DEFENCE R&D DÉFENSE

Coalition Computer Network Defence (CND) Common Operating Picture (COP) Concept

Lynne Genik, Julie H. Lefebvre, Mike Froh

13th ICCRTS Presentation (Paper 074)

June 17, 2008

Defence Research and Development Canada
Recherche et développement pour la défense Canada
Canada

Introduction

- A Coalition Computer Network Defence (CND) Common Operating Picture (COP) is a means of sharing, assessing, and displaying CND information across coalition boundaries
- The ultimate goal is to provide computer network defence (CND) situational awareness (SA)
- This work was started under a NATO exploratory team with the goal of conceptually defining a Coalition CND COP and its concept of operations
  - We focus on the automated exchange of multinational CND information, as opposed to technologies for secure information exchange

The Situation Today

- Militaries are heavily reliant on communications networks and are becoming increasing so with the move towards network-enabled operations
- Multinational CND information sharing exists between some nations in simple forms (email, phone, web page) with humans involved
- Most research and development efforts have focused on intrusion detection information sharing
- CND COPs are now under development, for example, Canada's Joint Network Defence and Management System (JNDMS)

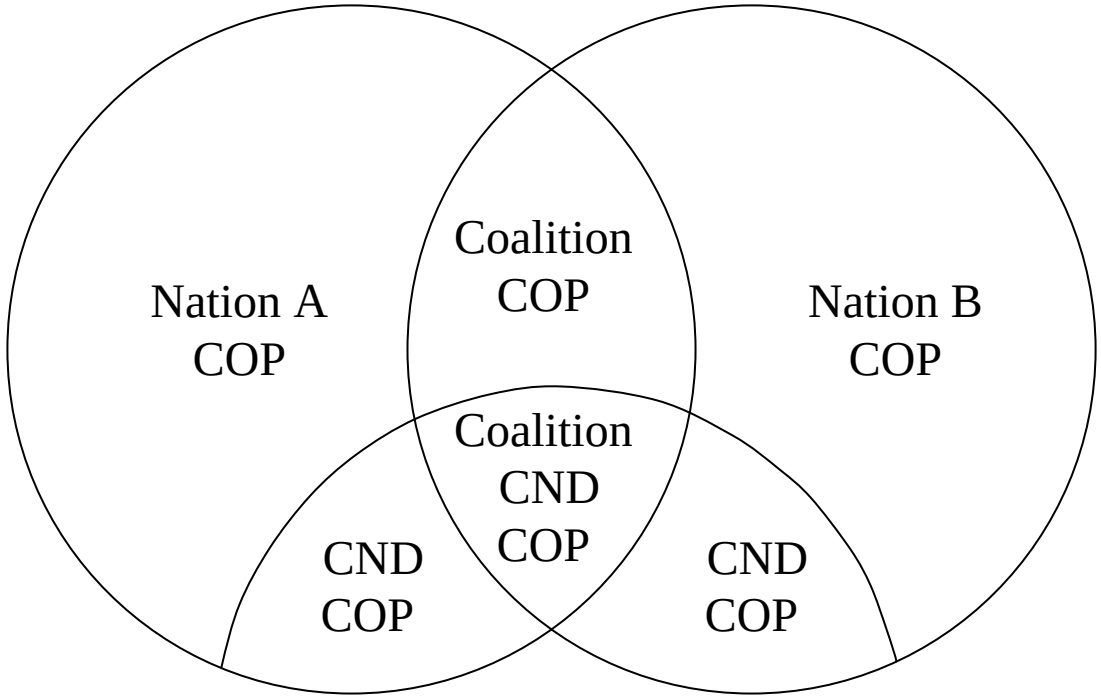
Why Automate?

1. Human resistance to sharing
   - Information may not be shared or there may be delays in dissemination
   - Reasons include lack of trust of coalition members, unclear policy on when to share, no perceived benefit to sharing, sharing being a lower priority task, etc.
2. Rapid event time scales
   - Network tempo is extremely fast (for example, Slammer worm)
3. Information exchange volume
   - Potentially huge
   - Can easily exceed manual methods for processing
4. Information complexity
   - Many potentially disparate sources
   - Requires correlation, fusion, etc.

