



AFRL



Perspectives on Cognitive Communications for future Military Space Missions

Dr. (Richard) Scott Erwin
Chief Scientist (Acting),
Space Vehicles Directorate
Air Force Research Laboratory



Agenda

- Sensor Calibration
- Current Space Environment & Drivers
- Future Space Communications Environment
- AFRL 101
- Some AFRL Programs of Interest
- Collaboration Opportunities
- Summary

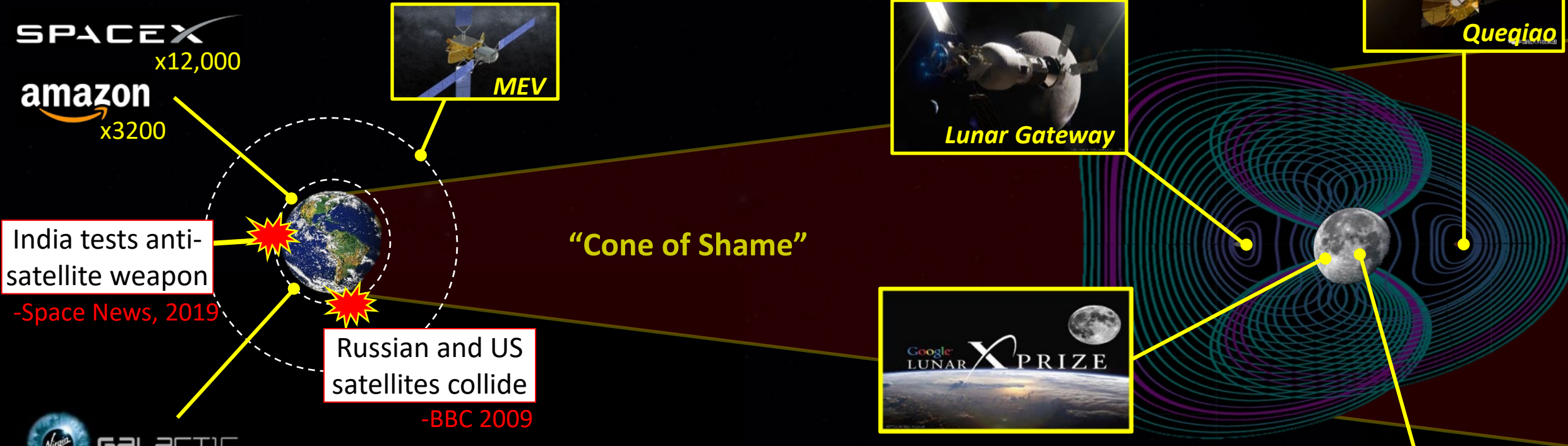


Sensor Calibration: my background on these topics

- 1997: Ph.D. @ U. Michigan complete, start @ AFRL
- 1999: Tech Lead, Controls Program
- 2000: PM, Large Deployable Optics Program
- 2002: RVSV Branch Tech Advisor
- **2005: Command, Control, & Comm (C3) Tech Area Lead**
 - **Focus: SATCOM & Space C2 Prog & Cognitive Radios for Contested Comms, On-Board Autonomy**
- 2009: Assistant to the RV Chief Scientist
- 2011 – 2016: PM, Guid., Nav, & Control Program
- **2016 – 2017: Visiting Researcher, U. California Santa Barbara**
 - **Research: zero-sum games, beginning of R&D on DRL methods for games (e.g., AlphaStar)**
- 2018 – 2020: Principal Investigator, EAGLE-Mycroft Mission
- 2020 – 2021: Lead, Special Projects
- **2021 – Present: Acting Chief Scientist, Space Vehicles Directorate**

21st Century Space

Economic and national interests create new challenges



India tests anti-satellite weapon
-Space News, 2019

Russian and US satellites collide
-BBC 2009

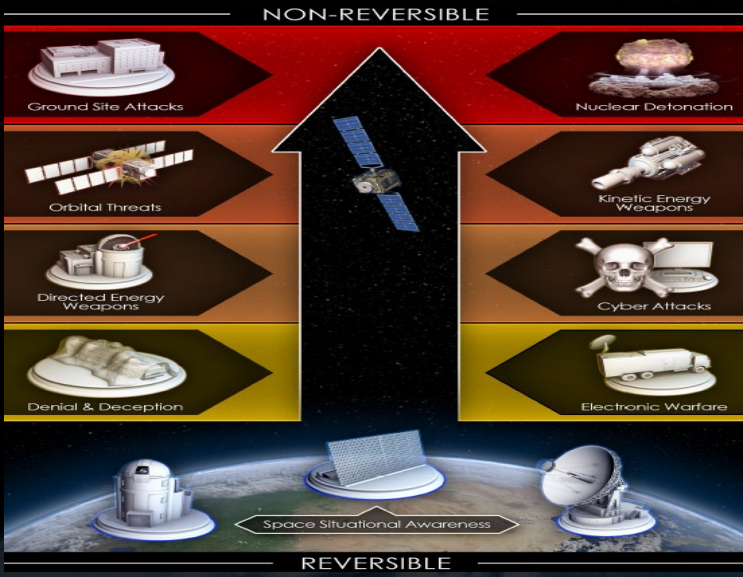
GALACTIC
 planet.
 See change. Change the world.
 BLACK SKY
 Be The First To Know

1969	Today	2030+
~1500 objects	~10 ⁴ objects; human-operated	~10 ⁶ objects, autonomous
GEO, Lunar, Keplerian	GEO, Keplerian	Cis-lunar, non-Keplerian
~7 nations in space	~90 nations; commercial	?? nations, commercial; non-state

DSI™
 DEEP SPACE INDUSTRIES
 LUNAR RESOURCES
 PLANETARY RESOURCES

Complexity and Challenges

Achieving decisive, independent effects from space has many technical challenges

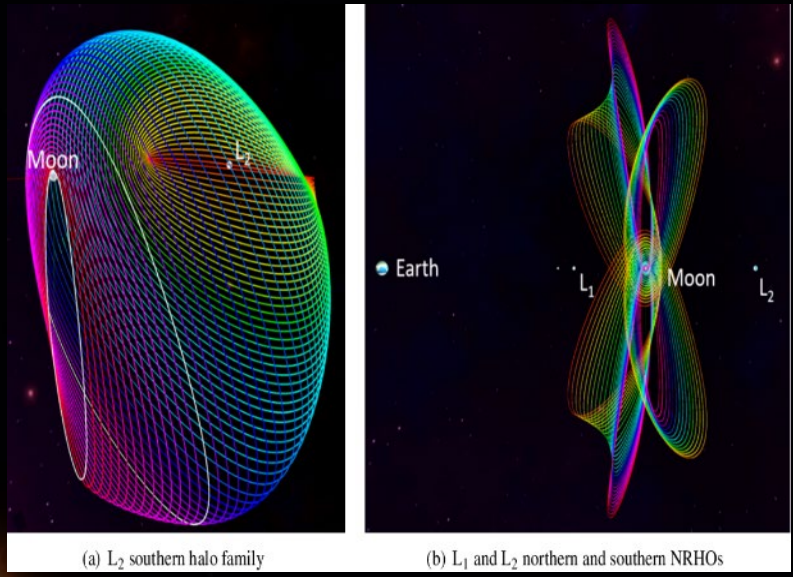


Survivability

Distance

Communications

Cyber Security



Maneuver, logistics, propulsion dominated

Complex flight dynamics and control

Domain effects on payload

Space domain awareness



On-board autonomy and machine learning

Data source expansion and data fusion

Platform diversity and proliferation

Resilient Networking



Space is Vital to US Economic and National Security

The USSF Is Dedicated To Accessing, Protecting & Defending the Space Domain

VITAL TO OUR WAY OF LIFE



The U.S. Harnesses The Benefits Of Space Everyday For Communications, Global Markets, Weather, Scientific Exploration And More

The Global Space Economy Continues To Grow From \$450 Billion To An Estimated \$1 Trillion By 2040

VITAL TO MODERN WAY OF WAR



Potential Adversaries Have Recognized The U.S. Military's Dependence On Space And The Advantages Space Provides, And Are Developing Their Own Space Capabilities

In A Conflict, They Intend To Degrade Our Space Capabilities To Reduce Our Military Effectiveness and Degrade Our American Way Of Life

