IT Security vs. Defensive Cyber Operations:

The evolution of CAF Cyber

Master Warrant Officer Alex Arndt

Canadian Forces Network Operations Centre

1 November 2018

Canada

Outline

- “The Centre”
- How does CAF Cyber fit in?
- CFNOC evolution
- ITS vs. DCO
- SSE – Where are we now?

MWO Alex Arndt

- MOSID 00378 – Cyber Operator
- 28 years in the CAF
- Experience includes Infantry, SIGINT, EW and Cyber
- Graduate of the Army Technical Warrant Officer Programme
- Over 15 years of Cyber Operations experience
- Several Industry Certifications
  - CISSP, SANS GCIA and GCIH, EC-Council ECIH

Canadian Centre for Cyber Security (aka “The Centre”)

- The CCCS is announced in January 2018
- Government of Canada released National Cyber Security Strategy in June 2018
  - Three areas of focus: Security and Resilience, Cyber Innovation, Leadership and Collaboration
- The CCCS brings three organizations together to provide Leadership
  - CSE (ITS Branch)
  - SSC (SOC)
  - PS (CCIRC and GetCyberSafe)

Canadian Centre for Cyber Security (aka “The Centre”)

- CCCS consolidates ITS functions into one integrated team:
  - Defence of Government of Canada systems
  - Expert advice and guidance
  - Threat assessments and reporting
  - Coordinated incident response
  - Secure solutions and services
  - Cyber security training and education
- PS remains responsible for ITS policy

CAF integration into CCCS

- CAF has only one Cyber Unit (CFNOC)
- Historically CFNOC has performed similar functions to CCCS, in partnership with other CAF/DND partners
  - DIMEI (ITS engineering)
  - Dir IM Secur (ITS policy and SA&A)
  - ISSOs (IR actions and reporting)
- CFNOC will continue to collaborate with CCCS to ensure ITS delivery is responsive, efficient and effective for DND/CAF networks
- Establishment of CCCS allows for evolution towards DCO

Canadian Forces
Network Operations Centre (CFNOC)

Mission: CFNOC will gain and maintain cyber superiority within the DND/CAF's cyber AOR in order to assure friendly forces freedom of action.

What does CFNOC do?

CFNOC conducts defensive operations within DND/CAF's cyberspace to detect, defeat, and/or mitigate offensive and exploitive actions to maintain freedom of action.

Defensive Cyber Operations - Internal Defensive Measures (DCO-IDM)

Defensive Cyber Operations (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

