DARPA S&T Program

Dick Urban
Special Assistant to the Director
Defense Advanced Research Projects Agency

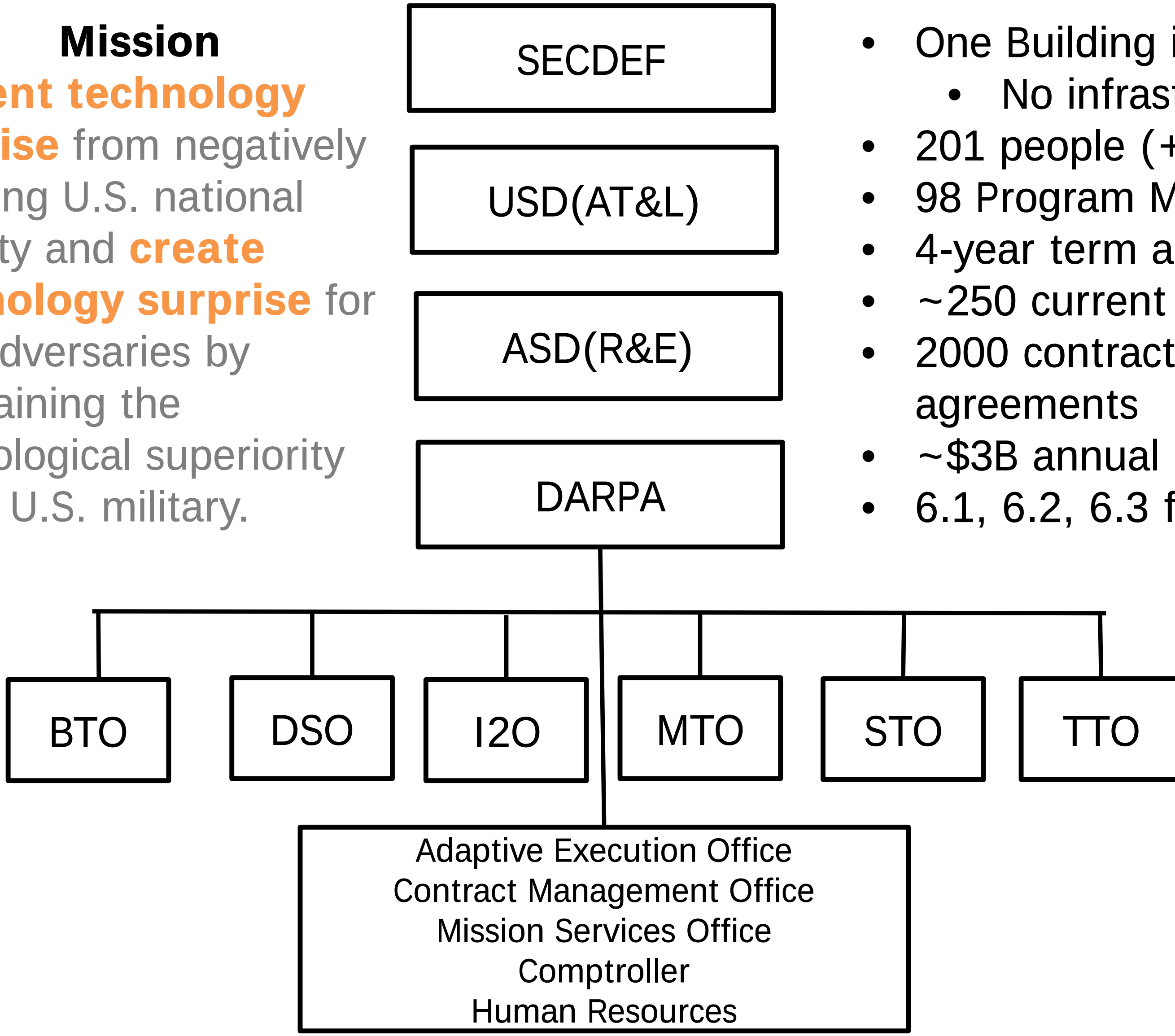
NDIA S&ET Conference

April 12, 2016

DARPA Mission and Organization

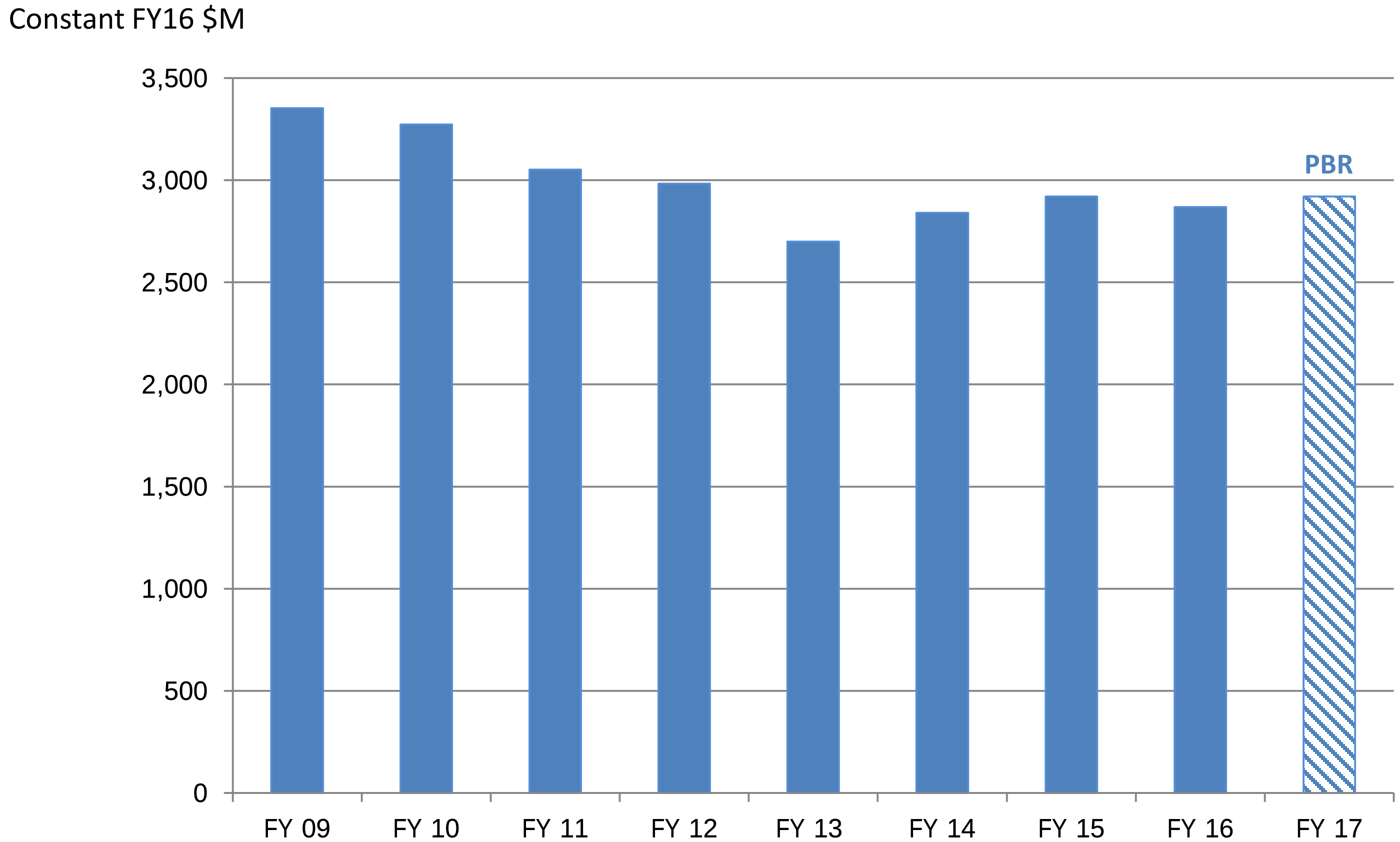
Mission

Prevent technology surprise from negatively affecting U.S. national security and **create technology surprise** for U.S. adversaries by maintaining the technological superiority of the U.S. military.



