DoD Cyber Technologies and Opportunities

ACSAC National Cybersecurity Research Directions Panel

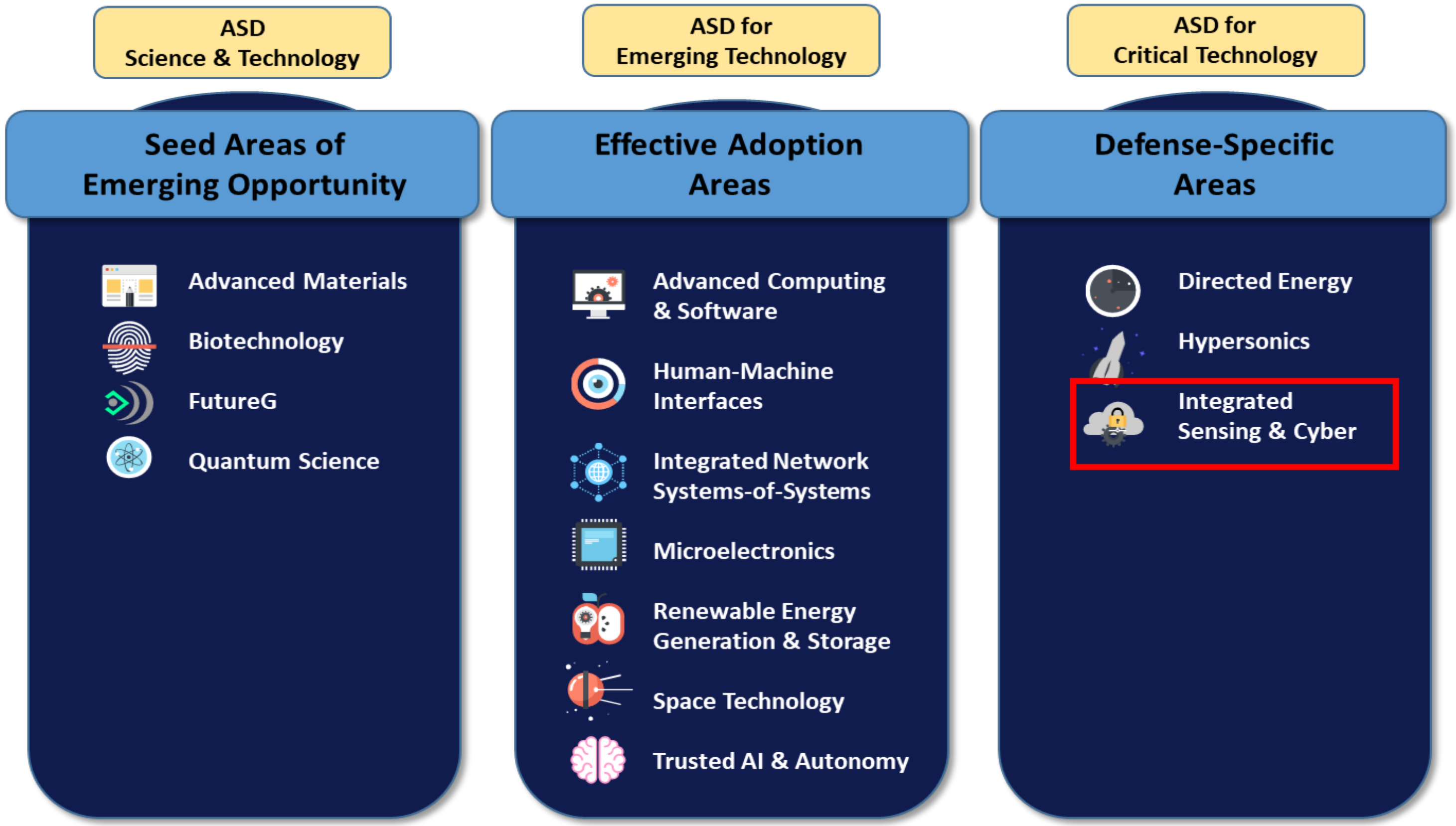
Chester “CJ” Maciag
Director, Cyber Technologies and Academic Outreach

ASD(CT), Integrated Sensing and Cyber
Office of the Undersecretary of Defense for Research and Engineering

DoD Capability and Technology Demand Signals

Defense-Wide Capabilities/Technology

- National Defense Authorization Act
- National Security Strategy
- National Defense Strategy
- SECDEF Memos
- USD(R&E) Direction
  - 14 Critical Technology Areas



