

The Army Cyber Institute

The U.S. Army's Cyber Think Tank



19 Sept 2024

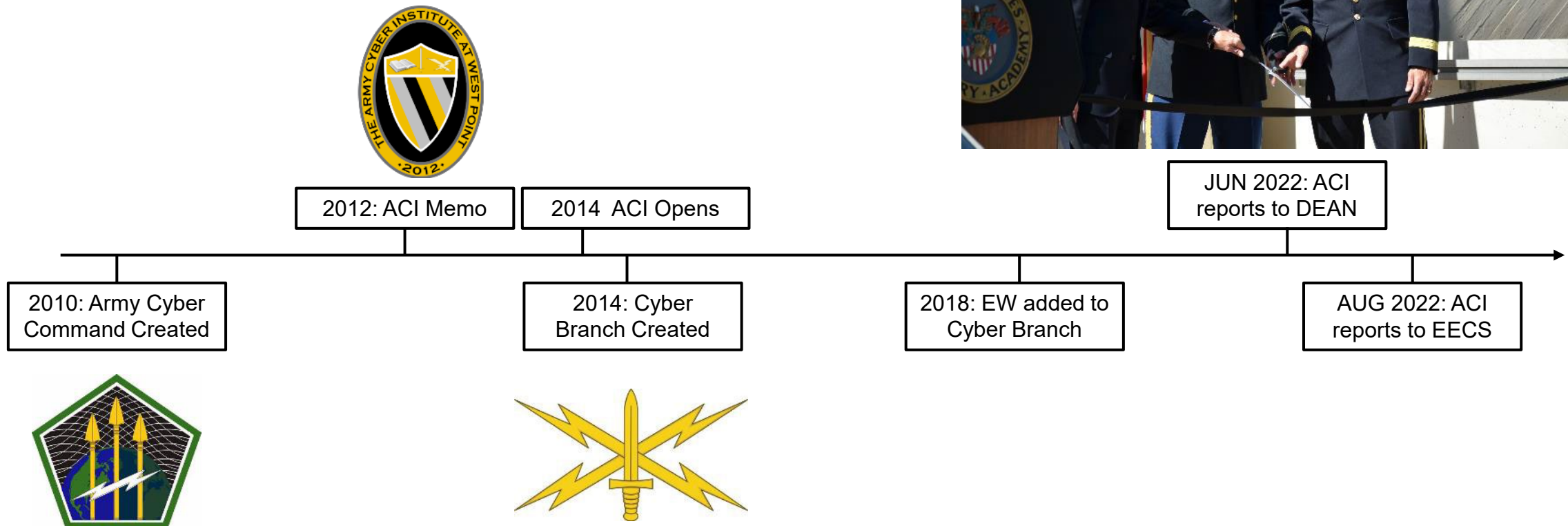
COL Hamilton



- History of the ACI
- Vision and Mission
- ACI's Value Proposition
- Army Cyber Enterprise
- ACI Key Stakeholders
- People of the ACI
- Research Areas
- Recent Highlights



SECARMY 2012 – “Army’s premier resource for strategic insight, advice, and exceptional subject matter expertise on cyberspace-related issues affecting the Army’s operations, organizations, and institutions.”



Vision

The premier independent think-tank that provides indispensable intellectual capital to address the Army's complex cyber problems.

Mission

ACI conducts interdisciplinary advisement, research, and analysis on resourcing, policy, and technologies within the cyberspace domain in support of the Army's strategic objectives.



Secretary of the Army



Chief of Staff of the United States Army



US CYBER COMMAND



ARMY FUTURES COMMAND



ARMY TRAINING & DOCTRINE COMMAND



UNITED STATES MILITARY ACADEMY



PEO IEW&S
PEO EIS
PEO STRI
PEO C3T



Resource & Policy

Professionals in developing, acquiring, fielding, and sustaining the world's best equipment and services



HQDA G3/5/7
DCS G6
HQDA CIO
HQDA PCA



Resource & Policy

Integration & resourcing of Army Cyberspace Operations, Information Operations, Electronic Warfare, & Space capabilities



ARMY CYBER COMMAND



Operations

Integrating Army Networks, Cyberspace Operations, Electronic Warfare, & Information Operations



DEVELOPMENT COMMAND



Science & Technology

Speed of delivery and integrating technology into existing weapon systems



ARMY CYBER CENTER OF EXCELLENCE



Institutional

Trains & Educates / Personnel & Force Modernization Proponent for Signal, Cyber, and Electronic Warfare



ARMY CYBER INSTITUTE



Research & Outreach

Army's Think Tank for Cyberspace Research, working directly with Industry and Academia



