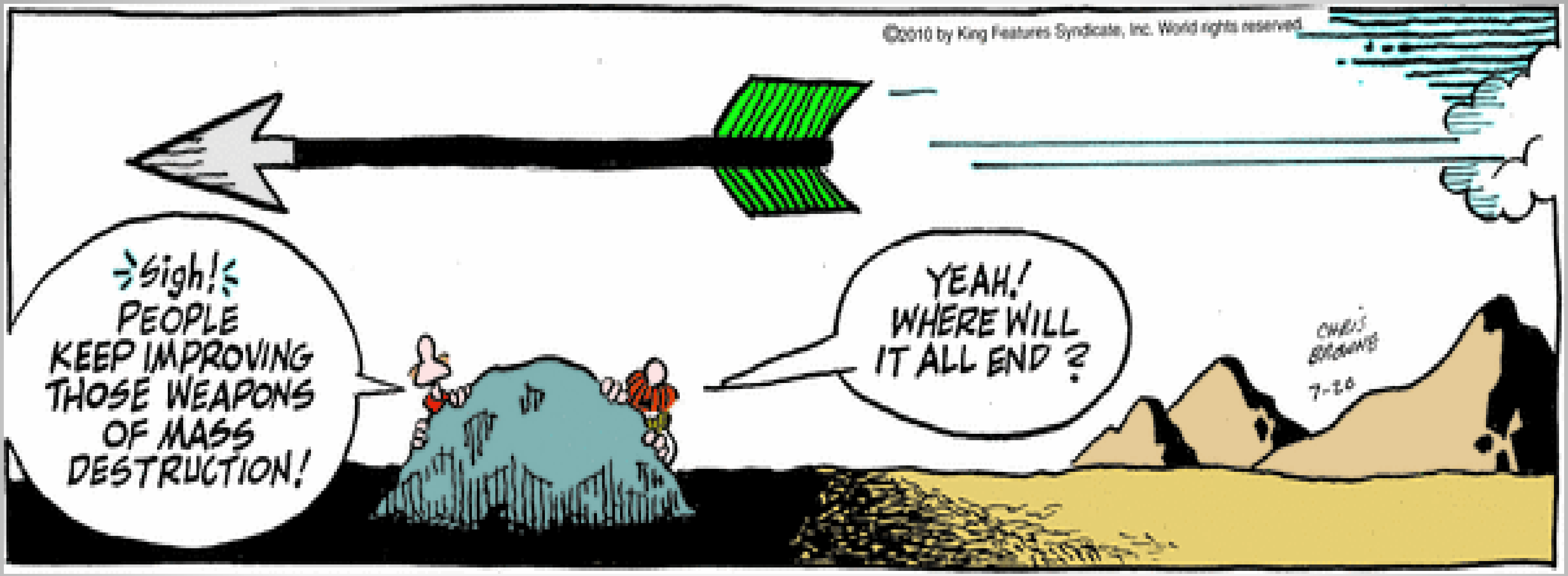
Cleared for Public Release
The presentation has been reviewed for security and policy IAW AFI 35-102
CASE NUMBER: AETC-2010-0992
SUBJECT: Blue Horizons IV: Deterrence in the Ager of Surprise (Slide Presentation)

Blue Horizons IV
Deterrence in the Age of Surprise (AY 10)

Slides are UNCLASSIFIED

Thesis Question



Sigh! PEOPLE KEEP IMPROVING THOSE WEAPONS OF MASS DESTRUCTION!
YEAH! WHERE WILL IT ALL END ?
CHRIS BROWNE 7-26

Answer:

Never!

Thesis Question (Restated)

How should the Air Force posture itself to best deter attacks using nanotechnology, biotechnology, directed energy, nuclear weapons, and attacks in space and cyberspace in the 2030-2035 timeframe from nation-states, groups and individuals?

- This is more than merely an Air Force problem -- but the Air Force has a major role to play
- This is a wicked problem -- but we can't not do this

It is a briefing more about ideas than things – requiring changes today to create substantial effect by 2035

This briefing – culminating 4 years of research – is about DETERRENCE…

…combining operational expertise with academic rigor to identify the USAF’s principal challenges in 2035…

…but it’s is also about a set of ideas to refine the direction of the AF to be relevant and valuable to the nation

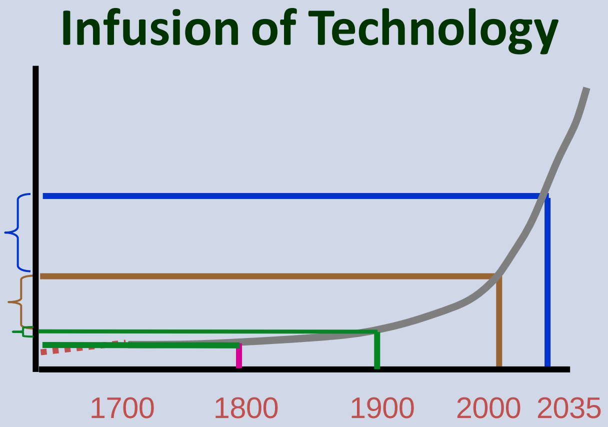
Overview

- Enduring Truths and Threats
  - Previous Blue Horizons Findings
- Methodology for the 2010 Study
  - Who, What, How
  - The Structure of Deterrence
- Delphi Results
- Implications for the USAF

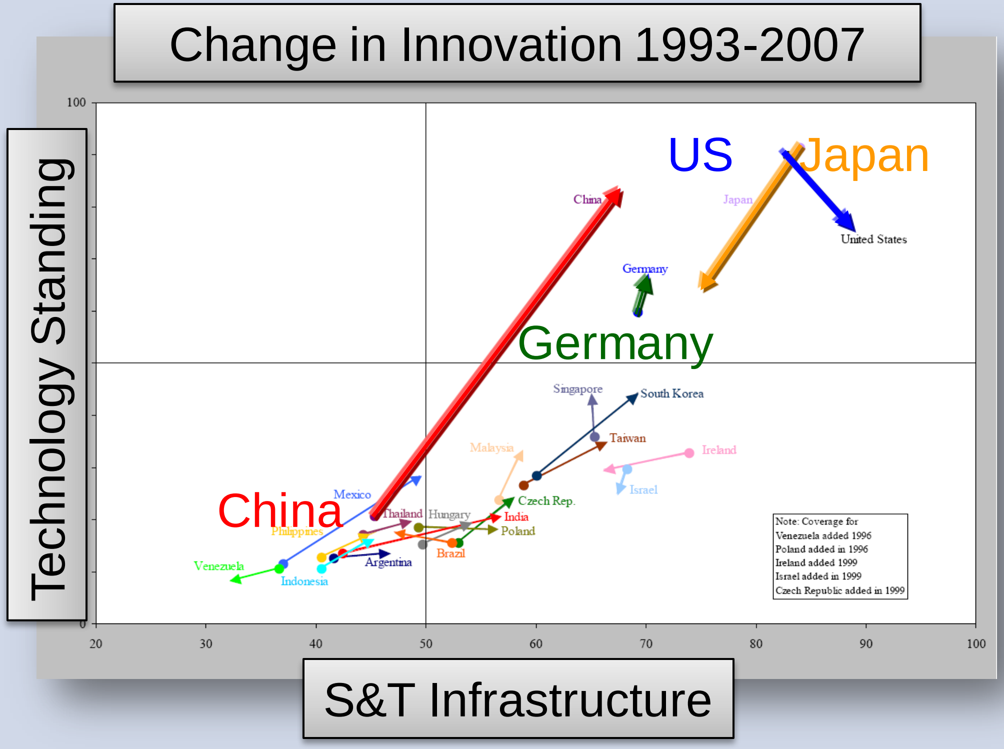
Overview

- Enduring Truths and Threats
  - Previous Blue Horizons Findings
- Methodology for the 2010 Study
  - Who, What, How
  - The Structure of Deterrence
- Delphi Results
- Implications for the USAF

Enduring Truths

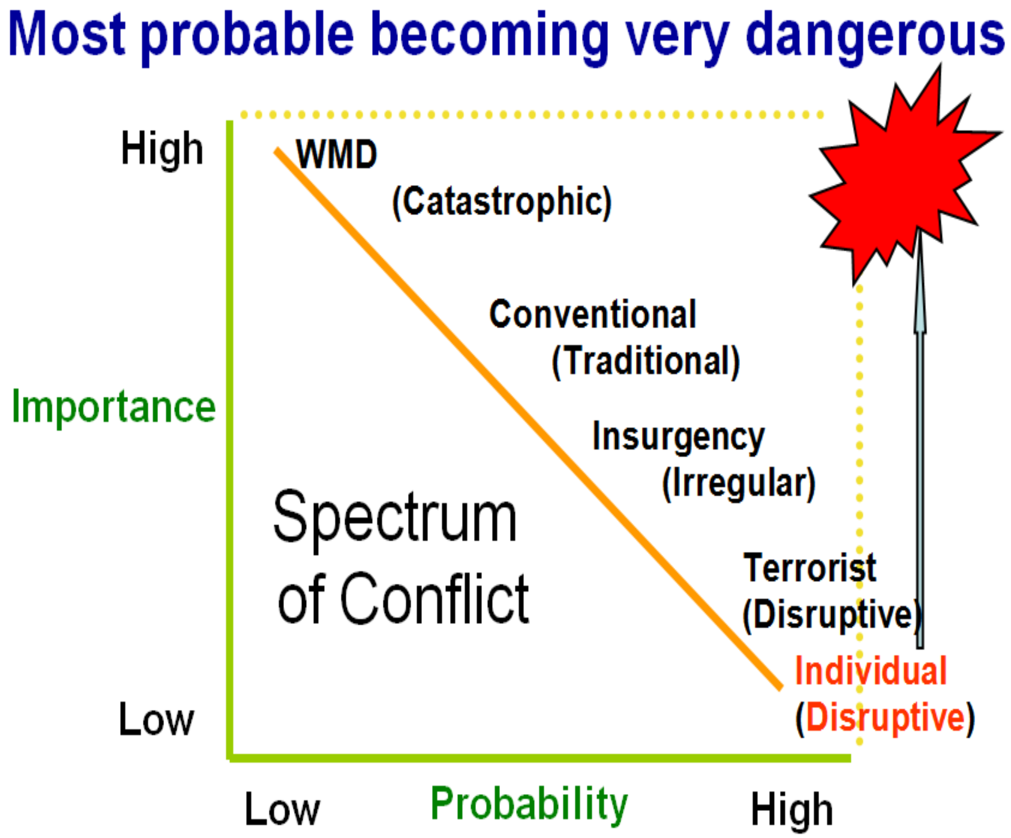
Truth	Effect
Tech change inevitable and accelerating	 Amount of new technology introduced 1800 - 1900 Amount of new technology introduced 1900 - 2000 Amount of new technology introduced 2000-2025