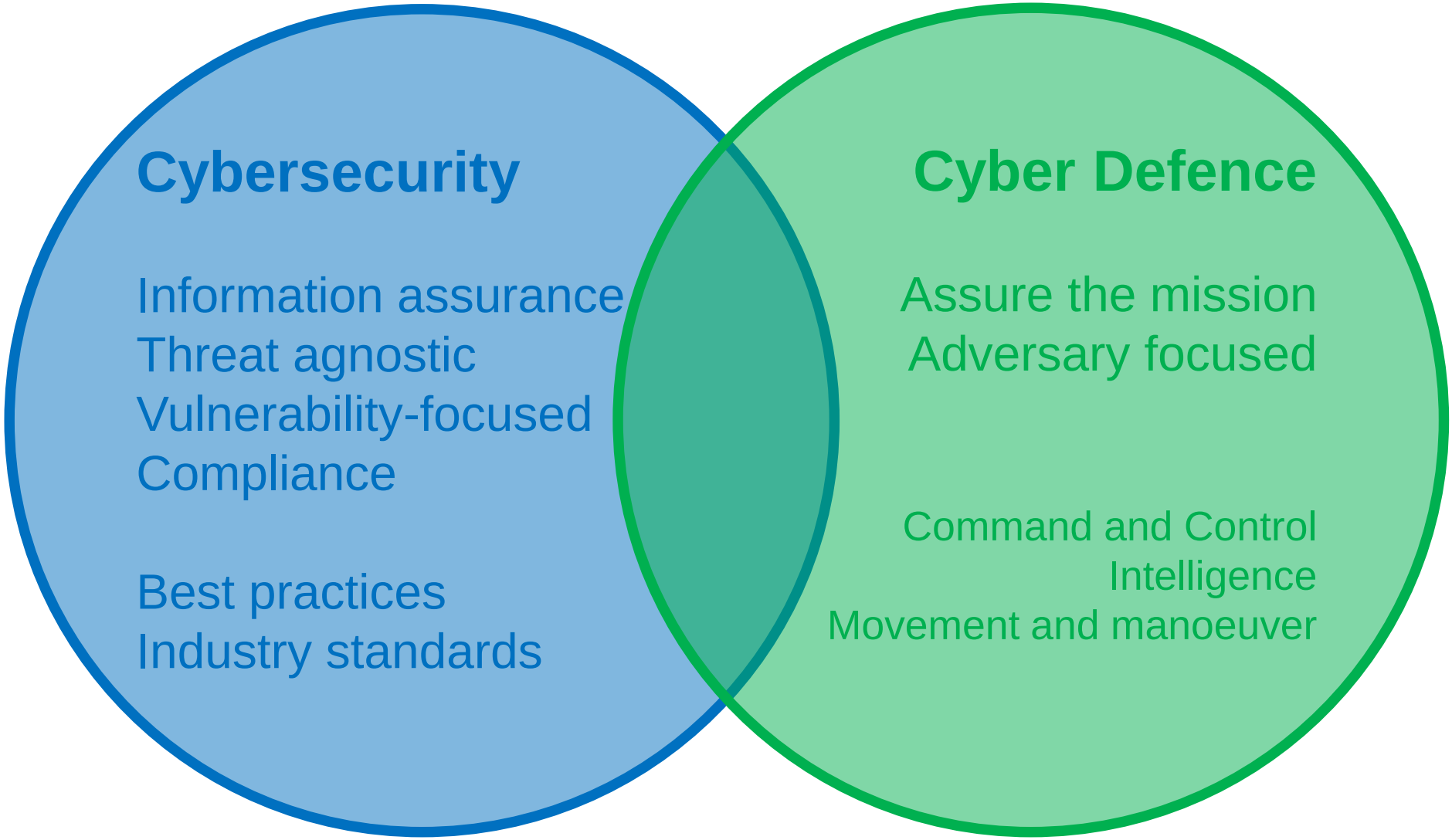
Defensive cyber operation - Internal defensive measures (DCO-IDM)

Measures and activities conducted within one's own cyberspace to ensure freedom of action

