IT Security Professionals Role in Enabling Forces for Mission Success in Globally Integrated Operations

BSides

September 2014

BGen R. Mazzolin, DGIMO/DJ6

Evolving Role of the IT Security Professional

- Historical Perspective
- Strategic Imperatives
- From Support to Operations
  - Strategic Imperatives
  - Threats
  - Cyber and Operations

Historical Perspective

- Early Days – Pre Internet
  - Discrete Communication Systems
  - Quantifiable measures
  - Prescriptive Standards
- Emergence of Networking
  - Certification and Accreditation
  - COMPUSEC – Rainbow Series of Standards
  - ITSEC + Physical, Procedural and Personnel
- Today
  - Dynamic technology evolution
  - Evolution from Infosec to Enterprise Risk Management

Strategic Imperatives

- External Drivers
  - Volatile, Uncertain, Complex and Ambiguous (VUCA) Strategic Planning Environment
    - MENA: Regional Issues
    - Asia – Pacific
    - Post Afghanistan
  - Global Economic Downturn = “Efficiencies Initiatives”
    - SR, DRAP, ASR (Shared Services Canada)

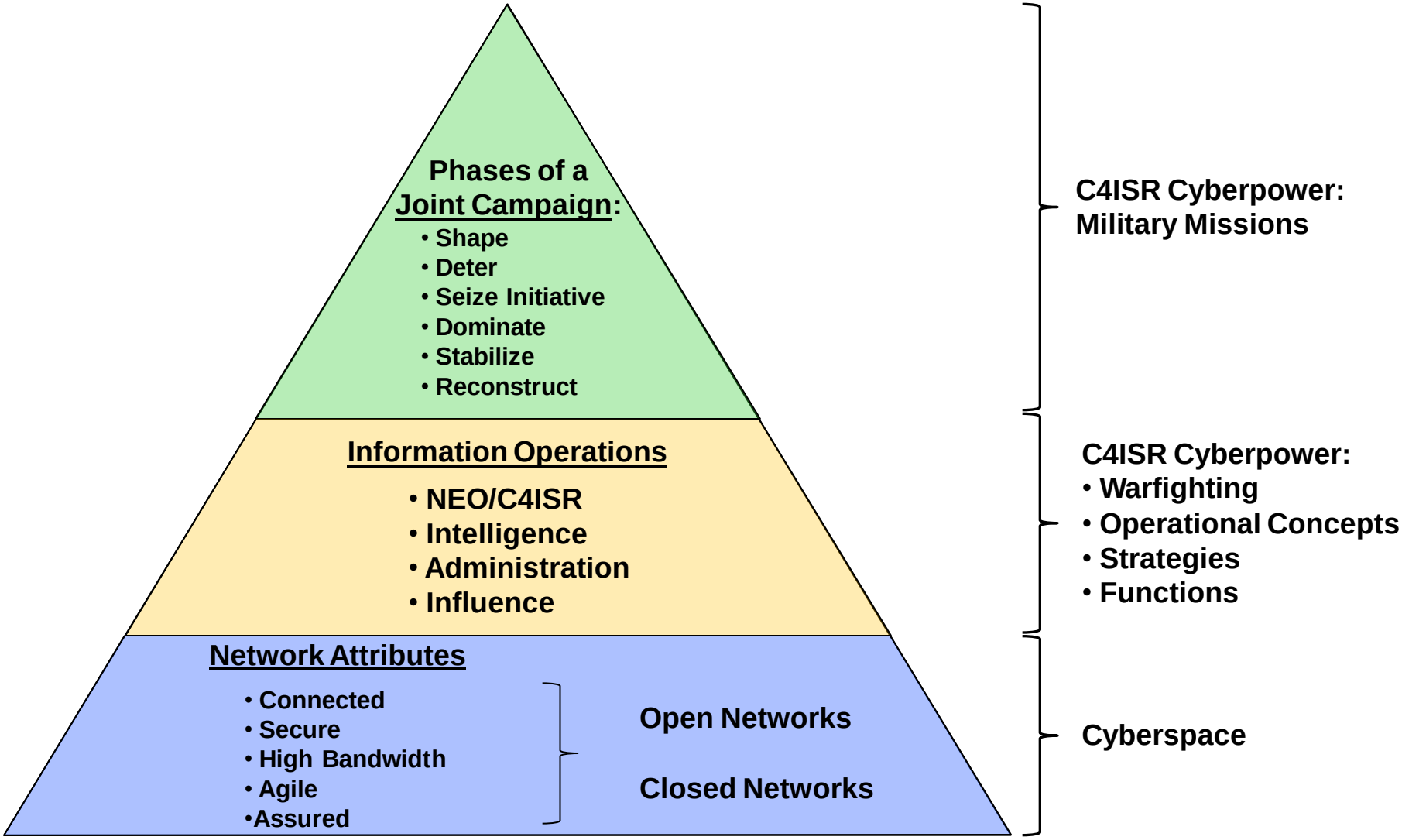
Strategic Imperatives

  - PCO and TBS Engagement and Oversight
  - Focus on “Canada First” – The North
  - Defence as part of the national security construct
- Internal Drivers
  - Affordability of the DND/CF/Government Programmes
  - CF Transformation/Defence Renewal
  - Government role in Public Safety/Cyber