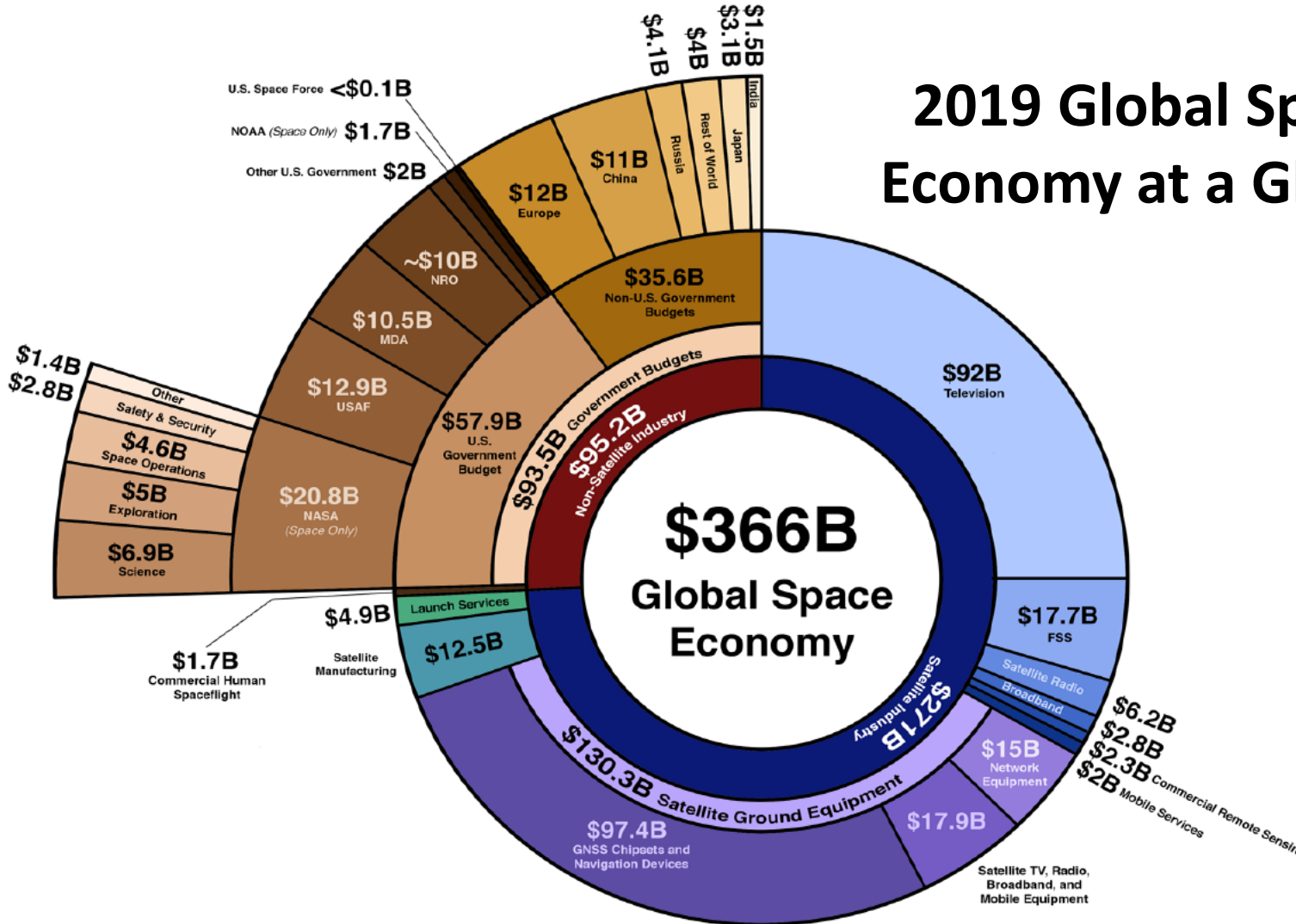
US Must Remain THE Leader in Space: Freedom of Action & Being First

Freedom Of Action In Space Must No Longer Be Assumed, It Must Be Underpinned By Strength And Leadership



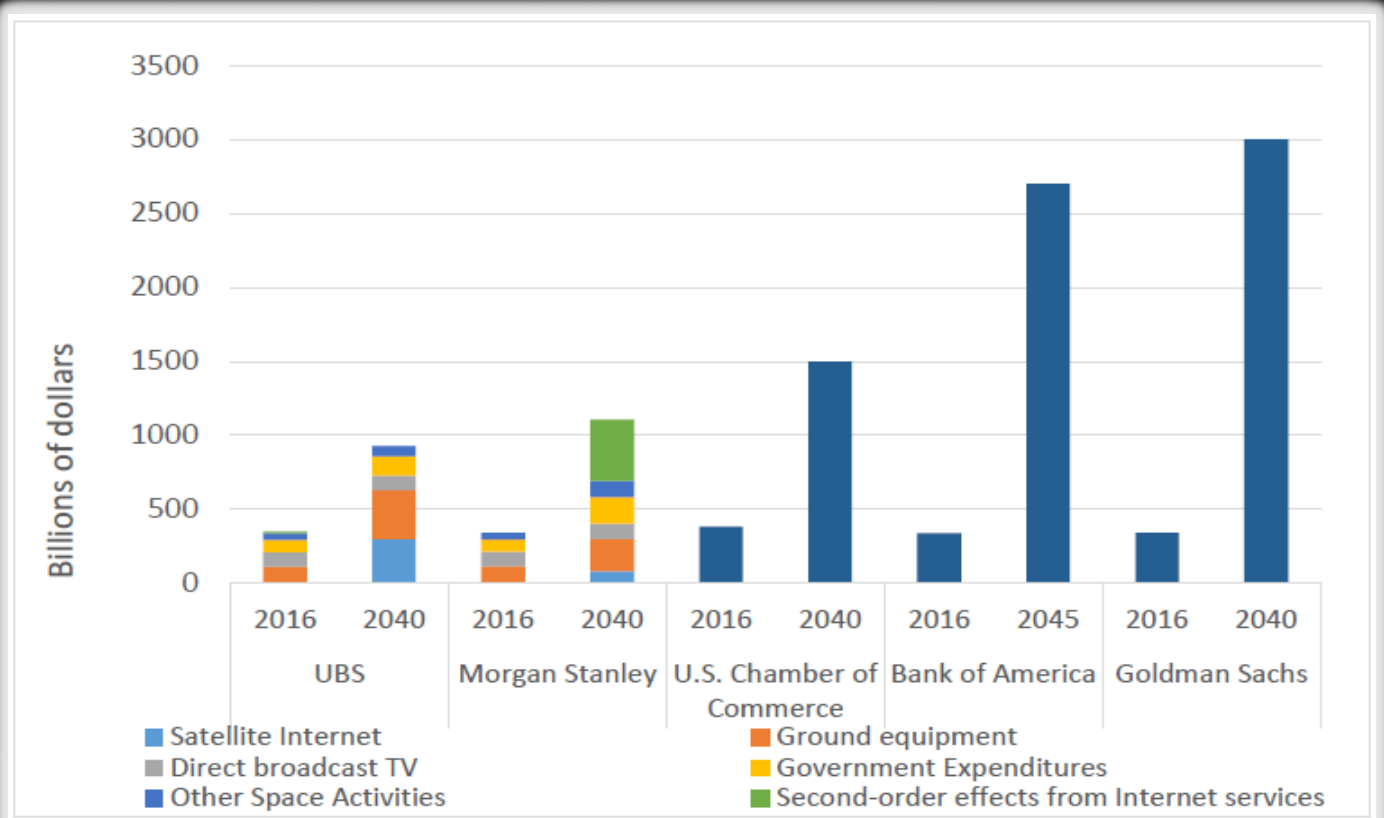
Space Plays a Major Role in Everyday Lives and will Continue to Grow

2019 Global Space Economy at a Glance



Market Perspective

Continued Growth will Drive the Importance of Space



Sources: UBS 2018; Morgan Stanley Research 2017; U.S. Chamber of Commerce 2018; Bank of America Equity Research 2017; Goldman Sachs Equity Research 2017

Note: We represented Goldman Sachs "multi-trillion" forecast as \$3 trillion.

Figure ES-3. Projections of the Size of the Future Space Economy

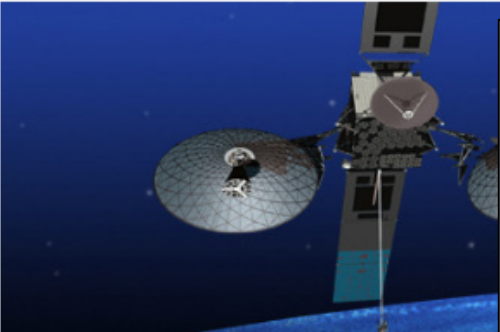
RF SatComm in Contested Environments

SCIENTIFIC METHOD —

Satellite-jamming becoming a big problem in the Middle East and North Africa

Events associated with the Arab Spring have put a new focus on satellite ...

