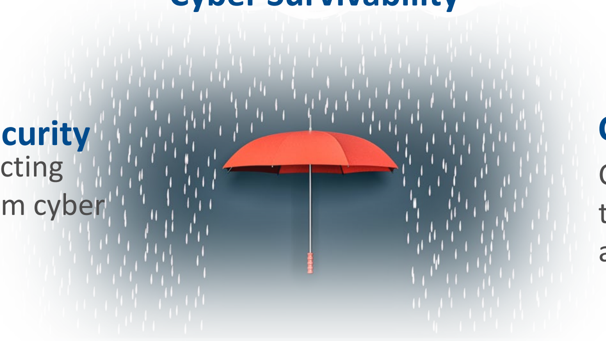
the system's ability to prevent, mitigate, and recover from cyber events

Prevent: The ability to protect critical mission functions from cyber threats.

Mitigate: The ability to detect and respond to cyber-attacks, and assess resilience to survive attacks and complete critical missions and tasks.

Recover: The resilience to recover from cyber-attacks and prepare mission systems for the next fight."

Cyber Survivability



Cybersecurity

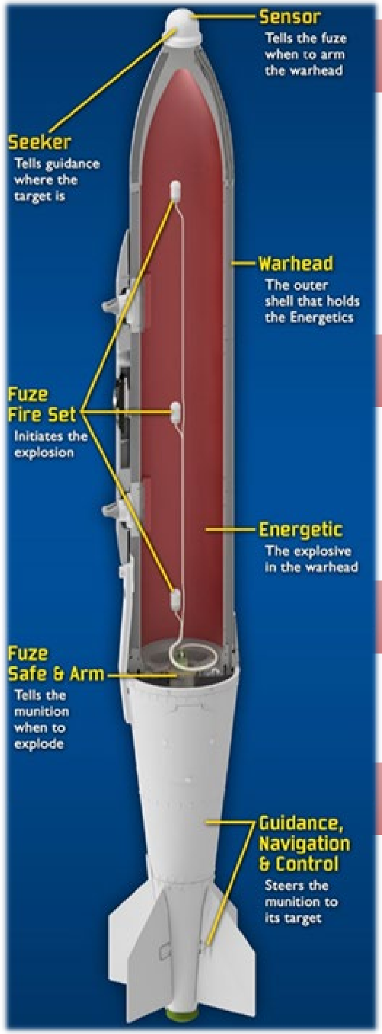
Cybersecurity is the practice of protecting systems, networks, and programs from cyber attacks

Cyber Resilience

Cyber resilience is ability to recover from, in a timely manner, conditions, stresses, cyber attacks, or compromises to a good known state

[1] Conventional cybersecurity can be identified with the baselines in NIST SP 800-53 [11] or with the Framework Core of the Framework for Improving Critical Infrastructure Security (often referred to as the NIST Cybersecurity Framework or NCF [13]). Some of the functionality identified in the exemplar language for the CSAs goes beyond the baselines, e.g., anti-tamper measures identified for CSA 01; [2] Appendix C to Enclosure D of the 2015 JCIDS Manual [5] provides a content guide for the System Survivability KPP, which includes discussion of resilience.

RW Weapon Cyber Areas of Interest


Sensor
Tells the fuze when to arm the warhead
Seeker
Tells guidance where the target is
Warhead
The outer shell that holds the Energetics
Fuze Fire Set
Initiates the explosion
Energetic
The explosive in the warhead
Fuze Safe & Arm
Tells the munition when to explode
Guidance, Navigation & Control
Steers the munition to its target

Assured Autonomy

Achieving secure continual assurance that includes the assurance of safety, trust, and functional correctness of the autonomous system that learns, recognizes, and evolves while its environment changes.

Embedded Systems Assurance

Successful execution of missions through trusted and untrusted components in a secure SW-HW mission stack

Zero Trust

Inherently no internal or external trust for systems

Secure Collaborative Network and Communications

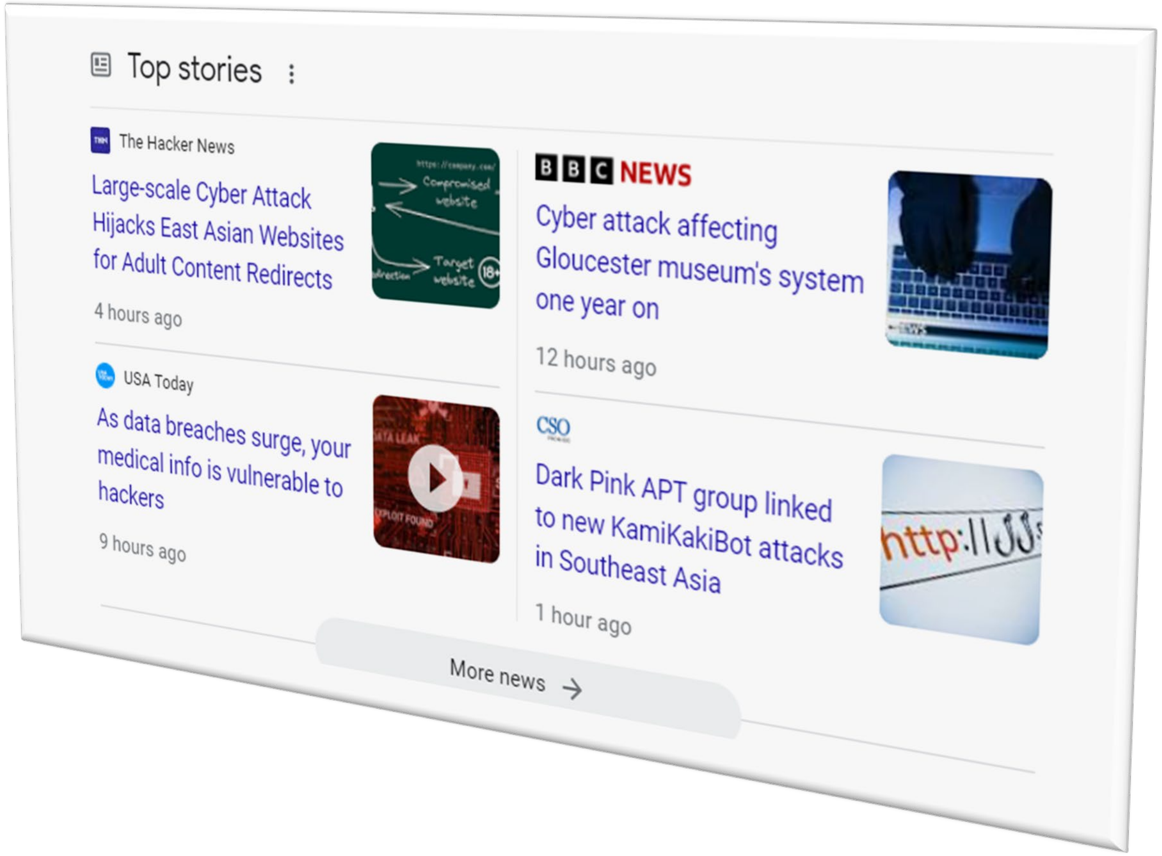
Electronic information sharing capability in which two or more systems can exchange data in a secure environment

