Cyber Operations in the Canadian Armed Forces

Master Warrant Officer Alex Arndt

Canadian Forces Network Operations Centre

Agenda

- Problem Space
- Definition of Cyber Warfare
- Key Terminology
- Defence Policy Review: Overview of Cyber-related Initiatives
- Realities versus Expectations
- Challenges
- Cyber Operator Occupation

MWO Alex Arndt

- MOSID 00378 – Cyber Operator
- 27 years in the CAF
  - Experience includes Infantry, SIGINT, EW and Cyber
- Graduate of the Army Technical Warrant Officer Programme
  - Expertise in Capability Development, Project Management, Trials Management and Procurement
- Nearly 15 years of Cyber Operations experience
- Several Industry Certifications
  - CISSP, SANS GCIA and GCIH, EC-Council ECIH

Problem Space

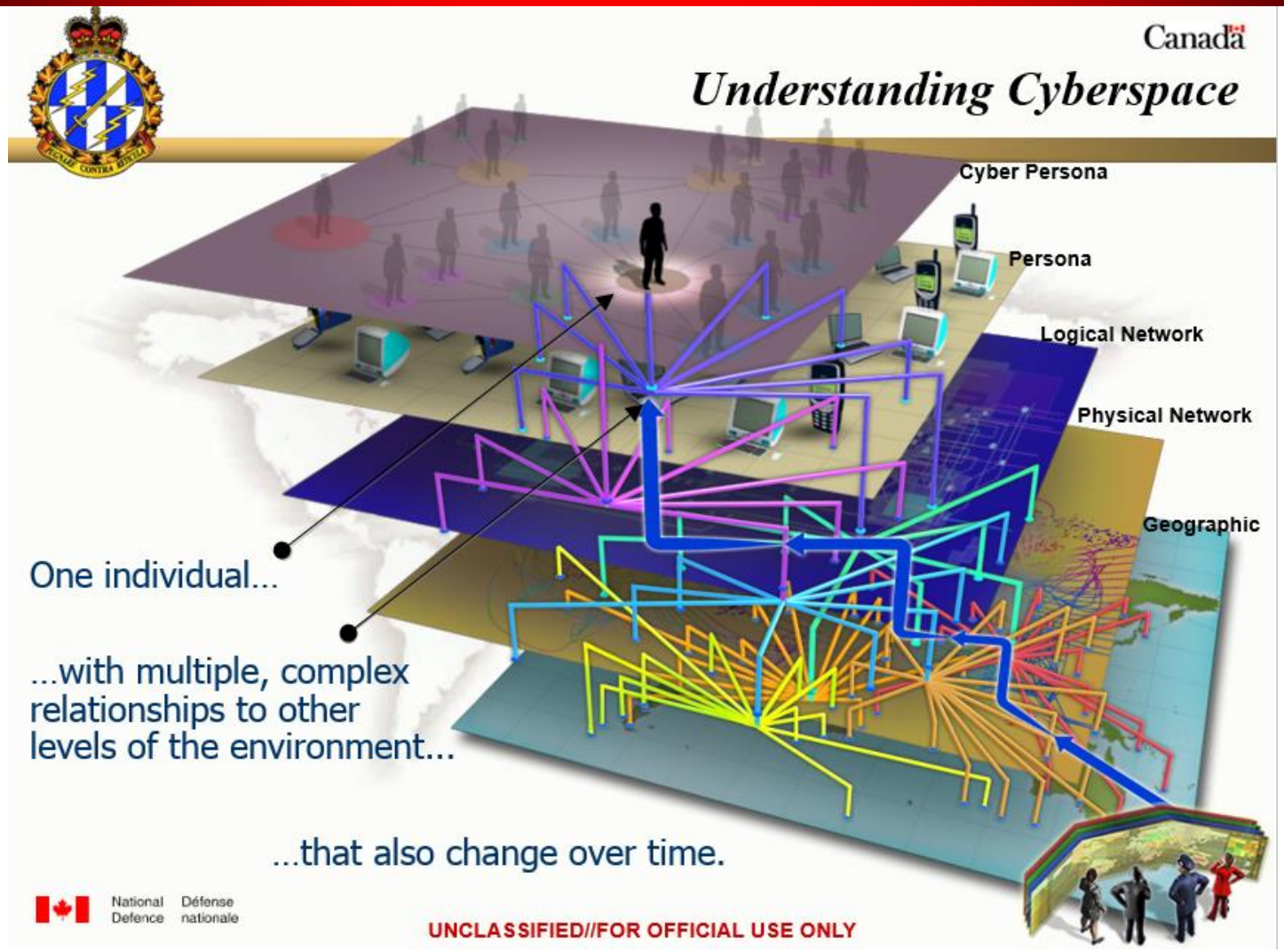
- Canada through its new Defence Policy, has announced its intention to develop active cyber capabilities
- Up until recently,Canada lacked dedicated Cyber Forces to conduct Cyber Operations
- Legal, Policy and Authority challenges required Legislative and Procedural review