DAVE KLINGLER - 3/28/2012, 4:30 AM



The Arab Spring has had yet another consequence—satellite jamming threatens the satellite operators' business. Two operators, Arabsat and the Satellite 2012 Conference in Washington, D.C. last week, announced a 21-country consortium that provides broadcasting to over 100 countries. NileSat is an Egypt-based operator that carries 415 channels to the Middle East. It also provides broadband, telephone, and VSAT service.

Jamming and rounding up satellite dishes has become a common part of the unfavorable coverage in their own (or sometimes other people's) countries. BroadcastEngineering.com detailed the decision of the United Nations (ITU) to condemn satellite jamming in Iran as "contrary to Article 17 of the ITU Radio Regulations." That decision came after complaints by several broadcasters, including Voice of America, World Service, and Voice of America. Last year Reuters reported that jamming of satellite services occurred in Libya during the uprising.

But the issue may not be limited to Middle East governments. The English website claimed in January that British technicians were jamming the Hotbird sat network from a site in Bahrain. If that's accurate, it may be acceptable to jam European companies' satellites as long as the broadcaster is not in the United States.

Any attempt to jam satellites in the United States is generally tracked by the Federal Communications Commission (FCC).


The Economist | World politics | Business & finance | Economics | Science & technology | Culture

GPS jamming

Out of sight

Satellite positioning-data are vital—but the signal is surprisingly easy to disrupt

2013 | From the print edition | *Timekeeper*



Every day for up to ten minutes near the London Stock Exchange, someone blocks the signal from the global positioning system (GPS) network of satellites. Navigation systems in cars stop working and timestamps on trades made in financial institutions can be affected. The incidents are not a cyber-attack by a foreign power, though. The most likely culprit, according to Charles Curry, whose firm Chronos Technology covertly monitors such events, is a delivery driver dodging his bosses' attempts to track him.

GPS signals are weak. Mr Curry likens them to a 20-watt light bulb viewed from 12,000 km (19,300 km). And the jammers are cheap: a driver can buy a dashboard model for £50 (\$78). They are a growing menace. The bubbles of electromagnetic noise they create interfere with legitimate GPS users. They can disrupt civil aviation and kill mobile-phone signals, too. In America their sale and use is banned. In Britain they are illegal for anyone to use deliberately, but not, yet, to buy. Ofcom, a regulator, is mulling a ban. In Australia years ago officials have destroyed hundreds of jammers.

DEFENSE SYSTEMS


BATTLESPACE TECH
CYBER DEFENSE
MOBILE RESOURCES
EVENTS

C4ISR
DEFENSE IT
UNMANNED SYSTEMS
NEWSLETTER
ADVERTISE

C4ISR

Report: NATO worried about comms gaps, Russia's jamming power

BY GEORGE LEOPOLD • JUL 09, 2015



Secure, interoperable communications are essential in an increasingly mobile military.

Recent U.S.-NATO military exercises have revealed difficulties in maintaining secure communications among western allies as they focus greater attention on Russian forces and

YESFORN!

<https://www.afspc.af.mil/News/Photos/igphoto/2002092512/>



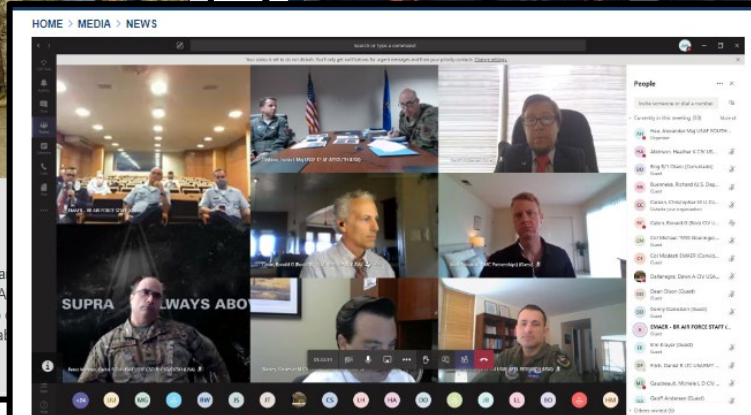
Team Vandenberg Hosts Combined Space Operations Coalition Summit

Defense personnel from Australia, Canada, France, Germany, the United Kingdom, and the United States gathered for a photo during the Combined Space Operation Coalition Summit at Vandenberg Air Force Base, California, on August 22, 2019. The primary objective for the summit was to work with coalition partners to work ahead to transition the Combined Space Operations Center to Full Operational Capability at A1C Aubree Milks/Released)

<https://www.nasa.gov/press-release/us-japan-sign-space-collaboration-agreement-at-nasa-headquarters>



US, Japan Sign Space Collaboration Agreement at NASA Headquarters



NEWS | Aug. 13, 2020

SOUTHCOM Hosts New U.S. Space Force 'U.S.-Brazil Space Engagement Talks'

By U.S. Southern Command Public Affairs

U.S. Southern Command hosted U.S. Space Force and Brazilian counterparts for the newly established virtual U.S.-Brazil Space Engagement Talks. Not only is this the first senior space flag officer event between the U.S. and Brazil, but it is the first such event for the U.S. Space Force.



MSMU/HAD: Integrated commercial and allied sensors into DoD TCPED, test in warfighter exercises

<https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/2312182/southcom-hosts-new-us-space-force-us-brazil-space-engagement-talks/>



Expansive Space Portfolio

One AFRL – works across vast technological areas, finding synergies that allow us to move faster to field critical space programs

Space technologies
Space experimentation

Space Vehicles
RV

Space Domain Awareness
Laser & high power microwave effects

Directed Energy
RD

Space access
In-space propulsion
Space logistics

Aerospace Propulsion
RQ

Super computing resources
Digital transformation

Compute Resources
RC

Materials & manufacturing
Laser hardening
Additive manufacturing

Materials
RX

Information
RI

Networks & comms
Cyber
Multi-domain C2

Human Effects
RH

Operator performance
Autonomous systems
Operator training

Munitions
RW

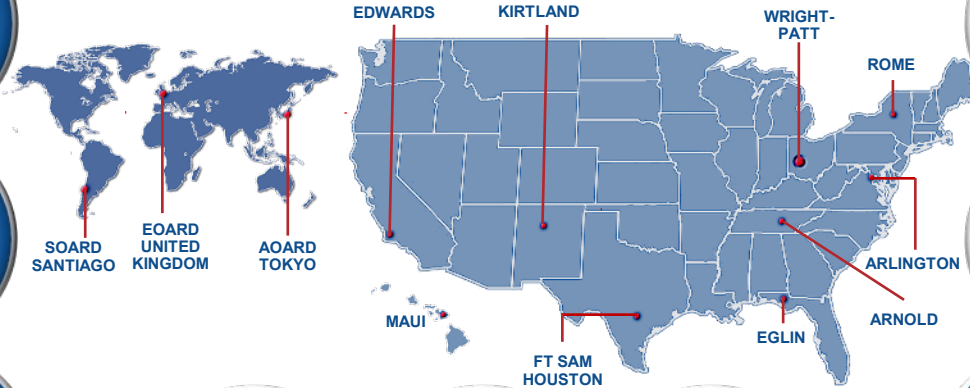
Small platform PNT, sensors, and components

Sensors
RY

Sensor & data exploitation
Cognitive EW
Position, Nav, & Timing

Basic Science
OSR

Basic science – materials, quantum, power, etc
International research



AFWERX
RG/SB

Classified Programs

SDPE
RS

Innovation
Tech and industrial base expansion

Inform S&T Vector
Experimentation
Operational assessment
MS&A and Studies

AFRL Future Vision

Today
Stovepiped Missions Areas
0-5 yrs



Attributes

- Stovepiped acquisition and ops
- Strategic requirements focused
- Lengthy requirements process
- Large, costly programs
- Incremental technology
- Limited resiliency

Mid-term
Hybrid Architecture
5-15 yrs



Attributes

- Mixture of strategic and tactical
- Orbital regime diversification
- Platform size variation
- International, commercial and DoD coordination and integration
- Multi-path communication

Far-term
Heterogeneous Architecture
15-30 yrs



Attributes

- Resembles more of the modern day internet – IoT of Space
- Ubiquitous communication
- Integrated autonomy and ML/AI
- Truly integrated multi-domain
- Ubiquitous information exploitation and decision making

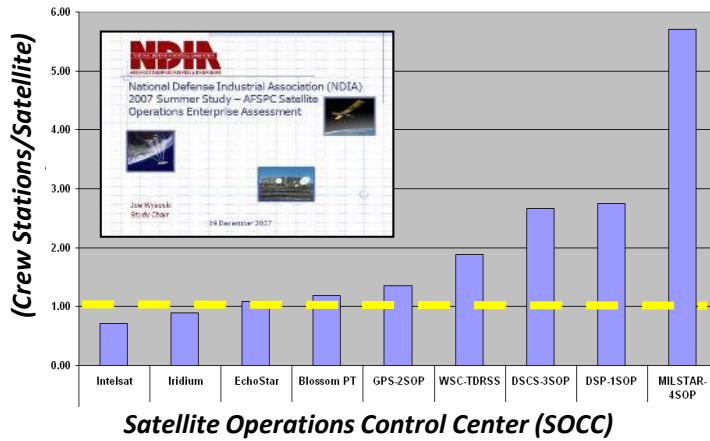
Autonomous Systems

The good we desire...

