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'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.

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

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

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

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.

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.

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

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
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
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

Full spectrum operational and threat intelligence expertise

Integrated national and Internet-scale solutions
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
- Hundreds of certified ethical hackers
- 3,000 Cyber professionals across Raytheon
- 40 Specialists deployed globally each month
- Customers in 80 countries
- A leader in Next-generation high-consequence missions

- >$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
- 400+ Contracts
  - Including DHS DOMino
  - Most of our best work is classified

- Champion the development of Cyber talent and leaders
- 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
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 FFIRA report)
- Security breaches have increased by 67% since 2014 and 11% since 2018 (Source: Accenture)

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

Ground Support and Labs
- Maintenance instruments
- Maintenance personnel

Sensing and Communications
- Satellite Comm’s
- EO/IR pod

Weapon Systems
- Targeting Systems
- Stores Management
- Smart Weapons

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

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

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

4. Malware spreads laterally from another infected aircraft exploiting implicit trust

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

*All similar to actual incidents we’ve 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.

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).

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

* 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


- **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.”

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

• 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 Technologies: Avionics Products

CADS: Intrusion Detection System for the Avionics Bus

Product features:
• Platform Baselining
• Anomaly Detection
• Real-time Alerting
• Logging & Post Mission Analysis

“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.
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.
Recruiting, Training, and Retaining Cyber Talent

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

ATTRACTION:

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

VIRTUAL CAREER FAIR
THURSDAY, APRIL 2
11 a.m. to 1 p.m. EDT
5 p.m. to 7 p.m. EDT
TEXT “NEW CAREER” TO 97211

RETENTION:

- 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

STRENGTH IN DIVERSITY

“The culture at Raytheon is extremely diverse. The people that I work with are polite, professional and always willing to help. The diverse educational background of those I work with makes it seemingly impossible for us not to solve any issue presented to us.”
- Syreeta Dukes, Database Administrator

NOW HIRING

Secure
Strong
Stable

THE POWER OF IDEAS

“Being able to work in a cohesive team environment, where new ideas are welcome, makes me come to work every day.”
- Tiffany Brooks, Supply Chain Manager
Cyber Workforce Development

CYBER WORKFORCE ASSESSMENT
- Individual Assessment
- Team Assessment
- Enterprise Assessment
- Job Analysis

TALENT MANAGEMENT
- Staff Augmentation
- Recruiting
- Outsourcing
- Apprenticeships
- Hire & Develop
- Internal Talent

CYBER TRAINING
- Curated COTS Training
- Professional Training
- Custom Security Stack Training
- Role-Based Training
- Certifications
- Customized Learning Journeys

25
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

- Talent Acquisition
- Organizational Design
- Succession Planning
- Learning & Talent Development
- Performance Development
- Compensation and Benefits
- Employee Engagement
- Career Development
- Real Operating Plan
- Strategic Dialogue
- Management

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
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.