HQDA PCA

*Resource &
Policy*



★★★
DAMO-SO

*Resource &
Policy*



★★★★★
**ARMY
CYBER COMMAND**

Operations



★★★
**ARMY CYBER CENTER OF
EXCELLENCE**

Institutional

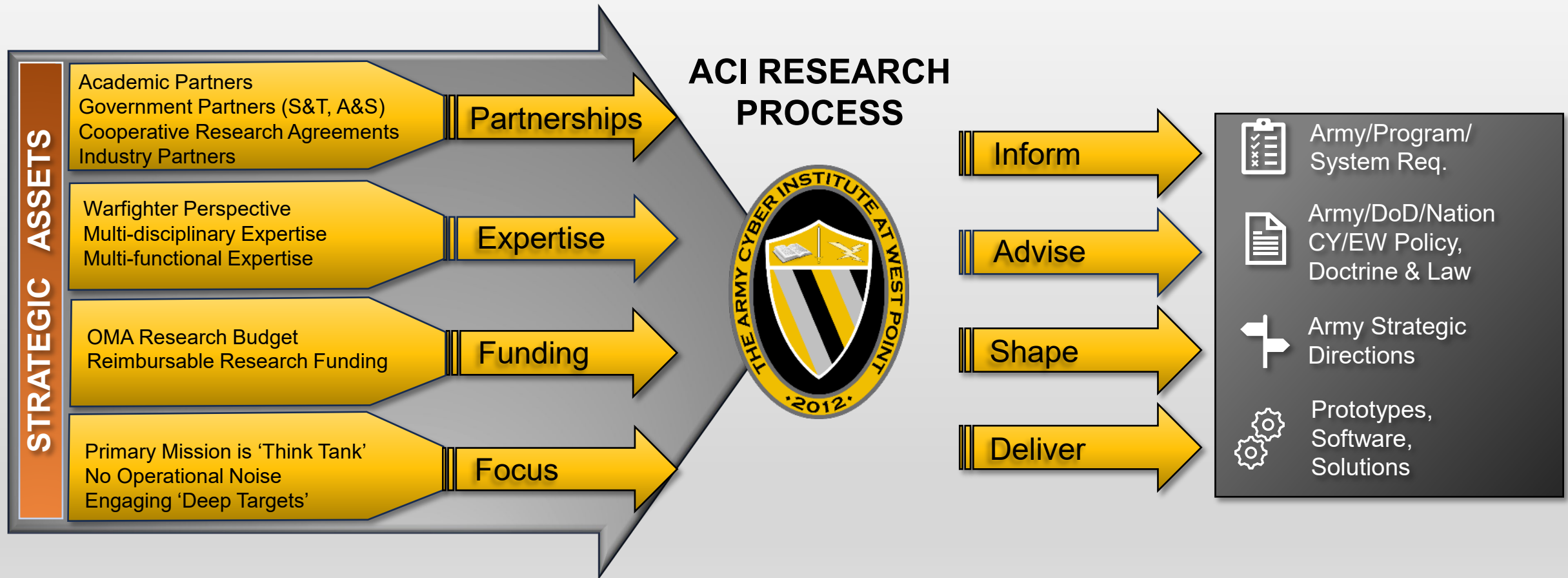
★
CYBER SCHOOL

Professional Military Education



A Unique Value Proposition

Multi-disciplinary and multi-functional research and analysis with a **Warfighter's perspective** that creates strategic value for the Army by providing advice on the **problems of tomorrow**.

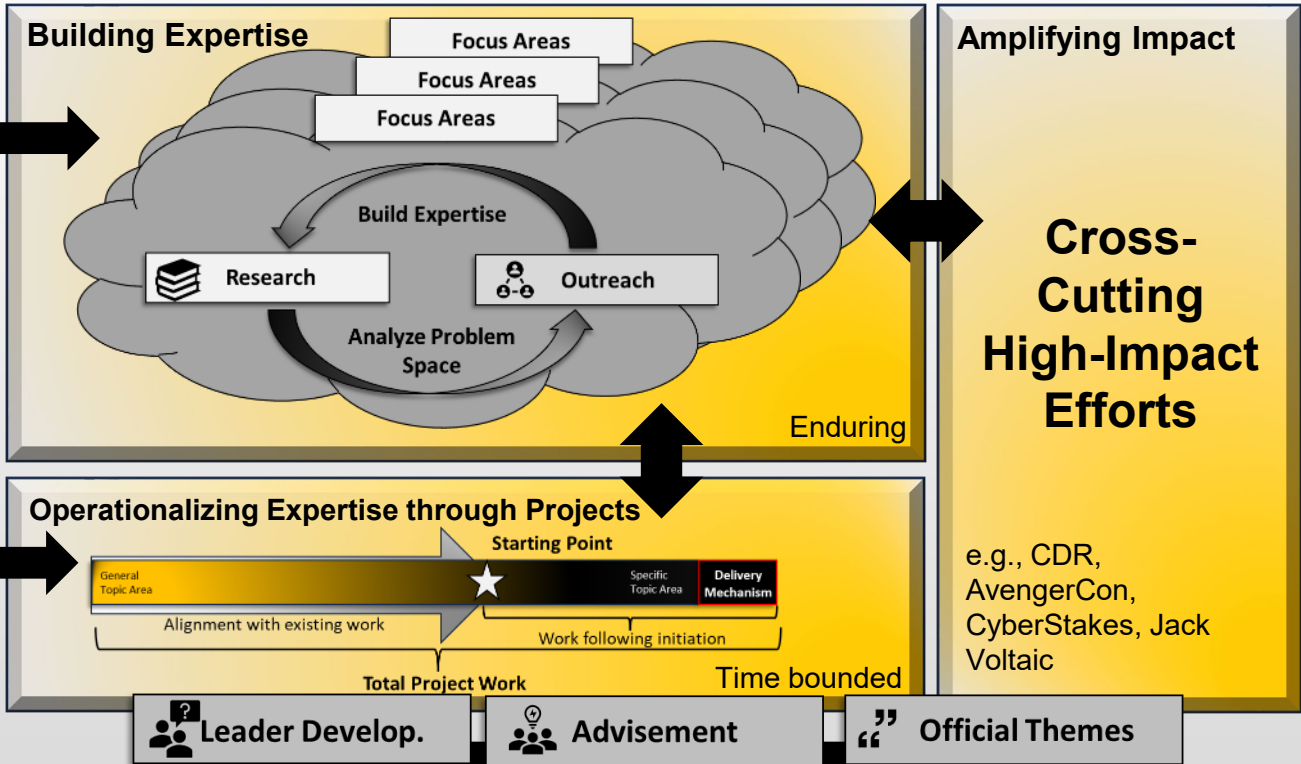


Strategic sharing of research outputs enhancing understanding across the force, elevating tradecraft, and shaping lethality.