Persistent Vigilance



Efficiency/Manpower Reduction



Superhuman Capabilities



Resilience via Emergent Behavior

The uncertainties we fear...

Inscrutability

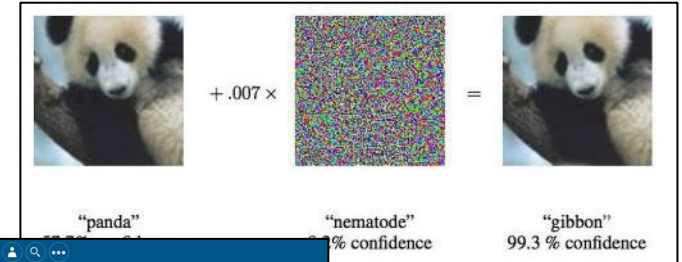


Ethics/Policy/C2/Responsibility



Undesirable Emergent Behavior

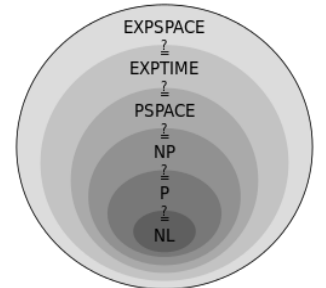
Co-Optability



Cyber Vulnerabilities



Complexity/Tractability (V&V)





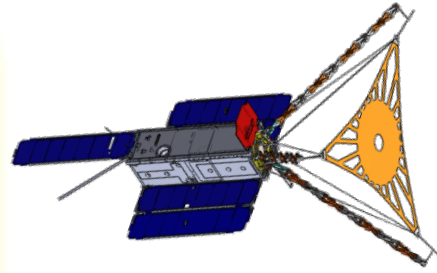
Current Areas of Research

- **Small Satellite space communications testbeds**
- **Hybrid Architecture (commercial-allied-Gov't) systems integration**
- AI-enabled networks in contested environments
- **AI-enabled PNT (broadcast comms)**
- Comms-PNT mission/payload integration
- Space EW (EP/ES/EA)
- **Space cyber-security**
- Trust in Autonomy (Machine/Machine and Machine/Human)
- Human-Autonomy Interface



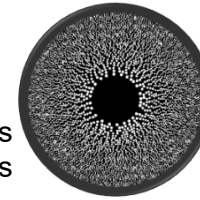
Example Area: AFRL Small Satellite Portfolio 2022

XVI: Link-16 in space



FalconSat-7: A CubeSat Solar Telescope

Photon Sieve Telescopes for Small Sats



Suchai: Understanding the ionosphere to improve communications

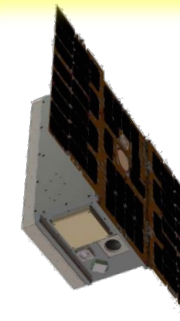
STARGATE: Ground systems, software, cloud ops, integration of commercial satellite C2



Ascent: Cubesat technology in GEO

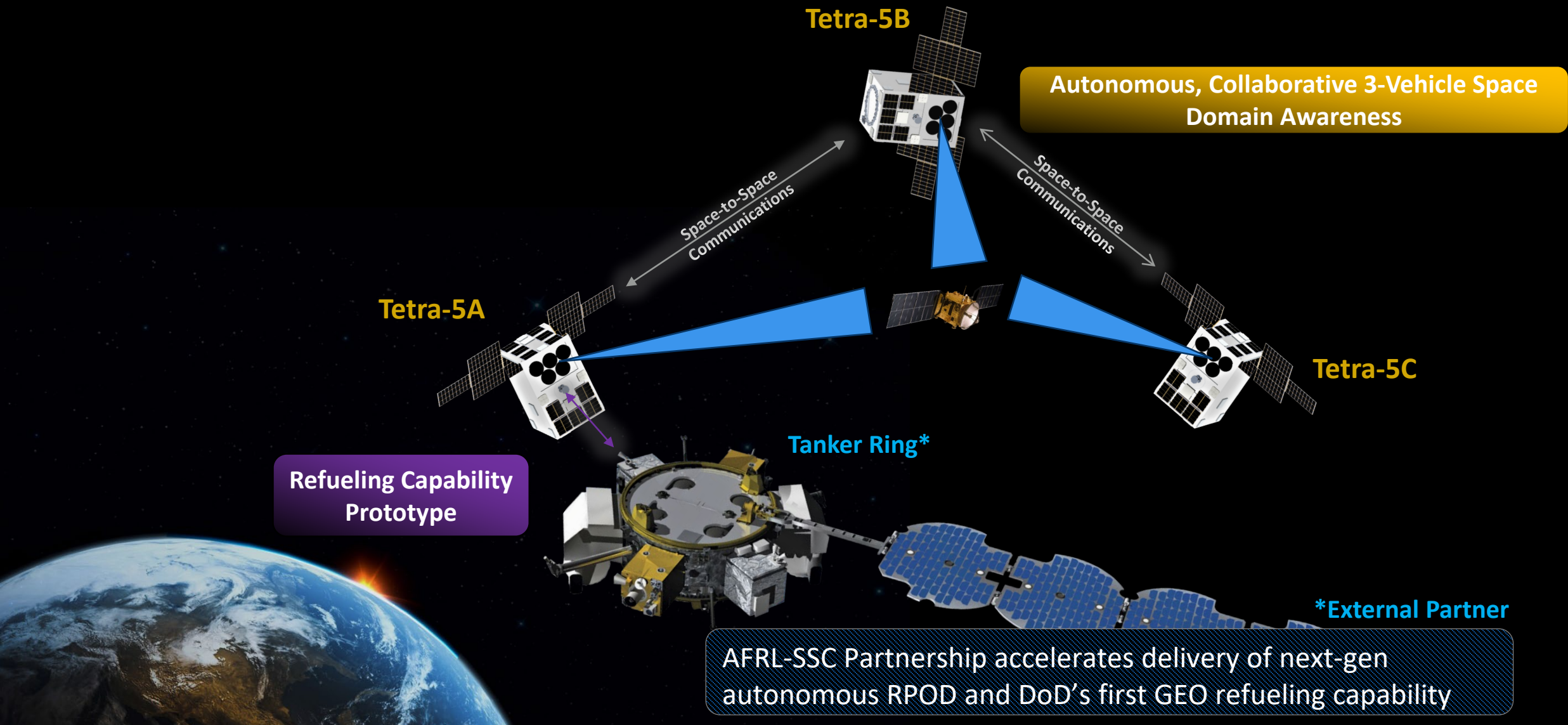
University Nanosat Program since 2004

2004	2010	2013	2015	2018
Delta-4 3-CornerSat Arizona State University, New Mexico State University, and University of Colorado-Boulder NS-1/2	STP-S26 FASTRAC University of Texas-Austin NS-3	Falcon 9 CUSat Cornell University NS-4 DANDE U Colorado-Boulder NS-5	ORS-3 Ho'oponopono* University of Hawaii NS-6 Copper* St. Louis University NS-6	ORS-4 Argus* St. Louis University NS-7 Electron CHOMPTT* University of Florida NS-8
2019	2020	2021	2021+	
STP-2 Falcon Heavy Oculus-ASR Michigan Technological University NS-6 Prox-1 Georgia Institute of Technology NS-7	ARMADILLO* University of Texas-Austin, Georgia Institute of Technology NS-7	Electron ANDESITE* Boston University NS-8 LauncherOn* University of Colorado-Boulder NS-8	TBD MAXWELL University of Colorado Boulder NS-9 MOCI University of Georgia NS-9	GLADOS State University of New York at Buffalo NS-8 MSAT Missouri University of S&T NS-8