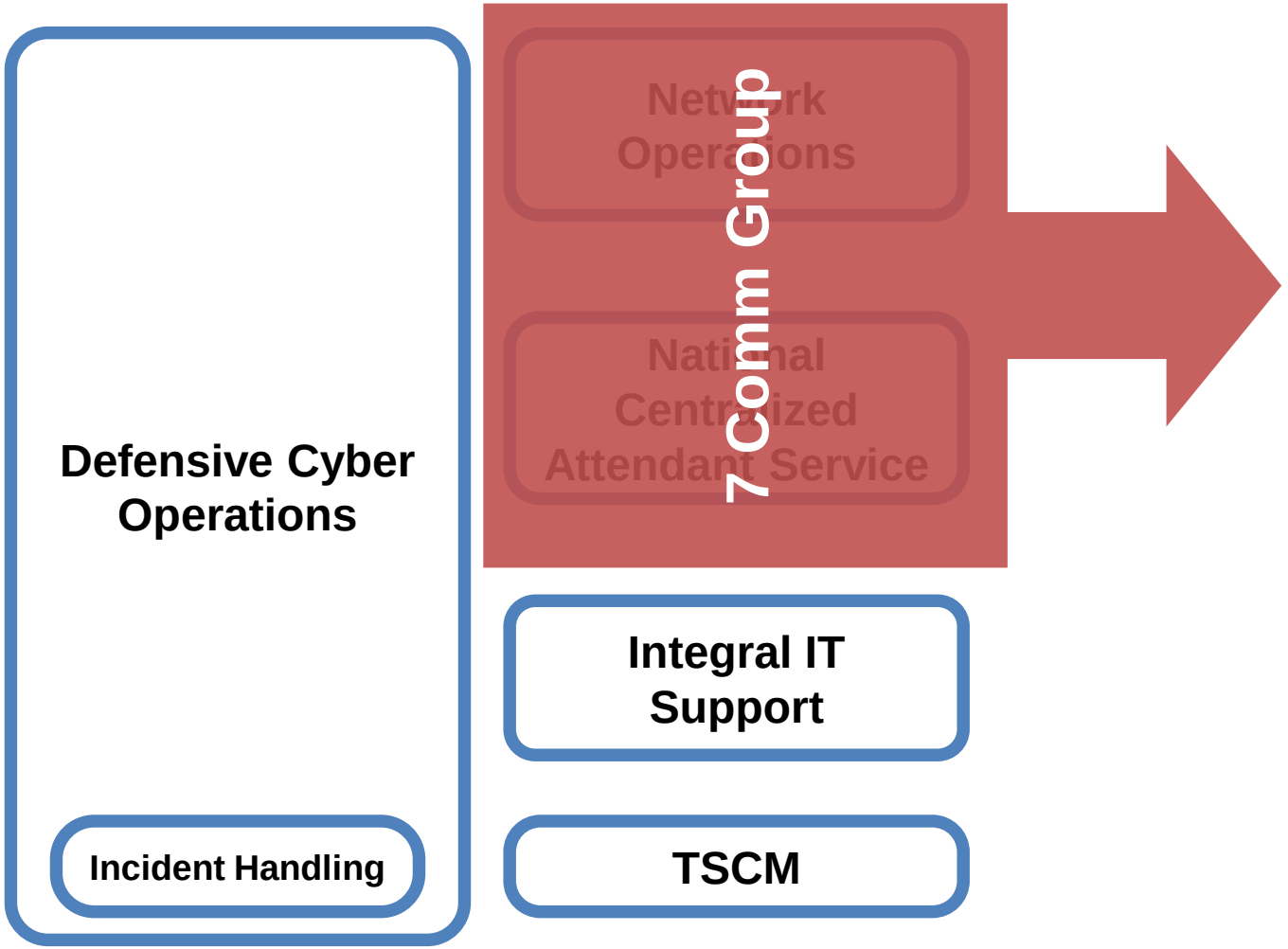
A quote from the Commander of CFIOG…

“CFNOC’s role is not to be another layer of IT Security but to defend against and defeat our adversaries in this battlespace…” – Colonel Dave Yarker