Research Strategic Approach

Stakeholder Input
Security Environment Trends
Internal Analysis & Assessments
Partner Constellation Awareness

Focus Areas



Amplifying Impact

Cross-Cutting High-Impact Efforts

e.g., CDR, AvengerCon, CyberStakes, Jack Voltaic

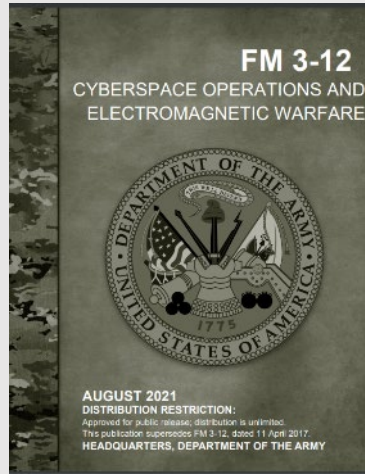
Value to the Army and the Nation

Primary Stakeholders
Other Partners
Advance the Field

Expert Products

ACI conducts research, analysis and outreach focused on areas of forecasted needs and gaps. ACI leverages its expertise and understanding of the problem space to inform specific initiatives through which it delivers value to the Army and the Nation. It primarily delivers value to the primary stakeholders, amplified by select, high-impact ACI efforts.

ACI's Value - Interdisciplinary Research & Analysis



Cyber, Electrical
Engineering, Computer
Science

Policy



A mix of academic disciplinary specialties, Army occupational specialties, and ranks

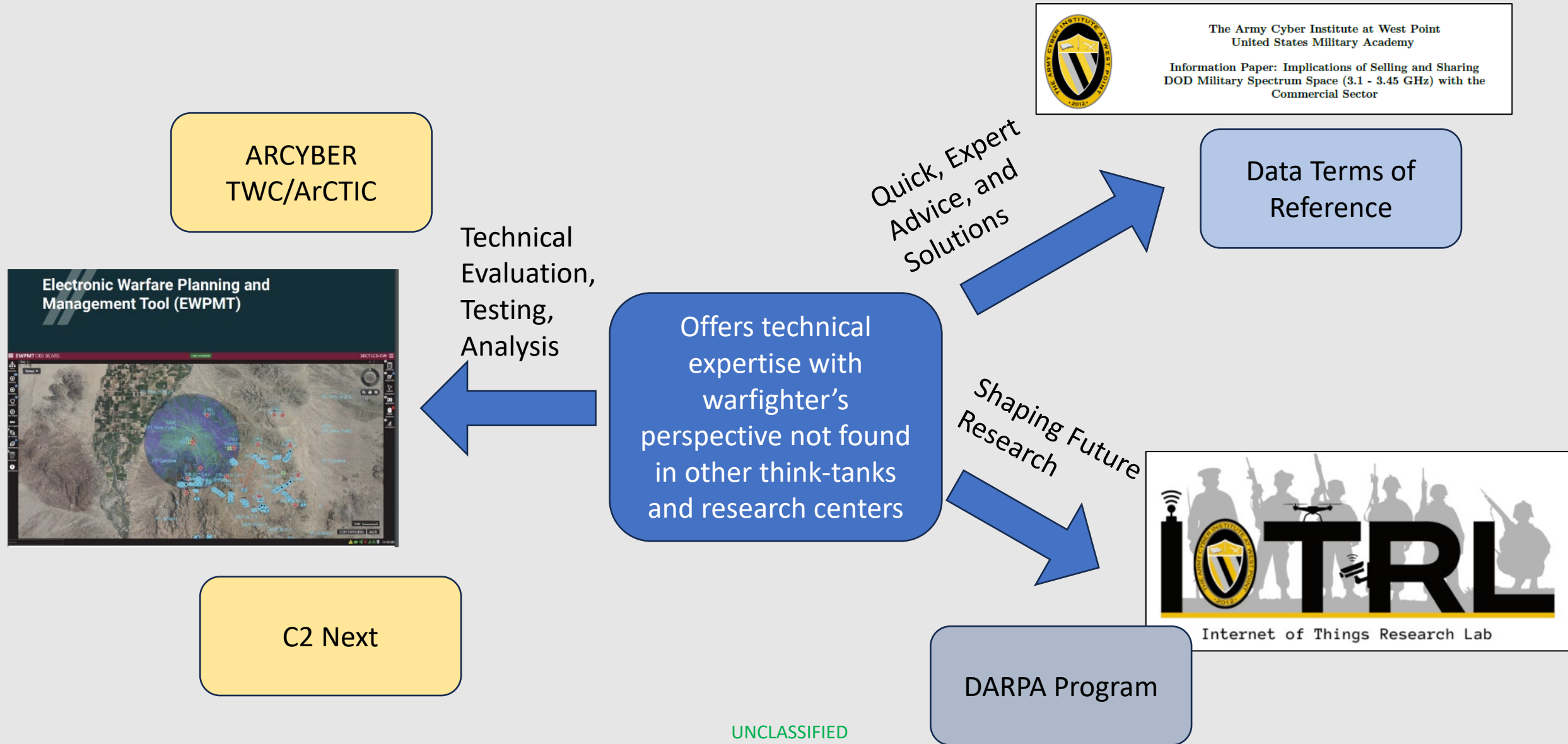
Sociology, Psyops,
Cyber

History,
Policy

Data Brokers and the Sale of
Data on U.S. Military Personnel
Risks to Privacy, Safety, and National Security