Recurve: Advanced mesh radio

Tracker Prime/Tetra-5 OV-1



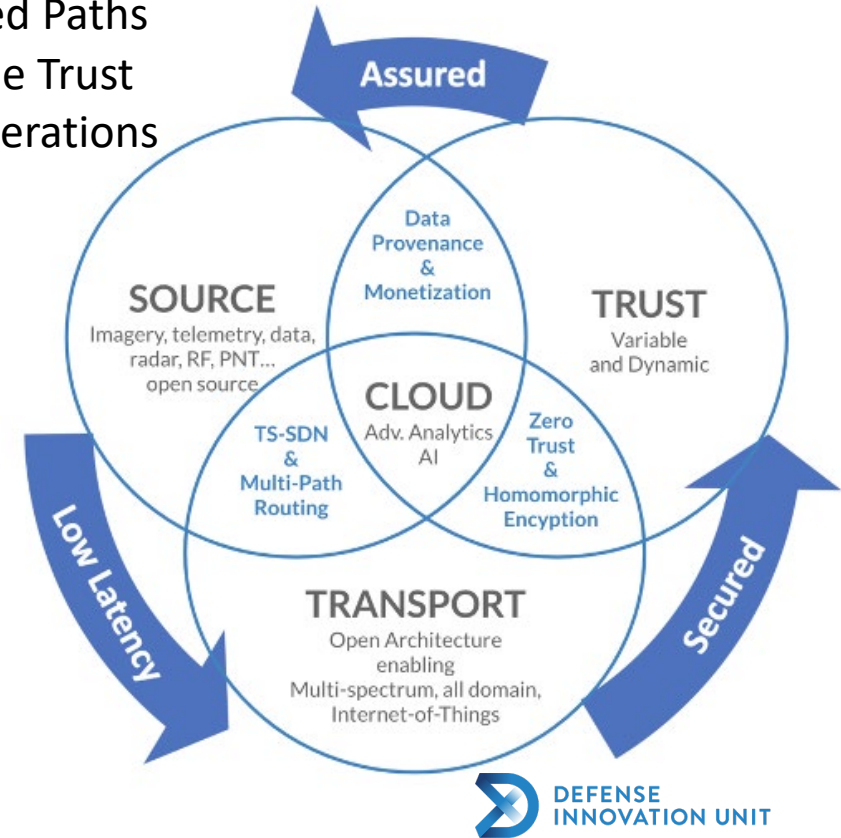


RAPID and Space Data Transport



How to Bring Resilient Persistent SATCOM to the Joint Fight?

- Broadband, Internet of Things
- Multi-Orbit / Decoupled Paths
- Cybersecurity / Variable Trust
- Advanced Network Operations

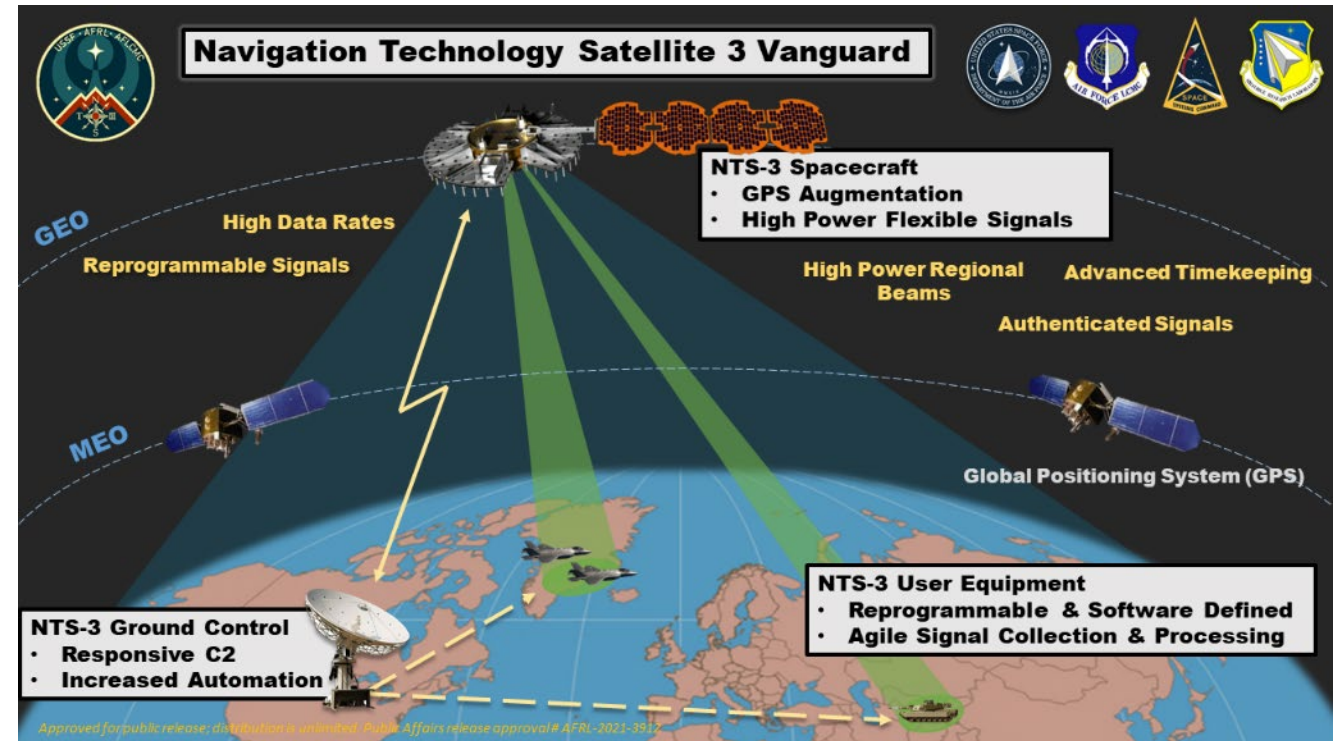


We are meeting commercial where they are: In the cloud...



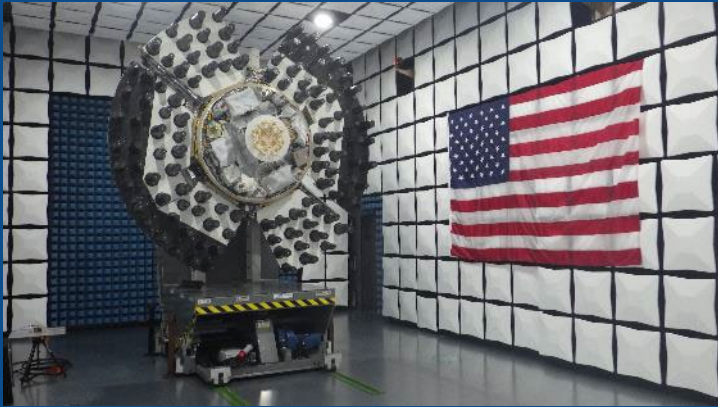
Resilient & Flexible Satellite Navigation (NTS-3)

- NTS-3 is the first integrated, end-to-end US SATNAV demo in almost 50 years
- Testbed for agile, reprogrammable SATNAV
- Seek warfighter access to trusted PNT in contested domains
- One element of a diversified future US architecture for positioning, navigation, and timing (PNT)
- Leverages innovations in communications with increased flexibility and automation throughout all segments



