Cyber Security Capabilities Overview

Raytheon Canada Limited
Marius Ghinescu
Raytheon at a Glance

OUR BUSINESSES ARE ORGANIZED BY KEY MISSION AREAS

IDS
Headquartered in Tewksbury, Massachusetts, Integrated Defense Systems specializes in air and missile defense, large land- and sea-based radars, and systems for managing command, control, communications, computers, cyber and intelligence. It also produces sonars, torpedoes and electronic systems for ships.

IIS
Headquartered in Dulles, Virginia, Intelligence, Information and Services designs and delivers solutions and services that leverage its deep expertise in cyber, analytics and automation. Software, systems integration, and the support and sustainment of Raytheon and other companies’ systems for intelligence, military and civil applications are delivered across five markets: space, digital battlespace, cyber, intelligent transportation and high-consequence training.

RMS
Headquartered in Tucson, Arizona, Raytheon Missile Systems is the world’s premier missile maker, providing defensive and offensive weapons for air, land, sea, and space, including interceptors for U.S. ballistic missile defense. The business also builds net-enabled battlefield sensors and includes Raytheon UK.

SAS
Headquartered in McKinney, Texas, Space and Airborne Systems builds radars and other sensors for aircraft, spacecraft and ships. The business also provides communications, electronic warfare and high-energy laser solutions, and performs research in areas ranging from linguistics to quantum computing.

FORCEPOINT™
Headquartered in Austin, Texas, Forcepoint safeguards users, data and networks against accidental or malicious insider threats and advanced outside attacks across the entire threat life cycle, in the cloud, on the road and in the office. A joint venture of Raytheon and Vista Equity Partners, Forcepoint enables better decision-making, more efficient security and simplifies compliance as it protects and empowers more than 20,000 commercial and government organizations worldwide.

Raytheon Canada Limited
Raders
90% of Defence Business in Canada
Raytheon’s Footprint in Cyber Space
Raytheon’s Strengths

We take a holistic approach to the world’s toughest cyber challenges
Raytheon’s Strengths

Deep Domain Expertise

- 50 years as an intelligence industry prime
- $5.6 billion invested in cybersecurity
- Since 2006, 21 acquisitions of best-of-breed cybersecurity providers
- Unique 31,000-square-foot Cyber Operations, Development and Evaluation (CODE) Center that validates product and solution resiliency (new CODE centres in UK, Australia and Canada)
- Managed security services featuring proactive threat hunting and Virtual Security Operations Center

Large-scale Systems Integration

- National-level, scalable solutions
- Internet-scale big data and analytics
- Solutions-focused, product-agnostic approach
- Cyber mission resiliency solutions to protect against advanced threats
- U.S. DHS-certified threat screening service provider
Raytheon’s Strengths

Innovation as a Driver

- Finalist in ongoing DARPA Cyber Grand Challenge
- Internet-scale vulnerability research: 500 million+ tests/week
- Global network of cyber centers to demonstrate, build and test cutting-edge technologies
- World-class cyber range, part of global network of cyber centers
- Automated Threat Intelligence Platform
Raytheon’s Strengths

Partnerships with Industry and Government Leaders Worldwide

- Nation-scale cyber solutions
- Raytheon customers in 133 countries
- 64% of our professionals sit side-by-side with the customer
- 26 cyber facilities worldwide
  - Global Cyber Solutions Center (Dulles, Va)
  - Cyber Innovation Center (UK, Australia and Canada)
  - Cyber Solutions Integration Laboratory (Dulles, Va.)
- University partnerships to develop cyber talent worldwide

Wide Range of Customers

- Intelligence Community
- Department of Defense
- International
- Fortune 500
- Critical infrastructure
- Federal civilian agencies
Our Solutions

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

- Managed Security Services
- Cyber Hardening
- Threat Research and Assessments
- Cyber Ranges Code Center
- Converged Cyber™
- Cybersecurity Operations Centers (CSOC)
- Cyber Analytics
- Computer Network Defense
- Proactive/Dynamic Defense
- Cyber Training
Managed Security Services

Virtual Security Operations Center (V-SOC)

- Proactive, data-driven, and tailored approach to defend clients against the most sophisticated threats
- Intelligent automation reduces need to manually identify and respond to low level risks, allowing analysts to focus on more damaging threats

Proactive Threat Hunting

- Identify and eliminate intrusions to aggressively and continuously protect critical infrastructure

Detect, Isolate and Eradicate Threats

Automated Threat Intelligence Platform (ATIP)

In less than 12 minutes, our hunting approach and technology helped a Fortune 500 hedge fund find malware that could have resulted in significant losses.
Cyber Hardening

Innovative Solutions

Our network of SME experts find the exploitable vulnerabilities, determine mission impact and mitigate vulnerabilities.