Enduring Truths

<table>
<tr><th>Truth</th><th>Effect</th></tr>
<tr><td>Tech change inevitable and accelerating</td><td rowspan="4">


NSF Study by Georgia Tech, 2008
</td></tr>
<tr><td>Dominance no longer possible</td></tr>
<tr><td></td></tr>
<tr><td></td></tr>
</table>

Enduring Truths

Truth	Effect
Tech change inevitable and accelerating	
Dominance no longer possible	
Devastating power moving from nation to group to individual	

Result: Number of Pertinent Actors Increases

The old threat paradigm: ***Nations*** -- 192 Nations in the United Nations

The new threat paradigm: ***Groups*** – in the 10,000s?

The emerging threat paradigm: ***Individuals*** ~ 8,000,000,000+

Machine Agents ~ ???

This exponential increase in the number of actors transforms deterrent calculus from a "simple" bilateral or multilateral problem to a chaotic challenge

Result: The super-hybrid threat presents a far more complex deterrent challenge

Enduring Truths

Truth	Effect
Tech change inevitable and accelerating	**Science & Technology Driven By** • Profit • Political/social pressures • Scientific curiosity • Military requirements **Facts to Contemplate** • ~70% of US R&D privately funded • ~76% of all R&D outside of US **Conclusion** • US Government has little say over what is developed, who gets it or how it will be employed
Dominance no longer possible	
Devastating power moving from Nation to Group to Individual	
US Government has little control over shape, direction or proliferation of technology	

Future of Humanity is an Old Story

Human evolution presents a puzzle. No one thing seems to explain humanity's sudden takeoff in the last 45,000 years.

The answer lies in an idea borrowed from economics, **collective intelligence**: the **amount of interaction between individuals** that determines a population's inventiveness and rate of cultural change.

Humans' story has been the gradual spread of specialization and exchange. Prosperity consists of **getting more narrow in what you make and more diverse in what you buy.**

--Matt Ridley, *Wall Street Journal,* 22 May 2010

How Collective Intelligence Will Change The Character of Future Threats

- ✓ Collective intelligence generates innovation fostering specialization
- ✓ Globalization harnesses more minds, accelerating interactions
- ✓ As more people (or machines) interact, innovation increases exponentially

What's Different About Deterrence in 2035?
Collective intelligence generates new capabilities at an accelerating pace, creating new concepts and systems barely imaginable today
Number of actors with power to challenge the state multiplies
Machines become decision makers —possibly eclipsing humans
Nano and biotechnology applications become disruptive

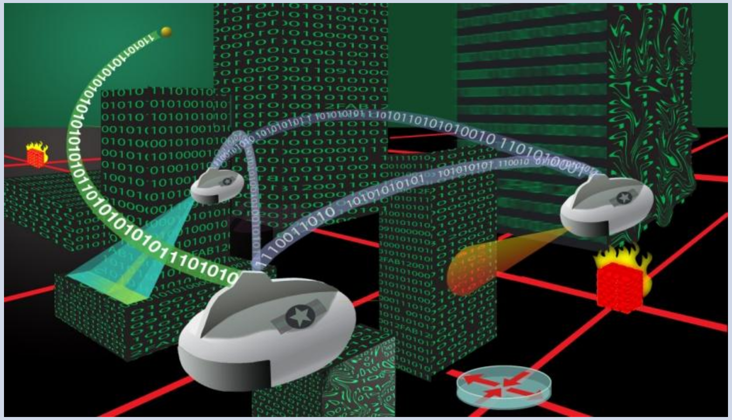
Harsh Realities

We Are In An Age of Surprise

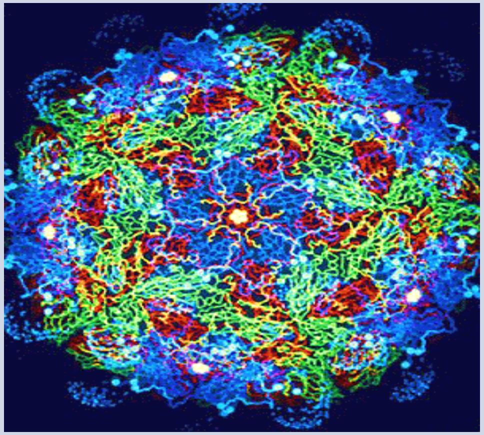
- ✓ Moving into a world we did not expect, doing things we did not plan to do with old enemies that have become new friends
- ✓ Exponential growth of technology has dramatically altered the threat landscape
- ✓ This chaotic, rapidly changing world is a reality with which we must deal
- ✓ Therefore the AF must continue to anticipate

AF must expand its view of threats, reallocate resources to counter the unexpected, embrace all consequences from focus on ISR and accept leadership in the type of warfare expected in 2035

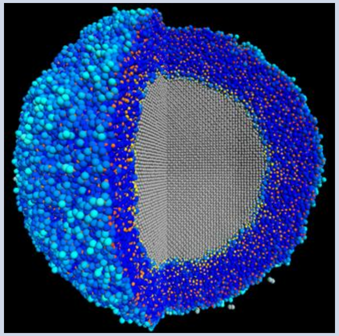
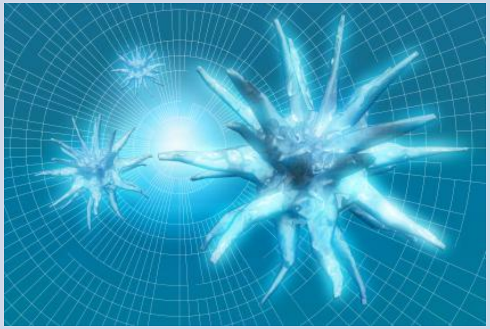
Cyberspace

Examples	Implications
Much of national critical infrastructure, on which USAF depends, is vulnerable--no business case to address – “it’s an insurance problem”	 • AF has a major stake in protection of national critical infrastructure • Study will show deterrence hinges on “transparency” & ISR • ISR in cyberspace must be accomplished across the range of potential actors
We are constantly under attack from actors ranging from individuals to nation-states now	
Cyberspace is where most ISR will be done in the future, and ISR is the original and traditional Air Force mission	

Biotechnology

Examples	Implications
Human Genome was fully decoded in 2003. Human Proteome Project completed first phase on September 23, 2010	 • Two ways to address this threat: • Never let it occur, by creating an environment of transparency… or • USG must be able to genetically decode the virus; rapidly prototype a vaccine; mass produce the vaccine, and distribute it nation-wide… all in 72-96 hours (vice 9 months for H1N1)
By 2025, genetically engineered cures to many diseases will be available	
…By the same time, a well-trained graduate student in microbiology will be able to engineer a deadly virus for which no immunity is even possible	

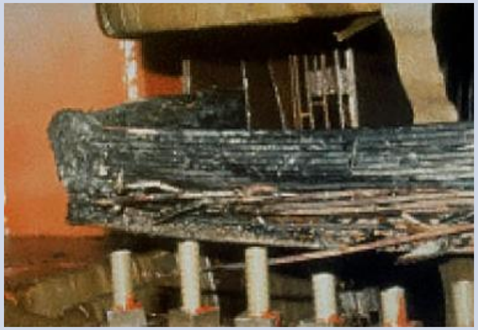
Nanotechnology/Nano-Energetics

Examples	Implications
Nano-energetics can theoretically improve conventional explosives 50 to 1000 fold; 5-10 fold in near term	  • Conventional weapons may attain nuclear-level yields (2000 pound bomb with 5-10 KT yield) – What is a WMD? • Small “dime”-sized explosive can destroy a civilian aircraft in flight • Corrosives can destroy vital AF systems
Nano-engineered corrosives cause rapid deterioration of metals and/or composite materials	
Nano fuels – less weight, increased power, solves logistics problems	

Nuclear Weapons

Concern	Implication
Traditional concerns about state use of nuclear weapons apply	 • While technology is “old” infrastructure costs are high – clearly not in the purview of individuals • Proliferation increases chances for a group to buy/steal a device
“Nuclear club” now stands at 9. Iran and Myanmar may both be close to joining	
Technology pre-dates the Edsel by 15 years; it is old; it is not “hard”; it will proliferate	