NTS-3 Technologies

Reprogrammable Satellite Transmitter



Responsive Ground Control

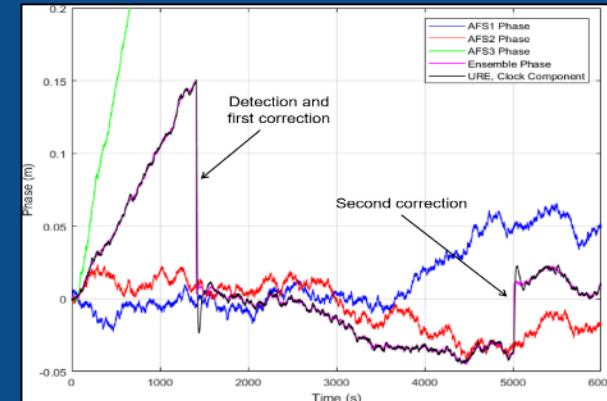


Credit: USAF

Software-Defined User Equipment

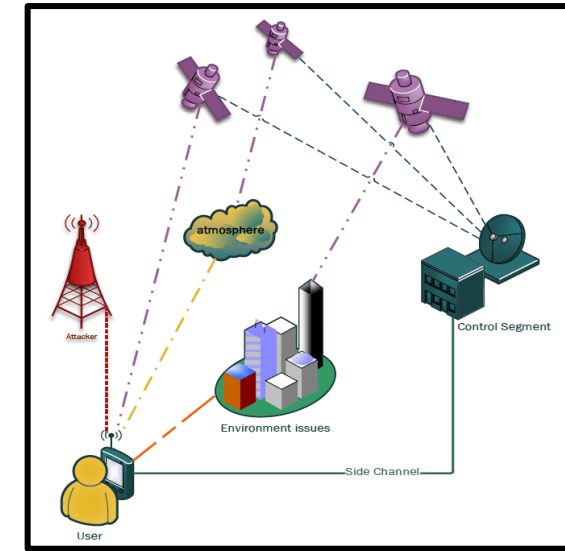


Automated Onboard Clock Anomaly Mitigation

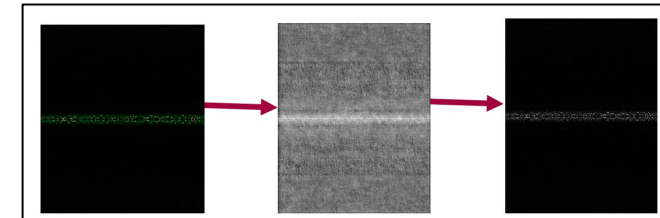


Machine Learning for PNT Resilience

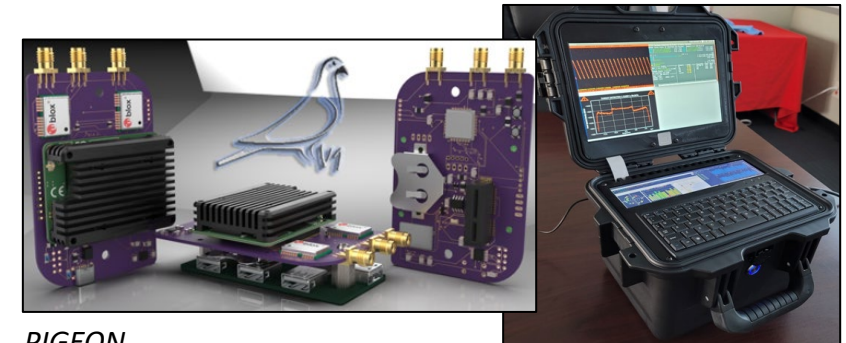
- Adversarial PNT attacks (jamming, spoofing) are becoming more common
- Project Goal: Use AI/ML methods to close the PNT OODA loop rapidly (CNN's)
- Challenge: Lack of contested environments datasets
- Portable Intelligence Gathering Experimental Observation Node (PIGEON) – edge node sensor
 - ID, classify, recommend PNT COA
 - Variational Autoencoder - 95% I/Q data size reduction w/out performance loss
- Machine Learning Toolset O/S (MLTos)
 - Provides ground truth datasets & tools for testing and evaluating models
- PIGEON & MLTos h/w and s/w developed are Gov't IP
 - Distributable under Distro-D (DOD/DOD Contractors)



PNT OODA Loop



Data Size Reduction via VAE



PIGEON

MLTos (laptop)

Hack-A-Sat: Satellite Security Innovation Through Competition

Why Enlist a Cadre of International Hackers to Compete?

Democratization of space

/// Space is no longer just accessible to governments

Make cyber security a priority for space

/// Emerging national security threat: security posture of space systems

Bridge the culture gap between space and cyber security communities

/// conversely: computing, automotive, medical, internet of things

Increase partnership with non-traditional industrial base

/// economies of scale: build commercial innovation base, not just defense industrial base



Hack-Sat 1:

Flat-Sat based competition with one indirect On-Orbit challenge.



Hack-A-Sat 2:

Flat-Sat based competition with Digital Twin access for testing.



Hack-A-Sat 3:

Build and launch Moonlighter and host a competition on Moonlighter FlatSat

Hack-A-Sat 4 & Beyond:

Moonlighter makes possible a future Hack-A-Sat series of events with highly realistic challenges focused on an on-orbit satellite.





Summary

- The Space Domain is a domain of competition
 - Economically & Geopolitically
- It is not yet a domain of conflict
 - AFRL's job is to have options for the US if that changes
- Use of AI/ML/autonomy in contested domains is complicated
 - Co-opting, herding, war-reserve modes, probing, GAN, ...
- AFRL is a leader in autonomy, and a “fast follower” on AI/ML
 - Projects demonstrating new space comm & PNT capabilities
 - Experiments providing data on architectures & integration
 - Actively looking for partners in space networking arena!



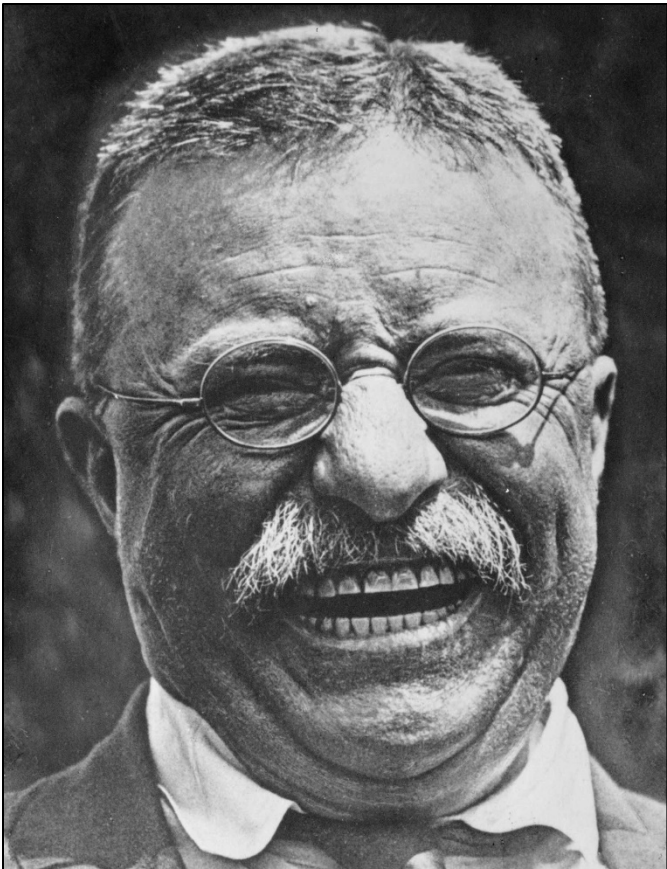
Collaboration Opportunities

- **Space Technology Partnership (NASA, USSF, IC)**
 - Trusted Space Autonomy topic area
- **AFRL Scholars Program**
 - <https://afrlscholars.usra.edu/>
- **NRC Research Fellows** (post-doc & faculty fellows; open to **industry** participants also!)
 - https://sites.nationalacademies.org/PGA/RAP/PGA_046587
- **Visiting Scientist Program** (AFRL S&E visits you)
- **Cooperative R&D Agreements** (CRDAs – Industry)
- **Educational Partnership Agreements** (EPAs – academia)
- **Memorandums of Agreement/Understanding** (MOA/MOU – gov't-gov't)
- **Small Business Innovative Research/Technology Transfer** (SBIR/STTR)

Contact me for more info or to find someone to work with: richard.erwin@spaceforce.mil



Last Thoughts...



"In any moment of decision, the best thing you can do is the right thing, the next best thing is the wrong thing, and the worst thing you can do is nothing."

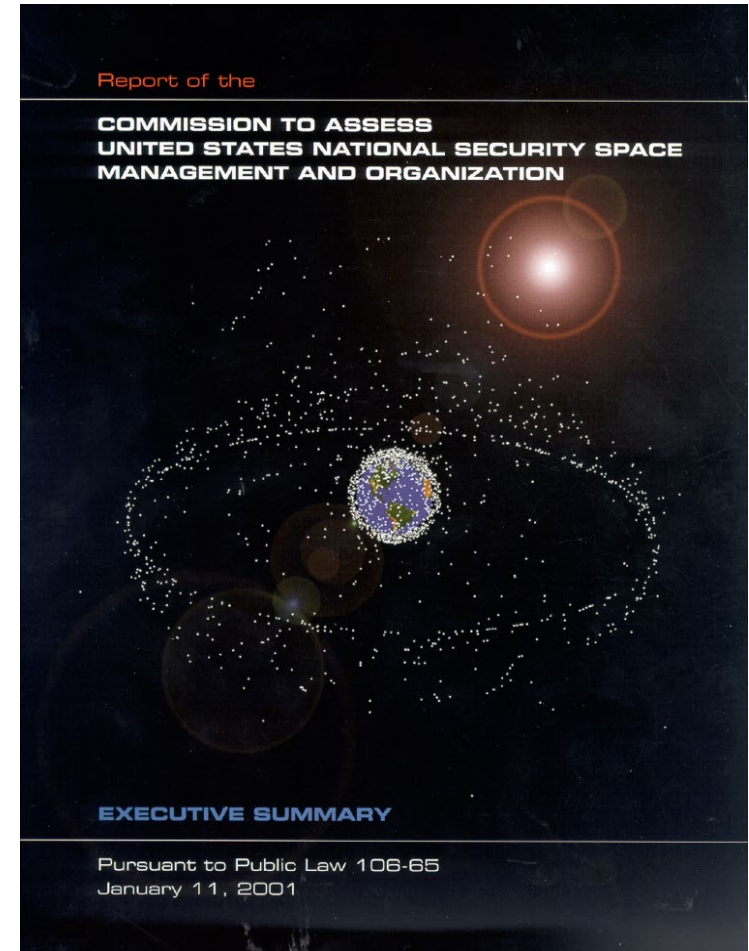
-- Teddy Roosevelt

Questions?



