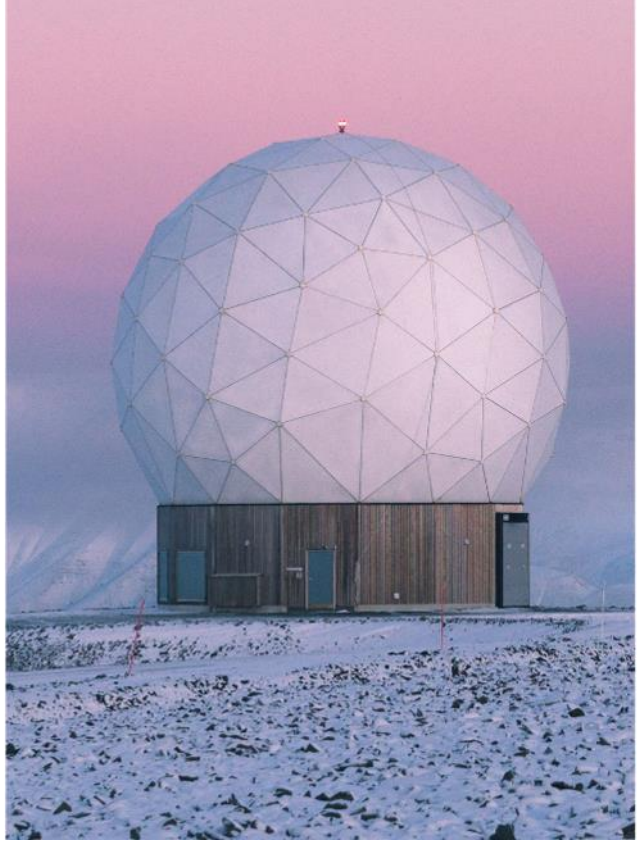





Raytheon Technologies

Cyber and Aviation Security

Mike Worden, CODE Center Chief Engineer
Heather Romero, RIS Anti-Tamper Tech Area Director

April 23, 2020

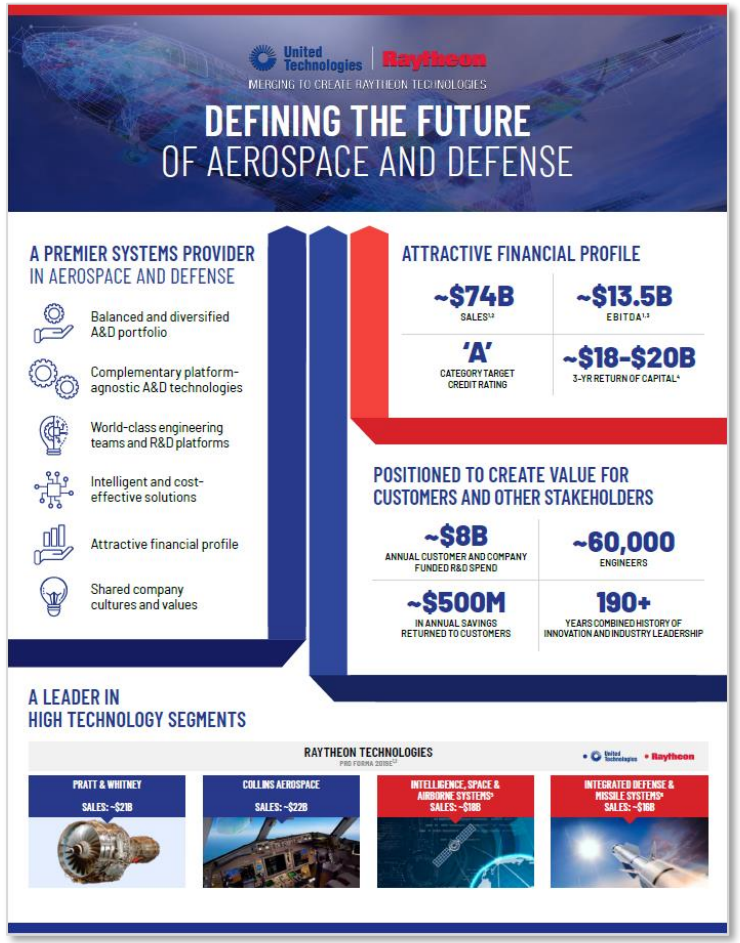
Agenda

- Raytheon Overview and Business Strategy
- Aviation CyberSecurity
- CyberSecurity Talent Acquisition

Raytheon Overview and Cyber Strategy

RAYTHEON TECHNOLOGIES

- A TECHNOLOGY AND INNOVATION LEADER SPECIALIZING IN DEFENSE, CIVIL GOVERNMENT AND CYBERSECURITY SOLUTIONS THROUGHOUT THE WORLD
  - 2018 NET SALES: $27 BILLION
  - 67,000 EMPLOYEES WORLDWIDE
  - HEADQUARTERS: WALTHAM, MASSACHUSETTS



Raytheon Technologies

ALIGNED WITH CUSTOMER PRIORITIES

MISSILE DEFENSE

Raytheon's broad portfolio of proven missile defense systems delivers multilayered protection to protect the U.S. and its allies against a growing range of current and emerging threats.

COMMAND AND CONTROL

Raytheon is a leader in command and control systems, combining sensors and advanced networks to create entirely new ways of perceiving the world.

SENSORS AND IMAGING

Raytheon's proven radars and sensors work together to help experts see further, track longer and prepare smarter.

CYBER

Raytheon offers end-to-end capabilities that help customers protect information and infrastructures from cyber threats, and confidently navigate the cyber domain.

ELECTRONIC WARFARE

Raytheon's advanced electronic warfare systems and capabilities give our warfighters the continued strategic advantage to effectively and safely execute their missions in the modern threat environment.