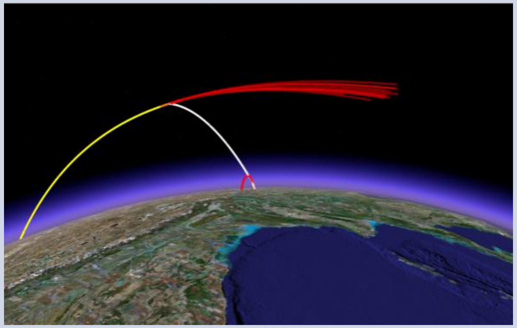
Directed Energy – HPM or EMP

<table>
<tr><th>Examples</th><th>Implications</th></tr>
<tr><td>Electrical grid vulnerable to stray voltage caused by HPM, EMP, and Solar Flares</td><td rowspan="3"> 
• Almost no civilian & few AF systems are hardened
• EMP or major solar flare (Carrington Event) are worst case scenarios
  • Solar flare is inevitable
  • Grid off-line – possibly for years
  • Civil disorder, significant deaths</td></tr>
<tr><td>Banking, utility, telephone, air traffic control, water systems all similarly vulnerable</td></tr>
<tr><td>We have comm-out recall procedures. Do we have comm-out deployment procedures? … Comm-out TPFDD development procedures?</td></tr>
</table>

Directed Energy – Lasers

Examples	Implications
Marginally-lethal and permanently-blinding hand-held lasers are already on the commercial market. Arctic Laser at right sells for ~$300	 • 299 attacks against aircraft in U.S. from Jan-Sept 15, 2010; 2700+ more by end of year • Blinding incidents on roadways in Germany • AC-130 Laser bored a hole through a Ford F-150 engine block
Diode and fiber-optic lasers both surpassed 100 KW levels in 2009	
AC-130 ATL successfully tested in 2009. China, India, Russia, and others have advanced programs – megawatt class coming	

Space

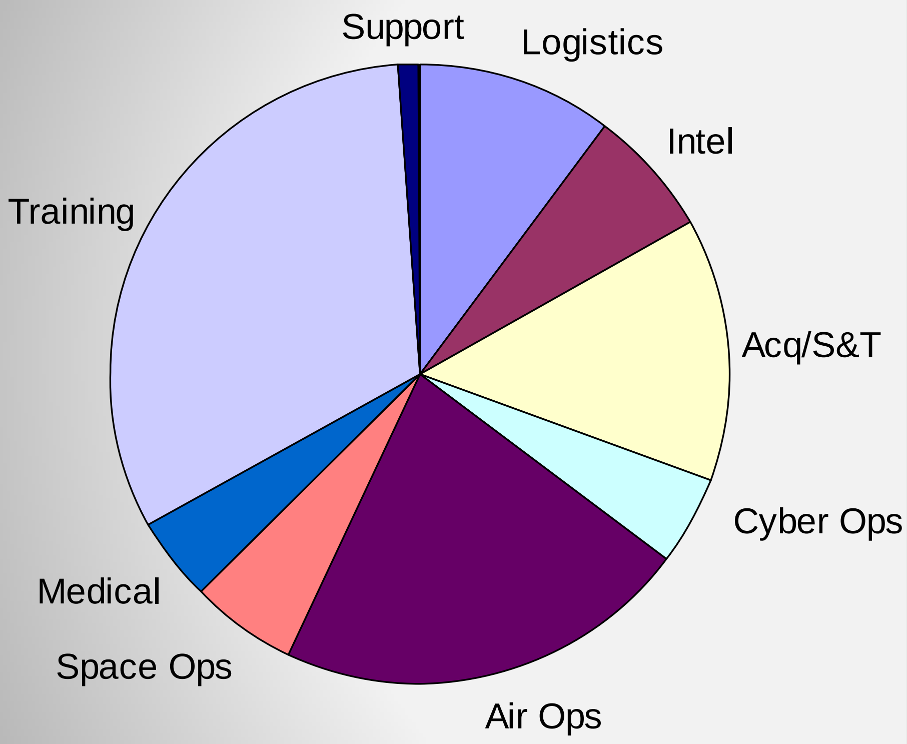
Examples	Implications
Space assets, military & civilian, vulnerable to attack from ground and space	 • Military ISR, communications, and some strike (Predator) capabilities at risk • Civilian critical capabilities (timing for banking, telecommunications, etc. at risk)
Little effort to harden civilian or military satellites	
Satellites vulnerable to attacks by direct ascent, directed energy, or attack satellites	

Overview

- Enduring Truths and Threats
  - Repeat Findings
- Methodology for the 2010 Study
  - Who, What, How
  - The Structure of Deterrence
- Delphi Results
- Implications for the USAF

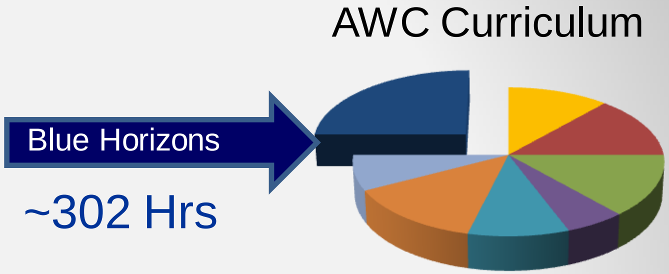
Blue Horizons 2010
Deterrence Study

Student Composition



19 Students…Top 12% of Cohort

Academic Program



~302 Hrs

• Classroom	60 Hrs
• Volunteer Elective	24 Hrs
• Research Paper	136 Hrs
• Group TDYs	~70 Hrs
• Sandia Nat'l Lab	
• Los Alamos Nat'l Lab	
• NASIC	
• AFRL Tech Directorates	
• Individual research TDYs	~12 Hrs

Study Design

Category	Nano	Nuclear	DE	Space	Cyber	Bio
Nation						
Group						
Individual		✗		✗		

- Students conducted research in 16 areas listed above
- Then developed findings utilizing a Delphi methodology
  - Two questionnaire rounds, 3528 discrete responses
  - Explored:
    - Difficulty of deterrence
    - Criticality of different types of undeterred attacks
    - Probability of different types of undeterred attacks