Rumsfeld Commission Report (2001)

- Space is spread across such a diverse set of agencies in the Government, that only the Office of the President of the United States has the power to set any kind of coherent National Space Policy
- Current DoD and IC Space Programs are not aligned with future challenges; only with Senior Leadership attention can the efforts be aligned and the required funding obtained
- The SecDef and the (then) DCI (now ODNI) must coordinate efforts in order to ensure that the whole of Government can be used to proper effect in the complex and changing space domain
- “Fourth, we know from history that every medium—air, land and sea—has seen conflict. Reality indicates that space will be no different. Given this virtual certainty, the U.S. must develop the means both to deter and to defend against hostile acts in and from space.”
- “Finally, investment in science and technology resources—not just facilities, but people—is essential if the U.S. is to remain the world’s leading space-faring nation.



Space as a Domain of Conflict

A PRODUCT OF THE NATIONAL AIR AND SPACE INTELLIGENCE CENTER

COMPETING IN SPACE

NON-REVERSIBLE

- Ground Station Attacks
- Orbit Threats
- Direct Ascent Weapons
- Direct Interception
- Direct Sabotage
- Direct Attacks
- Direct Interference
- Direct Disruption

REVERSIBLE

DENYING SPACE

Society increasingly depends on the services provided by satellites. What if GPS and other services were unavailable or compromised? Satellites, launchers, and payloads, like any other technology, could be the target of an attack. The plan would be to deny, disrupt, or destroy the satellite and its services. This could be done by attacking the satellite itself, the ground station, or the communication links to complete transactions. Many critical services that daily consumers use only in could be affected by weapons targeting our space services.

- Adversaries may jam global navigation and communication satellites used for command and control of naval, ground, and air forces, to include essential and commercial vehicles.
- Weapons designed to target satellites, launchers, and communication capabilities may deny the ability to locate, monitor, track, and target the enemy. For example, there can temporarily or permanently blind enemy satellites and other strategic systems.
- Adversaries may use anti-satellite missiles to shoot down satellites in low Earth orbit. China used an anti-satellite missile against its own defense weather satellite in 2007. The result of a missile shooting down a satellite can produce debris that may threaten satellites in nearby orbits.
- A number of foreign countries are believed to be testing on-orbit space-based anti-satellite technology and concepts. China and Russia continue to conduct sophisticated on-orbit activities that may threaten counter-space capabilities.
- Physical attacks against ground sites and infrastructure that support space operations can also threaten satellite services. Cyber capabilities could target space systems and supporting infrastructure.

Space-Based Weapons

Some space-based anti-satellite systems are satellites that target other space systems. Concepts for space-based anti-satellite systems may include and include designs to deliver a spectrum of reversible and non-reversible counter-space effects. These concepts span from simple interceptors to complex space-based systems, and can include kinetic kill vehicles, radiofrequency jammers, laser, directed energy, high-power microwave, and robotic mechanisms.

Some space-based countries are testing or researching sophisticated on-orbit technologies for satellite servicing and debris removal. These technologies could also damage satellites.



Table 1
TYPES OF COUNTERSPACE WEAPONS

Type of Attack	Kinetic Physical			Non-Kinetic Physical			
	Ground Station Attack	Direct Ascent ASAT	Co-Orbital ASAT	High Altitude Nuclear Detonation	High-Powered Laser	Laser Dazzling or blinding	High-Powered Microwave
Attribution	Variable attribution, depending on mode of attack	Launch site can be attributed	Can be attributed by tracking previously known orbit	Launch site can be attributed	Limited attribution	Clear attribution of the laser's location at the time of attack	Limited attribution
Reversibility	Irreversible	Irreversible	Irreversible or reversible depending on capabilities	Irreversible	Irreversible	Reversible or Irreversible, attacker may or may not be able to control	Reversible or Irreversible, attacker may or may not be able to control
Awareness	None	None	None	None	None	Only satellite operator will be aware	Only satellite operator will be aware
Confirmation success	None	None	None	None	None	Limited confirmation of success if satellite begins to drift uncontrolled	Limited confirmation of success if satellite begins to drift uncontrolled
Control	None	None	None	None	None	None	None

CHINA

Number of Successful Orbital Launches in 2019¹⁹

32

"No force will stop or shake China or its people from achieving its goals!"
PRESIDENT XI JINPING, 2019²⁰

IN THE PAST DECADE, China has been barreling toward its lofty space goals. In the 2010s alone, China conducted over 200 successful orbital launches.¹⁹ China's civil, military, and commercial capabilities are rapidly growing, and its 2020 plans show that the country aims to launch over 60 satellites into orbit via 40 launches over the coming year.¹⁹

China's civil space program is focused on its network of BeiDou positioning, navigation, and timing (PNT) satellites, similar to the U.S. Global Positioning System (GPS). China plans on launching two BeiDou satellites into geostationary orbit (GEO) in 2020 as well as further developing its Gaofen remote sensing satellite constellation. Since early 2010, Chang'e-4, the Chinese lunar lander mission that delivered a successful lunar rover called Yutu-2, has been conducting an exploration mission on the far side of the Moon. China plans to follow up this mission in late 2020 with Chang'e-5, a mission that aims to return samples from the Moon back to Earth for further study. To support its growing space capabilities, China has "built an expansive ground support infrastructure to support its growing on-orbit fleet and related functions including spacecraft and space launch vehicle (SLV) manufacture, launch, C2 (command and control), and data downlink."²⁰

China also intends to send a mission to Mars with an orbiter and probe. This mission will include 13 science payloads and is on track for a July 2020 launch.¹⁹ Three different launch vehicles are also scheduled to make their first flight in 2020: the Long March-5B, the Long March-7A, and the Long March-8.

SPACE THREAT ASSESSMENT 2020

National Air & Space Intelligence Center, *Competing in Space*, 2018, 15 pages

Center for Strategic & International Studies, *Space Threat Assessment 2020*, 80 pages



United States Space Force (est. 20 Dec 2019)

• Mission:

- Organize, train, and equip (OT&E) space forces in order to protect U.S. and allied interests in space and to provide space capabilities to the joint force. Its responsibilities include developing military space professionals, acquiring military space systems, [maturing the military doctrine for space power](#), and organizing space forces to present to the Combatant Commands

• Specifically responsible OT&E of forces for the following mission sets

- [space superiority](#); space domain awareness (military, civil, and commercial); [offensive and defensive space control](#); command and control of space forces and satellite operations; space support to operations (e.g., satellite communications); space service support (e.g., spacelift and space range operations for military, civil, and commercial operators); space support to nuclear command, control, communications and nuclear detonation detection; and missile warning and space support to missile defense operations.

• Functions

- Provide freedom of operation for the United States in, from, and to space
- Provide prompt and sustained space operations

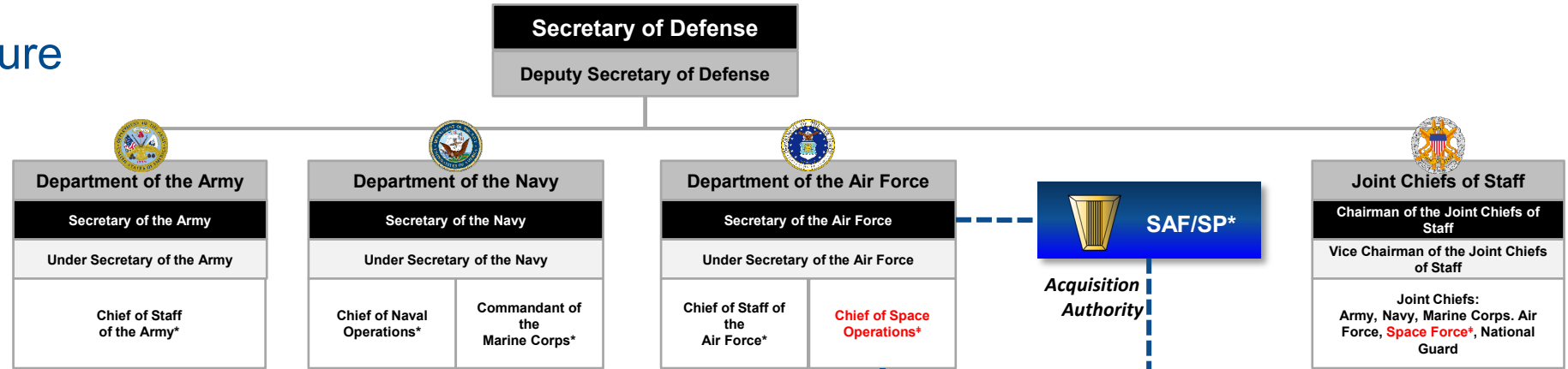
• Duties

- Protect the interests of the United States in space
- [Deter aggression in, from, and to space](#)
- Conduct space operations