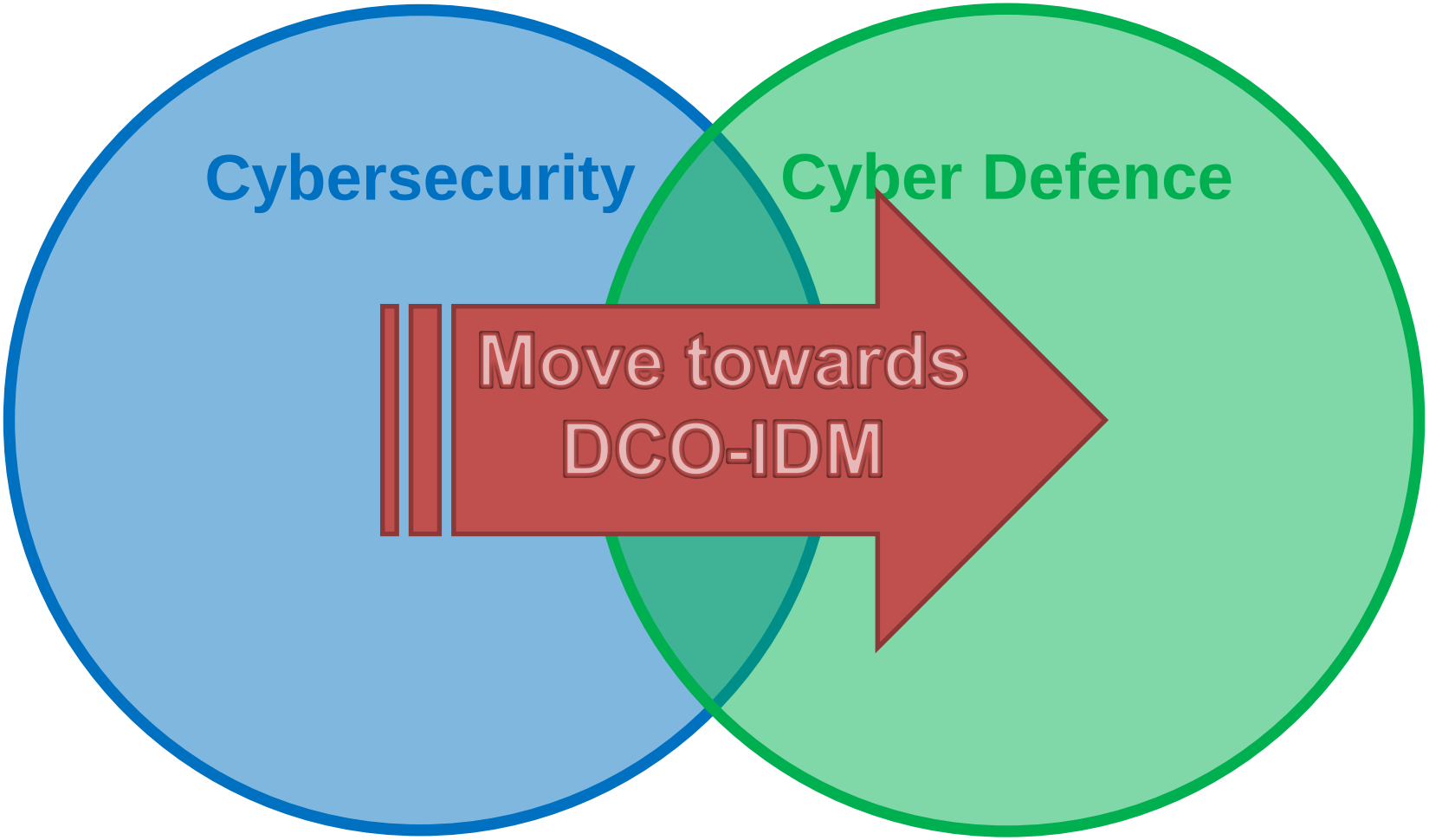
ITS vs. DCO


Cybersecurity
Information assurance
Threat agnostic
Vulnerability-focused
Compliance
Best practices
Industry standards
Cyber Defence
Assure the mission
Adversary focused
Command and Control
Intelligence
Movement and manoeuver

How has CFNOC changed?



CFNOC Evolution



SSE – Where are we now?

- Ongoing DCO-IDM evolution ensures that CAF Cyber is focused on supporting Commanders
- CAF DCO will not duplicate CCCS responsibilities writ large
- Initiatives 65 and 89 are being met
- Initiatives 75 and 88 continue to be worked on

SSE 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
- **Initiative 75 –** Assign Reserve Force units and formations new roles that provide full-time capability to the Canadian Armed Forces through part-time service
- **Initiative 88 –** Develop active cyber capabilities and employ them against potential adversaries in support of government-authorized military missions
- **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.

Canadian Forces Network Operations Centre

"Fight the Networks"

Canada