PRECISION WEAPONS

Raytheon's reliable and cost-effective precision weapons systems incorporate advanced technologies that enable U.S. and allied military services to hit the target and protect their warfighters from evolving threats.

TRAINING SERVICES

From live, virtual, gaming and constructive training to multinational force exercises, Raytheon trains people for the world's most important missions.

MISSION SUPPORT

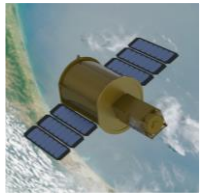
Raytheon is integrating the best defense systems with advanced commercial software to improve decision speed and quality across domains. Our innovative approaches and proven tools keep customers mission-ready and relevant while optimizing limited resources.

Raytheon's Footprint in Cyber Space











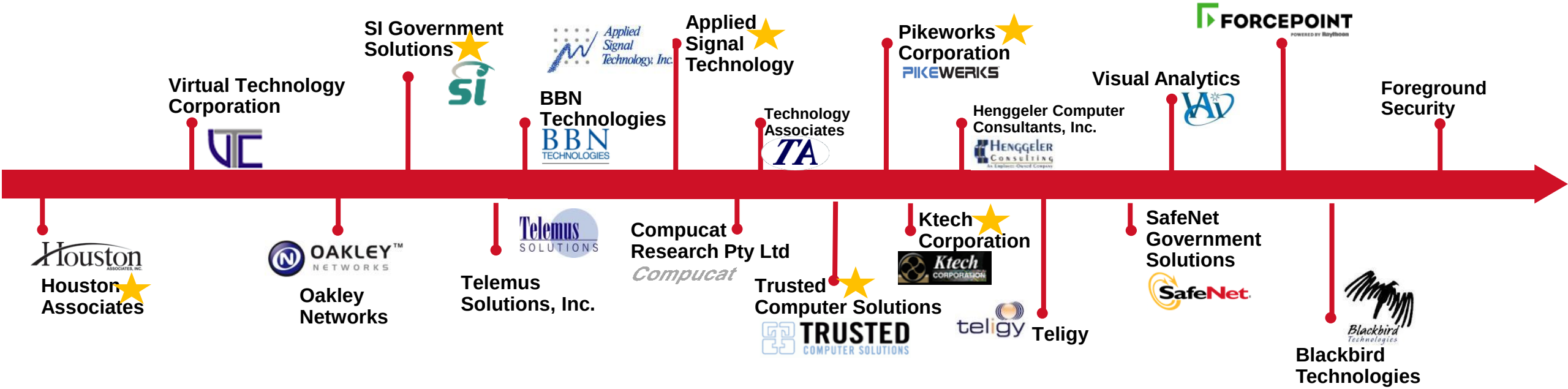




Cyber is part of everything we deliver

Raytheon Technologies

The Raytheon Cyber Bench



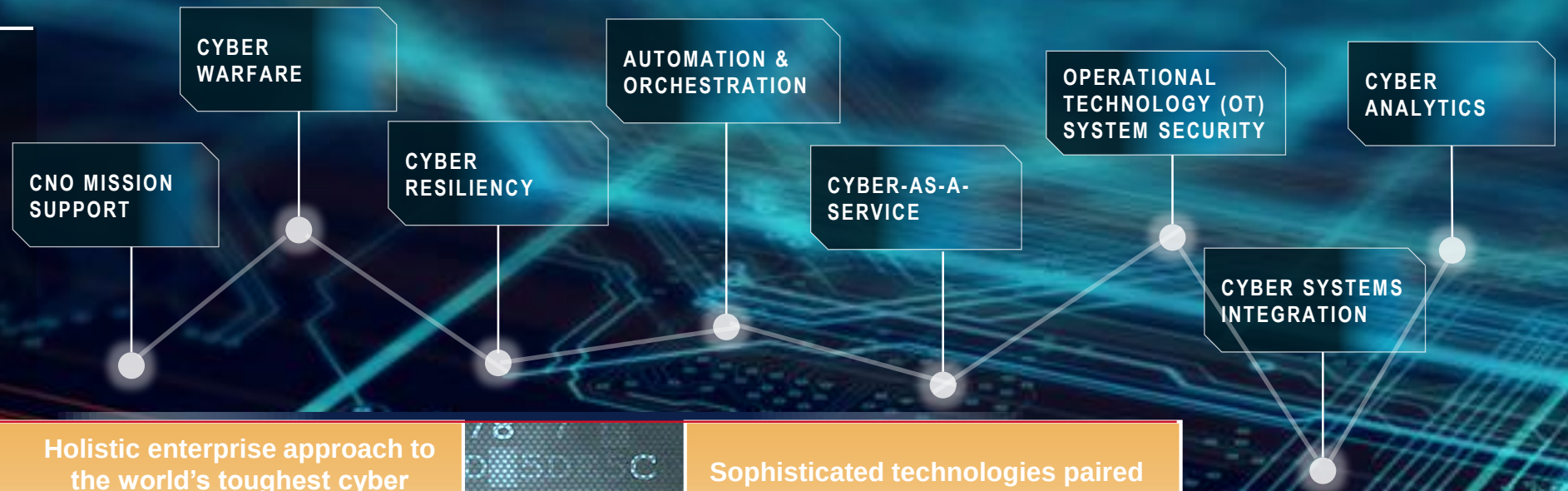
- 50 years as an intelligence industry prime, augmented with small business agility & national-scale systems engineering
- Many of our cyber acquisitions (★) transitioned DoD SBIR projects with a range of customers (AF, Army, Navy, SOCOM, DARPA, DTRA, MDA)

Integrating technologies to provide solutions for an evolving cyber threat

Raytheon Technologies Cyber Capabilities

Cyber environment:

- Cyberspace as a warfighting domain
- Convergence of defensive and offensive cyber operations and tools
- Critical infrastructure cybersecurity
- AI / ML, advanced analytics and automation for enhanced situational awareness
- Security for cloud migration
- Outsource to shared security services