ASD Science & Technology

Seed Areas of Emerging Opportunity

- Advanced Materials
- Biotechnology
- FutureG
- Quantum Science

ASD for Emerging Technology

Effective Adoption Areas

- Advanced Computing & Software
- Human-Machine Interfaces
- Integrated Network Systems-of-Systems
- Microelectronics
- Renewable Energy Generation & Storage
- Space Technology
- Trusted AI & Autonomy

ASD for Critical Technology

Defense-Specific Areas

- Directed Energy
- Hypersonics
- Integrated Sensing & Cyber

Integrated Sensing and Cyber

- National Cyber Strategy
- DoD Cyber Strategy
- CYBERCOM Command Challenges
- Section 1510 Non-Kinetic Force Development Plan

IS&C Strategic Vision

- Vision
  - Integration of platforms, sensors, and effects at the speed and scale of relevance
  - Sense, understand, react, and shape operations in the information environment (OIE) encountered by the joint force in highly contested environments

- Cyber - Major Focus Areas
  - Protect and innovate
  - See the battlespace
  - Support rapid decision making
  - Operations in the information environment

Approved for Public Release

Global Trends on Cyber S&T

Major Themes	Consequences (for both defense and offense)	Effect on S&T Strategy
TIMELINES SHRINKING	• ***Humans cannot fight at cyber speed without the right tools*** • Interactive ops are obsolete	• Emphasize mission assurance through trust and resilience over "monitor and react" • Use autonomy to extend reach of workforce
COMPLEXITY INCREASING	• Takes us further away from establishing and maintaining trust in our systems • Adds uncertainty, exacerbates security • Untrustworthy ecosystem (supply chain)	• Emphasize importance of trustworthy, automated tools and educated workforce • "Lone hacker" → "Experts with elite tools" • Manage complexity in blue systems
LANDSCAPES RAPIDLY CHANGING	• Constantly redefining battleground via new C4ISR technologies (e.g. 5G/6G, SDN, IoT, Autonomous Platforms, etc.). → New vulnerabilities surface all the time	• Proactively analyze emerging technologies • Continue to invest in broadly applicable tools to be able to rapidly adapt to new technologies and nation state adversaries
DOMAINS CONVERGING	• A tactical platform's attack surface extends out through all its apertures • Multi-domain stovepipes must end, need to use cyber to shape and deter conflict	• Study multi-domain interfaces, find 1+1>2 • Integration of SA / data streams, C2 for all-domain Information Operations (IO)

DoD Cyber S&T is the crucial enabler that ties together all-domain warfighting

Potential S&T Directions

- Tightly-coupled, mutually learning human-machine teams for cyber defense/offense
- Scalable formal methods and resilient architectures, modularity and composability
- Maneuver the cyber attack surface, orchestration of multiple simultaneous functions
- ML/AI for greater automation in cyber problems (tools-centric, human-assisted) Especially useful in expanding the "range of practicality" on Cyber's many undecidable problems
  - Program analysis, reverse engineering, and vulnerability discovery
  - Design and characterization of cyber effects
  - Characterizing attack-defense cycles
- Designed-in simplicity and minimalism: SW, FW, protocols, and architecture
  - Stretch goal: every line of code in memory should be contributing to the mission
- Self-aware and self-correcting SW, FW, and protocols
- Roles of next-gen computing and communications technologies in cyber operations (6G, new microelectronics architectures, autonomous platforms and complex sensors, brain-machine/brain-brain communications, etc.)
- Broad spectrum of coordinated cyber obfuscation and deception technologies
- Ubiquitous sensors feeding integrated Cyber-EW-Kinetic operations
- Seamlessly leverage all-domains in operations to create digital effects (esp. Cyber-EW)