Problem Space

- Clear direction and resource management required to ensure the appropriate personnel and budget are available

- Expectations need to be managed

Problem Space



Definition of Cyber Warfare

"The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic military purposes."

Reference: NATO AJP-3.20

Key Terminology

Cyber operational preparation of the Environment (Cyber OPE)

- Cyber activities conducted to prepare and enable cyber intelligence, surveillance, and reconnaissance in support of cyber operations.

Reference: Joint Doctrine Note – Cyber Operations

Key Terminology

Defensive cyber operation (DCO)

- A defensive operation conducted in or through cyberspace to detect, defeat and/or mitigate offensive and exploitive actions to maintain freedom of action. A DCO may include internal defensive measures and response actions.

Reference: Joint Doctrine Note – Cyber Operations

Key Terminology

Defensive cyber operation - Internal defensive measures (DCO-IDM)

- In DCOs, measures and activities conducted within one's own cyberspace to ensure freedom of action.

Reference: Joint Doctrine Note – Cyber Operations

Key Terminology

Defensive cyber operation - response action (DCO-RA)

- In DCOs, measures and activities conducted in or through cyberspace, outside of one's own cyberspace, against ongoing or imminent threats to preserve freedom of action.

Reference: Joint Doctrine Note – Cyber Operations

Key Terminology

Key Cyber Terrain

- Key terrain in the cyber context still needs to be defined. It is currently defined as “Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant.

Reference: Joint Doctrine Note – Cyber Operations

Key Terminology

Support cyber operation (SCO)

- A network operation tasked by, or under direct control of, a commander to support offensive and defensive cyber operations.

Reference: Joint Doctrine Note – Cyber Operations

Key Terminology

Offensive cyber operation (OCO)

- An active operation intended to project power in or through cyberspace to achieve effects in support of military objectives.

Reference: Joint Doctrine Note – Cyber Operations

Key Terminology – So what?

- Terminology is derived from Doctrine

- Provides the basis upon which Operational Planning Process is undertaken to define Cyber Operations and synchronize them with other Forces conducting Operations (e.g. coordinating DoS attack of adversary C2 network with the advance of ground forces into a given area)

Defence Policy Review – Cyber Related Initiatives

- The Canadian Government has laid out 7 initiatives that are related to Cyber in the new defence policy *Strong, Secure, Engaged*

- All initiatives provide the strategic direction necessary to realign resources and define, in broad terms, what is required to meet declared objectives

Defence Policy Review – Cyber Related Initiatives

- Represents the basis upon which future Doctrine, and Tactics, Training and Procedures (TTPs) for Cyber Operations will be developed

Defence Policy Review – Cyber Related Initiatives

Initiative 65

- Improve cryptographic capabilities, information operations capabilities, and cyber capabilities to include: cyber security and situational awareness projects, cyber threat identification and response, and the development of military-specific information operations and offensive cyber operations capabilities able to target, exploit, influence, and attack in support of military operations.

Reference: "Enhancing Defence Intelligence" in *Strong, Secure, Engaged. Canada's Defence Policy*

Defence Policy Review – Cyber Related Initiatives

Initiative 71

- Build CFINTCOM's capacity to provide more advanced intelligence support to operations, including through an enhanced ability to forecast flashpoints and emerging threats, better support next generation platforms, and understand rapid developments in space, cyber, information and other emerging domains.