Holistic enterprise approach to the world's toughest cyber challenges

Sophisticated technologies paired with hardened cyber defense

- CYBERSECURITY OPERATIONS CENTERS *CSOC*
- CYBER HARDENING
- MANAGED SECURITY SERVICES
- CYBER RANGES *CODE CENTER*
- CYBER ANALYTICS
- THREAT RESEARCH AND ASSESSMENTS
- PROACTIVE/ DYNAMIC DEFENSE & HUNTING
- CYBER TRAINING
- DEFENSIVE CYBER OPERATIONS
- OFFENSIVE CYBER OPERATIONS *Tools and Access*

Full spectrum operational and threat intelligence expertise

Integrated national and Internet-scale solutions

Raytheon Technologies

Cyber by the Numbers

Thousands of cyber and special mission experts world-wide

60% at customer sites

76% Clearances at or above DoD top secret

>$3.5 Billion

Invested in cyber R&D, infrastructure, and acquisitions in 10 years

18 Cyber and analytics acquisitions across Raytheon

#1 Identify and fix system vulnerabilities

>300 Million tests per week

Monitoring **250K** endpoints

Hundreds Of certified ethical hackers

3,000 Cyber professionals across Raytheon

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

Presented by Raytheon

Champion the development of **Cyber talent and leaders**

400+ Contracts

Including **DHS DOMino**

Most of our best work is classified

Customers in **80** countries

A leader in **Next-generation high-consequence missions**

40 Specialists deployed globally each month

The only large prime contractor to compete in DARPA's Cyber Grand Challenge

Capture the Flag DEFCON

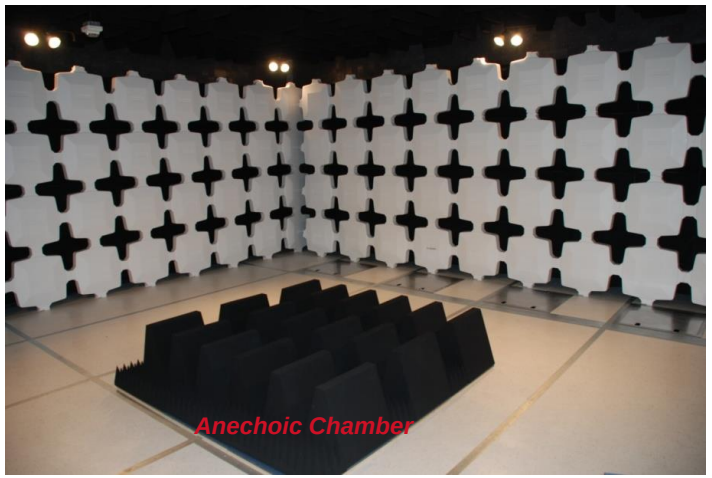
Providing secure solutions for Raytheon, government customers, commercial and international partners

CODE CENTER Overview

- A Live-Fire Cyber Range to Test Cyber-Resilience of RTN Products and train Cyber SMEs
- Located at RTN Dulles Hub (3 M north of Dulles Airport, VA)
- ~ 31K sq ft facility running at Multiple Security Levels (MSL)
- Achieved IOC in Dec 2011
- Remote Testing available


Data Center


HW Integration Lab


Anechoic Chamber


Team Rooms

Fully equipped cyber testing center

The Cyber Threat and Raytheon's Response

Evolution of the Threat

Accelerating Cyber threats forcing governments and industries to address their vulnerabilities

- Increased economic and reputational impact
- USG now openly identifying state-sponsored attacks
- Attacks moving from DDoS to destruction of assets Adversaries using Cyber as a military weapon

- U.S. federal agencies faced 31,107 cybersecurity incidents in 2018 (Source: 2018 FISMA report)
- Security breaches have increased by 67% since 2014 and 11% since 2018 (Source: Accenture)

APRIL 2007
ESTONIA

Denial of Service attack likely by **Russian activists** on the Estonian government

MARCH 2011
RSA

Nation state actors from China stole data related to RSA Secure tokens targeting defense secrets and related IP. **US replacement costs: $50M-$100M**

LATE 2014
YAHOO!

In late 2014 Yahoo! experienced one of the largest breaches in history, with over 500 million users information stolen in what is **believed to be a state-sponsored attack**

JUNE 2015
OPM

The largest breach of federal employee data in recent years. **China accessed up to 22 million personnel records for espionage purposes**

MAY 2017
WANNACRY

A worldwide ransomware campaign widely **attributed to North Korea** affects more than 200,000 computers in 150 countries

JAN 2010
GOOGLE

Hackers stole intellectual property and sought access to Gmail accounts; **the attack originated from China**

JUNE 2013
SNOWDEN

Edward Snowden **leaked up to 1.7 million classified files from the NSA** about the agency's surveillance programs

JUNE 2015
SAUDI ARABIA, ISRAEL

Cyber espionage attacks against critical government systems by **Iranian threat actors**

NOV 2018
AUSTAL

Australian shipbuilder Austal suffers a ransomware attack with company data, including some unclassified ship designs; **many news reports suggest Iran was behind the attack**

AUG 2008
GEORGIA

Hack on government computer networks likely by **Russian state actors** ahead of troop incursion

APRIL 2009
Lockheed JSF

JSF design and electronics systems files hacked by **China, which later produced the J20**

AUG 2012
SAUDI ARAMCO

DDOS attackers infected the hard drives of **over 30,000 computers**, effectively destroying data. US government officials suggest **Iranian regime was to blame**

NOV 2014
SONY

Attack against several internal data centers **(over 100TB of data)** delayed the release of *The Interview* – attributed to **North Korean state actors**

OCT 2016
DNC HACK

DHS and DNI name **Russia** responsible for **hacking the Democratic National Committee** to steal and disseminate over 20,000 emails