<u>Helps us deal with:</u>

TIMELINES SHRINKING

COMPLEXITY INCREASING

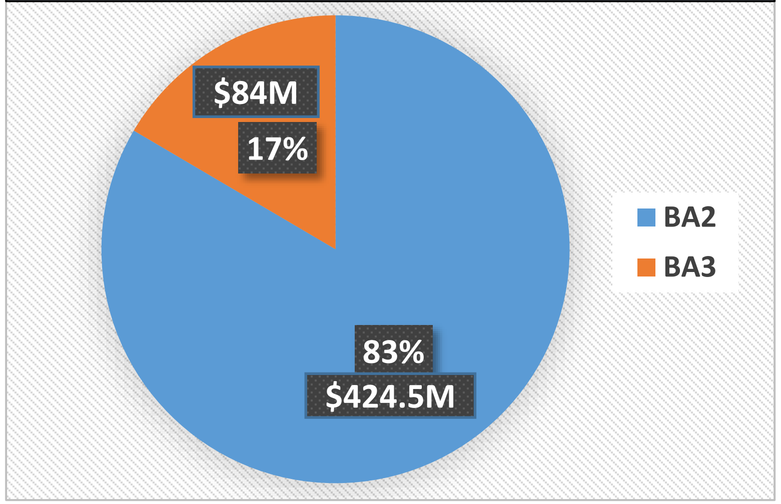
LANDSCAPES RAPIDLY CHANGING

DOMAINS CONVERGING

Approved for Public Release

Typical (Past) Cyber Budget and Performer Base

PB20: BY BUDGET ACTIVITY

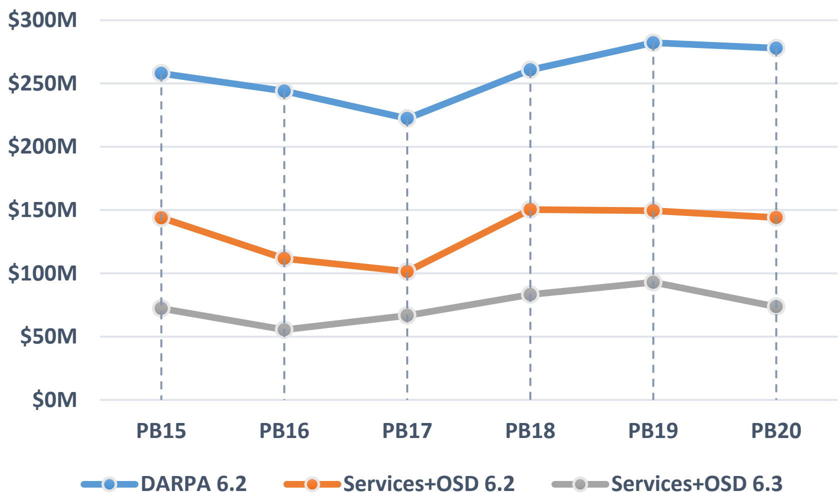


PERFORMERS FOR DOD CYBER S&T

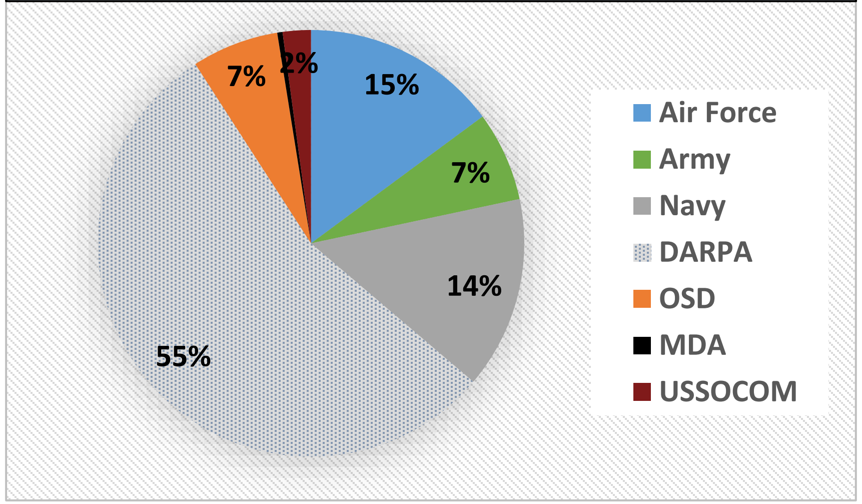
- Services & Agencies S&T Labs: AFRL, NRL, Warfare/Systems Centers, NSA/R, CCDC , MDA
- DOE Labs, FFRDCs, & UARCs
- Academia
- Industry Players
  - Defense Industrial Base
  - Non-traditional
  - Small Companies with Key Expertise & Products
- About 80% Extramural