Information Assurance

Latest techniques to protect, authenticate and provide secure access to information so users can trust the data.

C5I

Cyber is inextricably linked to Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems, combining sensors and advanced networks to create C5I.

Solving the hardest challenges. Hardening the most critical systems.
Raytheon protects the systems vital to the success of your routine, important and critical missions.

**Scanning Technology Horizons For the Latest Advancements and Threats**

- Reduce attack surfaces
- Conduct cooperative (Blue Team) and non-cooperative (Red Team) engagements
- Determine security control effectiveness
- Identify and preemptively close avenues of attack

**Malware and Forensic Analysis**

- Static and dynamic software analysis
- Network emulation of 100,000+ endpoints in the CODE Center

**Architectural Review for Cyber Hardening**

- Penetration testing with adversary mindset
- Identify likely vulnerabilities in system architecture

Raytheon Canada Limited
Cyber Ranges - Resiliency

The ultimate cyber proving ground for critical systems and technologies

- Test the resilience of critical technologies
- Industry-leading automation, flexibility and scalability
- Host of annual ICE Storm for all 17 intelligence agencies

Facilities

- Cyber Operations, Development and Evaluation (CODE) Center
- Global Cyber Solutions Center (GCSC)
- Cyber Innovation Center (CIC)
- Raytheon Vulnerability Research Ranges

Raytheon builds customized ranges for any customer need. Or, leverage our in-house range capability.

We identify system vulnerabilities, assess mission impact and deliver risk mitigation plans.
Converged Cyber

Integrated Cyber Defense and Correlated Threat Intelligence for International Customers

- Full picture of cyber threats from intelligence gathered from disparate sources

Elements

- Big data architecture
- Lawful intercept
- Threat intelligence
- Cyber threat simulation
- Defensive cyber operations
- Advanced OSINT

Eliminate Blind Spots in the Cyber Domain
Systems That Address Advanced Threats in High-risk Environments

- Partnerships with organizations and nations
- Mission-based solutions that incorporate active and passive defense
- Operational constructs and processes for agile threat response
- Scalable, service oriented architecture that easily enhances functionality
- Decades of intelligence and domain knowledge
- Cyber analytics that “connect the dots”
- Operator selection, training and mentoring

Raytheon delivers industry-leading cyber defense and integrated threat management.
Cyber Analytics

Leveraging Domain Intelligence to Predict the Next Attack

- Powerful analytics to reveal new threats
- Automation that streamlines analysis and enhances analyst productivity
- Connecting risks to operational and business goals

Advanced Simulation Meets Real-world Testing

- Execute complex analytics near real-time
- Identify events in hundreds of millions of streaming objects/day
- Assess cyber threat effects on vital missions in controlled environments

Raytheon’s analytics expertise enables you to effectively — and proactively — respond to evolving threats.
Computer Network Defense

National Scale Capability
We secure government information systems from cyber attacks and intrusions, up to the largest national systems

Network Resilience

- Protect, monitor, analyze, detect, and respond to unauthorized activity
- Ensure mission operations continuity before, during and after attacks

Raytheon scales to cover largest most complex systems.

U.S. Postal Service
We provide computer network defense for this high-profile agency

National Cybersecurity Protection System (NCPS)
Raytheon’s DOMino contract: $1.15 billion contract delivers full lifecycle development and sustainment for NCPS 100 plus federal and government agencies
Proactive and Dynamic Defense

Intelligence-driven Operations That Deliver Proactive Defense

- Fused multi-source information that “connects the dots”
- Monitoring network behavior to discover new attack vectors
- Cyber surveillance, reconnaissance and counterintelligence
- “Threat Hunters” proactively seek and remove advanced malware

Safeguarding the Network

- Layered defense with integrated and reinforcing features
- Data exfiltration prevention
- Rapid cyber threat information sharing and defense tuning

Raytheon delivers true proactive defense.
Cyber Training

Developing the Next-Generation Workforce

- Computer network defense and CSOC skills training for international and U.S. customers
- Cyber Incident Response Training
- 93 Foreground University courses
- 3-week intensive Cyberprofessional™ course at CODE Center & other locations
- Graduate level cyber “Black Belt” training
- Military Cyber Advanced Leaders course at Ft. Huachuca

Training for every U.S. Army intelligence specialist

Nearly 1,000 CISSP-certified cyber practitioners

Raytheon delivers true proactive defense.
Global Champion for Cyber Talent Development

Raytheon remains committed to the next generation of cyber experts.