SEPT 2017
EQUIFAX

In Feb. 2020 the U.S. DOJ charged **4 Chinese** Army personnel for the hack which compromised the private data of 145 millions Americans

Sources: Center for Strategic & International Studies (CSIS); Government Accountability Office (GAO)
Reuters

Notional Airframe

Aircraft Control

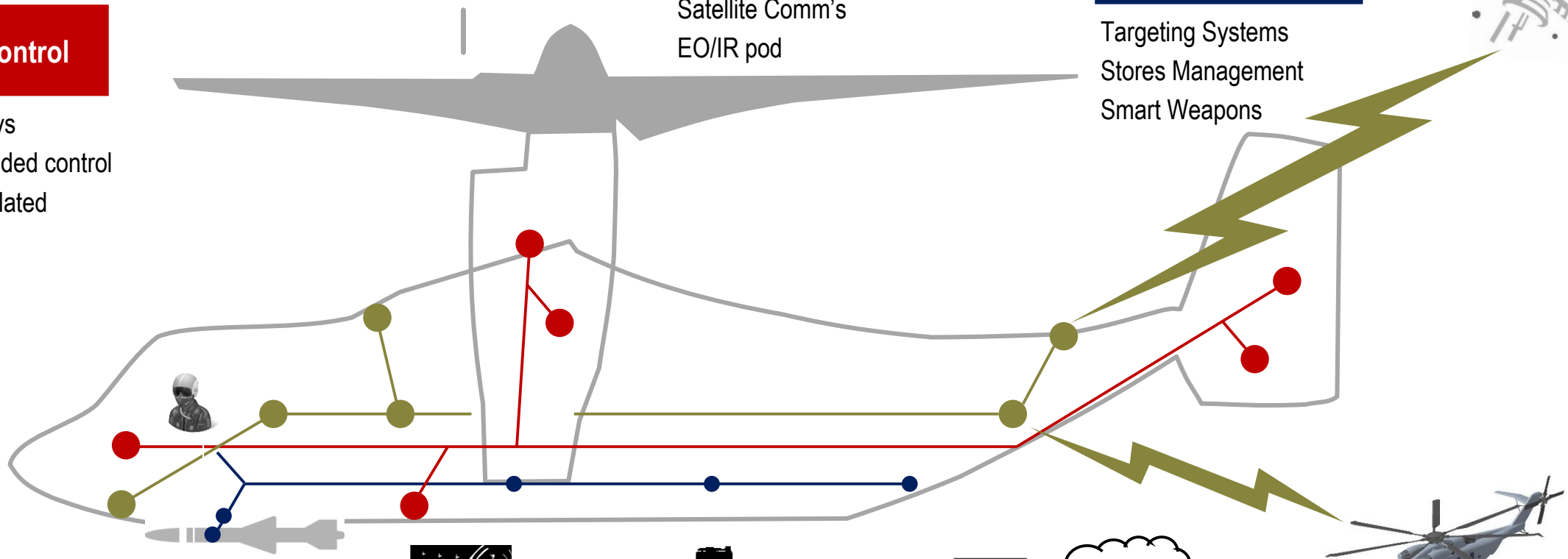
Cockpit Displays
Flight & embedded control
Flight-safety related
Navigation

Sensing and Communications

Satellite Comm's
EO/IR pod

Weapon Systems

Targeting Systems
Stores Management
Smart Weapons



Ground Support and Labs

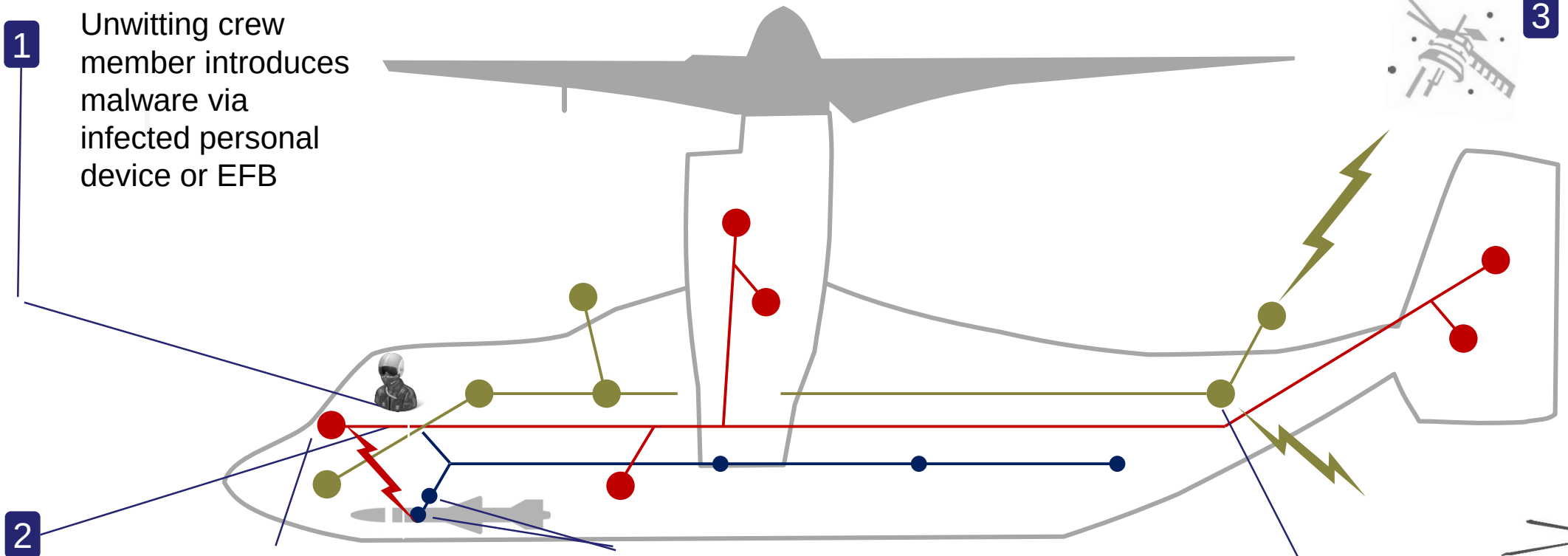
Maintenance instruments
Maintenance personnel