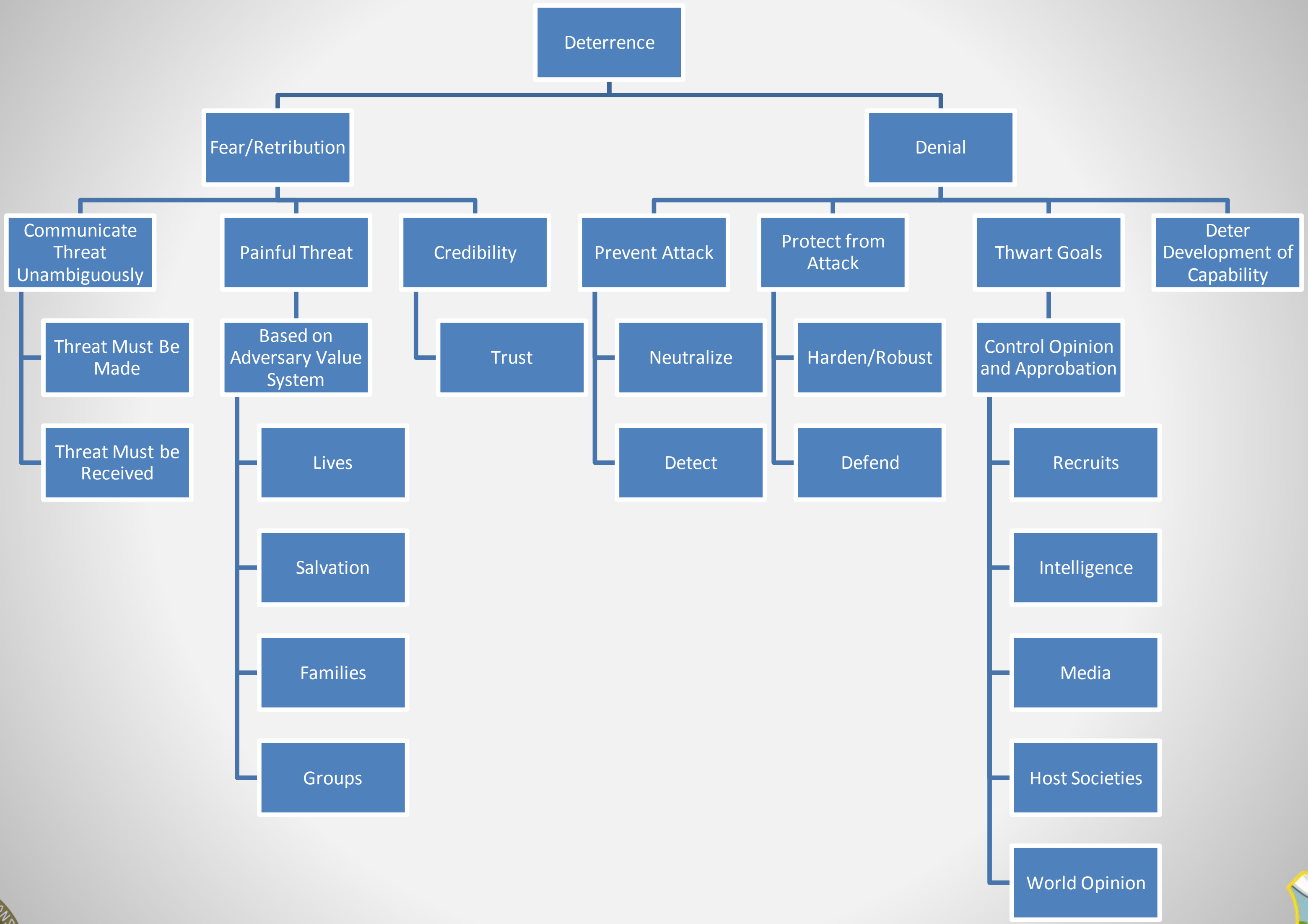
Threats Considered

Study's Scope

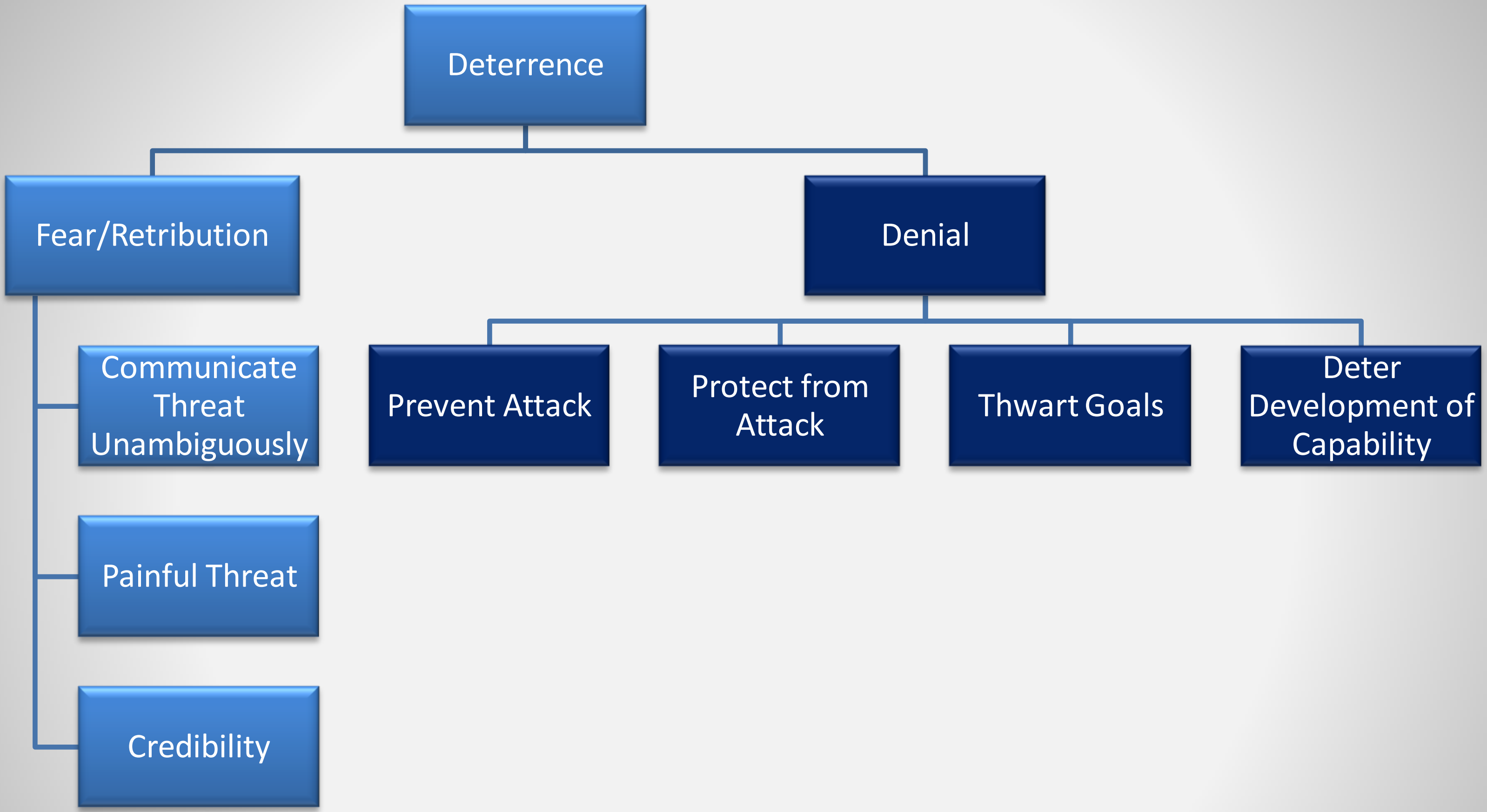
Threat	Definition
Catastrophic	Threatens national survival – eliminates USAF ability to accomplish its mission
Destructive	Seriously impacts US ability to function – significantly degrades USAF ability to perform its mission
Disruptive	Selectively impacts US regions/capabilities – affects USAF ability to complete its mission tasking
Nuisance	Often high psychological impact – low effect on mission accomplishment

The Delphi study revealed significant disagreement over definitions…reflects difficulty of discerning implications of future threats

Drew Upon Deterrence Theory



…Especially the Big Pieces



Deterrence As We Know It Today

An actor (nation-state, group, or individual) is deterred if:

Adversary's Assessment of Success
Probability x Value

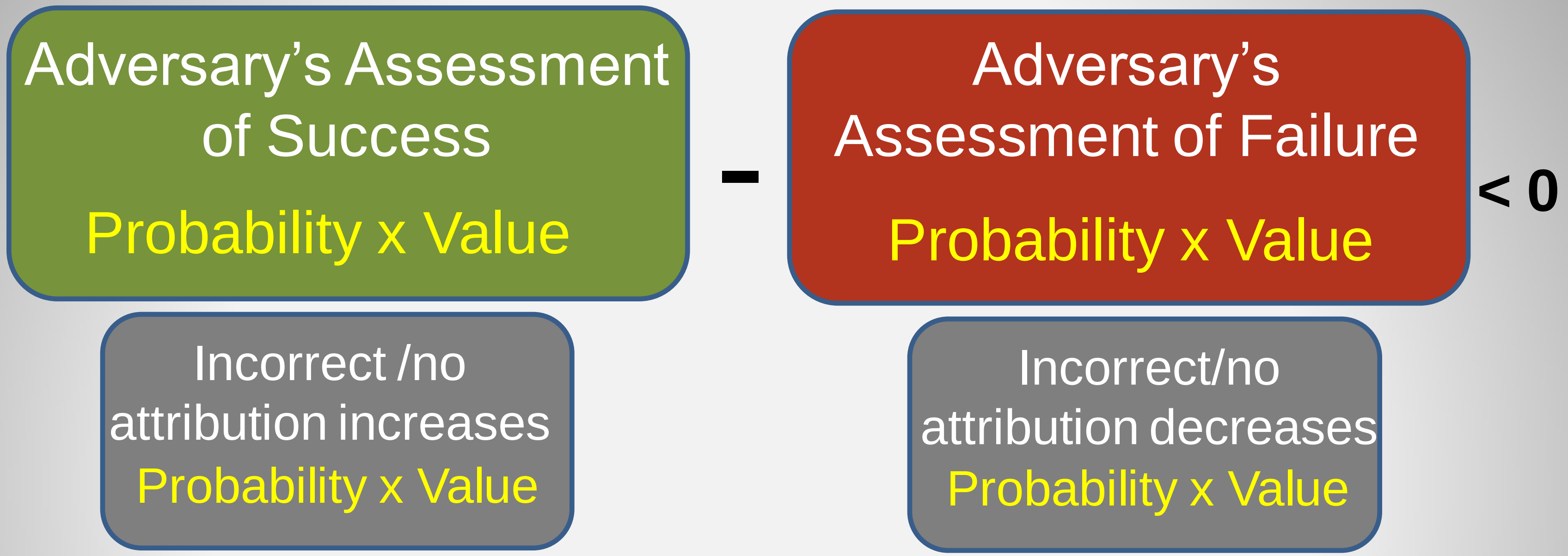
–

Adversary's Assessment of Failure
Probability x Value

< 0

- Grounded in risk of retribution (Deterrence by Punishment)
- Grounded in efforts to deny success (Deterrence by Denial)
- Assumes actors have a rational calculus
- Assumes attribution is non-problematic

