Controlled by: AFRL/RI
CUI Category: N/A
Distribution/Dissemination Control: Distribution A
POC: B. Wysocki, AFRL

Understanding Information Warfare

2022 CYBER SECURITY DAY

Indiana University of Pennsylvania

Dr. Bryant Wysocki
DAF Technical Advisor

Information Warfare is everywhere and growing

Information Warfare is **any action to Deny, Exploit, Corrupt or Destroy the enemy's information and its functions**; protecting ourselves against those actions and exploiting our own military information functions. (Air University)

Information warfare is an operation conducted in order to gain an information advantage over the opponent. (NATO paper on disinformation)

Information warfare is the manipulation of information trusted by a target without the target's awareness so that the target will make decisions against their interest but in the interest of the one conducting information warfare. (Wikipedia)

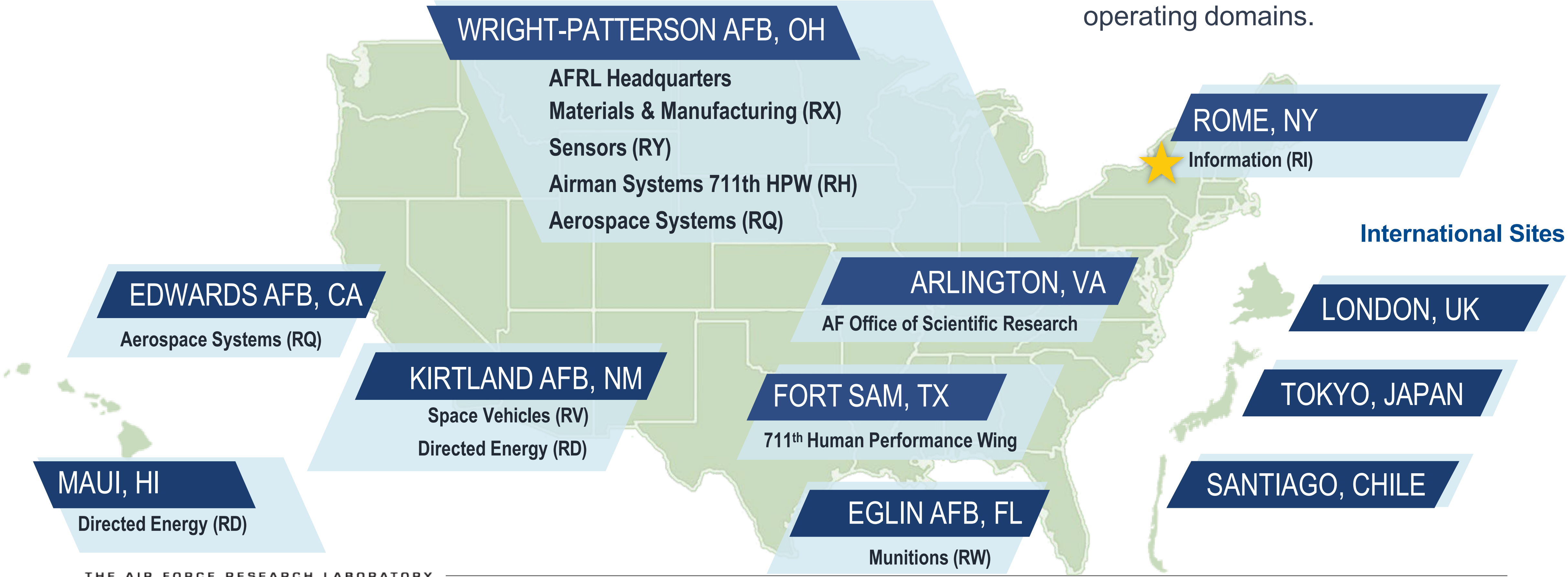
AFRL

THE AIR FORCE RESEARCH LABORATORY

LEAD I DISCOVER I DEVELOP I DELIVER

MISSION: We lead, discover, develop and deliver science, technology and innovation for Warfighters.

VISION: To arm Warfighters that dominate in time, space and complexity across all operating domains.