Data Loaders
Data Recorders

Ground Support Networks
Maintenance & Mission Planning

Mis-use Cases*

1 Unwitting crew member introduces malware via infected personal device or EFB



3 Over-the-air attack on navigation receivers and other data links to inject software payload. Use zero-day vulnerability in nav receiver software

2 Compromise software within ground systems (through insider, unsafe connections, etc.) Infect aircraft control system once connected

5 Malware introduced by maintenance platforms infects stores controller, and from there to weapon

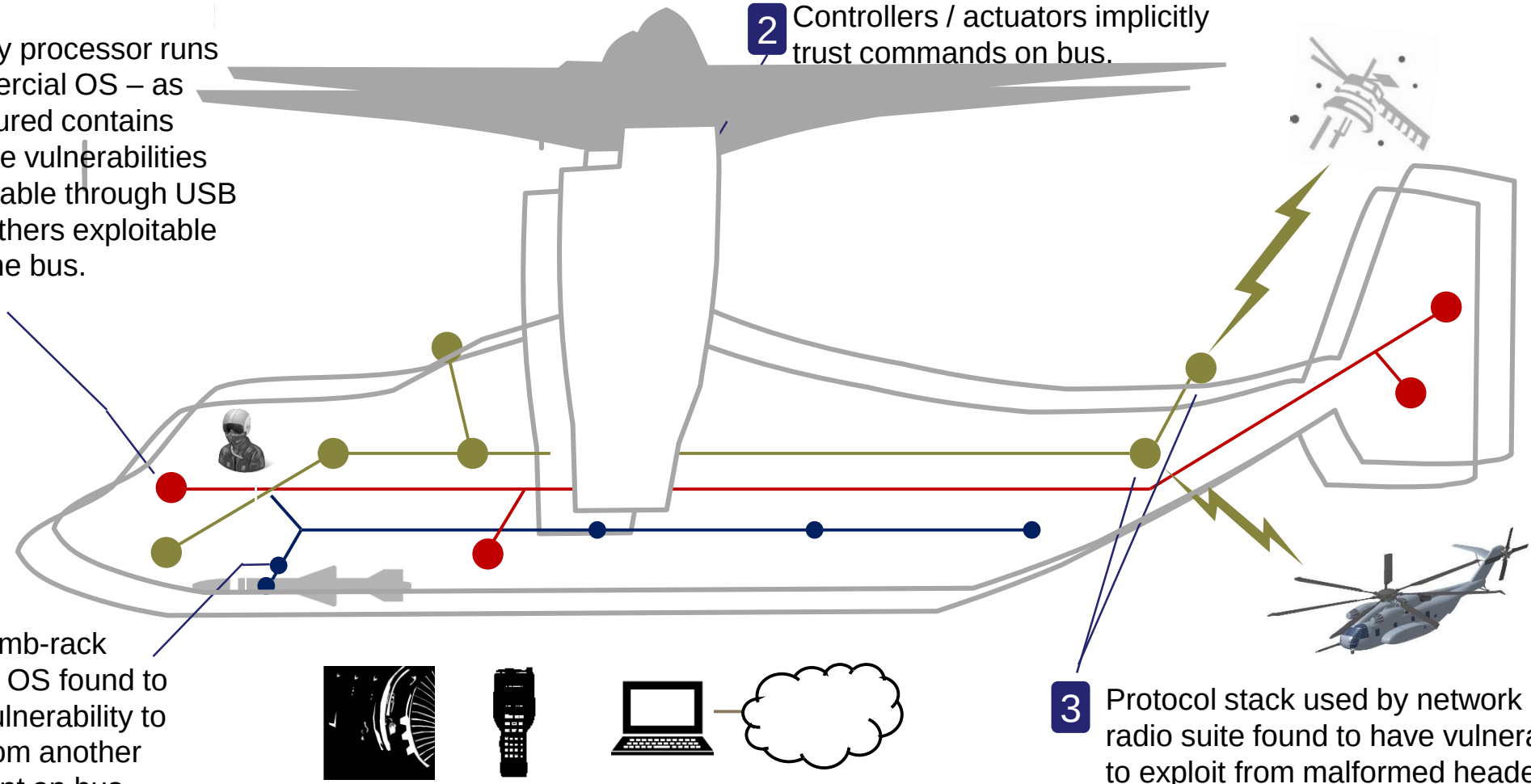
4 Malware spreads laterally from another infected air-craft exploiting implicit trust

**All similar to actual incidents we're seen and/or cases we've been able to replicate*

Vulnerabilities - Typical from our Experience*

1 Display processor runs commercial OS – as configured contains multiple vulnerabilities exploitable through USB port; others exploitable over the bus.

2 Controllers / actuators implicitly trust commands on bus.



4 Smart bomb-rack controller OS found to have a vulnerability to exploit from another component on bus

3 Protocol stack used by network processors in radio suite found to have vulnerability subject to exploit from malformed headers and payloads from another network node (RED side)

Raytheon Technologies

** Typical of significant findings we commonly see in our detailed vulnerability assessments. Does not imply actual findings against any specific platform.*

Other Threats

- **UAS Threats** -- “For under $1,000, you can go into most department stores and walk out with a very capable drone that can be used for nefarious reasons. Criminals, terrorists, state actors; just about anybody can exploit a drone for malicious missions.” -- Waseem Naqvi, Director, RTX

  (“Bad to the drone” https://www.raytheonmissilesanddefense.com/news/feature/bad-drone, Retrieved April 13, 2020)

- **GPS Threats** -- ”the Department of Aerospace Engineering and Engineering Mechanics at the Cockrell School of Engineering, the team was able to successfully spoof an $80 million private yacht using the world’s first openly acknowledged GPS spoofing device.”

