Cyber S&T Program Overview

Dr. Julie Lefebvre
Director S&T Joint Force Development

2013 DHS S&T CSD PI Meeting
16 September, 2013
SIX STRATEGIC PRIORITY AREAS:

1) Build agile forces to carry out missions in complex and hostile environments.
2) Protect and support Canadian Armed Forces members before, during and after operations.
3) Enable the acquisition, sharing and use of critical information in support of situational awareness and decision-making.
4) Develop and implement solutions to ensure an affordable, sustainable and effective Department of National Defence (DND) and Canadian Armed Forces (CAF).
5) Support public safety and security practitioners in their mission to protect Canadians.
6) Anticipate, prepare for, and counter the emergence of future threats.

DRDC supports innovation and S&T as an engine for generating solutions.
Cyber S&T Program Resources

• 5-8 M$/year
• 40+ researchers with Cyber Defence expertise across 3 Research Centres
• DRDC accesses external capacity in other government departments (OGDs), industry and academia; collaborates with international & domestic partners
Cyber S&T Program Outcomes

- **Resilient Architectures and Interoperable Networks**
  CAF have increased resiliency in deployed operational and tactical networks and systems in contested environments

- **Trust and Confidence**
  CAF gain trust in their ITI to achieve missions and confidence in their decision-making ability for conducting cyber operations

- **Cyber Operations Capabilities**
  CAF have improved capabilities for operating in a cyber environment

**CANADIAN ARMED FORCES (CAF) HAVE FREEDOM OF ACTION IN THE CYBER ENVIRONMENT, WHILE DENYING THE SAME TO THEIR ADVERSARIES**

**CRITICAL ENABLER**

**Cyber Network Operations (CNO) Experimentation and Training Capability**
Cyber S&T Program – Projects

Platform-to-Assembly Secured Systems

- Platform risk analysis
- Improve cyber defence and resilience at host and platform levels
- Advanced tools for vulnerability analysis and reverse engineering

Cyber Decision Making & Response

Support cyber decision making and defensive courses of action through
- Automated cyber defence capability
- Security & defence metrics for risk analysis
- Advanced cyber operations tools and methodologies
Cyber S&T Program – Projects (cont’d)

Cyber Capability Development Centre

An agile and effective Cyber Network operations (CNO) S&T infrastructure and service capability for research, experimentation, testing, validation, demonstration and training.

Tactical Network Operations

Securing next-generation tactical networks.

- Situational awareness and command & control enabling full-spectrum cyber operations in a tactical edge network
- Cross-layer security in distributed networks including physical layer effects
E- Security: Policy and Strategic Drivers

• NCSS - National Cyber Security Strategy

Specific Initiatives

Canada’s Cyber Security is built on three pillars

- Securing Government systems
- Partnering to secure vital cyber systems outside the Federal Government
- Helping Canadians to be secure online
Canada Safety and Security Program (CSSP)

The CSSP scope is to deliver S&T solutions, support and advice to respond to Canada’s public safety and security imperatives.

Some of the new investments (2013-14)

- Canadian SCADA-Smart Grid Industry/Academia/Government Workshop
- Data Centric Security Approaches for SCADA CYBER
- Collaborative Identification and Localization of Wireless Security Threats and Intelligent Countermeasure Deployment
- Data Mining Algorithms for Advanced Persistent Cyber-Threat Detection