WRIGHT-PATTERSON AFB, OH

- AFRL Headquarters
- Materials & Manufacturing (RX)
- Sensors (RY)
- Airman Systems 711th HPW (RH)
- Aerospace Systems (RQ)

ROME, NY

Information (RI)

EDWARDS AFB, CA

Aerospace Systems (RQ)

ARLINGTON, VA

AF Office of Scientific Research

KIRTLAND AFB, NM

Space Vehicles (RV)

Directed Energy (RD)

FORT SAM, TX

711th Human Performance Wing

MAUI, HI

Directed Energy (RD)

EGLIN AFB, FL

Munitions (RW)

International Sites

- LONDON, UK
- TOKYO, JAPAN
- SANTIAGO, CHILE

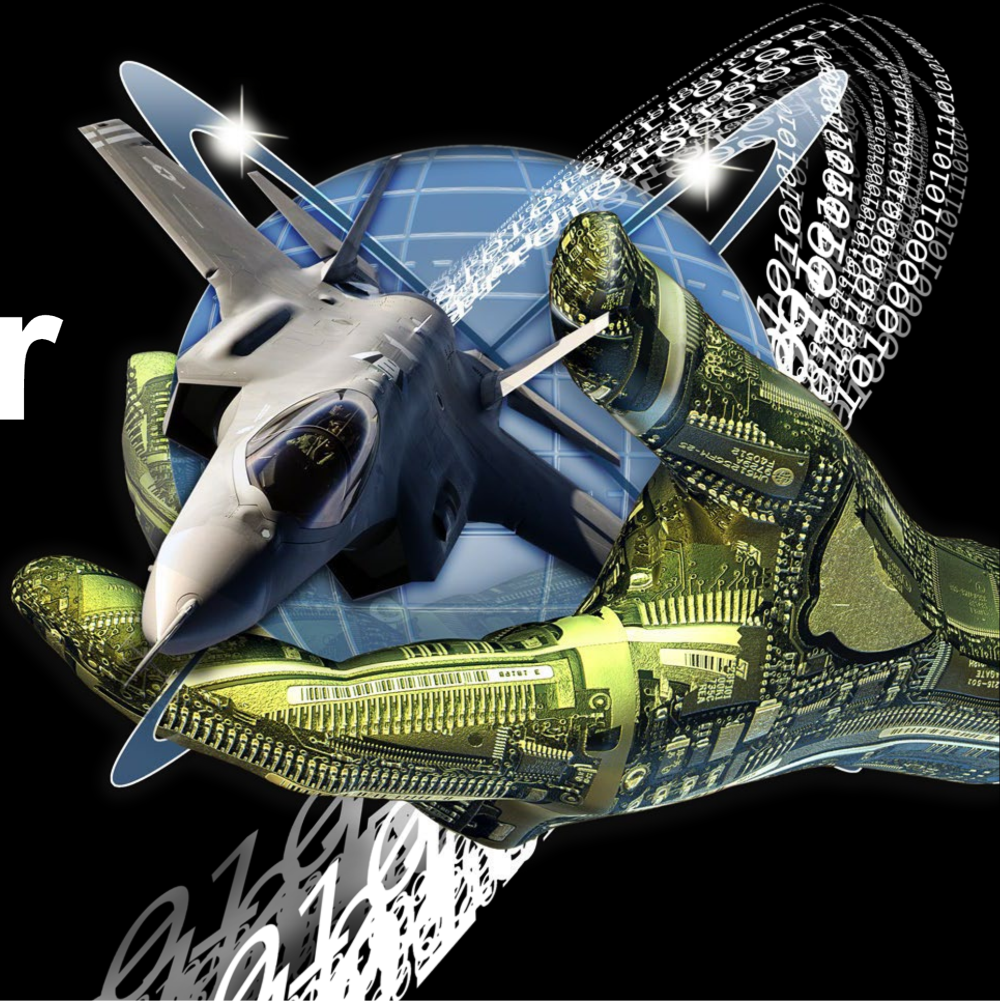
DISTRIBUTION A - Approved for public release AFRL-2022-4924

Information Directorate (RI)

MISSION:

To EXPLORE, PROTOTYPE, and DEMONSTRATE high-impact, game-changing technologies that enable the Air Force and Nation to maintain its superior technical advantage.