- (UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea, https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/, Retrieved April 13, 2020)

Aviation Cyber Security Solutions & Research

Raytheon Technologies: Counter UAS

- RTX's Windshear system rapidly integrates multiple counter-drone sensor and effector technologies to rapidly detect, track, and deter drone-related threats

  ("Raytheon Windshear", https://www.raytheon.com/sites/default/files/2019-01/4477216_CUAS_Infographic_FINAL_012519_Print.pdf, Accessed April 13, 2020)

- RTX high-energy laser weapon system uses an advanced variant of the company's Multi-spectral Targeting System, an electro-optical/infrared sensor, to detect, identify and track rogue drones

  ("Raytheon delivers first laser counter-UAS System to U.S. Air Force", http://raytheon.mediaroom.com/2019-10-22-Raytheon-delivers-first-laser-counter-UAS-System-to-U-S-Air-Force, Accessed April 13, 2020)

Raytheon Technologies: Avionics Products

CADS: Intrusion Detection System for the Avionics Bus

Product features:

- Platform Baselining
- Anomaly Detection
- Real-time Alerting
- Logging & Post Mission Analysis

"CADS: Intrusion Detection System for the 1553 Bus" https://www.raytheon.com/cyber/CADS, Accessed April 13, 2020)

A cyber anomaly detection system that provides commercial and military vehicle operators the capability to proactively identify cyber threats

Raytheon Technologies: Collins Research

Airports & Airspace of Tomorrow

- Includes research on SATCOM operations and flight safety

Cybersecurity

- Addressing the Risk Management Framework and Avionics

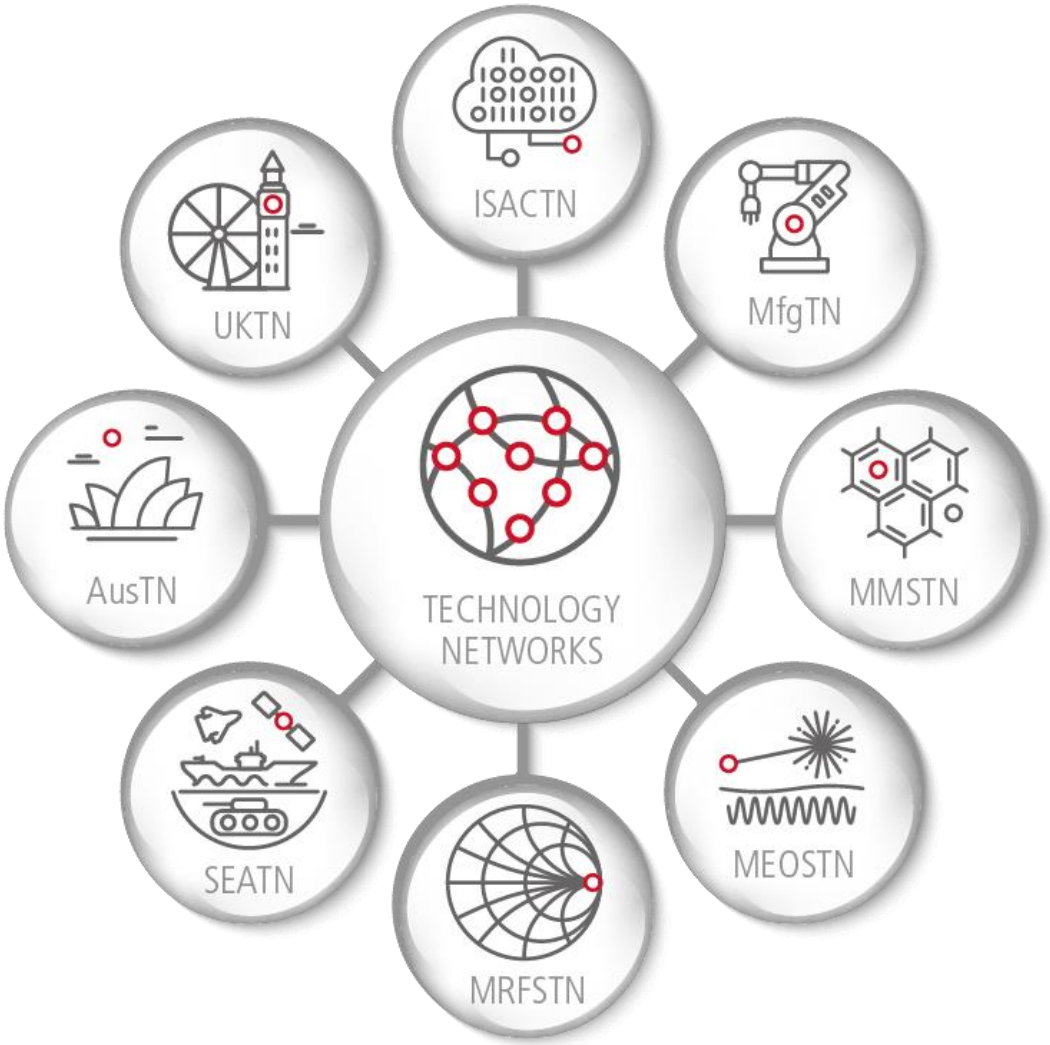
Connected Aircraft

- Research includes integration of Software Defined Networking

Avionics Research published at https://insights.rockwellcollins.com/

CyberSecurity Talent Acquisition

Technology Networks At A Glance



MISSION: To advance the knowledge of Raytheon engineers and enhance the quality and innovation of Raytheon products, systems and services through technical collaborations

100+
TECHNOLOGY INTEREST GROUPS

40K+
MEMBERSHIPS

95+
SYMPOSIA

375+
WORKSHOPS

EMPLOYEE RESOURCE GROUPS (ERGs)

PROMOTE DIVERSITY AND INCLUSION

Raytheon employees represent our talent, identity and future. **To advance an inclusive culture, Raytheon ERGs exist to lead and contribute to company projects and in our greater communities.** ERGs are forums where employees can communicate and network. An integral part of our culture, ERGs represent employees that possess particular insights stemming from unique experiences, valuable to helping Raytheon achieve its vision of global growth.