New Challenges to Deterrence



Adversary's Assessment of Success

Probability x Value

-

Adversary's Assessment of Failure

Probability x Value

< 0

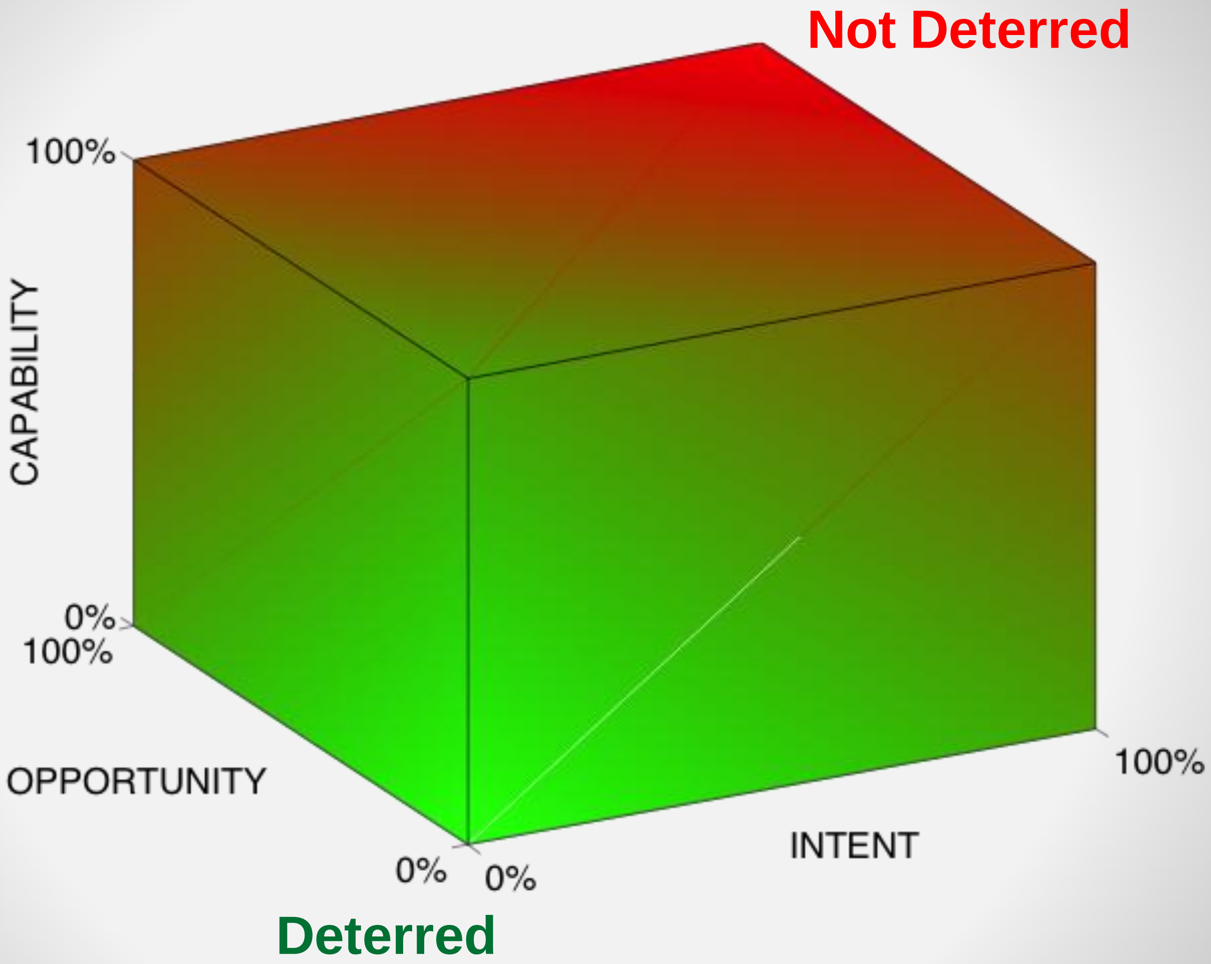
Incorrect /no attribution increases Probability x Value

Incorrect/no attribution decreases Probability x Value

- As attribution difficulty increases, probability of successful deterrence decreases
- If actors deflect blame to a third party, response based on "assumed attribution" can lead to unnecessary conflict

Getting attribution right is critical, both to deter and to avoid unintended consequences

Deterrence Put Another Way



If I can shape the threat's assessment of his capability, opportunity, or intent, then deterrence is successful

Deterrence Near the OODA Point

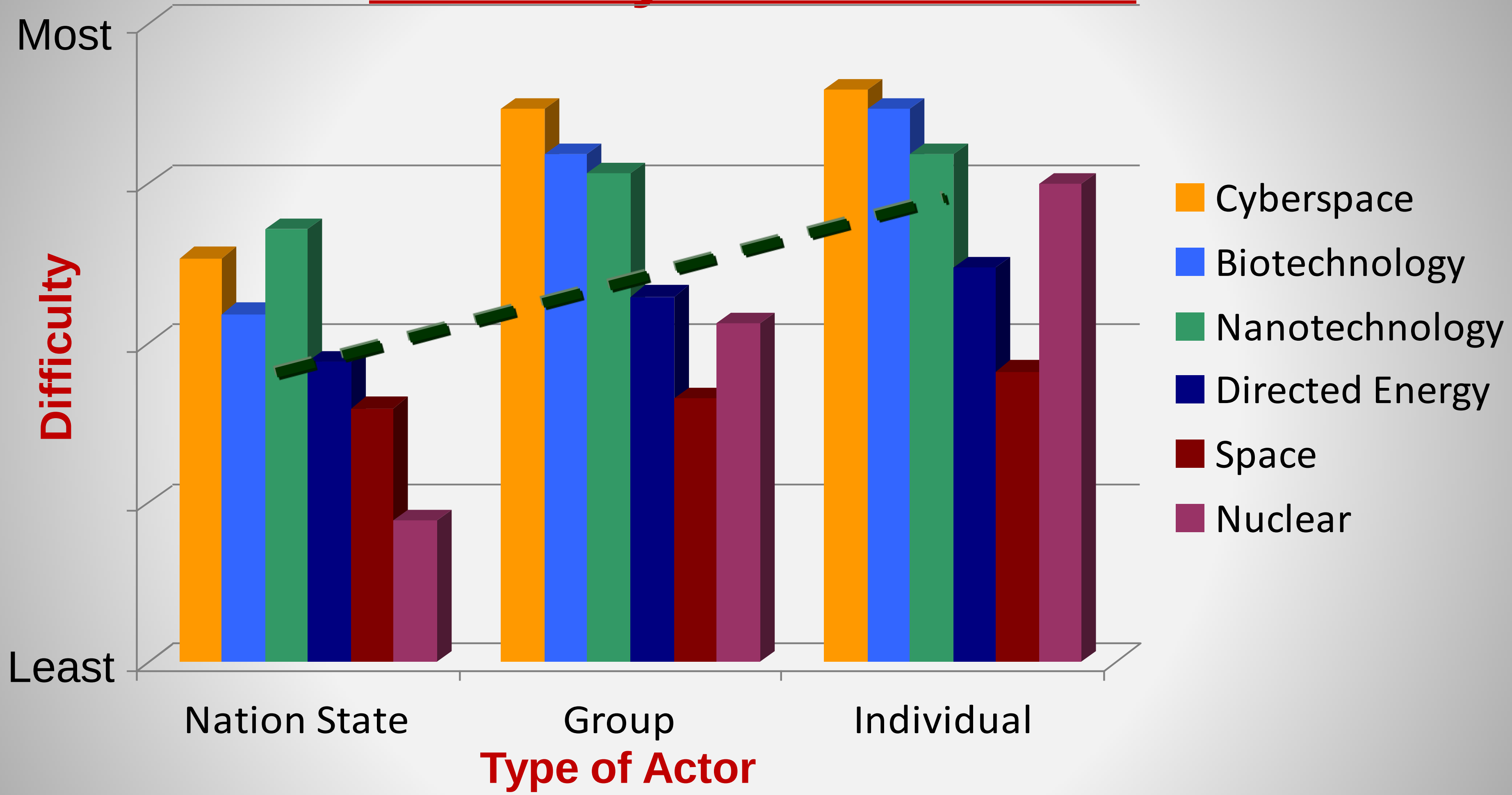
- Machine-to-machine responses (e.g., cyberspace) will form complex systems with potentially unforeseen tipping points
  - E.g., Several brokerage computers, all with different sell trigger points, generated the “Crash of 2:45 PM” where DOW fell 700 points in 5 minutes.
  - Deterrence algorithms and responses are vulnerable to same chaotic dynamic
- While humans are not immune (e.g., onset of WWI), historically we’ve had time
  - Time to attribute, time to think, time to respond

Time is disappearing. Credible deterrence requires ability to rapidly and accurately attribute and respond

Overview

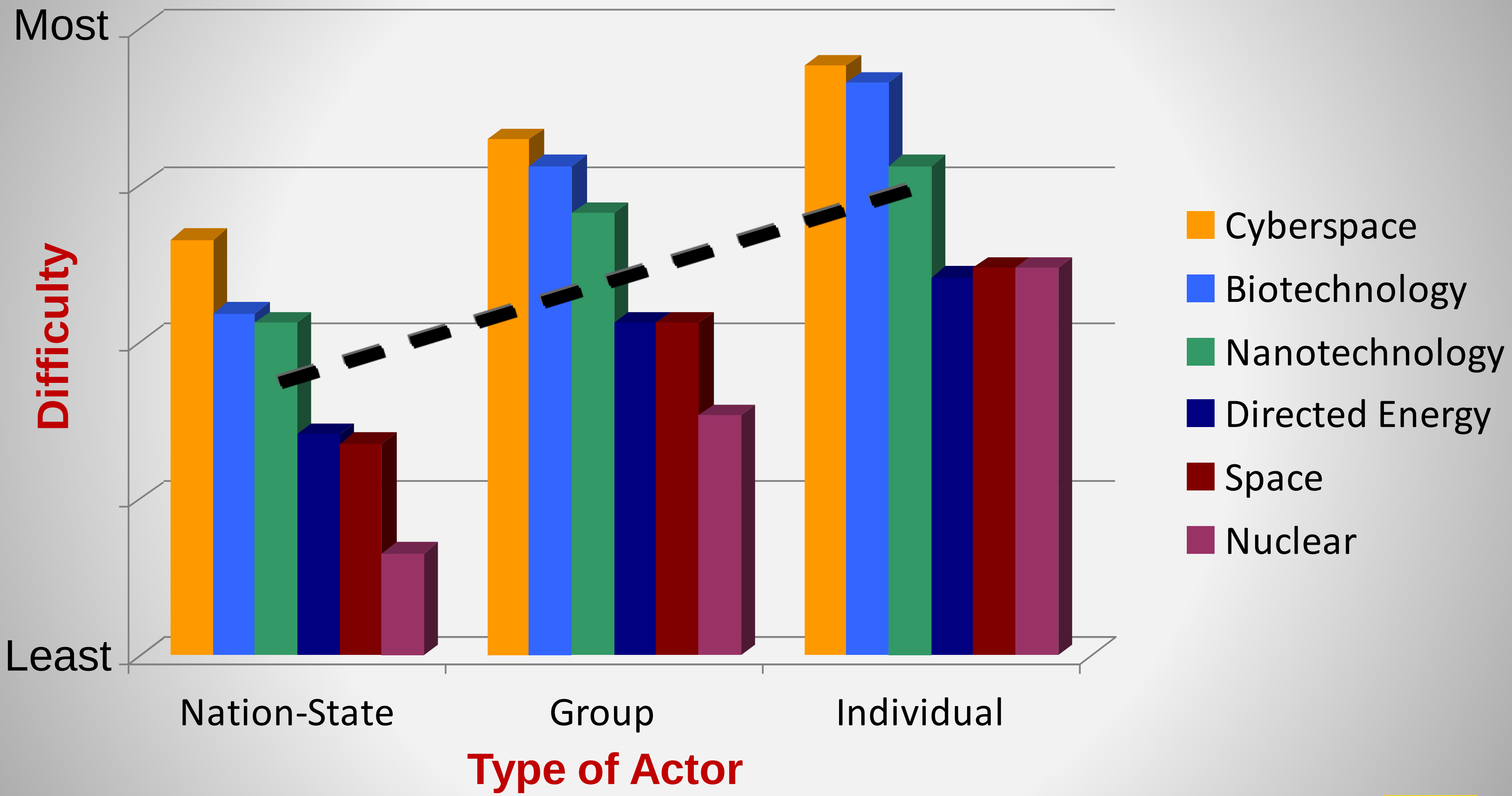
- Enduring Truths and the Threat
  - Repeat Findings
- Methodology for the 2010 Study
  - Who, What, How
  - The Structure of Deterrence
- Delphi Results
- Implications for the USAF