- One Building in Arlington, VA
  - No infrastructure
- 201 people (+SETA support)
- 98 Program Managers
- 4-year term appointments
- ~250 current programs
- 2000 contracts and other agreements
- ~$3B annual budget
- 6.1, 6.2, 6.3 funding only

DARPA Budget (constant FY16 $)



	FY 09	FY 10	FY 11	FY 12	FY 13	FY 14	FY 15	FY 16	FY 17
DARPA Topline (then year)	$3,014	$2,985	$2,835	$2,814	$2,580	$2,753	$2,872	$2,868	$2,973
FY 16 Deflators/Inflators (%)	89.90	91.22	92.93	94.34	95.59	96.92	98.36	100.00	101.81
DARPA Topline (Constant FY16 $M)	$3,353	$3,272	$3,051	$2,983	$2,699	$2,840	$2,920	$2,868	$2,920

Breakthrough Technologies for National Security
DARPA's Portfolio Today

Diminishing returns for monolithic systems

Rethink complex military systems

- Electromagnetic spectrum dominance
- Position, navigation & timing beyond GPS
- Air superiority in contested environments
- Maritime system of systems
- Robust space
- Overmatch on the ground
- Defense against mass terrorism

Information is exploding

Harness information

- Scalable cyber capabilities
- Electronics with built-in trust
- Big data tools
- Next-generation AI

First-mover advantage

Create technological surprise

- Outpacing infectious disease
- Neurotechnologies
- Synthetic biology
- Chemistry, physics, math, materials
- Understanding complexity
- Human-machine symbiosis

These focus areas are part of a broad and diverse portfolio of DARPA investments
Focus areas change over time as some succeed and others fail and as DARPA identifies new challenges and opportunities

Manned-Unmanned Systems
Autonomy Supporting Air Superiority

High-End Threat Increasing in Quantity and Quality

Chinese J-20 Stealth Fighter

Russian PAK-FA (T-50) Stealth Fighter

Russian SS-N-26 Cruise Missile

North Korean Musudan IRBM

Chinese Luyang III Destroyer

- Weapon capabilities enhanced by robust battle networks
- Networks draw on globally available communications and computing technology

Iranian Fateh-110 SRBM

Chinese Liaoning Aircraft Carrier

Iranian Kilo-class Diesel Submarine

Russian S-400 SAM

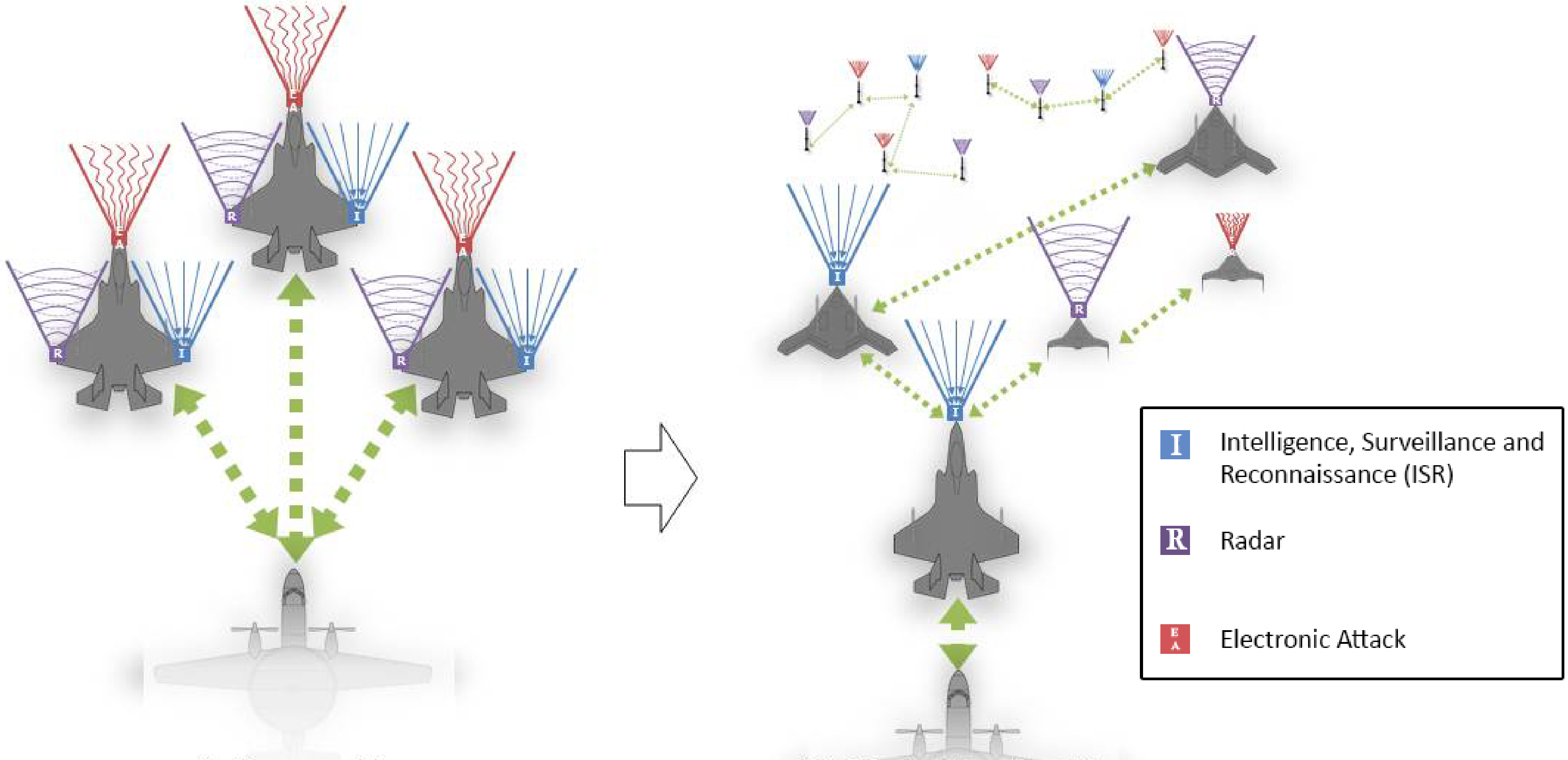
IRBM = Intermediate Range Ballistic Missile
SRBM = Short-Range Ballistic Missile
SAM = Surface to Air Missile

System-of-Systems Approach Exploits Opportunities to Address National Security Challenges