ERG VISION

Best-in-class global employee networks operating as valued strategic business partners, fostering employee success and an inclusive, engaged culture.

ERG MISSION

Energizing employees to support business objectives, growth and innovation across the enterprise; attracting, retaining and developing employees; and sustaining community connections.

RWN
Raytheon Women's Network

RAPA
Raytheon Asian Pacific Association

RADA
Raytheon Alliance for Diverse Abilities

YESNET
Young Employee Success Network

RAYVETS
Raytheon Employee Veterans Network

RAYBEN
Raytheon Black Employees Network

RAYPRIDE
Lesbian, Gay, Bisexual, Transgender, Queer and Allies

HOLA
Hispanic Organization for Leadership and Advancement

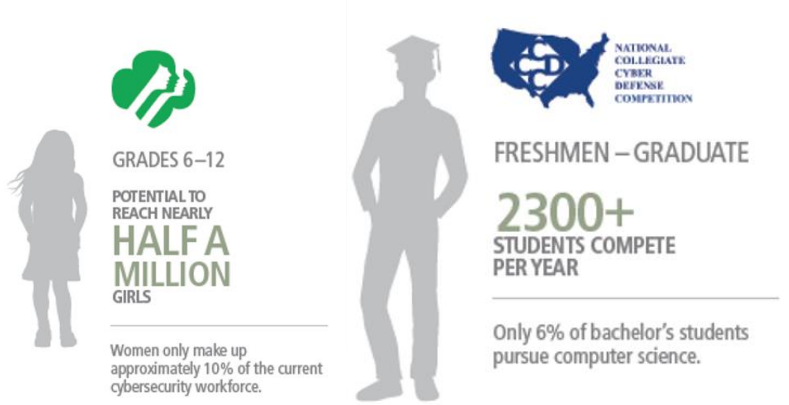
RAIN
Raytheon American Indian Network

Recruiting, Training, and Retaining Cyber Talent

EARLY TALENT INVESMENT

Raytheon Technologies' cyber CSR programs are tackling every side of the cyber workforce challenge from middle school to college and across the globe

- Girl Scouts
- Engagements with high schools
- NCCDC (National Collegiate Cyber Defense Competition)
- ISC (2) Women's Scholarships



ATTRACT PROFESSIONAL TALENT

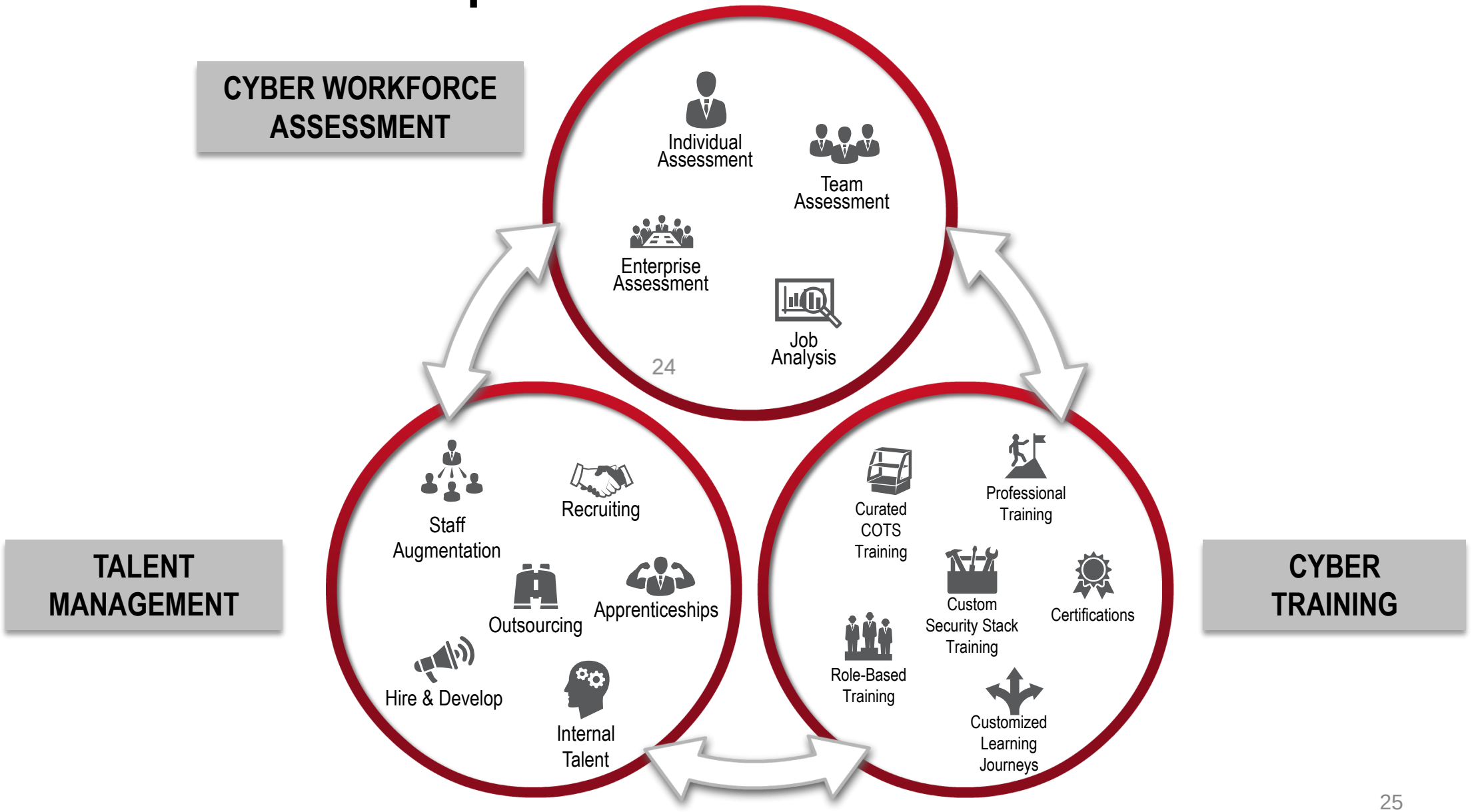
- Traditional and Tailored Sourcing
- Leveraging Technology
- Marketing Outreach
- Innovative Approaches
- Personal Touch