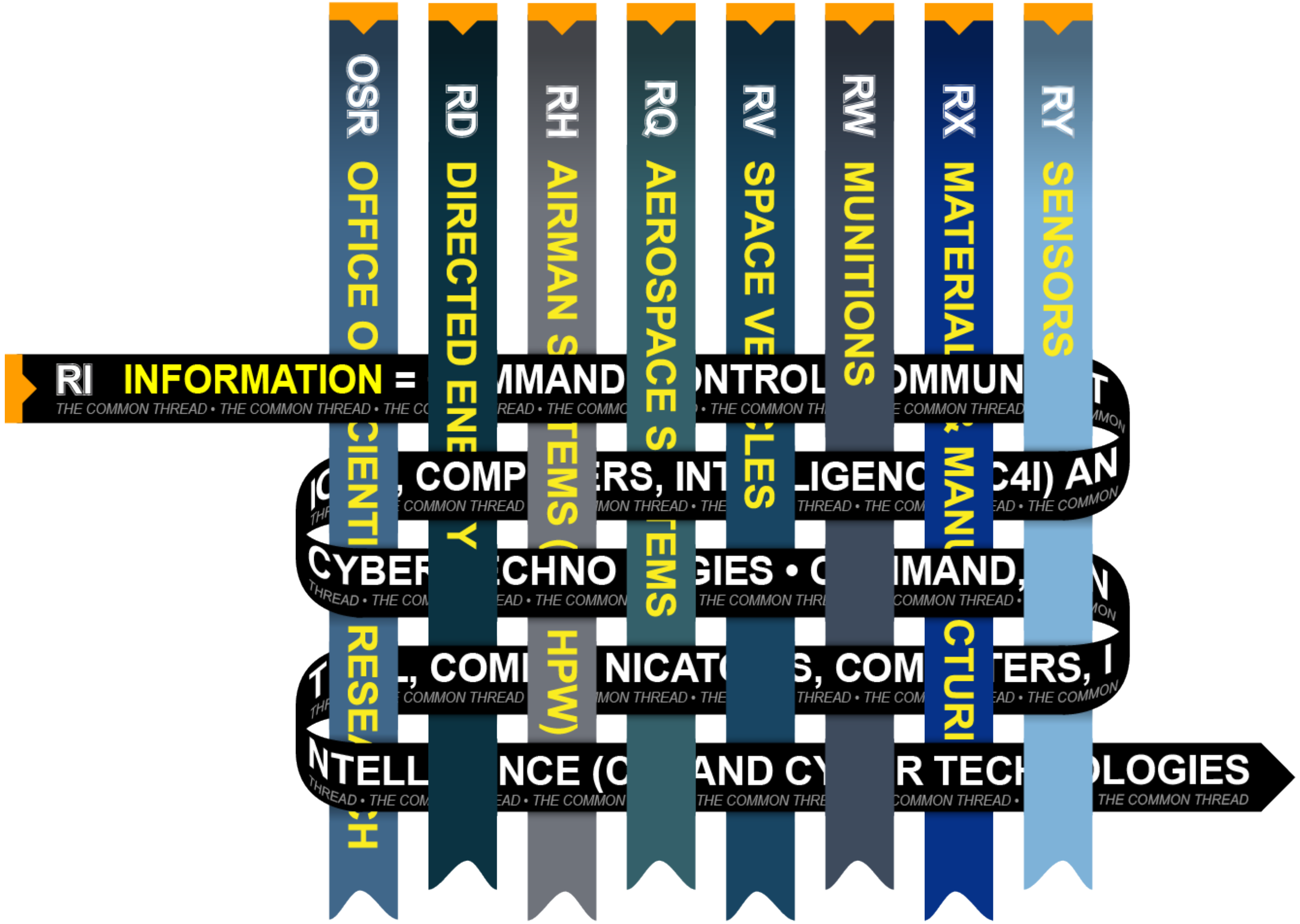
C4I&Cyber



VISION:

To <u>LEAD</u> the Air Force and Nation in COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, AND INTELLIGENCE (C4I) AND CYBER science, technology, research and development.