- Individual platforms, however capable, cannot meet challenge of highly networked, lethal, proliferated threat
- Challenges fielding and rapidly adapting systems in needed quantities
- Technology providing opportunities for more capability in smaller packages - obtained more rapidly and affordably
- System of Systems (SoS) Approach: Employ architectures networking lower cost, lower capability platforms with higher cost, higher capability platforms
  - Lower cost platforms enhance military effectiveness and survivability of higher cost platforms
  - Heterogeneity minimizes common failure modes/attack vulnerabilities
  - Can buy lower-cost SoS elements in quantity
  - Imposes cost and complexity on adversaries
  - Advanced integration technologies and open architectures reduce time, cost, and risk for integration of new capability into legacy platforms
  - Faster development time for new capability and opportunities across a more diversified industrial base

Air Superiority in Contested Environments

System of Systems (SoS) Integration Technology and Experimentation (SoSITE)

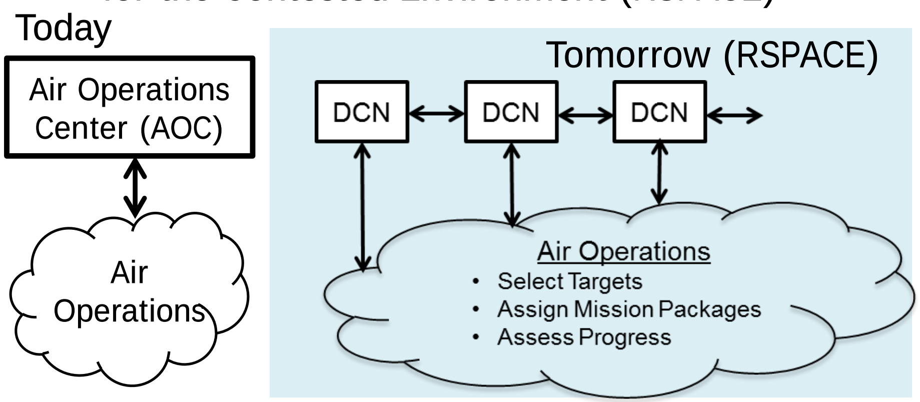


Platform centric
Vulnerable to countermeasures
Limited number of costly platforms
Multi-decade development cycles

Distributed functionality
Robust to countermeasures
Numerous low-cost platforms
Rapid development cycles

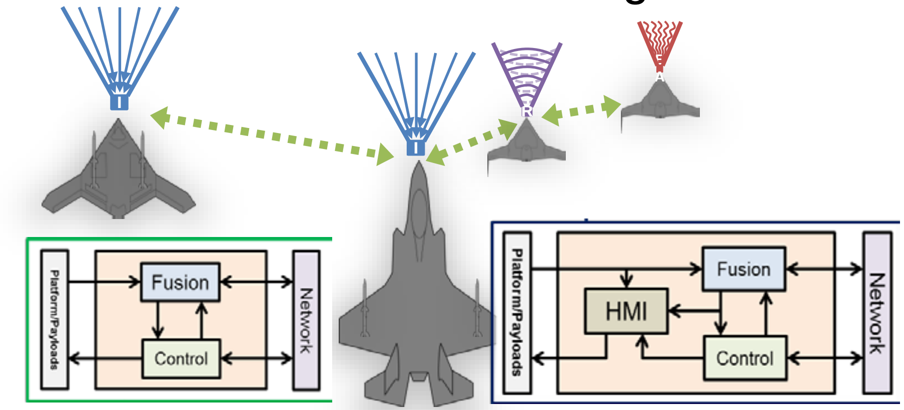
Air Superiority (Autonomy for System of Systems)

Resilient Synchronized Planning and Assessment for the Contested Environment (RSPACE)



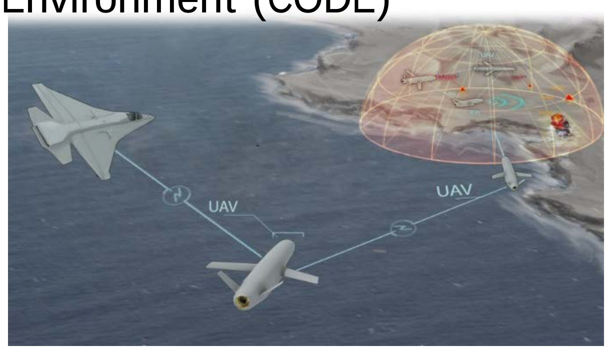
Select the platforms and payloads to accomplish the day's missions

Distributed Battle Management



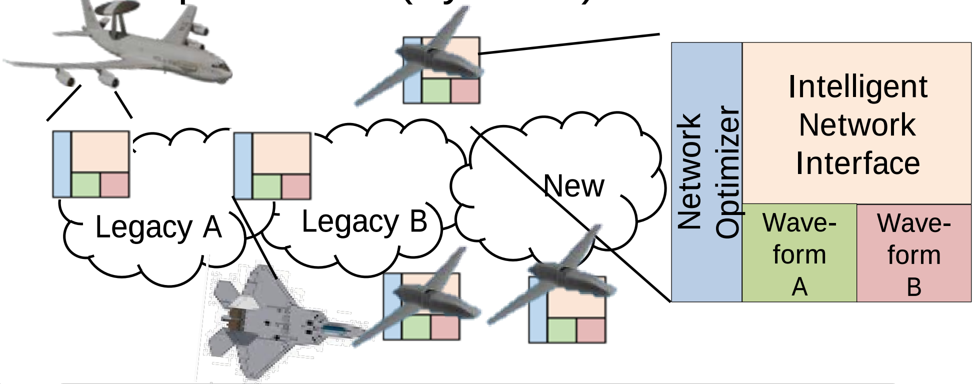
Decision aids to help operators and pilots manage air battles in real time

Collaborative Operations in Denied Environment (CODE)



Collaborative autonomy for teams of unmanned aircraft systems

Dynamic Network Adaptation for Mission Optimization (DyNAMO)



Dynamic airborne network interoperability and network adaptation

Gremlins

PROGRAM OVERVIEW

Gremlins will demonstrate a volley quantity air-launched, air-recoverable, unmanned air vehicle (UAV) technology to enable low cost distributed air operations

PROGRAM STATUS

Upcoming Key Decisions:

- Conduct exploratory trade studies to establish feasibility of technical approaches – FY 2016
- Conduct system and subsystem risk reduction test planning – FY 2017
- Develop objective system concepts and mission capability projections – FY 2017
- Complete Preliminary Design Review for demonstration system – FY 2017

Transition: Potentially USAF and USSOCOM

Technical Risk: Aerial recovery mechanization; Turbulent airflow transit; Efficient engine availability; C-130 integration

CAPABILITY OBJECTIVE/GOAL

- Enable launch and recovery of UAVs in volley quantities for anti-access environments
- Employ distributed payloads for targeting ground threats and collaborate with kinetic assets for strike
- Achieve affordability through opportunistic reuse of recovered UAVs, operated from low-cost host aircraft

PERFORMERS

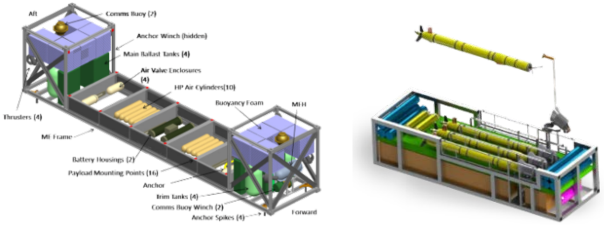
PERFORMER:	LOCATION:
Source selection in progress	