ACI's Value – Warfighter's Perspective



ACI's Value - Engaging Deep Targets

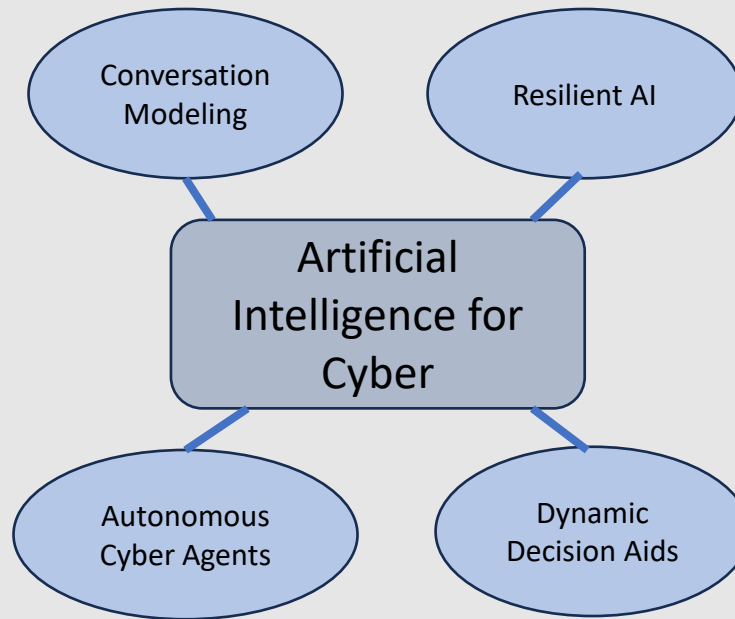
Focused on deep targets that are beyond the capacity of those in the current fight.



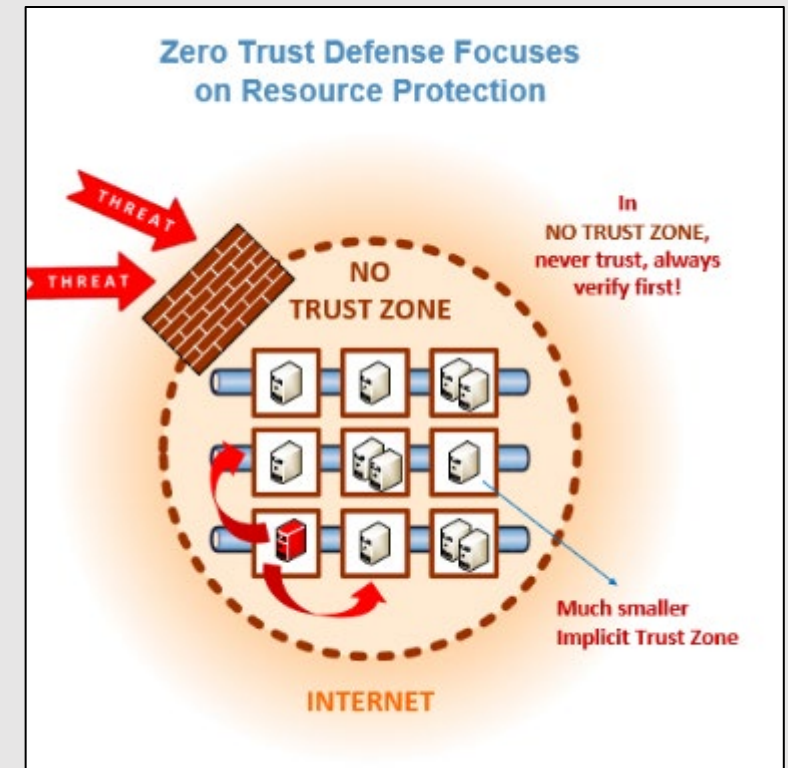
GDIL
Cyber Pacific
Exploring cyber defense laws and policies with Indo-Pacific allies and partners



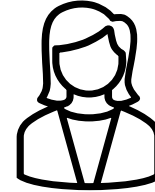
JACK VOLTAIC
CYBER RESEARCH PROJECT
Prepare | Prevent | Respond



UNCLASSIFIED



Who is the ACI?