Information Technologies Touch Every Core Mission


OSR OFFICE O CIENTI RESEA CH
RD DIRECTED ENE Y
RH AIRMAN S TEMS (HPW)
RQ AEROSPACE S TEMS
RV SPACE VE CLES
RW MUNITIONS
RX MATERIAL & MANU CTURI
RY SENSORS
RI INFORMATION = MMAND NTROL OMMUN T
, COMP ERS, INT LIGENC C4I) AN
CYBER CHNO GIES • C MAND,
T , COMI NICAT S, COM TERS, I
NTELL NCE (C AND CY R TECH OLOGIES
THE COMMON THREAD • THE COMMON THREAD • THE COMMON THREAD

C^{4}I&Cyber

Command, Control, Communications, Computers, Intelligence and Cyber

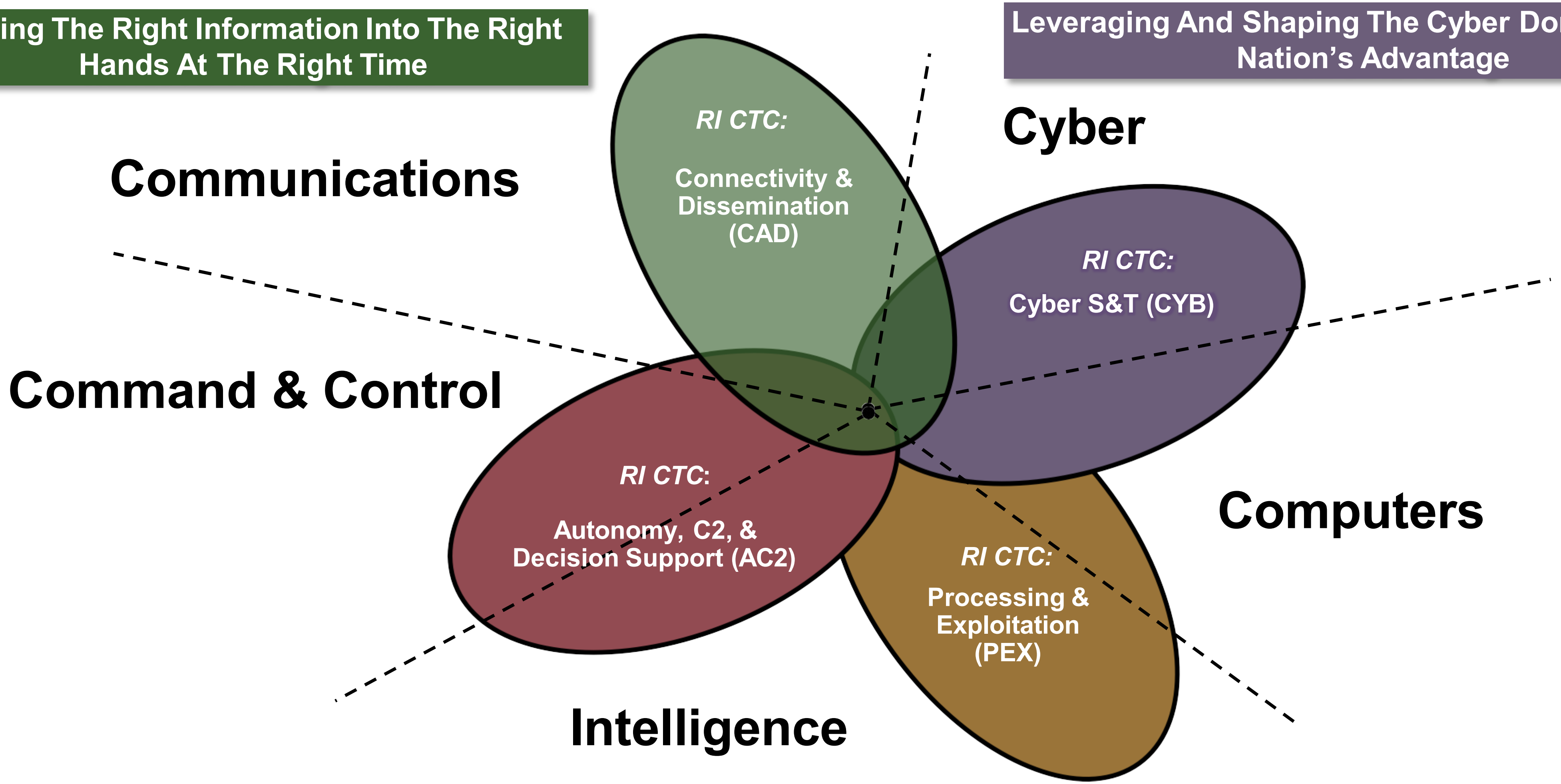
66% of RI programs are in collaboration with other AFRL TDs