Similar Challenges and Opportunities in Maritime Domain

- Key challenges motivating maritime domain focus
  - Very large number of threat missiles launched from diversity of platforms
  - Adversary ISR threatens battle group
  - Threat to US space-based ISR and communications
  - Eroding acoustic advantage undersea
  - Communications and operations challenged by environment
- Enabled by new advances in autonomous platforms
  - Provide persistence in all domains (surface, subsurface) with minimal operational burden
  - Lower cost than conventional manned platforms
  - Practical to proliferate over large operating areas
  - Cross-domain operations – air, surface, subsurface
- Technologies needed
  - Communications – low-latency, cross-domain, moderate to high bandwidth
  - Command & Control – cross-domain battle management to guide autonomy

Air: Tactically Exploited Reconnaissance Node (TERN)

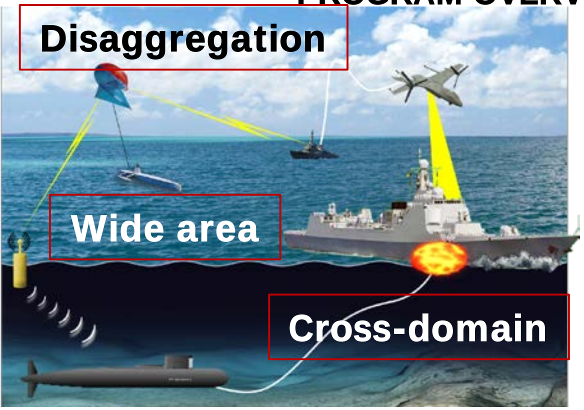
Surface: Anti-submarine warfare Continuous Trail Unmanned Vessel (ACTUV)



Hydra: Undersea deployment and employment of unique payloads

Cross Domain Maritime Surveillance and Targeting (CDMaST)

PROGRAM OVERVIEW



- Distribute functions to low cost systems
- Complete kill chains over wide areas
- Leverage all maritime domains

SoS approach to achieve maritime dominance

PROGRAM STATUS

Upcoming Key Decisions:

- Program Initiation (Q3FY16)
- SoS baseline architecture analysis (Q2FY17)

Transition: USN

Technical Risk:

- Integrating complex system of systems architectures
- Operating across air, surface, and sub-surface domains

CAPABILITY OBJECTIVE/GOAL

- SoS architectures for cost effective wide area dominance
- Integrate emerging manned and unmanned systems and sensor capabilities
- In-water experimentation to demonstrate new collaborative kill chain tactics and operations
- "System in the loop" live, virtual, and constructive test bed environment for evaluation of complex systems
- Methodologies and tools for complex SoS analysis

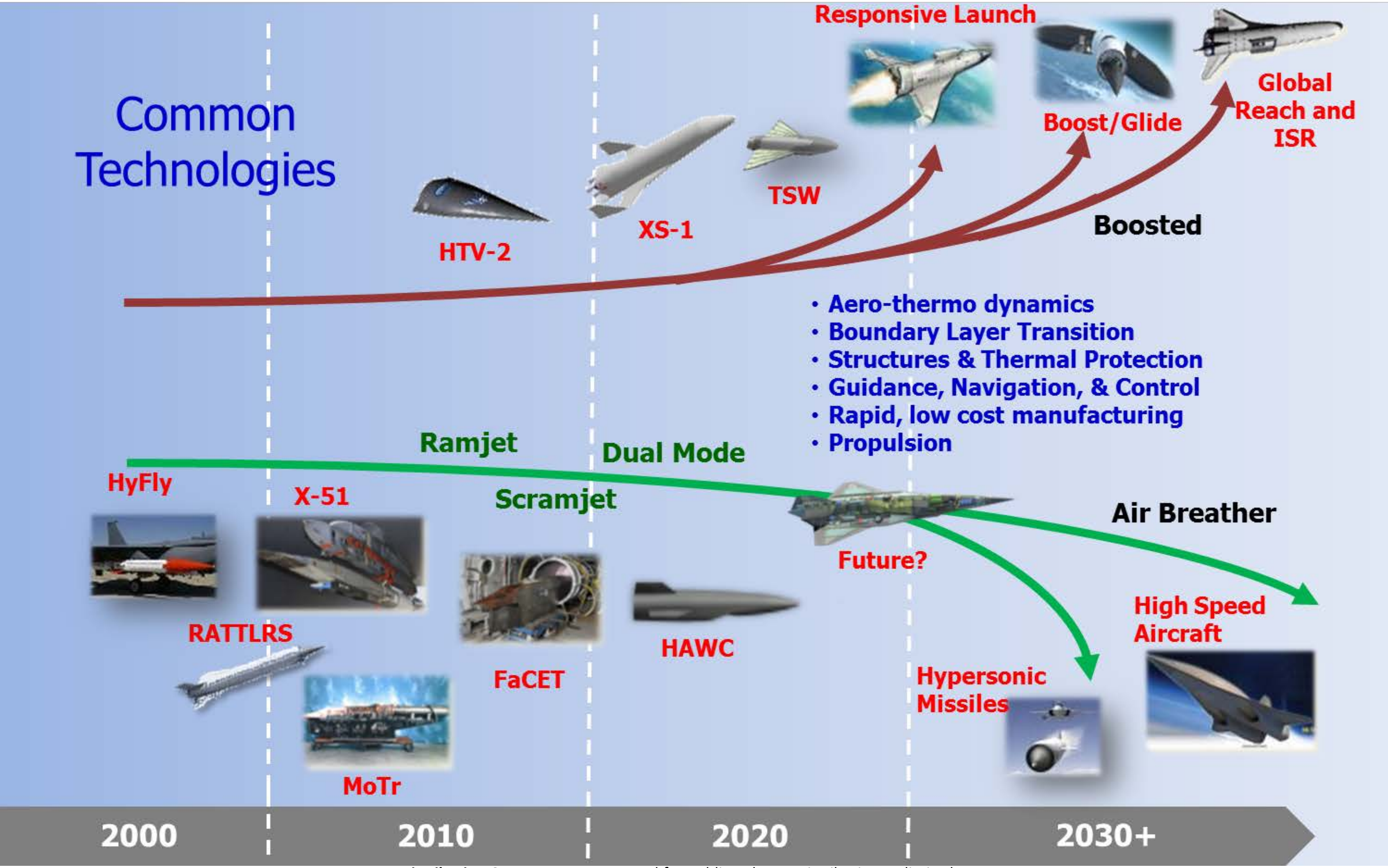
SoS System of Systems

PERFORMERS

PERFORMER:	LOCATION:
* Pending source selection	

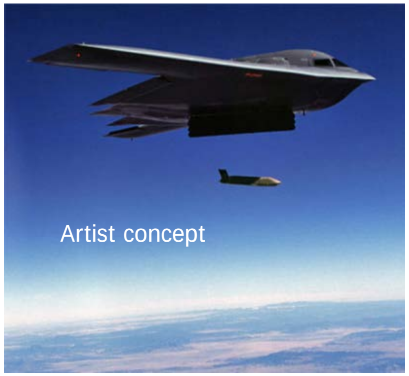
Hypersonics

DARPA Hypersonics Portfolio



Tactical Hypersonic Weapons

Tactical Boost Glide (TBG)



PROGRAM OBJECTIVES

- The TBG program is employing a disciplined systems engineering approach for defining demonstration system objectives and identifying enabling technologies needed for future boost glide systems
- The TBG program plans to focus on three primary objectives:
  - Vehicle Feasibility
  - Effectiveness
  - Affordability