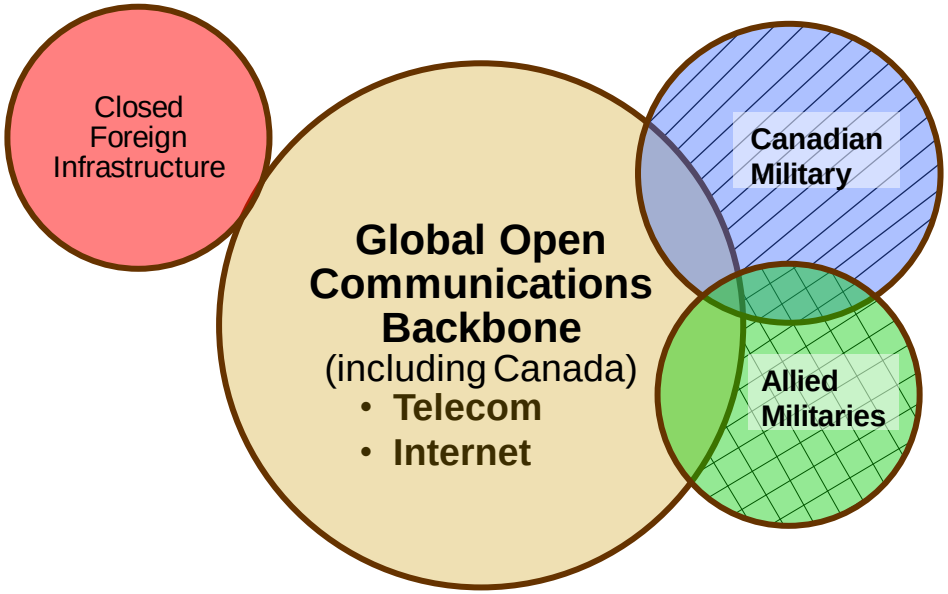
Simplifying The Complexity

- IT as a Central Enabling Capability
  - IT Infrastructure is the Operational Infrastructure
- The Complex
  - The Internet of Everything and Everyone – Impact on Contemporary Military Operations
    - Machine to Machine (M2M) Interaction
      - Interoperability
      - Resource Limitations – federal rationalization initiatives
      - Procurement and Industry Participation
    - Big Data and Business Intelligence (BI) – Painting a picture of the real world using all the virtual bits
      - Relationship to C2
  - State and Non-State Actors with $$$, Time and Skills
- Simplifying it down
  - It's not all virtual. Real physical infrastructure still needs to be connected and protected in the real world
  - It's not all new. EM spectrum has been understood and exploited for a long time.

Military Cyberpower



C4ISR-Cyberspace Connectivity



Emerging Threat Environment

- 42% increase in targeted attacks in 2012
  - 31% aimed at small businesses
  - 38% aimed at large companies
- 14 zero day vulnerabilities
- Spam volume decreased with 69% of email being spam
- Phishing attacks exploiting social networking up 125%
- Web based attacks up 30%
- 8% of new vulnerabilities on mobile operating systems
- 92% of breaches attributed to outsiders
- 19% of breaches attributed to state actors

- Insider Threat

» Source - Verizon and Symantec

Emerging Threat Environment

- Medium
  - Cloud
  - Social Media
  - Mobile
  - Remote Access
  - Analytical Data

- Mechanisms
  - Web and client- side attacks
  - Botnets
  - Targeted messaging attacks
  - Data Breaches
  - Identity Theft

Operations in the "Cyber" Environment

- Cyber Environment in a military context - What is it?
  - Current Definition: "The interdependent networks of information technology structures, including the Internet, telecommunications networks, computer systems, embedded processors and controllers, as well as the software and data that reside within them."
- More than fixed strategic infrastructure IP based CNO
  - Underlying C4 support – both strategic and deployed
  - Platform based Surveillance, Target Acquisition and Reconnaissance systems
  - Joint Electromagnetic Spectrum/Network Operations

Operational Focus

- Post-Afghanistan
  - Evolving nature of international strategic struggle
    - Economic capital and Innovative capacity is national vital ground
    - Influence via web presence
  - Evolving nature of contemporary military and national security operations
    - High intensity/Low density/geographically dispersed/short duration
    - Reliance on sensors
  - Opportunity to reset and reshape to address the FSE
    - Network based capability plays key role

Operational Focus

- Sp to CAF Operations
  - Ongoing Sp to Op Reassurance and 23+ CAF missions
    - Op Centres/Op Support Hubs
  - Refocus on traditional warfighting
  - Renewed focus on Domestic Operations
    - Linkage to 1st Responders
    - CF role in “domestic cyber”
  - Sp to RCN and RCAF
    - Deployed Platforms/RF links
    - Networked support
  - Corporate IM/IT Operations
    - HR, Materiel, R&D – Provides Force Disposition
    - Target is intellectual capital
- Relationships
  - Within CF – CJOC, ECSs, SJS, CFD
  - Evolving relationships with SSC, CSEC, PSC, IC and Industry
  - Defence as an integral member of the national security community.

Operations in the "Cyber" Environment

- Leading the CAF in translating the FD work into an operational cyber capability.
  - Reliance on Defence Industry for solutions and support
  - Part of the national defence and security "fabric" – added responsibility
  - Strategic/Operational/Tactical operations in the Cyber domain
  - Continuum of Operations
    - Defensive/Offensive
    - Influence Activities – messaging through internet and other means
  - EM Spectrum and Influence/Information Operations have historically been central to operations in other nations

Operations in the "Cyber" Environment

- Injecting cyber into the strategic and operational planning processes - Security central to operations – Not just a service
  - Business Continuity Planning
    - Emerging technologies
    - Building a security program that protects an organizations most critical assets
  - Incident/Problem Management
  - Assessing and managing risk in an outsourced environment
    - Supply Chain risk management
    - Assessing vendor risk
    - Cloud/Big Data
  - Architectural definition and system development
    - Network vulnerability assessment
    - Thoughtful risk based analysis
    - Securing mobile technologies

Key Issues and Challenges

- **Evolving from information security to enterprise risk management in support of dynamically evolving operations**
- **Encouraging operational and technical innovation within a secure IT infrastructure**

QUESTIONS