- **16% Provide $**
- **52% SME Time**
- **32% $ + SME**

Information Directorate Core Technical Competencies (CTC)

Putting The Right Information Into The Right Hands At The Right Time

Leveraging And Shaping The Cyber Domain To The Nation's Advantage


Communications
Cyber
Command & Control
Computers
Intelligence
RI CTC:
Connectivity & Dissemination (CAD)
RI CTC:
Cyber S&T (CYB)
RI CTC:
Autonomy, C2, & Decision Support (AC2)
RI CTC:
Processing & Exploitation (PEX)

Mastering Complexity of Multi-domain Command & Control

Exploiting Computing and Algorithms to Transform Big Data Into Information

AFRL Cross-Directorate Cyber Collaborations

RI

- Mission Assurance
- Command & Control / Visualization
- Cyber Operations
- Communications & Networking
- Processing & Exploitation
- Signals Intelligence
- Electronic Protection

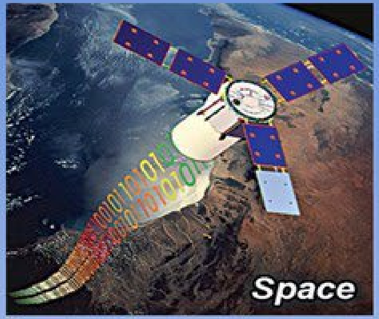
711HPW

- Cognitive Task Analyses
- Operator Selection & Training
- Adaptive Interfaces / Visualization

RY

- Electronic Warfare
- Avionics Protection

RV



- Space System Hardening

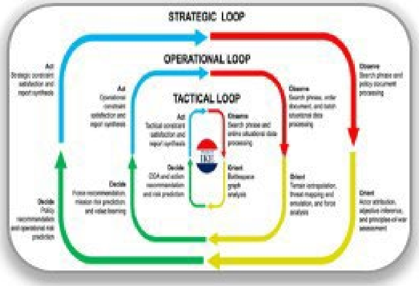
RW

- Munition Systems Cyber Resiliency

AFRL's Cyberspace Capability Leadership

DISTRIBUTION A - Approved for public release AFRL-2022-4924.

Cyber S&T CTC Lines of Effort

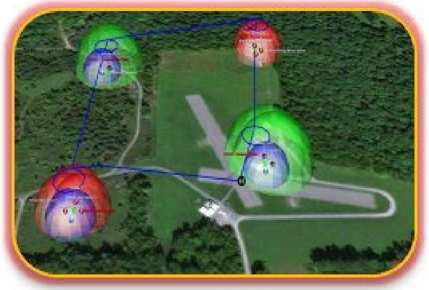


Cyber Warfighting

Cyber warfighting technologies that support joint, integrated DCO-OCO-DODIN operations across all domains and levels of conflict. **Vision:** Cyber operations on par and integrated with air and space.

Cyber Assurance

Integrated components and processes that provide measureable and provable guarantees for current and future system architectures. **Vision:** Mission assurance in environments of heterogeneous trust.



EM-Cyber Convergence

Fusion of wired & wireless capabilities with advanced signal processing, enabling future integrated multi-domain ops and emerging missions. **Vision:** Cyber ops agnostic to medium and geography.