- **Cyber Deception**
- **Anti-Fragility**
- **HW/SW Assurance**
- **Open Source & Standard Security**

Common Proposer Challenges

- Risks and New Attack Surfaces
- Early, Often Test and Evaluation
- Integrated Offensive and Defensive Cyber Capabilities
-

KNOW THE SUPPLY CHAIN!



Top stories

The Hacker News

Large-scale Cyber Attack Hijacks East Asian Websites for Adult Content Redirects

4 hours ago

BBC NEWS

Cyber attack affecting Gloucester museum's system one year on

12 hours ago

USA Today

As data breaches surge, your medical info is vulnerable to hackers

9 hours ago

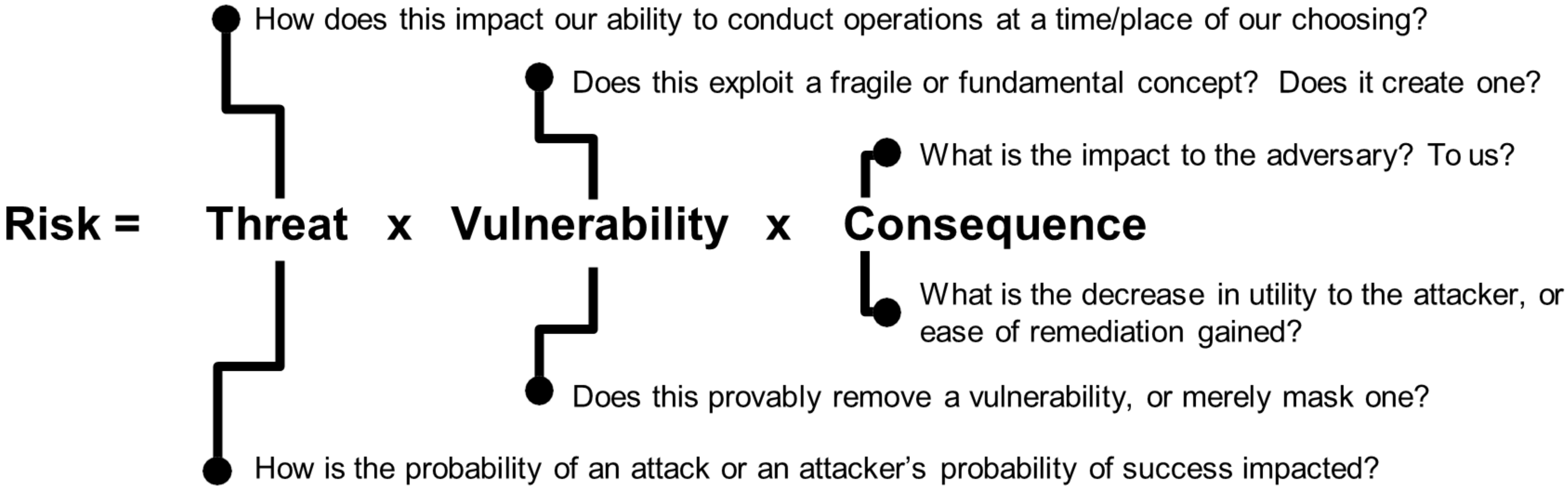
CSO

Dark Pink APT group linked to new KamiKakiBot attacks in Southeast Asia

1 hour ago

More news →

Cyber Principles



How does this impact our ability to conduct operations at a time/place of our choosing?

Does this exploit a fragile or fundamental concept? Does it create one?

What is the impact to the adversary? To us?

Risk = Threat x Vulnerability x Consequence

What is the decrease in utility to the attacker, or ease of remediation gained?

Does this provably remove a vulnerability, or merely mask one?

How is the probability of an attack or an attacker's probability of success impacted?

- **Cyber operations are driven by risk**
- **Context is essential to understanding cyberspace**
- **Evidence is a first principle of cyber research**

Risk in **Context** articulating **Benefit**

Engagements

BROAD AGENCY ANNOUNCEMENT (BAA): FA8651-22-S-0001

- Team Collaborators
  - Chief, Lt. Ford Johnathan
  - Ms. Juanita Riley
  - Ms. Melody Wilkinson
  - Mr. Sookil Lee

QUESTIONS?