The TBG program is a joint DARPA/Air Force effort that aims to develop and demonstrate technologies that enable air-launched, tactical-range hypersonic boost glide systems

Hypersonic Air-breathing Weapon Concept (HAWC)

PROGRAM OBJECTIVES

- Transformational changes in responsive, long-range strike capabilities against time-critical or heavily defended targets. Joint DARPA/Air Force (AFRL) program
- Advanced air vehicle configurations capable of efficient hypersonic flight
- Hydrocarbon scramjet-powered propulsion to enable sustained hypersonic cruise
- Thermal management approaches designed for high-temperature cruise
- Affordable system designs and manufacturing approaches

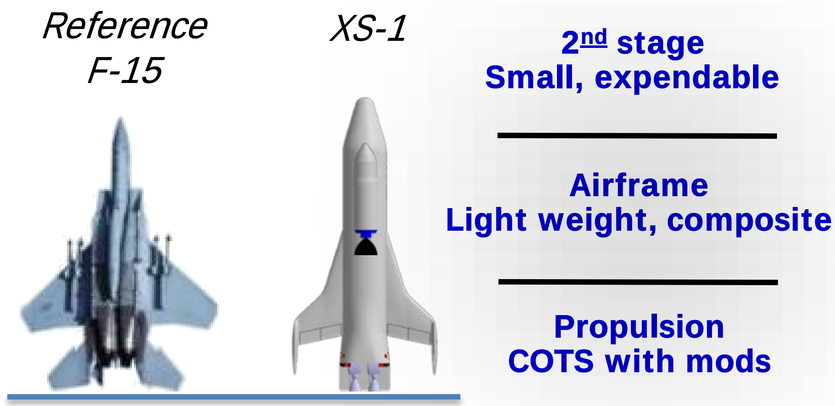
HAWC seeks to demonstrate the critical technologies and attributes of an effective and affordable hypersonic cruise missile

XS-1 – Experimental Spaceplane

Technical Objectives

- Fly 10X in 10 days (akin to SR-71)
- Launch demo payload to orbit
- Design for recurring cost 10X < Minotaur IV:
  - 3K to 5K lb payload
  - Cost < $5M (at >10 flights/yr)

Notional Configuration

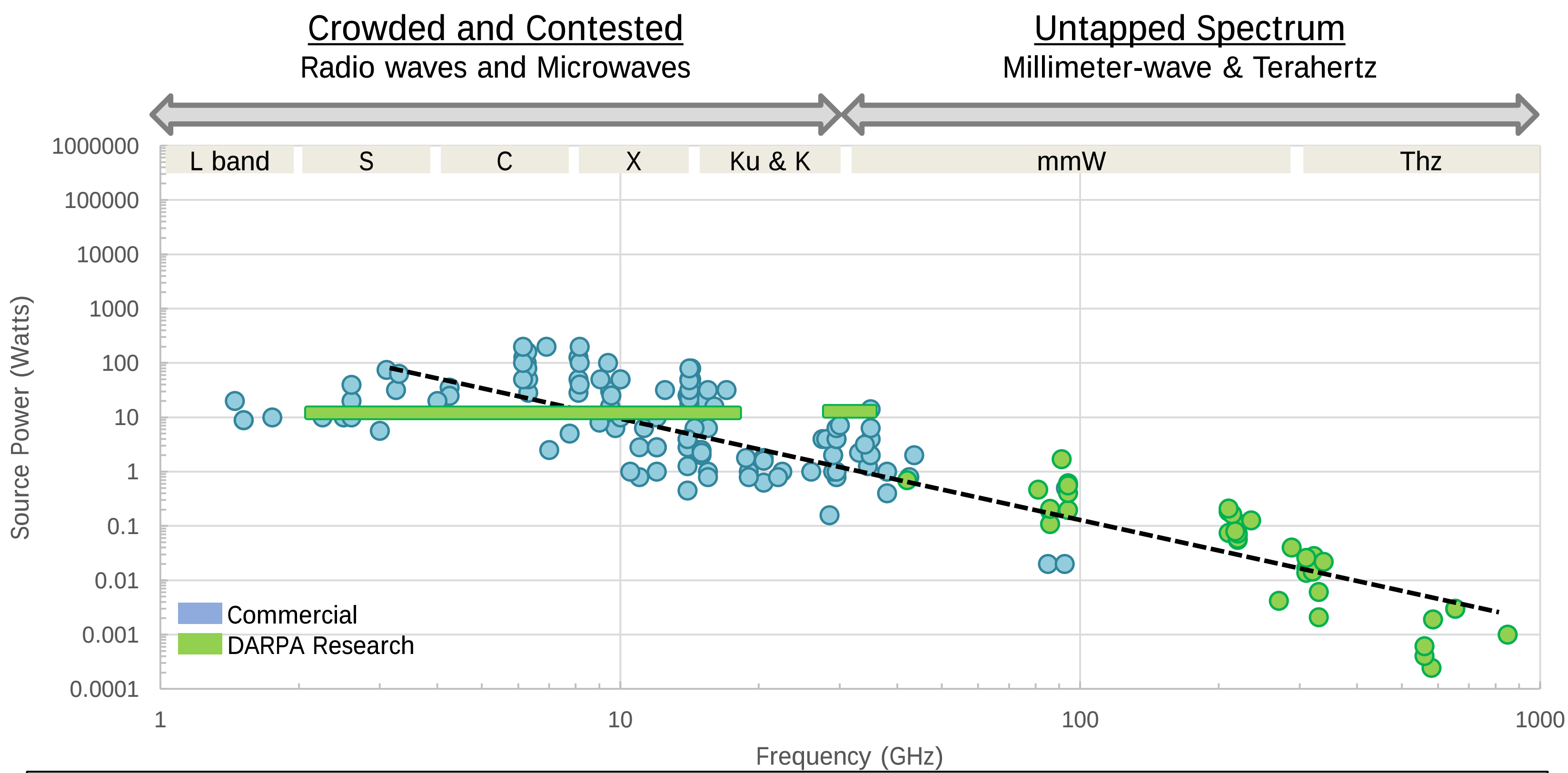


Program Goals

- Breaks cycle of escalating space system costs:
  - Order of magnitude lower launch cost … changes how spacecraft are built
  - Enables new space system architectures
- X-Plane enables new types of aircraft and hypersonic test capabilities
- Responsive launch of 3 to 5K lb payloads now:
  - Deploys single smallsat or constellations for rapid operational employment
  - Affordable launch of “disaggregated” (downsized) DOD payloads
  - Future scaling supports larger payloads & sortie aircraft