HISTORICAL TRENDS

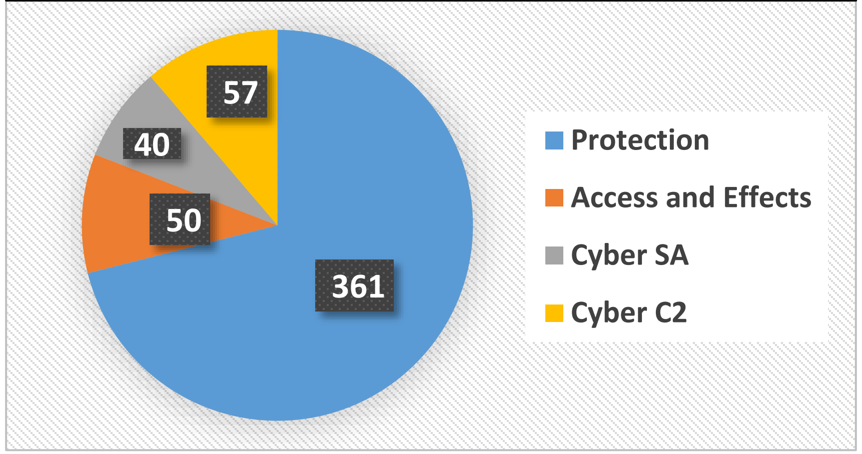
(IN THEN-YEAR DOLLARS)



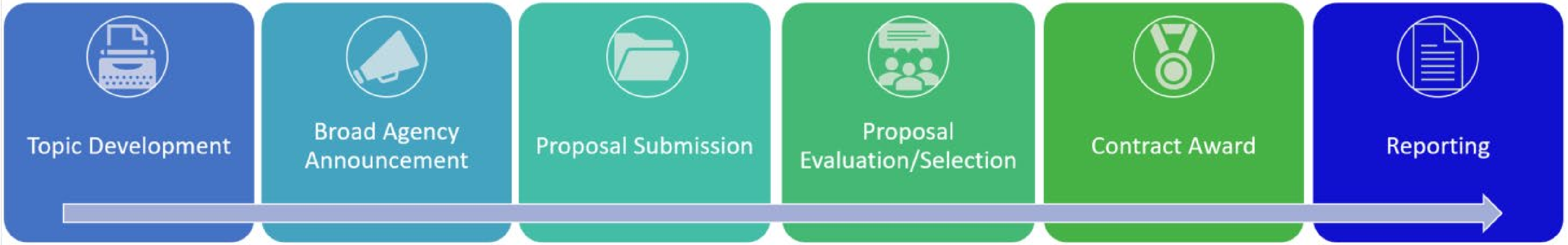
PB20: BY SERVICE / AGENCY (of $508.5M)



PB20: BY TIER 1 TAXONOMY AREA



Industry Engagement: DoD SBIR/STTR Process and Components



- Department of the Army
- Department of the Navy
- Department of the Air Force
- Defense Advanced Research Projects Agency
- Defense Health Agency
- Defense Logistics Agency
- Defense Microelectronics Activity
- Defense Threat Reduction Agency
- Chemical and Biological Defense
- Missile Defense Agency
- National Geospatial-Intelligence Agency
- Office of Secretary of Defense
- Space Development Agency
- United States Special Operations Command

USD(R&E) Technology Vision for an Era of Competition

Succeed through Teamwork: Maximize our asymmetric advantages by partnering with the larger innovation ecosystem, from industry to universities and to laboratories, allies and partners.