MILITARY (~30) & CIVILIAN (20)

Academy Professors, Research Faculty, and Research Scientists

MULTI-SPECIALITY



MULTI-DISCIPLINARY

Computer Science, Electrical Engineering, Law, History, Data Science, Cryptography, Cognitive Science, Sociology

ACROSS RANKS



PROFESSIONAL SUPPORT STAFF



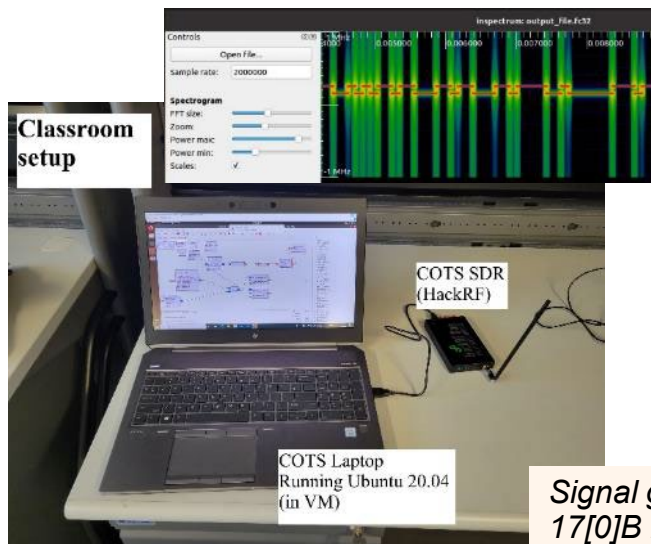
Digital Force Protection

Produces and integrates research at the intersection of technology and society. Pursues policy and technological solutions to problems involving operations security, force protection, and commercial data.

- Privacy-enhancing technology
- Commercial data and PAI, and their implications for national security
- Mis/Disinformation, narratives, and social media
- Warfighter assessment support (Pacific Sentry, Avenger Triad)



*"Powerful Narratives"
Threatcasting Report on
China's Potential Rise to
Global Primacy*



*Signal generator for
17[0]B EW
Qualification Course*

Cyber Operations – Research & Engineering

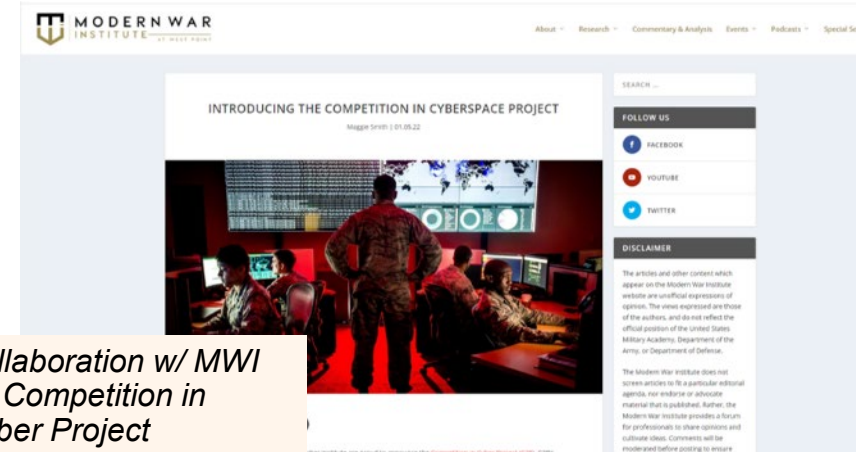
Provide research, development and advisement to yet unserved portions of the Army in the development of their organic cyber operations capability.

- Electronic Warfare Kit and & Combined Arms Training Center Support
- Clone Code Detection (finding vulnerabilities like log4j)
- Electromagnetic Warfare Professional Military Education Course Advisement

Law, Policy, & Strategy

Focus on providing legal, policy, and ethical frameworks that guide and assist cyber operators in carrying out their missions.

- Support to OSD for DoD Cyber Strategy
- Professional Military Education review and update to Marshall Center and SAMS
- Cyber Pacific Research with UT-Austin



Government and industry partners

UNCLASSIFIED

Data and Decision Sciences

Develop and apply computational, mathematical, statistical, and cognitive methods, algorithms, software, and decision-support tools to analyze large and heterogeneous collections of data to generate actionable insights that enable decision advantage and information dominance.

- Internet of Battlefield Things (IoBT), Generative Methods for Cyber (GM4C), and Autonomous Cyber (AuCyber)
- Intelligent Cyber-Systems and Analytics Research Lab
- Advisement to AFC, DARPA, JAIC, DoD CDO, OUSD(R&E)

JACKVOLTATIC

CYBER RESEARCH PROJECT

Prepare | Prevent | Respond

a repeatable and scalable framework

Increase communication

Improve information sharing and response coordination

- Self-assessment
 - Minimal cost/maximum impact
 - Increased frequency
 - Progress tracking
- Inter-dependency Analysis
 - Insight into partner readiness through cooperative exercise planning
 - Planning assumption gap identification
- Decision Support
 - Help prioritize resource allocation based on exercise results
 - Inform planning assumptions



Events

2016 – New York City
(JV 1.0)

2018 – Houston (JV 2.0)