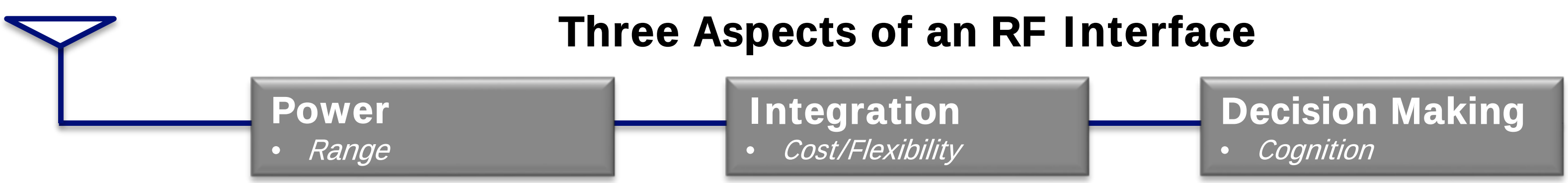
Electromagnetic Spectrum Dominance

The Electromagnetic (EM) Spectrum

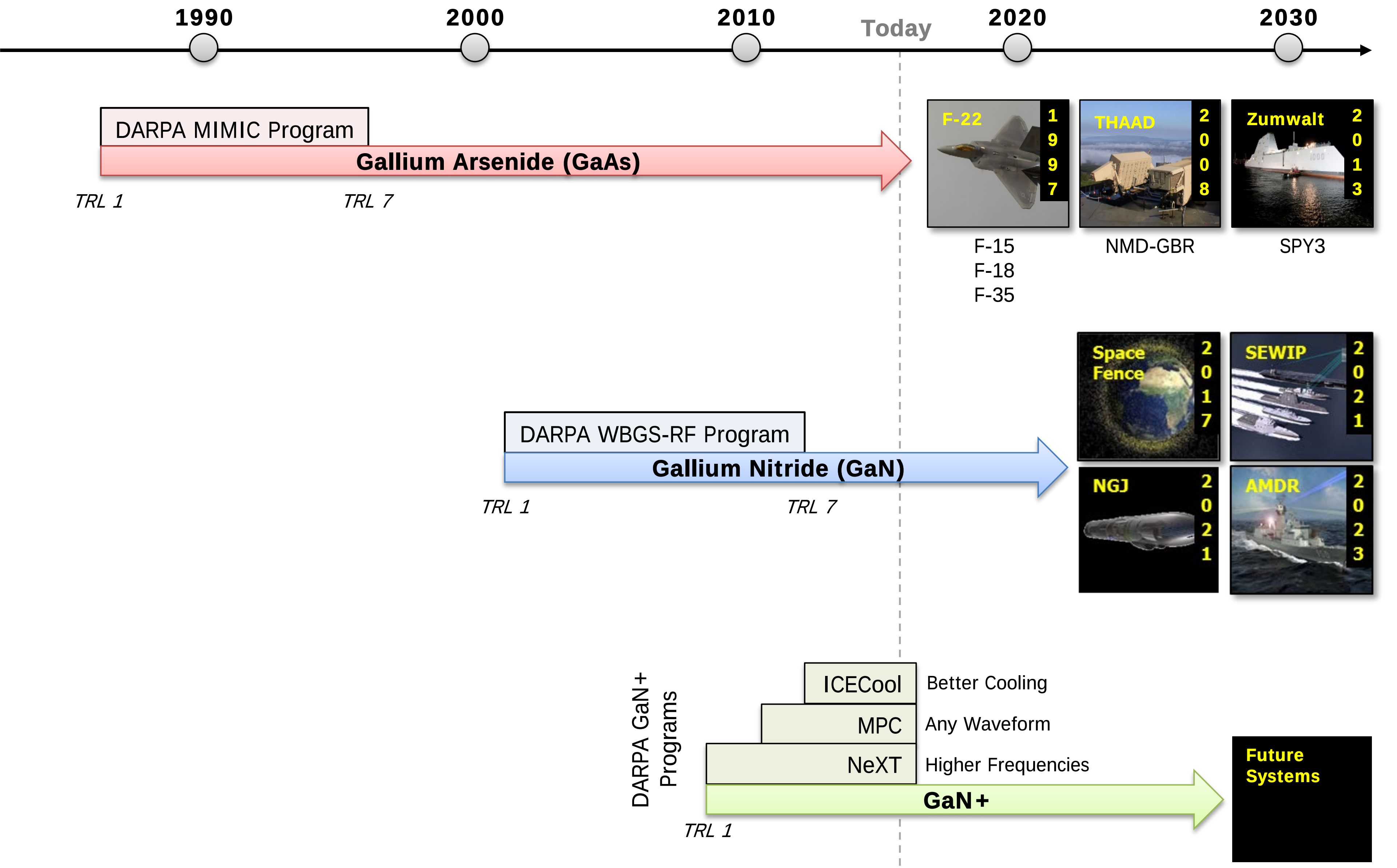


DARPA is working to facilitate operation in a crowded spectrum

Three Aspects of an RF Interface

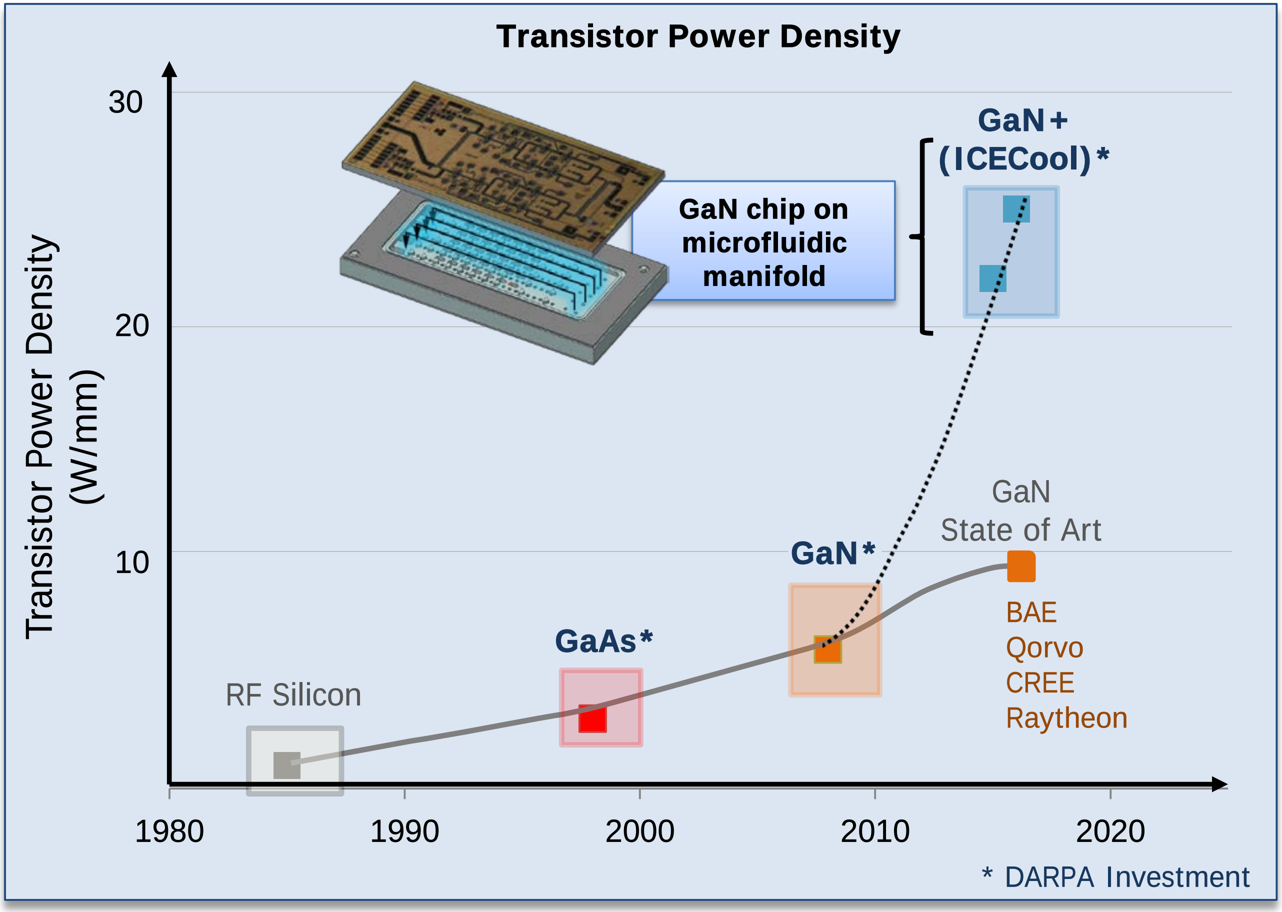


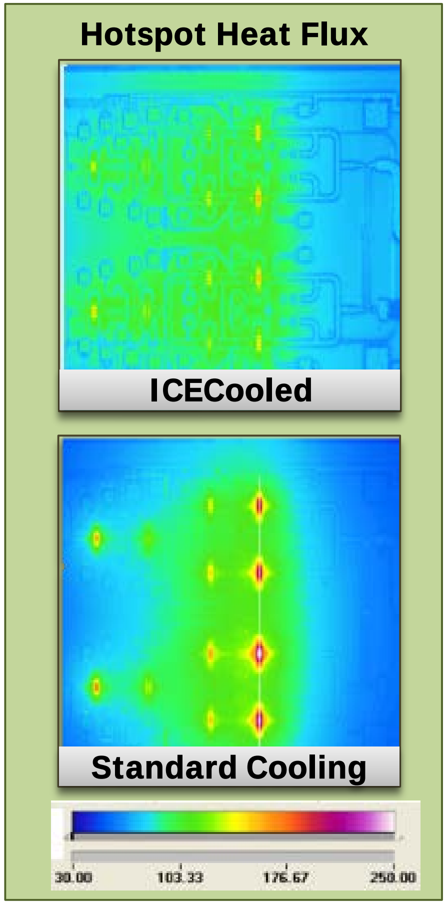
Power –
Defining How We'll Fight Tomorrow



Distribution Statement A: Approved for Public Release, Distribution Unlimited

Power –
ICECool for On-Chip Thermal Cooling

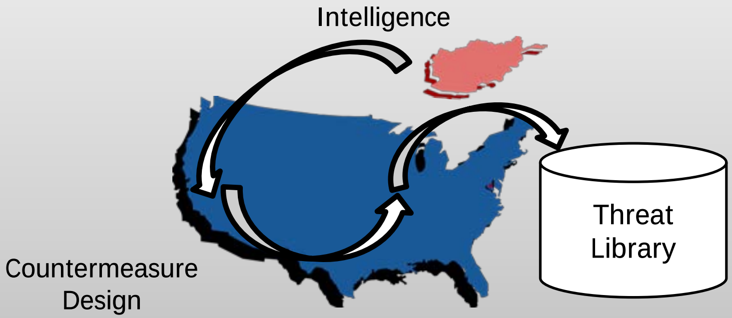




ICECool allows for higher power at lower temperatures than state-of-the-art GaN devices, leading to higher reliability, greater output power (6.8x), and greater range for radar (1.6x) and comms (2.6x)

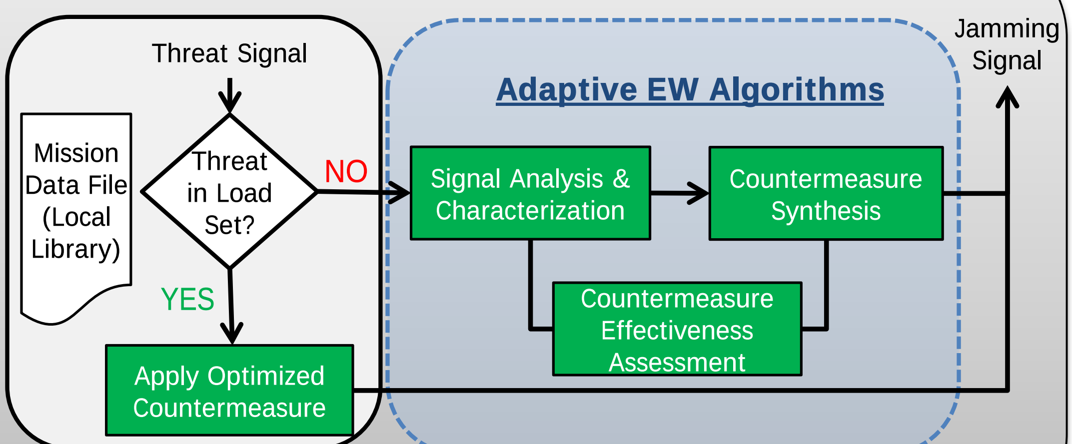
Decision Making – ARC and Blade for Real-Time Threat Response

Today's Approach – Update in the Lab



Months to years to update library and counter new threats

Cognitive Electronic Warfare – Update In-Theatre



Seconds to minutes to counter new threats