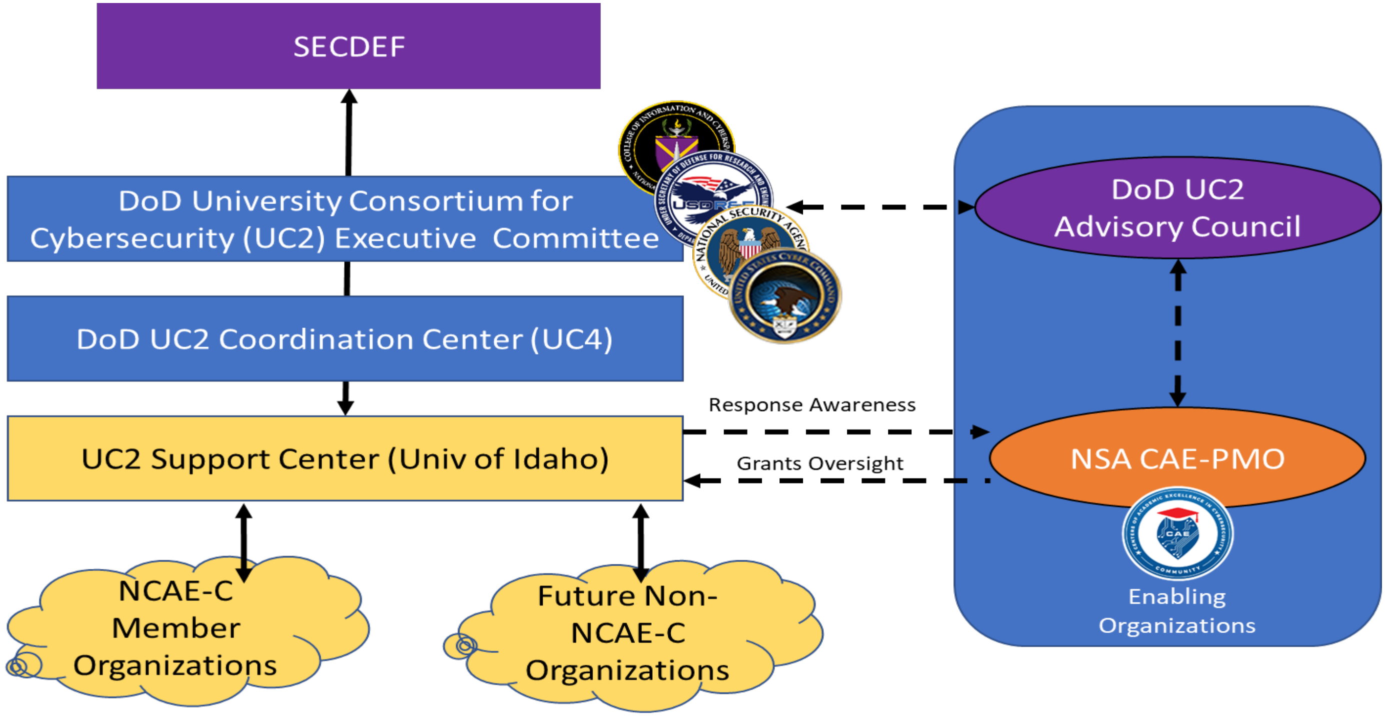
Approved for Public Release

DoD University Consortium for Cybersecurity (UC2)

https://cic.ndu.edu/UC2/Work-With-Us/

Mission: Establish a consortium of universities to assist the Secretary of Defense on cybersecurity matters

- **Advise the Secretary on the needs of academic institutions** related to cybersecurity and research conducted on behalf of the Department
- **Serve as focal point for closer collaboration between academia and the Department of Defense (DoD)** on cybersecurity matters
- **Provide SECDEF timely access to the expertise of the institutions** of the consortia on matters relating to cybersecurity
- **Align support efforts of consortia members** in support of DoD


SECDEF
DoD University Consortium for Cybersecurity (UC2) Executive Committee
DoD UC2 Coordination Center (UC4)
UC2 Support Center (Univ of Idaho)
NCAE-C Member Organizations
Future Non-NCAE-C Organizations
DoD UC2 Advisory Council
Response Awareness
Grants Oversight
NSA CAE-PMO
Enabling Organizations

Accomplishments

- Three RFIs released covering 5 priority DoD topics
- 24 responses from academia // 8 invited presentations
- Webcast and follow-up matchmaking discussions

Work with DoD - Helpful Websites

- Defense SBIR/STTR Innovation Portal (DSIP) - https://www.dodsbirsttr.mil/submissions
- DoD SBIR/STTR - https://rt.cto.mil/rtl-small-business-resources/sbir-sttr/
- Federally Funded Research and Development Centers - https://www.nsf.gov/statistics/ffrdclist/
- Minerva Research Institute - https://minerva.defense.gov/
- National Security Innovation Network (NSIN) - https://www.nsin.mil/
- System for Award Management (SAM) registration - www.sam.gov

- Defense Counterintelligence and Security Agency (DCSA) facility and personnel clearance procedures and requirements - https://www.dcsa.mil/mc/ctp/fc/
- Export Control - https://www.pmddtc.state.gov/ddtc_public
- Invention Reporting - www.iedison.gov
- Technical Reporting - https://discover.dtic.mil/submit-documents/
- Defense Contract Audit Agency - https://www.dcaa.mil/Guidance/Audit-Process-Overview/
- Procurement Technical Assistance Centers - https://www.aptac-us.org/

Backup