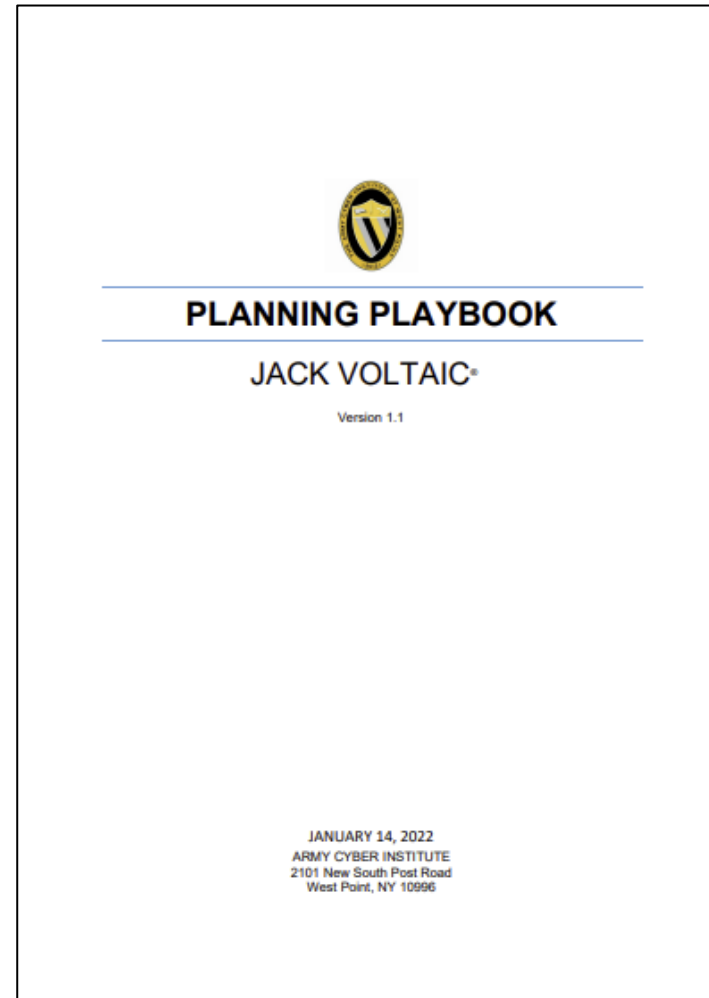
2019 – Workshops in 6 cities
(JV 2.5)

2020 – Savannah and
Charleston (JV 3.0)

2021 – Citadel

2022 – Georgia Cyber Center

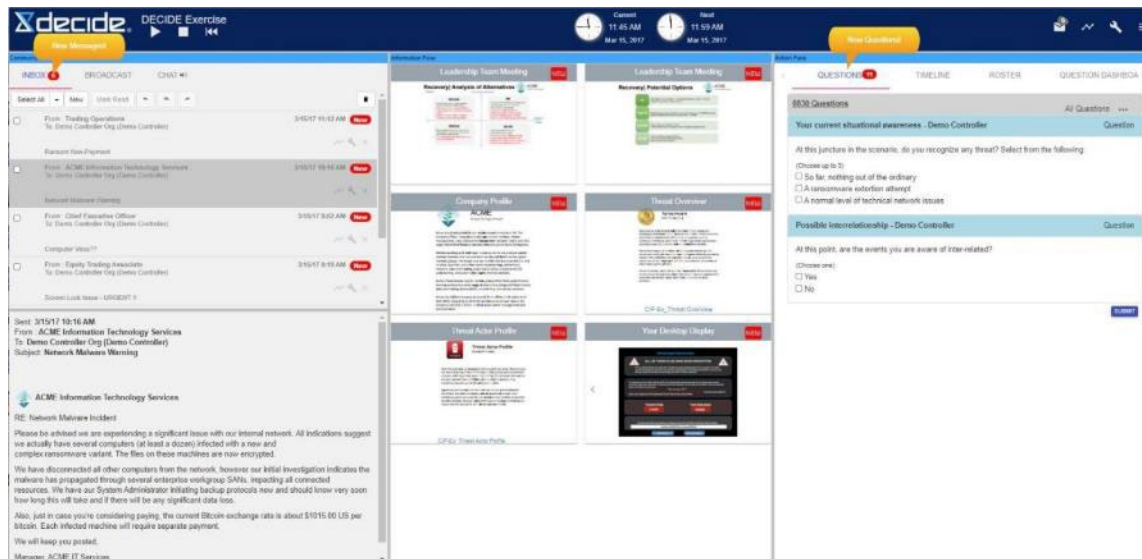
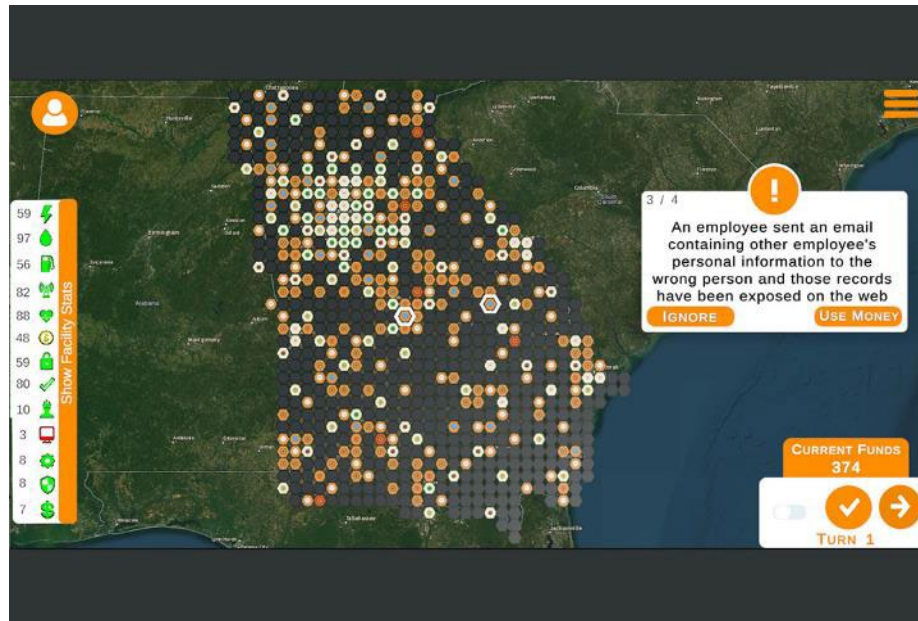
2023 – AFCEA Atlanta