National Cyber Security Alliance Partnership
- Commission annual original research
- Securing Our Future: Closing the Cybersecurity Talent Gap
- Raytheon sits on NCSA board

Supporting the National Collegiate Cyber Defense Competition through 2016
- Raytheon sponsors, provides technology for and hires from the nation’s largest collegiate cyber competition

Khalifa University Partnership
- Hosted UAE Security Forum: Bridging Cyber Talent Gap
- Cyber workshop and student competition

Raytheon Women’s Cybersecurity Scholarship
- Scholarships for women pursuing cybersecurity degrees
- Partnered with (ISC)2 Foundation to foster more female experts in burgeoning field
Forcepoint Joint Venture

Background

- Built on the successful integration of Websense®, Raytheon Cyber Products and the recently-acquired Stonesoft
- Forcepoint empowers organizations to drive their business forward by safely embracing transformative technologies – cloud, mobility, Internet of Things (IOT) and others
- Unified, cloud-centric platform safeguards users, networks and data while eliminating inefficiencies of point products
- 83% financial backing and ongoing access to intellectual property from Raytheon

Products

- Network Security
- Insider Threat Data Protection
- Cross Domain Access & Transfer
- Security for Cloud
- Content Security
- Advanced Analytics
- Web Filtering
Raytheon’s leading-edge cyber solutions enable you to secure your space and stay ahead of cyber threats.

Leverage Raytheon’s Full-spectrum, End-to-end Solutions

- A uniquely holistic approach to cybersecurity
- Global partnerships fueled by decades of expertise
- Firm commitment to the future of cyber, wherever it may lead
- Seeking Small Medium Businesses to partner and integrated within our global supply chain
Cyber Resiliency and Training
Backup information
IIS Cyber Solutions

Response Center Offerings

National Response Center

Enterprise Response Center

Primary Response Center

- SIEM
- Incident Response
- SOP Repository
- Trouble Ticketing

- Analysis Labs
- Malicious Code
- Incident Response
- Forensics
- Cross-Site Information Sharing

- Big Data Analytics
- National-Level Edge Monitoring
- Third-Party Site Integration

Infrastructure

- Active Directory
- Domain Name Service
- Patch Management
- Configuration Management

Converged Cyber™

- SIGINT
- Social Media
- Lawful Intercept
- e-Government Data

- Other Open Source
- External Shared Intel Data

Solution Description

- Response Center Offerings (includes Forcepoint products) provide nations and commercial enterprises with advanced network and infrastructure protection. Professional services include vulnerability assessments, penetration testing, managed detect and response, cyber range and cyber academy training.

- Converged Cyber™ includes the addition of correlated digital collections (open source, lawful intercept, etc.) to create a holistic view of cyber threats and to help with determining intent, future actions and attribution.

Key Discriminators

- Investments in Global Cyber Security Centres (CODE™) and Cyber SILs
- Past performance with US IC and DOD (tradecraft, analytics, threat intelligence)
- Market leader in identifying advanced persistent threats
- Raytheon’s DOMino contract: $1.15 billion contract delivers full lifecycle development and sustainment for National Cybersecurity Protection System (NCPS). The NCPS assists more than 100 federal civilian government agencies with the protection of their networks against advanced cyber threats.
- Knowledge transfer through training and technology insertion.