Delphi Results:
Difficulty of Deterrence



Nations: Restrained by culture, law, interests
Individual: Unrestrained absent governance or attribution

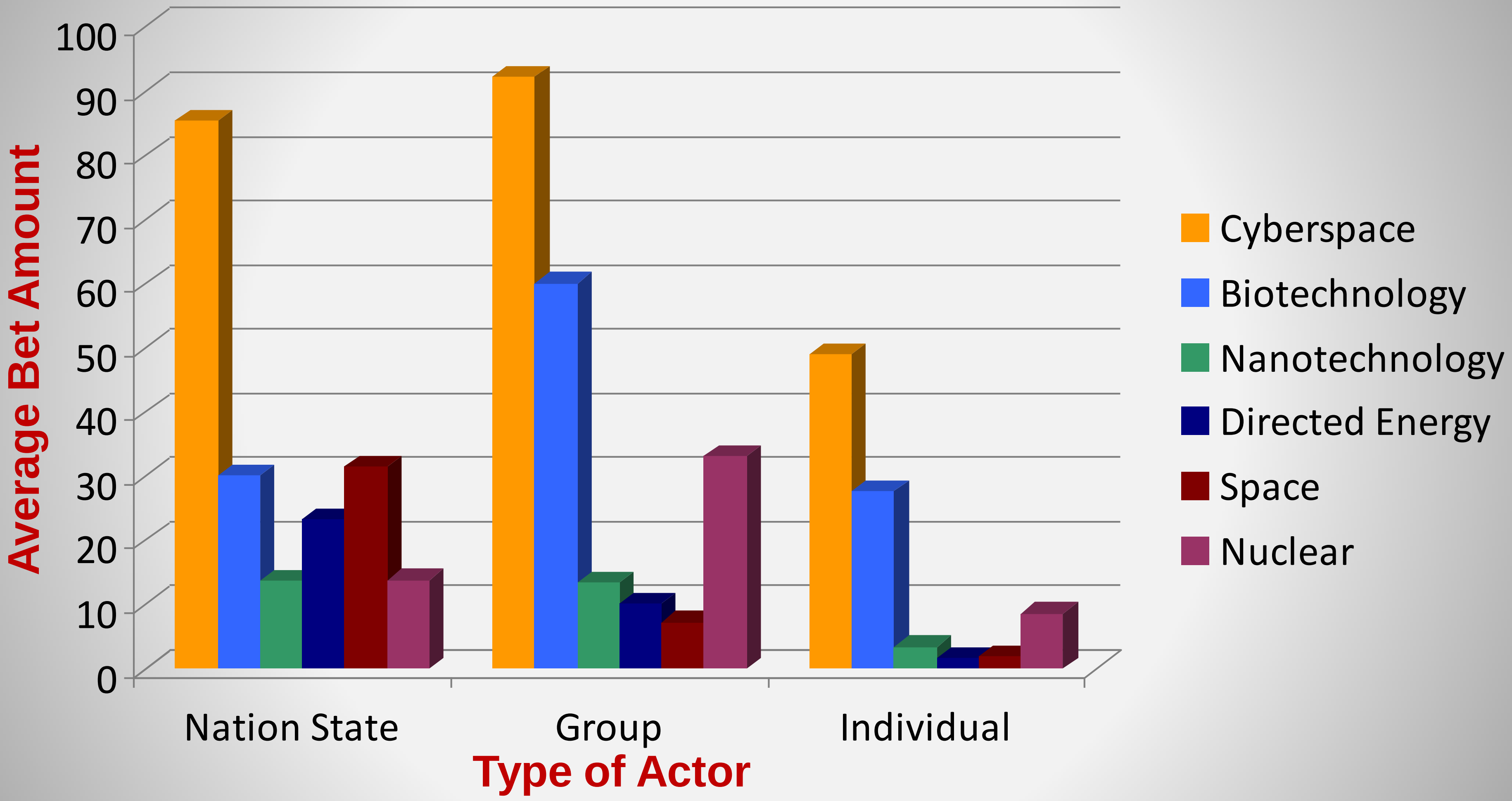
Delphi Results:
Difficulty of Attribution



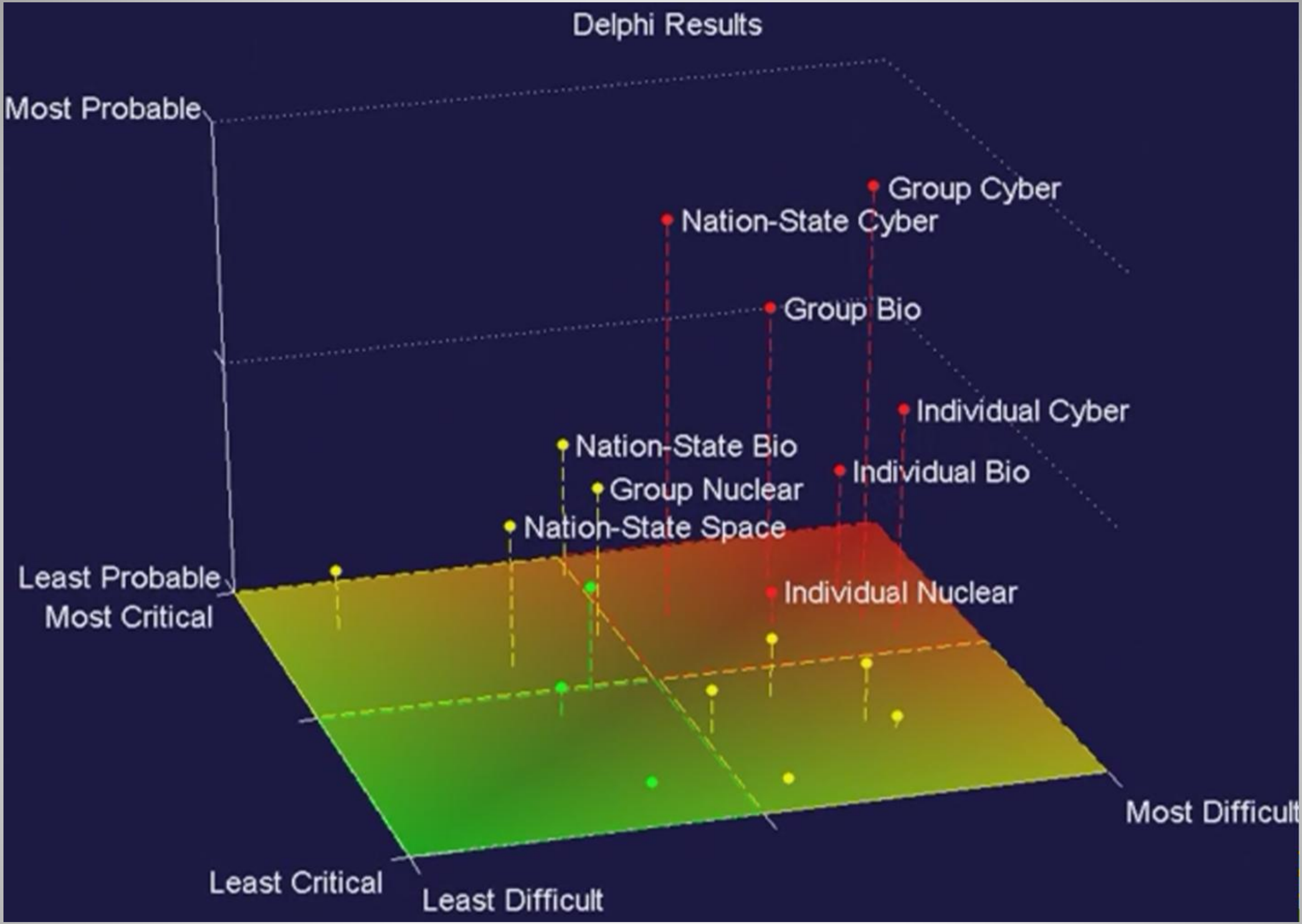
Nations: Location certain – interests & capabilities visible
Individual: Lost in a sea of actors with varying capabilities

Delphi Results:

Bets on Likelihood of Attack



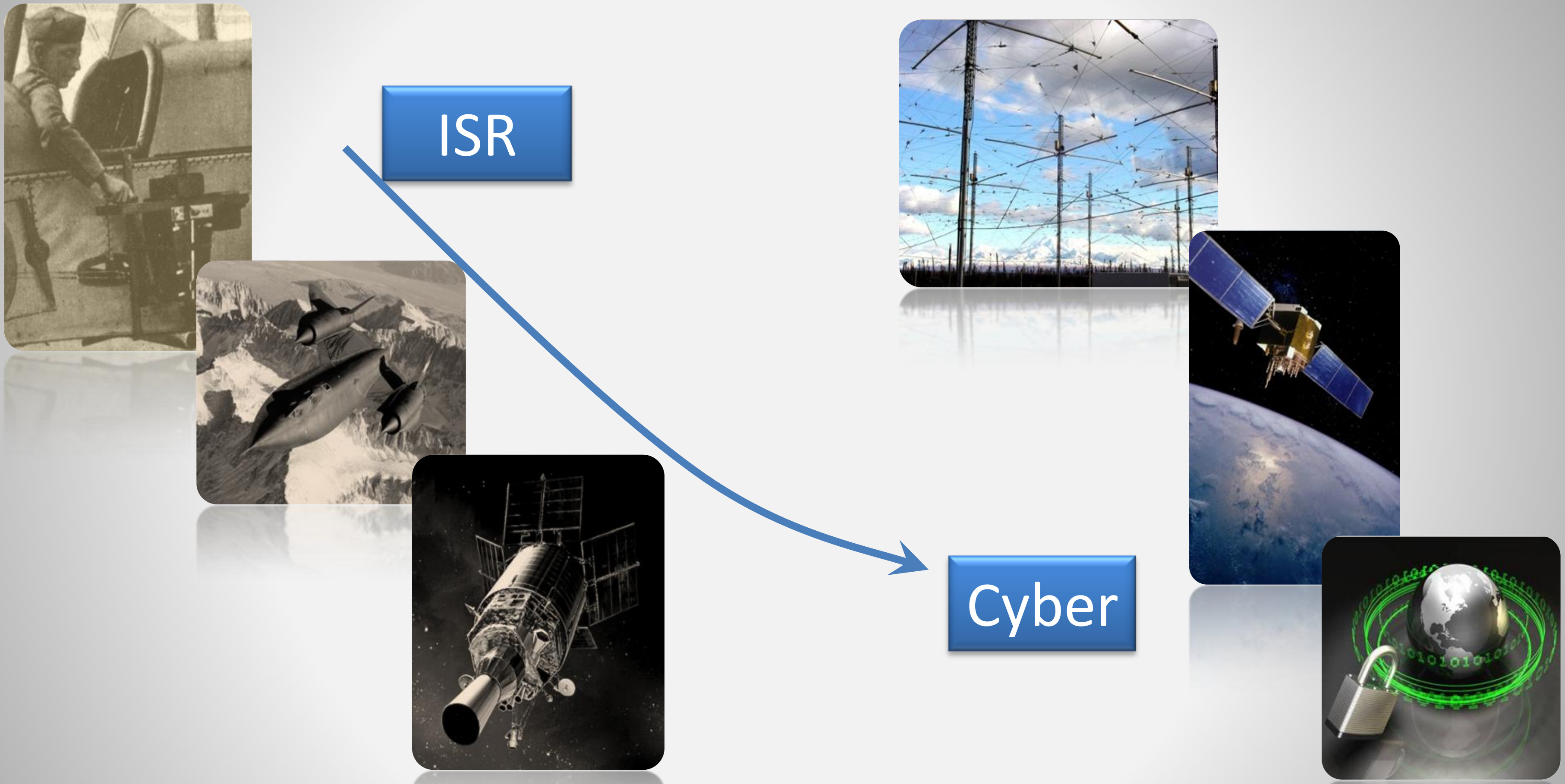
Threats that are hard to attribute are the most likely to occur


Delphi Results
Most Probable
Least Probable
Most Critical
Least Critical
Least Difficult
Most Difficult
Group Cyber
Nation-State Cyber
Group Bio
Individual Cyber
Nation-State Bio
Individual Bio
Group Nuclear
Nation-State Space
Individual Nuclear

Overview

- Enduring Truths and Threats
  - Repeat Findings
- Methodology for the 2010 Study
  - Who, What, How
  - The Structure of Deterrence
- Delphi Results
- Implications for the USAF

Needed: An Updated Vision for Global Vigilance



ISR

Cyber

Answer: Transparency

What is Transparency?

- An updated concept for Global Vigilance consisting of:
  - Global ISR of persons and items of interest
  - Assessed & filtered to produce targeted persons & things
- In order to
  - Deny an opportunity to attack, defend against a capability, or degrade an intent and,
  - Communicate the ability to do so to those whom we wish to deter

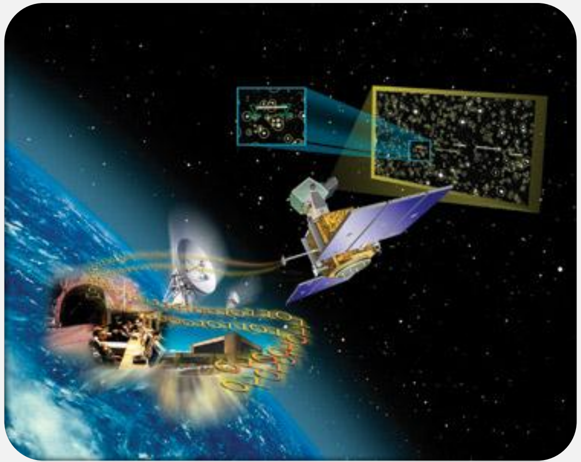
Rough Requirement Scale: Track ~40,000 objects and ~200,000 people worldwide

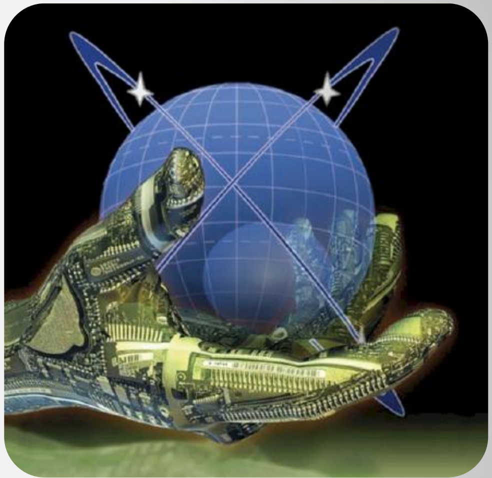
USAF pioneered decapitation and leader coercion strategies—this vision takes it to the next level

The Answer Begins With Our History

The USAF's tradition is to apply technology innovatively to find and strike targets

Air


Space


Cyber

Find, Fix, Target, Track, Engage, Assess
A 60-year summation of experience in Global Vigilance integrating ISR, Strike C2, Training, TTPs

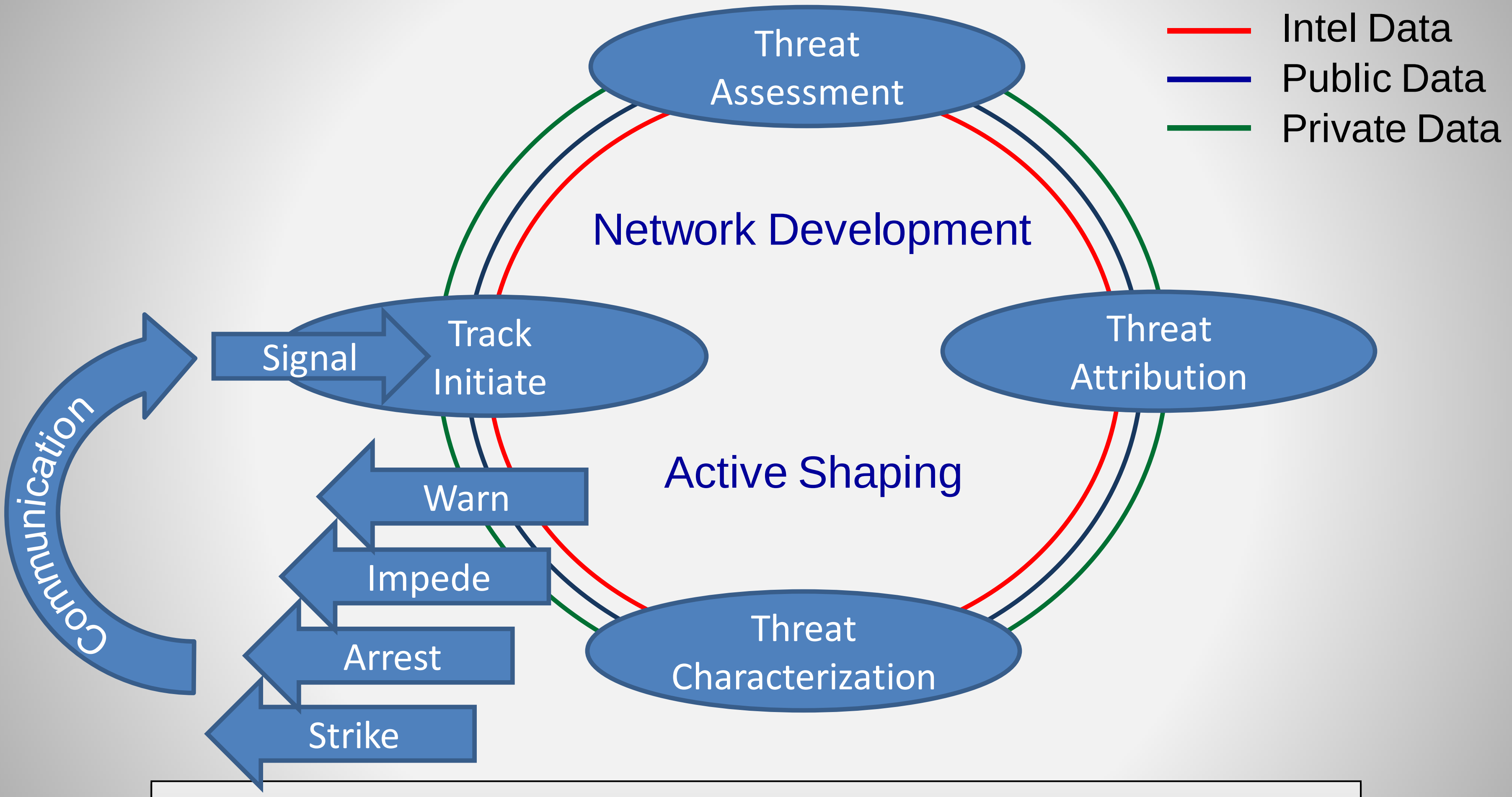
USAF leadership in action: GPS, AOC-like command centers, Distributed Operations, Time-Sensitive Targeting, Networked Cross-cueing

What Are Transparency’s Elements?