<https://cyber.army.mil/Research/Jack-Voltaic/>

On-going Projects

- NUARI *DECIDE* Platform extensions (1-year)
- RIT gamification grant (2-year)
- Indiana Univ. educational techniques grant (2-year)
- SherpaWerx CIKR Critical Infrastructure Community Building grant (1-year)
- Stanford Univ. legal and policy issues for CIKR grant (2-year)
- WinkStink contract for informational videos (1-year)



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY  **AMERICA'S CYBER DEFENSE AGENCY**

Search

Topics ▾ Spotlight Resources & Tools ▾ News & Events ▾ Careers ▾ About ▾

[Home](#) / [Resources & Tools](#) / [Services](#)

SERVICE

CISA Tabletop Exercise Packages

Tools for stakeholders to conduct planning exercises on a wide range of threat scenarios.

Task type: Increase your resilience **Readiness Level:** Foundational

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#), [MULTIFACTOR AUTHENTICATION](#), [CYBER THREATS AND ADVISORIES](#)

GAO Highlights

February 2023

CRITICAL INFRASTRUCTURE PROTECTION

Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities

Highlights of [GAO-23-105806](#), a report to congressional committees

Why GAO Did This Study

Critical infrastructure provides essential functions—such as supplying water, generating energy, and producing food—that underpin American society. Disruption or destruction of the nation's critical infrastructure could have debilitating effects. CISA is the national coordinator for infrastructure protection.


The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 includes a provision for GAO to report on the effectiveness of sector risk management agencies in carrying out responsibilities set forth in the act. This report addresses (1) how the act changed agencies' responsibilities, and the actions agencies have reported taking to address them; and (2) the extent to which CISA has identified and undertaken efforts to help agencies implement their responsibilities set forth in the act.

GAO analyzed the act and relevant policy directives, collected written responses from all 16 sectors using a


What GAO Found

GAO found that the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 expanded and added responsibilities for sector risk management agencies. These agencies engage with their public and private sector partners to promote security and resilience within their designated critical infrastructure sectors. Some officials from these agencies described new activities to address the responsibilities set forth in the act, and many reported having already conducted related activities. For example, the act added risk assessment and emergency preparedness as responsibilities not previously included in a key directive for sector risk management agencies. New activities officials described to address these responsibilities included developing a risk analysis capability and updating emergency preparedness products.

The 16 Critical Infrastructure Sectors



Source: GAO analysis of Presidential Policy Directive-21 | GAO-23-105806

 **U.S. Department of Defense**
Office of Local Defense
Community Cooperation

Association of Defense Communities Defense Communities National Summit

Office of Local Defense Community Cooperation Town Hall
March 7, 2023

Presented By:
Patrick J. O'Brien
Director

About NICCS Become a Training Provider Cybersecurity News & Events Subscribe to our Newsletter

NICCS™

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

Education & Training Workforce Development Cybersecurity & Career Resources

Education & Training > NICCS Education & Training Catalog > DRI International > Cyber Resilience for the Business Continuity Professional

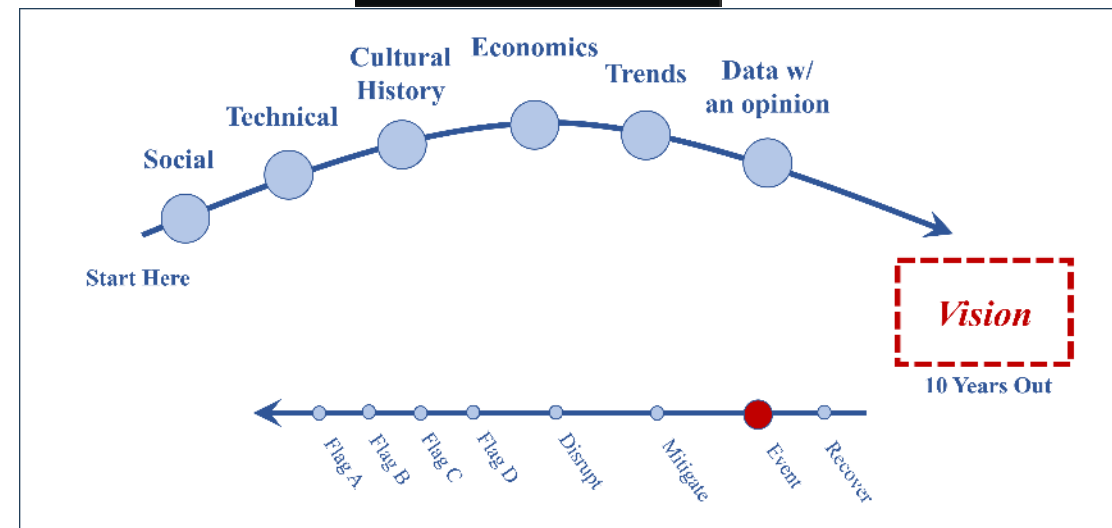
Cyber Resilience for the Business Continuity Professional