RETAIN TALENT

- Cater culture to the needs of cyber talent
- Offer talent opportunity to learn and develop across the full spectrum of cyber areas
- Employee engagement
- Retention incentives

Raytheon Technologies

Cyber Workforce Development



Strategic Workforce Planning and Cyber

Workforce Planning

Execute & Monitor
(Forecast vs. Actuals)

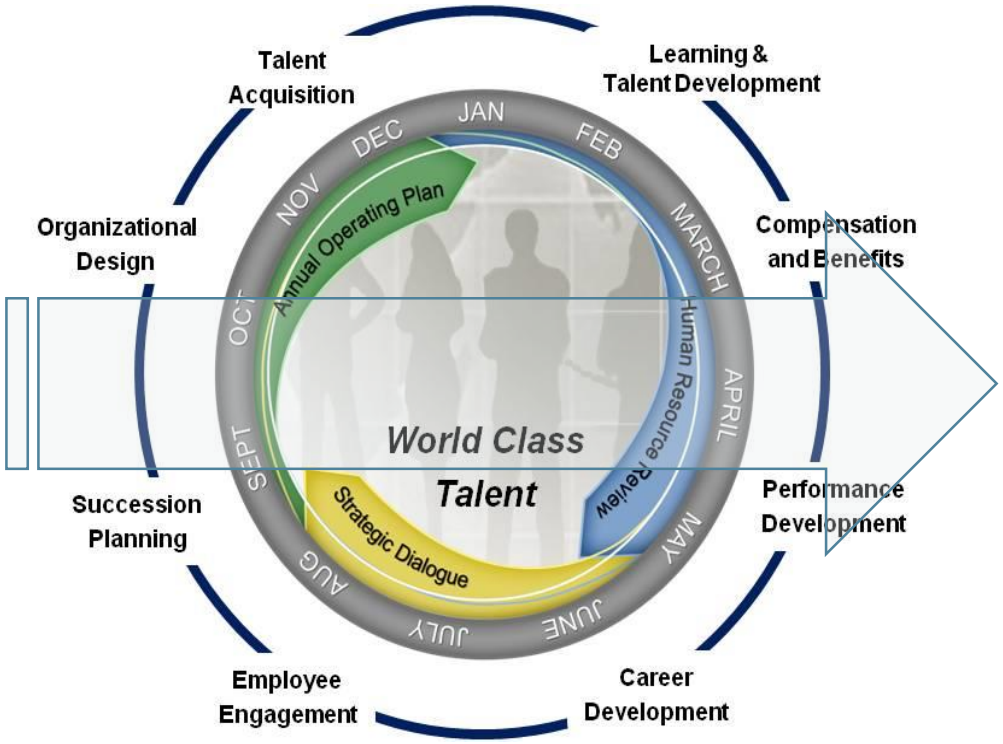
Build Workforce Plan
(Gap Fulfillment Actions)

Gap Analysis Against Current Workforce Capability/Supply

Forecast Workforce Demand Profile
(Headcount Level and Mix)

Assess Environment, Business Strategy & Financial Plan

Integrated Solutions



Deliberate Actions

Build — Internal development and rotation of Raytheon talent

Buy — Hire/acquire employees from externally

Contract — Leverage contract labor as a temporary solution for surge support

Retain — Targeted actions to reduce undesired employee turnover & transfer knowledge

Engage — Create an environment that maximizes employee contribution & productivity

Holistic Perspective + Data-Driven Insight = Purposeful Action

Raytheon Technologies

Cyber Learning

- Cyber Elite Program
- Cyber Learning
  - Internal programs that develop cyber talent
  - Programs are both “entry level” and “advanced”
  - Incorporates outside/industry recognized certifications
- University Partnerships
- Cyber Academy
  - Provides hands-on cybersecurity training and educational programs

RTX developed courses to build Cybersecurity workforce

Questions

- Raytheon Technologies is focused on:
  - providing cyber security solutions to customers
  - innovative technology to address evolving threat landscape
  - developing cyber security workforce

Cyber protection for governments, businesses and nations

Bios

Heather Romero is the Anti-Tamper/Secure Processing Technical Area Director for Raytheon Intelligence & Space. Her primary focus areas include innovative cyber research, systems integrity and software assurance.

She holds a Bachelor of Science degree in computer engineering from California Polytechnic State University in San Luis Obispo, California and a Master of Science in Cyber Security Engineering from the University of Southern California.

Mike Worden is an Engineering Fellow at Raytheon Technologies. His current position is Chief Engineer of the CODE Center, the Cyber Testing Range for Raytheon Technologies, where he is responsible for evaluating the cybersecurity of complex systems and components. Mike's research focuses is on avionics security, cyber resiliency, and automation of cyber testing.

He holds a BS in Computer Science from the US Military Academy at West Point, a Masters in Information System Security from the University of Denver and is pursuing a Ph.D from Colorado State University.