Business Model

- Capability Delivery
- Professional Services
- Managed Services

Go-to-Market

- Direct from U.S.
- Local Partnership
Cyber Resilience Products - Forcepoint

PURPOSE-BUILT COMPANY → HUMAN CENTRIC CYBERSECURITY

- One of the largest private cybersecurity companies in the world, with thousands of enterprise and government customers in more than 150 countries.
- Created by Raytheon in 2016 to commercialize defense-grade technologies for the enterprise security market.
- Supporting global governments, defense and intelligence communities to ensure success of the world’s most high-consequence missions.
Risk Adaptive and Security Effectiveness: OPPORTUNITIES TO UPGRADE CYBER POSTURE

TEAM RAYTHEON SECURITY EFFECTIVENESS

- Anti-Virus
- Firewall
- Secure Web Gateway
- Next Generation Firewall
- Email Gateway
- * Cross Domain Solutions
- Data Loss Prevention
- Insider Threat
- Next Generation Firewall
- Cloud Security Access Brokers
- User and Entity Behaviour Analytics

ITAR CONTROLLED CROSS DOMAIN SOLUTIONS
- Team Raytheon High Speed Guard
- Team Raytheon Data Guard
- Team Raytheon SimShield
- Team Raytheon Trusted Gateway System
- Team Raytheon Trusted Thin Client
- Team Raytheon Trusted Mail System
- Team Raytheon WebShield
- Team Raytheon Trusted Print Delivery

Threat-centric  Data-centric  Risk adaptive

Source: Gartner, Cybersecurity Maturity Curve

*includes Controlled Cross Domain Solutions deployed within Five Eyes community
Cyber Security Definitions (Canadian reference)

**Cyber Security**: The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.

**Resilience**: The ability to recover from or adjust to, network change, attack, misfortune, damage, or destabilizing perturbations in the cyber, operational and natural environment.

a. **Need**: A capacity that can readily recover from, or adjust to, the operational situation while maintaining quality cyber security and DCO capability. The capacity considers the present and evolving threats and the evolution of technologies within the cyber domain, ensuring the confidentiality, integrity and availability of operational information and cyber security information.

b. **Outcome**: A technical and informational capability that enables seamless operations within DND/CAF and with our key allies and partners.
Cyber Resilience

<table>
<thead>
<tr>
<th>ANTIcipate</th>
<th>WIThSTAND</th>
<th>RECOVER</th>
<th>EVOLVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise and Information Assurance (IA) Solutions</td>
<td>Enterprise and Information Assurance (IA) Solutions</td>
<td>Advanced Persistent Threat (APT) Solutions</td>
<td>Monitoring and Traffic Analysis</td>
</tr>
<tr>
<td>Monitoring and Traffic Analysis</td>
<td>Vulnerability and Security Assessments</td>
<td>Cyber Operations, Development, and Evaluation (CODE) Center</td>
<td>Vulnerability and Security Assessments</td>
</tr>
<tr>
<td>Vulnerability and Security Assessments</td>
<td>Computer Network Operations (CNO)</td>
<td>Training Solutions</td>
<td>Advanced Persistent Threat (APT) Solutions</td>
</tr>
<tr>
<td>Computer Network Operations (CNO)</td>
<td>Supply Chain Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Integrity</td>
<td>Advanced Persistent Threat (APT) Solutions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti Tamper</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Holistic Resiliency Solutions That Effectively Counter Cyber Threats**
## Cyber Resilient Solution

### Secure Lifecycle Development

<table>
<thead>
<tr>
<th>Secure System Architecture &amp; Engineering</th>
<th>Products and Solutions</th>
<th>Vulnerability &amp; Security Assessment Services</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification, Accreditation, and risk assessment</td>
<td>Endpoint / insider threat protection</td>
<td>Code validation</td>
<td>Continuous monitoring</td>
</tr>
<tr>
<td>Security requirements analysis &amp; definition</td>
<td>Cyber Situational Awareness, Visualization, and Command &amp; Control</td>
<td>Black/white box testing</td>
<td>Incident response</td>
</tr>
<tr>
<td>Process analysis, tailoring, and compliance</td>
<td>Cross-domain information sharing</td>
<td>System level scanning</td>
<td>Threat databases</td>
</tr>
<tr>
<td>Analysis and development of policies, regulations, and standards</td>
<td>Zero-day malware detection</td>
<td>Red-teaming</td>
<td>Collecting intelligence to predict threat behavior</td>
</tr>
<tr>
<td>Software assurance</td>
<td>Counterfeit protection</td>
<td>Full spectrum cyber assessment labs</td>
<td>Command and Control blocking</td>
</tr>
<tr>
<td>Security design tools</td>
<td>US Government certified cryptography</td>
<td>Supplier screening</td>
<td>Metrics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical infrastructure (non-military) assessment</td>
<td>Network mapping and route verification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Counter-intelligence research</td>
</tr>
</tbody>
</table>