Information Warfare

Employment of Military Capabilities in and through the Information Environment

Threats in the News

BBC News 12.17.2018 ***(Information Operations)***
Russia "meddled in all big social media" around US Election

CNN 12.3.2021 ***(CyberOps/Exploitation)***
Suspected Chinese hackers breach more US defense and tech firms

RUSSIA
DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF ENERGY UNITED STATES OF

ABC News 12.19.2020 ***(CyberOps/Exploitation)***
Pretty clear "Russia behind SolarWinds hack, Pompeo Says, becoming 1st US official to blame Moscow

CNN 3.8.2022 (*Cyber Operations/Exploitation)*
Cybersecurity firm says Chinese hackers breached six US state agencies

Bloomberg Businessweek 12.21.2021 ***(CyberOps/Ransomeware)***
The hackers who help keep Kim Jong Un in power (North Korea)

The CyberSecurity 202 – Analysis 2.7.2022 ***(CyberOps/Exploitation)***
The News Corp breach illustrates how badly China wants to hack the U.S.

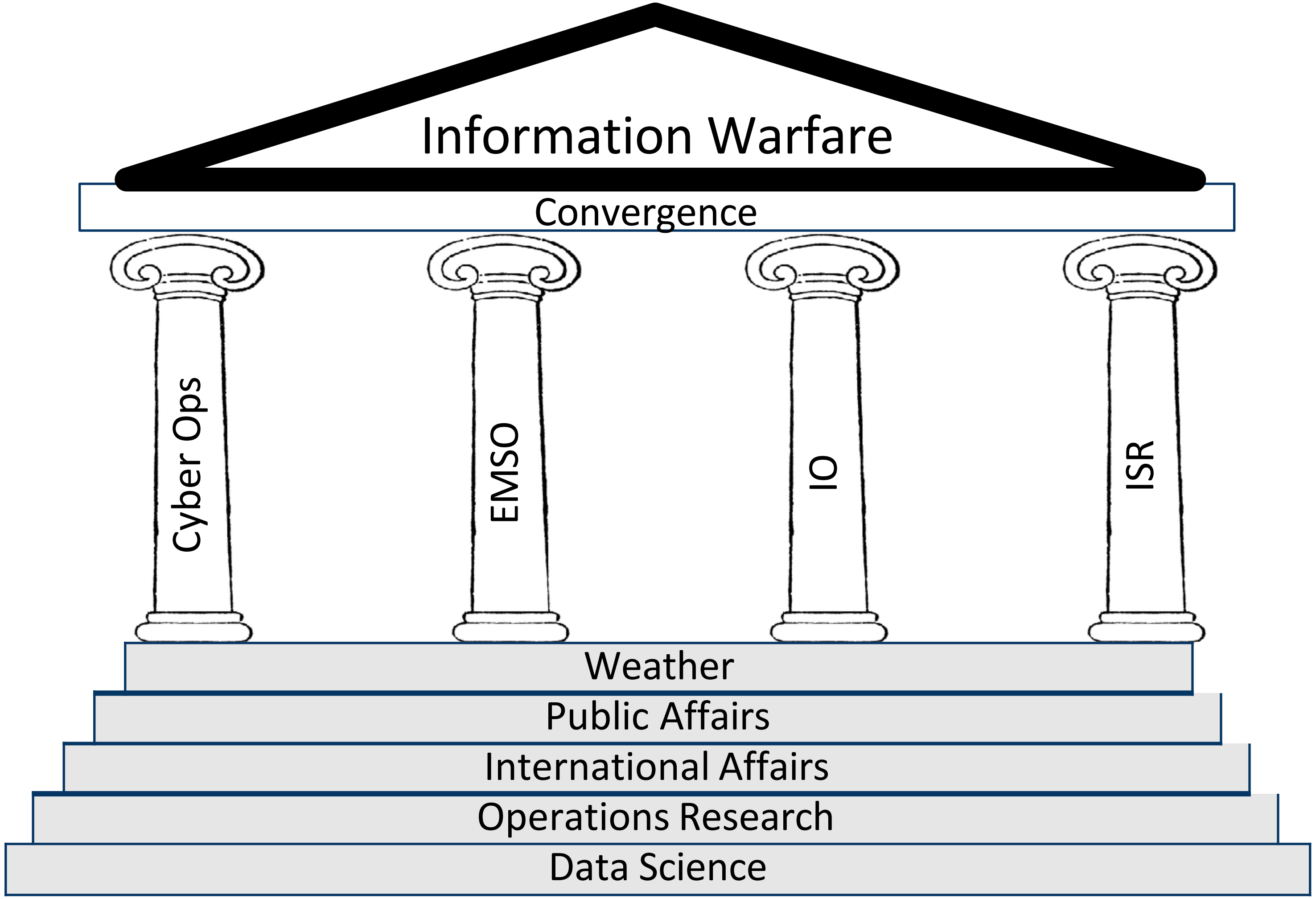
DISTRIBUTION A - Approved for public release AFRL-2022-4924