Online, Instructor-Led

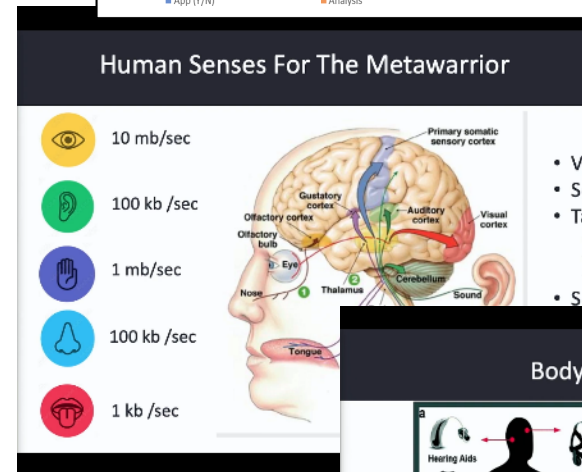
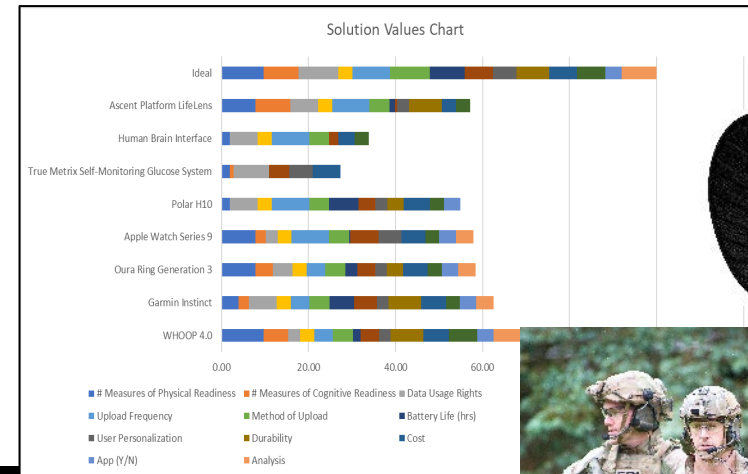
Organizations today are confronted by a wide range of cyberattacks, and your organization is no exception. There are countless opportunities for hackers to cause massive disruptions, all of which will require a response that will involve you. That's why this course is an absolute must. More than just another statement of the problem, Cyber Resilience for the Business Continuity Professional provides a comprehensive, practical, and actionable framework for developing and implementing a robust cyber resilience strategy.

More courses from this provider:
[DRI International](#)
Contact Information
[DRI International](#)

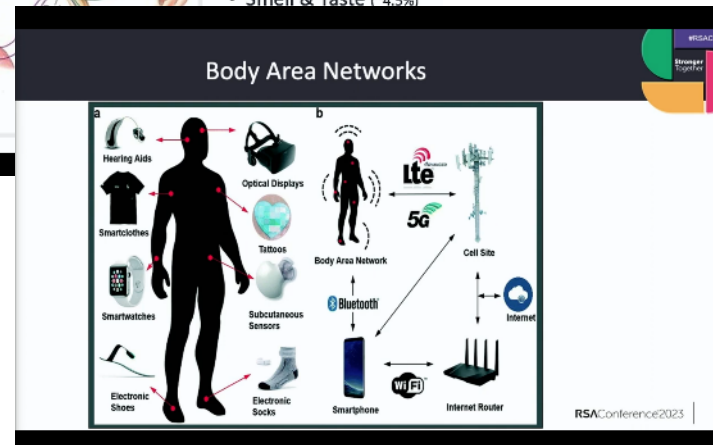
- **Threatcasting** is a systematic examination of what can go *wrong* in the future → and what to do about it
- Topics:
 - Information warfare,
 - Cyber enabled financial crimes (USSS),
 - WMDs,
 - Extremism
- So What? FBI (OTD) has asked for assistance to learn the method and collaborate
- <https://cyber.army.mil/Work-Areas/Threatcasting/>



- Objective: Identify how **decision making** is affected by connected devices
- Clients: OTD, IT Branch, HRT
- Primary Use Cases: **Purposeful study** of emerging tech (threatcasting): Wearable health devices, medical devices
- Future: User interfaces, cognitive deception, smart clothing, brain interface tech
- So What?: Cybersecurity concerns, data & privacy concerns; How to measure “readiness” and “influence”?



- Vis
- Sou
- Tac
-
- Hot/Cold
- Smell & Taste (~4.5%)





4-5 Apr 24
West Point,
NY

Founded in 2015, JSAC's mission has remained consistent: strengthen industry and government collaboration to defend against current and future cyber threats by leveraging the unique communities of the service academies.

Key Speakers and Panels:

- GEN Haugh
- John J. Garstka (OUSD)
- Morgan Adamski (NSA)
- Service PCA/Govt Panel
- Cyber Threat Sharing and Attack Surface Management Panel

Audience:

- Cadets (USMA, USAFA, USCGA)
- Senior Govt and Military Leaders
- Service Academy Graduate Industry Leaders



Questions & Discussion



Army Cyber Institute

<https://cyber.army.mil/>



Cyber Defense Review

<https://cyberdefensereview.army.mil/>



@ARMYCYBERINSTITUTE



@ARMYCYBERINST



@THEARMYCYBERINSTITUTE