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
Defense-Wide Capabilities/Technology

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

Integrated Sensing and Cyber

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

Approved for Public Release
• 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
### Major Themes

<table>
<thead>
<tr>
<th>TIMELINES SHRINKING</th>
<th>Consequences (for both defense and offense)</th>
<th>Effect on S&amp;T Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Humans cannot fight at cyber speed without the right tools</td>
<td>• Emphasize mission assurance through trust and resilience over “monitor and react”</td>
<td></td>
</tr>
<tr>
<td>Interactive ops are obsolete</td>
<td>• Use autonomy to extend reach of workforce</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COMPLEXITY INCREASING</th>
<th>Consequences (for both defense and offense)</th>
<th>Effect on S&amp;T Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Takes us further away from establishing and maintaining trust in our systems</td>
<td>• Emphasize importance of trustworthy, automated tools and educated workforce</td>
<td></td>
</tr>
<tr>
<td>Adds uncertainty, exacerbates security</td>
<td>• “Lone hacker” → “Experts with elite tools”</td>
<td></td>
</tr>
<tr>
<td>Untrustworthy ecosystem (supply chain)</td>
<td>• Manage complexity in blue systems</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LANDSCAPES RAPIDLY CHANGING</th>
<th>Consequences (for both defense and offense)</th>
<th>Effect on S&amp;T Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constantly redefining battleground via new C4ISR technologies (e.g. 5G/6G, SDN, IoT, Autonomous Platforms, etc.). → New vulnerabilities surface all the time</td>
<td>• Proactively analyze emerging technologies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Continue to invest in broadly applicable tools to be able to rapidly adapt to new technologies and nation state adversaries</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DOMAINS CONVERGING</th>
<th>Consequences (for both defense and offense)</th>
<th>Effect on S&amp;T Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>A tactical platform’s attack surface extends out through all its apertures</td>
<td>• Study multi-domain interfaces, find 1+1&gt;2</td>
<td></td>
</tr>
<tr>
<td>Multi-domain stovepipes must end, need to use cyber to shape and deter conflict</td>
<td>• Integration of SA / data streams, C2 for all-domain Information Operations (IO)</td>
<td></td>
</tr>
</tbody>
</table>

---

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)
Typical (Past) Cyber Budget and Performer Base

**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

**PB20: BY BUDGET ACTIVITY**
- $84M (17%)
- $424.5M (83%)

**PB20: BY SERVICE / AGENCY (of $508.5M)**
- Air Force: 15%
- Army: 7%
- Navy: 2%
- DARPA: 17%
- OSD: 14%
- MDA: 7%
- USSOCOM: 15%

**PB20: BY TIER 1 TAXONOMY AREA**
- Protection: 361
- Access and Effects: 40
- Cyber SA: 50
- Cyber C2: 57

**HISTORICAL TRENDS (IN THEN-YEAR DOLLARS)**
- PB15: $0M
- PB16: $50M
- PB17: $100M
- PB18: $150M
- PB19: $200M
- PB20: $250M

- DARPA 6.2
- Services+OSD 6.2
- Services+OSD 6.3
Industry Engagement: DoD SBIR/STTR Process and Components

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.
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

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

- Minerva Research Institute - https://minerva.defense.gov/
- System for Award Management (SAM) registration - www.sam.gov

- Export Control - https://www.pmddtc.state.gov/ddtc_public
- Invention Reporting - www.iedison.gov
- Procurement Technical Assistance Centers - https://www.aptac-us.org/