Science and Technology at-a-Glance

Major Themes	Consequences (for both defense and offense)	Effect on S&T Strategy
TIMELINES SHRINKING	• Cyber-speed decisions required at all levels • All domain is expanding to include new non-DOD entities and emerging IO tech • Contested	• Early and persistent engagement • Emphasize mission assurance • MVPs, DevSecOps, pipelines for S&T
COMPLEXITY INCREASING	• Multi-system-service-national-infrastructure • More interdependencies and data sharing • Cyber-attack consequences hard to predict • Beyond human capacity, AI assisted missions	• Emphasize minimalism and simplicity • Build systems that work in 'zero trust' • Take advantage of the complexity • End of sustainment -> continuous delivery
LANDSCAPES RAPIDLY CHANGING	• Constantly redefining battleground via new C4ISR technologies and applications, microelectronics, ML/AI, and Autonomy → New vulnerabilities surface all the time	• Budget is unstable and slow • Cyber cannot be an afterthought. • More coordination required everywhere • Volatility in S&T priorities and landscape
DOMAINS CONVERGING	• Rapid advance of effects • A platform's attack surface extends out through all its apertures • Single-domain stovepipes weaken impact	• Legacy and SOTA interoperability • Cyber cannot be an afterthought • Demands more coordination Labs/PEOs

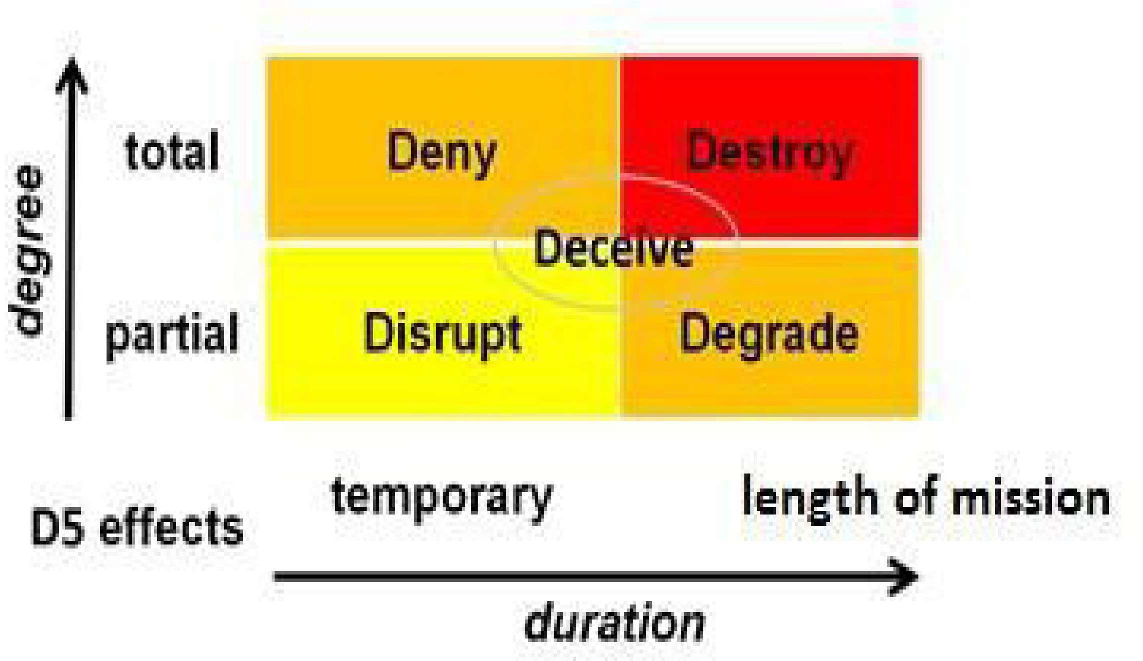
Science and Technology is a crucial enabler.