Machine Learning will allow DoD systems to rapidly analyze and adapt to unanticipated threats

ARC Transition

F-35

EA-18G

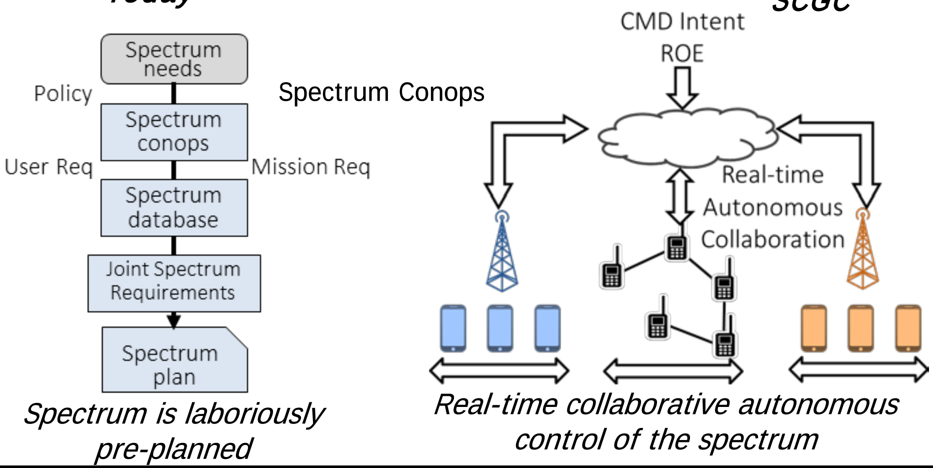
F/A-18

BLADE Transition

Integrated Electronic Warfare Suite (IEWS)

Spectrum Collaboration Grand Challenge

PROGRAM OVERVIEW



PROGRAM STATUS

Upcoming Key Decisions: Planning for BAA in Q4FY2016

Transition: Potential technology transition to the Services and Interagency partners

Technical Risk:

- The development of a remotely accessible test bed to emulate dynamic RF environment at scale

CAPABILITY OBJECTIVE/GOAL

- Conduct a technology challenge for radio networks to autonomously and collaboratively manage and optimize the RF spectrum, without prior knowledge of each other
- Examine and exercise machine learning solutions that will enhance the efficiency and effectiveness of DoD spectrum operations
- Demonstrate that autonomous spectrum operations can overcome inefficiencies in the current spectrum planning process which will not be able to meet growing DoD needs and reliance on RF Spectrum