- Leverages Technical Developments
  - Everything can be recorded in the future synched in time across multiple spectra
  - Can synchronize public, private, classified environments
  - Acquire systems that fully leverage these development or fill gaps
- Enhanced Through Innovation
  - Algorithms that enable rapid sorting/fusing of data, pattern recognition and profiling
  - TTPs and policy actions to permit coalition and interagency collaboration
- Enabled by C2
  - A global capability to prioritize, move and act rapidly

These elements are at the center of the USAF’s comfort zone—we can and should lead in this arena

How Transparency Operates



The USAF should lead by scaling its F2T2EA processes developed over the past decade to find, monitor and deter the key actors who can hurt us

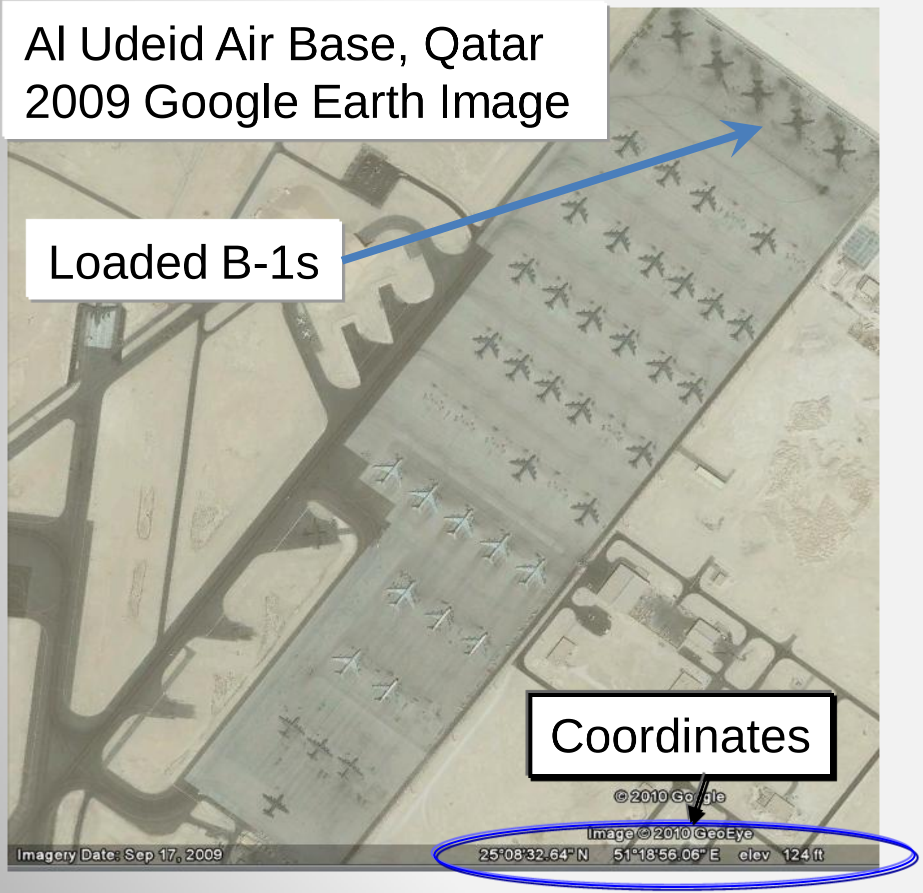
Transparency: A Second Pillar of US Deterrence?

- Benefits similar to Air Superiority
  - Facilitates attack and defense
  - Has a deterrent quality all its own
  - However, it’s about knowledge and perception rather than control
- Stood alongside Global Strike, has potential to provide a second pillar of US deterrence
  - In 2030, attribution will be a pacing requirement
- Developing the capability requires vision, R&D, CONOPS, policy changes, organizational capacity, and people

**USAF established the terms of reference for cyber—
we should lead here too**

Needed: A Way To Improve Resiliency of Forces

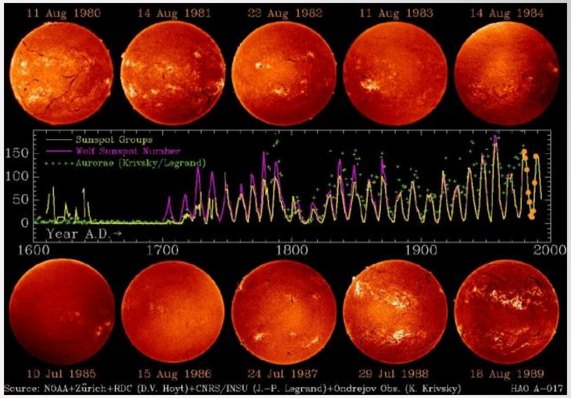
Enemy also has access/transparency


© 2010 Google
Image © 2010 GeoEye
Imagery Date: Sep 17, 2009
25°08'32.64" N 51°18'56.06" E elev 124 ft

Al Udeid Air Base, Qatar
2009 Google Earth Image

Loaded B-1s

Coordinates



Source: NOAA+Zürich+RDC (D.V. Hoyt)+CNRS/INSU (J.-P. Legrand)+Ondrejov Obs. (K. Krivsky)

The enemy may be nature…

…or lurking on the 'net.

We must protect our capabilities

Answer: Immunization

What is Immunization?

- A multi-layered approach to reduce an attack’s effectiveness
  - Physical safeguards
  - Functional resilience
  - Procedural workarounds
  - Flexible mitigation capacity
  - Cognitive resilience (within the population and military)
- As threats become more numerous and capable, deterrence by denial gains in importance
  - Requires time, resources, practice to attain
  - Achieving deterrence requires demonstrations and successful detection of probes

Not new—but requires more emphasis than in the past

Implications of Immunization for the USAF

- Adds pressure to budgets
  - Immunization requires more people and materiel
- Increases requirements on joint interdependence
  - Who is responsible for airfield G-RAMM defense?
- Forces re-examination on how USAF presents forces
  - Consider threats to bases, logistics, communications
  - Consider increased demands of alternative concepts
  - Explore new technologies for aircraft sheltering, airfield repair, space surrogates, cyber resiliency, EMP hardening

Entering an inherently cost imposing world…
persistent attacks will come from a variety of sources

Recommendations for the USAF (1)

- Develop a Global Vigilance strategy for 2035
  - Reestablish the AF as a leader in EW with increased R&D of equipment and increased training *
  - Broaden the AF as a leader in ISR with increased R&D of equipment and increased training
  - Complete Institutional Integration of RPA, Space & Cyberspace Operations
  - Focus Title 10 wargames on vetting new technologies, innovative ideas, and future CONOPS *
  - Examine whether organizational changes are needed to support execution of a Global Vigilance strategy
  - Form an informal interagency study group to define the capabilities, capacities, organization, authorities and systems needed to fully enable transparency (PPD-8)

(* Items from CSAF Vector Statement 4 July 2010)

Recommendations for the USAF (2)

- Form an Air Force Red Team to assess service immunization needs for 2035
  - Provide an overall risk map to USAF missions based on vulnerabilities to EMP/HPM, G-RAMM, ballistic missile, biological, chemical, nanotechnological, nuclear and cyber attacks
    - Map and track interdependent relationships (joint, national critical infrastructure, interagency, etc…)
    - Assess and make visible mission risk based on sister service funding, outlays, readiness
  - Include R&D in future year budgets to address key vulnerabilities
    - E.g., "Capitalize in improvements in directed energy by moving out of the lab with lethal and non-lethal, ultra-precise systems." *

(* Items from CSAF Vector Statement 4 July 2010)

Issues for Other Departments

- Homeland Security
  - Immunization of national critical infrastructure against HPM/EMP, cyber, nanotechnology, biotechnology, and smuggled nuclear attack
- Center for Disease Control/National Institutes of Health
  - Immunization issues surrounding biological attack or natural mutation of serious pathogen
  - In 2009 we recommended a “Manhattan Project” on bio-genetics. The clock is ticking, and time is short.

The Way Ahead

- In early vetting …
  - Strongly recommended that DNI & DHS see this brief
  - Request your sponsorship of this presentation to the EXCOM, Armed Forces Medical Intelligence Center, and to other agencies you see as appropriate
- PPD-8 (National Preparedness) has part of its genesis in this study
  - Our asking questions in research phase generated NSS interest
  - Interagency group has formed to study solutions to critical infrastructure vulnerabilities to attack/natural disasters
  - Request guidance as to whether and how this study should inform DOD participation
- Request permission to present to any/all interested audiences and publish alongside our other studies
  - Public release clearance/classification review already complete

Ready for Your Questions