USAF Operating Concept for Information Warfare 30 Mar 2022



D5 Effects

- Specify the impact to compromised MEF in terms of disruption, degradation, denial, destruction based on degree and duration of effect
- The fifth D: deception, can achieve any of the other four D effects by convincing a user or system of the presence or absence of an effect.



D5 effects	temporary	length of mission
total	Deny	Destroy
partial	Disrupt	Degrade

Deceive

Cyber Vulnerability Assessment

1. Identify the mission of the System Under Test (SUT).
2. List the Mission Essential Functions (MEF).
3. Map MEF cyber dependence along the six phases of the information lifecycle: generation, processing, storage, communication, consumption and destruction.
4. Draw an information boundary for the SUT.
5. Enumerate Information Exchange Requirements (IER) between the SUT and outside world.
6. Characterize each information flow across the information boundary
7. Estimate the mission impact of a compromise in the confidentiality, integrity or availability in each information flow.
8. Specify impact to compromised MEF as disruption, degradation, denial, destruction or deception.
9. Categorize vulnerability as architecture, specification or implementation.
10. Design cooperative tests to verify impact of information compromise.

In the fight

U.S. Army Cyber Command

DISTRIBUTION A - Approved for public release AFRL-2022-4924.

How can you help?

Be Aware AND minimize your digital footprint

Digital Exhaust: What Everyone should know about Big Data, Digitization and Digitally Driven Innovation by Dale Neef

Be Informed about how your information can be used

The Social Dilemma – Documentary on NETFLIX

Be a discerning consumer of information

Influencing your perceptions

Get involved, we can use your help!

Come Join us at AFRL! afresearchlab.com

INFORMATION DIRECTORATE: C^{4}I&Cyber

Global Persistent Awareness

Resilient Information Sharing

Rapid, Effective Decision-Making

Complexity, Unpredictability, and Mass

Speed and Reach of Disruption and Lethality

DISTRIBUTION A - Approved for public release AFRL-2022-4924

Questions

LEAD · DISCOVER · DEVELOP · DELIVER

DISTRIBUTION A - Approved for public release AFRL-2022-4924.

Image Reference slide

- Slide 2 - IW

Image on left Cyber Warrior: “Cyberwarfare and information warfare…” c4ISRnet.com, 4.25.2017
Image on upper right: “Information Warfare – Modern Diplomacy” moderndiplomacy.eu 3.7.2018
Image on lower right: “Information Warfare in 2021 – Are you protected from cyber attacks? – Connected IT Blog - Community.connection.com 19 Feb 2021

•Slide 3 - IW Global Power Competition Image of Chinese Flag – upload.Wikimedia.org/Wikipedia/commons
Image of Russian Flag – upload.Wikimedia.org/Wikipedia/commons

- Slide 4 - Threats in the News

Image upper left: BBC News – “Russia meddled in all big social media around us Election” - 12.17.2018
Image upper center: The Daily Beast – “China reveals its Cyberwar Secrets” - 4.14.2017
Image upper right: ABC news – “Pretty clear Russia behind Solar Winds …” - 12.19.2020
Image lower left: South China Morning Post scmp.com - 8.19.2020
Image lower center: Vox.com “How North Korea stole 235 gigabytes of classified US and South Korean military plans” – 10.13.2017
Image lower right: China’s next generation of hackers techcrunch.com - 11.12.2021

- Slide 5 - USAF OC for IW

Image created by Scott Shyne (AFRL/RIG) 4.12.2022

- Slide 6 - In the fight -

Images: all official logos of USCYBERCOMMAND and their respective service commands

- Slide 7 - How can you help?

Image upper left: Wellframe.com/industry-insights “Harness your digital exhaust”
Image upper right: humanetech.com “The Social Dilemma”
Image lower left: news.standford.edu “The best way to counter fake news is…” 10.25.2021
Image lower right: project-manus.mit.edu/monthlychallenge277-2776493 “we-want-you-uncle-sam-we–want-you”