PERFORMERS

PERFORMER:	LOCATION:
TBD	TBD

Cyber

CYBER: Trustworthy Computing and Information

Cyber protection	Cyber response	Cyber operations

Cyber protection

- High Assurance Cyber Military Systems (HACMS)
- Mission-Oriented Resilient Clouds (MRC)
- Automated Program Analysis for Cybersecurity (APAC)
- Mining and Understanding Software Enclaves (MUSE)

Cyber response

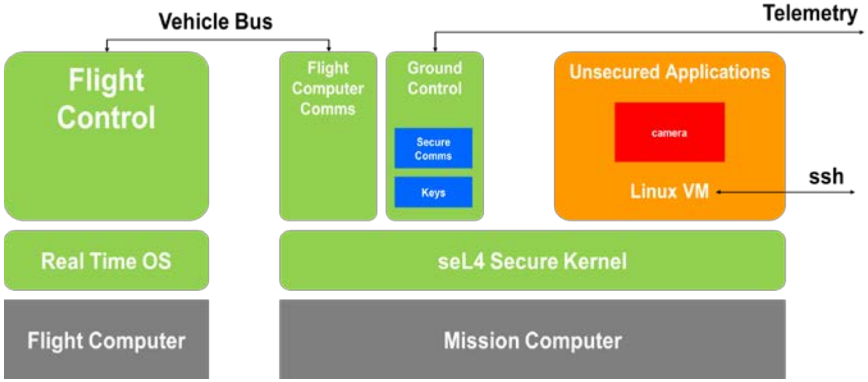
- Cyber Grand Challenge
- Edge-Directed Cyber technologies (EdgeCT)
- Cyber Fault-tolerant Attack Recovery (CFAR)
- Transparent Computing (TC)
- Extreme DDOS Defense (XD3)

Cyber operations

- Plan X
- Network Defense
- Rapid Attack Detection, Isolation and Characterization Systems (RADICS)

High-Assurance Cyber Military Systems (HACMS)

- Use formal methods (structural mathematics) to create cyber resilient vehicles
  - Create technology for the cost-effective construction of high-assurance cyber-physical systems, where high assurance is defined to mean functionally correct and satisfying appropriate safety and security properties
  - Produce high-assurance operating system components and control systems
  - Develop a suite of program synthesizers and formal-methods tools
  - Generate an integration workbench containing all HACMS tools and assured components
- Live attacks on Unmanned Little Bird were prevented




Boeing Unmanned Little Bird

Leveraging the Analog Domain for Security (LADS)

PROGRAM OVERVIEW

Using the analog domain for cyber security of the IoT

PROGRAM STATUS

Upcoming Key Decisions: Contract awards Q3FY2016

Transition: PACFLT N6T, SOCOM, NSA, CIA, ARCyber, AFRL, NASIC

Technical Risk: Sensing data fidelity with high-accuracy introspection and multimodal data fusion

CAPABILITY OBJECTIVE/GOAL

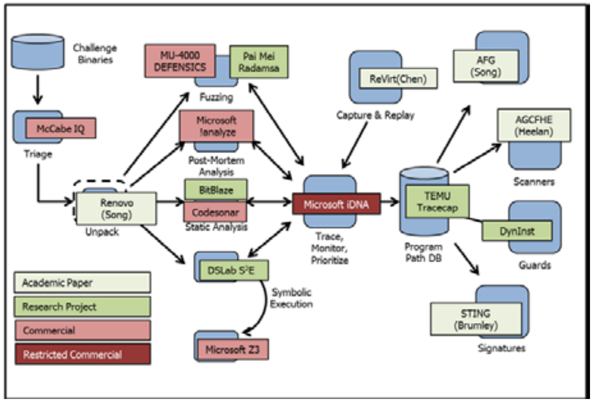
- Use involuntary analog emissions of digital devices across different sensing modalities (EM, acoustic, power) to detect anomalies and attacks, focusing on Internet of Things devices
- Develop systems and components that can monitor the running state of digital devices and identify the presence of attackers based on their involuntary analog emissions
- Map device firmware, configuration, and data to cyber-relevant analog emissions model

PERFORMERS

PERFORMER:	LOCATION:
TBD	TBD

Cyber Grand Challenge (CGC)

PROGRAM OVERVIEW



First automated cyber defense tournament

PROGRAM STATUS

Final Event – August 4, 2016 (7 Finalists) ($2M Prize)

The world's first all-computer Capture the Flag tournament live on stage co-located with the DEF CON Conference in Las Vegas where automated systems may take the first steps towards a defensible, connected future.

Transition: CYBERCOM, ARCYBER, DHS

Technical Risk: First-generation cyber reasoning prototypes face integration and research risk

CAPABILITY OBJECTIVE/GOAL

- Create automation revolution by challenging prototypes to compete in first automated cyber defense tournament
- Change the conversation about national cyber power from artisan expertise to supercomputer systems
- Create a training and technology measurement capability for US Cyber Forces
- Create a standardized corpus for testing security adaptation
- Create a community which continues to use the power of competition to drive automation revolution

PERFORMERS

PERFORMER:	LOCATION:
For All Secure	Pittsburg, PA
GrammaTech	Ithaca, NY
Lekkertech	San Francisco, CA
SIFT	Minneapolis, MN
SRI	Menlo Park, CA
Trail of Bits	New York, NY
UC Berkeley	Berkeley, CA
NARF	Washington D.C.
Kaprica	Austin, TX
Cromulence	Melbourne, FL

Rapid Attack Detection, Isolation and Characterization Systems (RADICS)

PROGRAM OVERVIEW

Detecting and respond to cyber-attacks on U.S. critical infrastructure

PROGRAM STATUS

Upcoming Key Decisions: Source selection

Transition: Military Services, Combatant Commands, DISA, DHS

Technical Risk: Produce a rapid recovery capability where there is no incentive for commercial investment to address a high-impact low-frequency problem; ability to identify and mitigate malware installed on Operational Technology (OT) devices

CAPABILITY OBJECTIVE/GOAL

- Response to a widespread and persistent cyber-attack on the power grid and its dependent systems
- Provide early warning of an impending cyber attack
- Provide out-of-band sensing of the state of the grid to counter spoofing of utility telemetry
- Maintain and expand situational awareness in the immediate aftermath of an attack
- Create and maintain isolated emergency networks for data and voice communication in the aftermath of an attack
- Rapidly localize and analyze cyber intrusions into power grid infrastructure

PERFORMERS

PERFORMER:	LOCATION:
Soar Technologies	Ann Arbor, MI
Charles Stark Draper Laboratory	Cambridge, MA
Raytheon BBN Technologies	Columbia, MD
BAE Systems	Arlington, VA

2016 Major Agency Events
Military Services and Cyber & Hacker Community

DARPA DEMO DAY

Pentagon

May 11, 2016

Demonstrate DARPA technologies to military and DoD customers
to stimulate transition and new applications and
to share our visions for future national security capabilities

All Pentagon badge holders are welcome, as are visiting U.S. Government civilian/military CAC holders and blue Intelligence Community badge holders. These individuals can receive a temporary, no-escort-required badge by checking in at the Pentagon Visitor's Center near the Metro Entrance.

CGC CYBER GRAND_CHALLENGE

Las Vegas

August 4, 2016

Create automatic defensive systems capable of reasoning about flaws, formulating patches, and deploying them on a network in real time

The world's first machine-only hacking tournament www.darpa.mil