Reference: "Enhancing Defence Intelligence" in *Strong, Secure, Engaged. Canada's Defence Policy*

Defence Policy Review – Cyber Related Initiatives

Initiative 75

- Assign Reserve Force units and formations new roles that provide full-time capability to the Canadian Armed Forces through part-time service, including:
  - Light Urban Search and Rescue;
  - Chemical, Biological, Radiological and Nuclear Defence;
  - Combat capabilities such as direct fire, mortar and pioneer platoons;
  - **Cyber Operators**;
  - Intelligence Operators;
  - Naval Security Teams; and
  - Linguists.

Reference: "A New Vision for the Reserve Force" in *Strong, Secure, Engaged. Canada's Defence Policy*

Defence Policy Review – Cyber Related Initiatives

Initiative 87

- Protect critical military networks and equipment from cyber attack by establishing a new Cyber Mission Assurance Program that will incorporate cyber security requirements into the procurement process.

Reference: “Cyber Capabilities” in *Strong, Secure, Engaged. Canada’s Defence Policy*

Defence Policy Review – Cyber Related Initiatives

Initiative 88

- Develop active cyber capabilities and employ them against potential adversaries in support of government-authorized military missions.

Reference: “Cyber Capabilities” in *Strong, Secure, Engaged. Canada’s Defence Policy*

Defence Policy Review – Cyber Related Initiatives

Initiative 89

- Grow and enhance the cyber force by creating a new Canadian Armed Forces Cyber Operator occupation to attract Canada's best and brightest talent and significantly increasing the number of military personnel dedicated to cyber functions.

Reference: "Cyber Capabilities" in *Strong, Secure, Engaged. Canada's Defence Policy*

Defence Policy Review – Cyber Related Initiatives

Initiative 90

- Use Reservists with specialized skill-sets to fill elements of the Canadian Armed Forces cyber force.

Reference: “Cyber Capabilities” in *Strong, Secure, Engaged. Canada’s Defence Policy*

Realities versus Expectations

Active Cyber Capabilities

- In *Strong, Secure, Engaged*, it states that the CAF will assume a more assertive posture in the cyber domain by hardening our defences, and by conducting active cyber operations…
  - Rules of Engagement will need to be clarified
  - Investments will be required to explore and develop appropriate capabilities

Realities versus Expectations

Availability of Cyber Operators

- Recruiting will take place in a '**competitive environment**' to attract Canada's best and brightest talent
- **Significant training** will be required to develop specialists in this domain
- It will be challenging to meet all current and future demands.

Challenges

National and International Laws

- Cyber operations will be subject to all applicable domestic law, international law with proven checks and balances.

Challenges

National Security Policy and Legislation

- They are constantly being reviewed to ensure that the CAF have the appropriate framework to conduct its operations as mandated by the Government.

Challenges

Recruitment, Training and Retention

- The Canadian Government and CAF recognize that the pool of talent is shared with Industry
- Salary considerations are only a small part of the problem

Cyber Operator Occupation

- Authorized in 2016
- Created on 31 January 2017
- First round of Regular Force selection occurred in summer 2017
- First Regular Force Cyber Operators selected and converted in October 2017

Cyber Operator Occupation

- Second round of Cyber Operator selection for Reg F and Reserves is currently underway; completion expected in Feb 2018

- Direct Entry with CAF-endorsed programs by Summer 2018. Direct Entry with minimum entry standards by Summer 2019. Minimum entry standards to be promulgated by Jan 2018

- Opportunity for Reservists with unique set of skills and knowledge to be part of the CAF Cyber Force either as Cyber Operators or in other capacities

Cyber Operator Occupation
Primary Reserve

- The Primary Reserve provides an opportunity for the CAF to identify and harness Cyber talents

- Information Systems Security Professionals working in the Private or Public Sector across the country have an opportunity to support the Canadian Armed Forces (CAF) Cyber Force through part-time employment

Cyber Operator Occupation
Primary Reserve

Please contact your local Recruiting Centre to get information about the Regular Force and Reserve Force opportunities in the new Cyber Operator (MOSID 00378) occupation

Questions?