### Training

- Off-the-shelf or custom
- Executive awareness for leaders
- Expert training
- Instructor-led or Web-delivered
- Developed and taught by expert practitioners
# CODE Centres - Cyber Protection System

## Cyber Test Ranges

<table>
<thead>
<tr>
<th>Scale</th>
<th>Fully Scalable and extensible</th>
<th>Deployment Automation</th>
<th>Support RF Testing</th>
<th>Anechoic Chamber</th>
<th>Hardware in the loop</th>
<th>Layer 1 Switches</th>
<th>Pen Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nation Scale</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Medium Scale</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Primary Scale</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Pen Testing**
  - Supports more than 175 virtualized environments
- **Training**
  - Automated Scoring
  - Supports about 20 teams and about 200 events/year
  - Capture the Flag, Red-on-Blue
- 16 Racks of HW, 100+ WKS
- Example: Emulate all power plants in a country

- **Pen Testing**
  - Supports more than 75 virtualized environments
- **Training**
  - Automated Scoring
  - Supports about 6 teams and about 100 events/year
  - Capture the Flag, Red-on-Blue
- 6 Racks of HW, 80 WKS, 6 video walls
- Example: Emulate one power plant

- **Pen Testing**
  - Supports around 20 virtualized environments
- **Training**
  - Automated Scoring
  - Supports 2 teams and about 30 events/year
  - Capture the Flag, Red-on-Blue
- 1 Rack of HW, 10 WKS, 1 video wall
- Example: Emulate a department in a power plant

## SCALABLE ARCHITECTURE FOR CYBER TESTING, SIMULATION, DEMONSTRATION, AND VULNERABILITY ASSESSMENT
Correlated Digital Monitoring
Market Driven Capabilities to Expand Situational Awareness through Cyber

CONVERGED CYBER SOLUTION ACHIEVED THROUGH EXPANDED DIGITAL COLLECTION AND CORRELATION
The State of Cyber Security Training

**Current State**
- Outgrowth from traditional IT certification
- Focus on information assurance and data centers
- Focus on cyber defense vice offense
- Minimal dynamic defense relative to hardening national assets
- Static course curriculum with limited experiential learning
- STEM educational courses not adequate
- Certifications do not map to new cyber work roles
- Limited understanding of Electronic Warfare (EW)
- Cyber warrior demand far outweighs supply

**Future State**

We envision…
- **Education** as the foundation; continuous learning is accessible
- Cyber warriors will have **ninja-like expertise**
- Comprehensive training is **permeated** across all functions
- Training delivered by operations experts
- Real world dynamic learning environment
- Anticipates future threats and emerging technologies
- Offense and defense (including EW) are integrated and operational.
- Cyber **certifications**, a predictor of job readiness
- **Scalability** is achieved: Pipeline of experts
Cyber Learning at All Levels

**Executive / Decision-Maker**

**Objective**
Increase understanding of the cyber threat environment to enable better decision making in managing cyber technology and resources

**Targeted Learners**
Commanders and Senior Executives

**Delivery**
Lecture, Web-based Vignettes, Modeling and Simulation

**Duration:** 3 Hours and/or 2 Days

**Manager**

**Objective**
Provide students with the knowledge to manage resources to solve challenging cyber problems within appropriate mission environments

**Targeted Learners**
First-line supervisors and managers who serve in a cyber role who need a strong technical overview of cyber and cyber-related activities

**Delivery**
Lecture, Web-based Vignettes, Modeling and Simulation

**Duration:** 1 Week

**Practitioner**

**Objective**
Provide students with the knowledge and ability to solve challenging cyber problems (e.g. SOC operations, re-blue teams)

**Targeted Learners**
Information technology and mission systems professionals who serve in a cyber and/or cyber-related role

**Delivery**
Lecture, Web-based Vignettes, Modeling and Simulation

**Duration:** 3 Weeks to 3-5 years
National Cyber Academy Offering

- Blue print for establishing and operating an Academy that can be equipped to service nation state cyber and IT training needs
- International standard for skills training and serves as a regional asset for education, research and innovation
- Flagship cyber curriculum and specialty courses designed to develop a skilled workforce via a proven career path
- Anticipates future threats and emerging technologies to augment bespoke training plans
- Multiple entry/exit ramps to enable structured educational focus in gaps in skill sets needed to perform a desired role
- Train the Trainer to enable autonomy in ongoing education process and allows customers to develop their own cyber capabilities to support specific needs