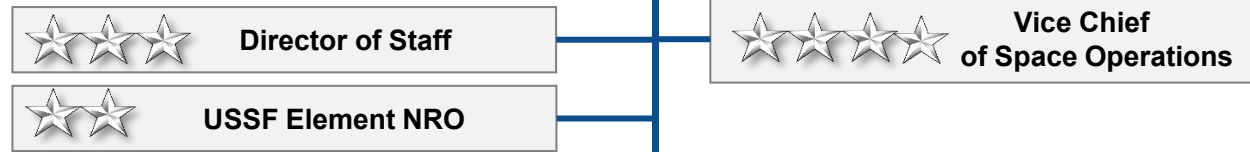


The USSF Structure

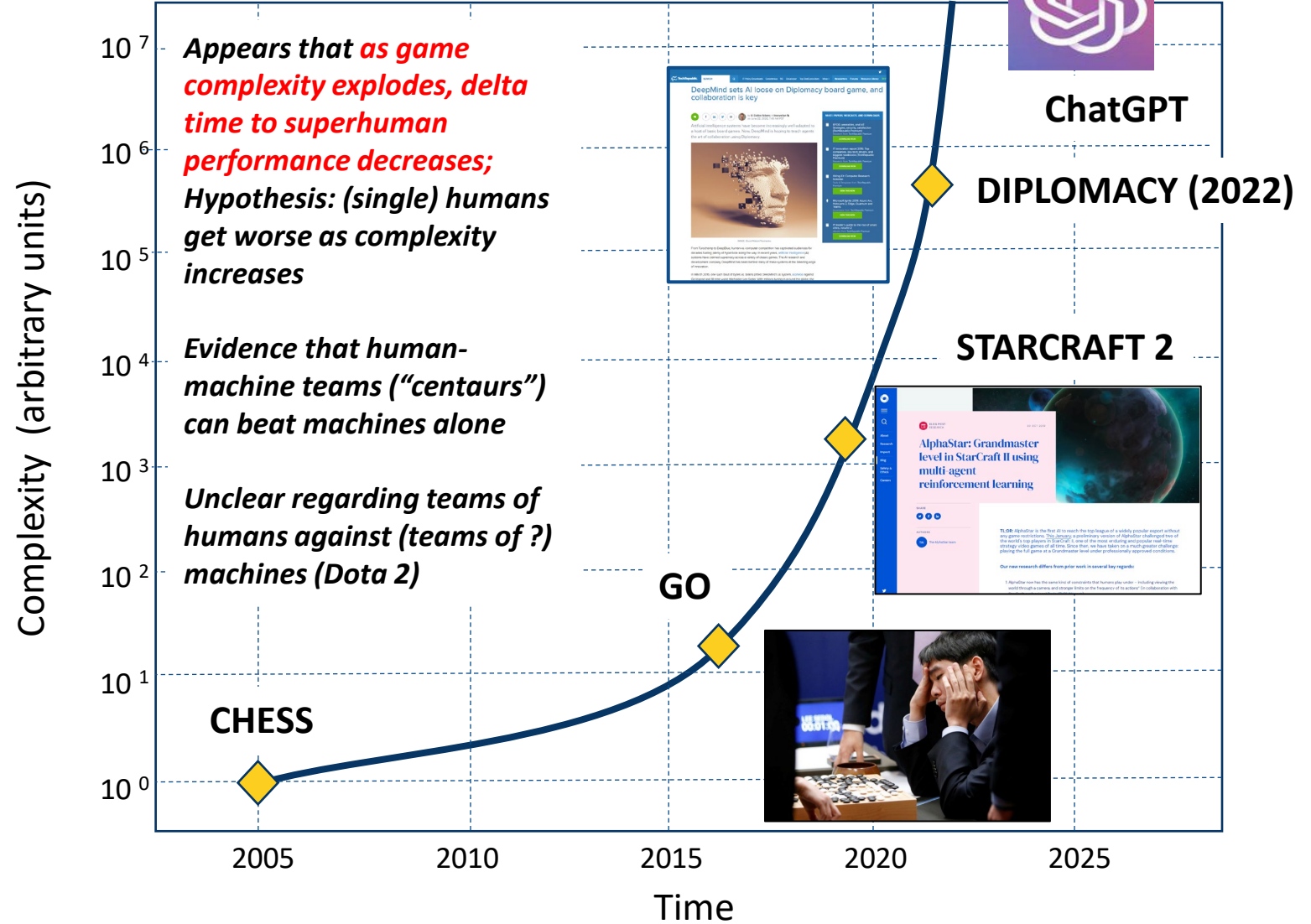
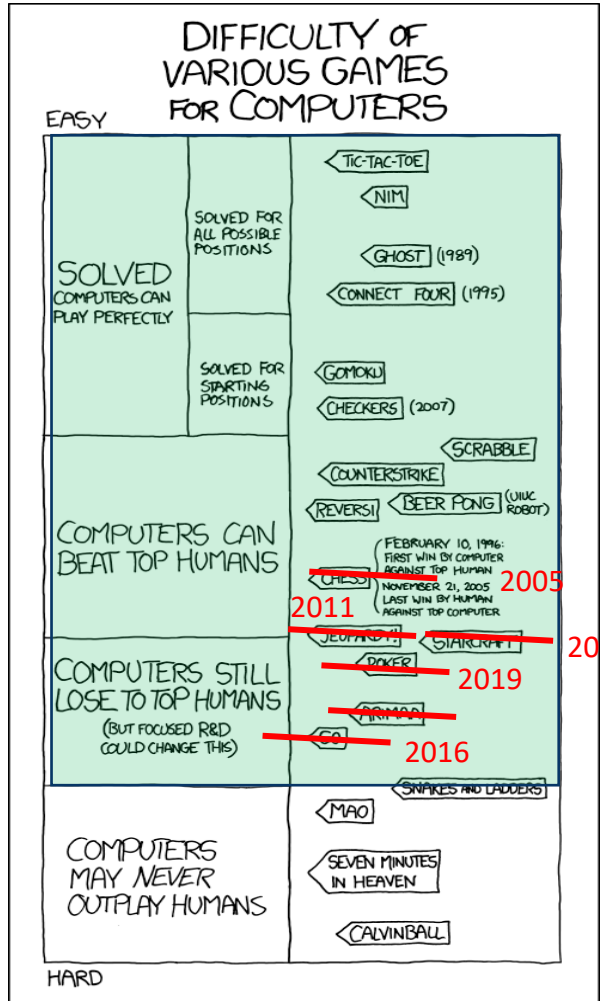


*JCS member

* Invited by the CJCS to participate in the JCS process in anticipation of his membership on the JCS a year after the enactment of the NDAA for FY 2020



Machine Learning Tech

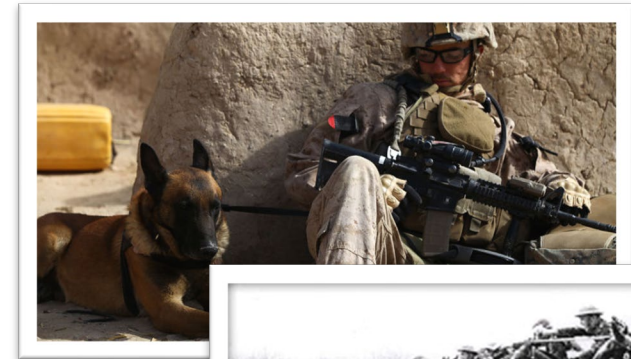




Trust in Autonomy

(will we let it be autonomous?)

- What is right model/analogy?
- Suggestion: Humans trusting non-humans
 - Esp. in war situation: dogs, elephants, horses, birds
 - Human has to establish trust with a non-human intelligence
 - Perfection is not a pre-requisite for use (Horses killed 20 people in the U.S. in 2015; dogs: 31)
 - Problem: can't imprison/execute/sue machines (no closure)



Machines are not humans – need to look beyond human-to-human trust models for synthetic autonomous systems