CND SA Information Requirements

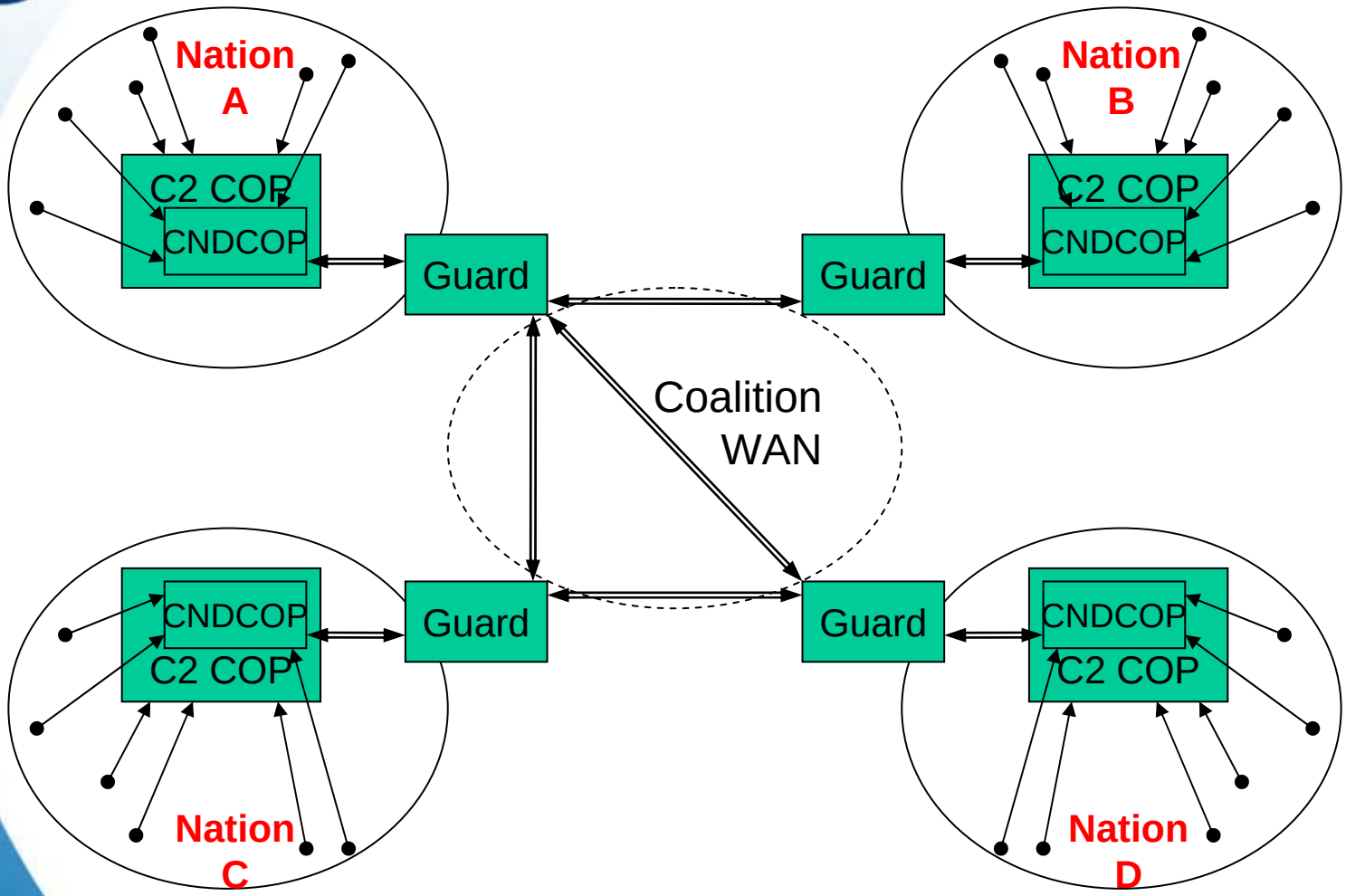
- More than intrusion detection information
- Includes network management and security information, such as
  - Information technology (IT) services
  - IT infrastructure
  - Vulnerabilities
  - Safeguards
  - Exploits
  - Threats
  - Alarms
  - Incidents

Coalition CND COP Vision

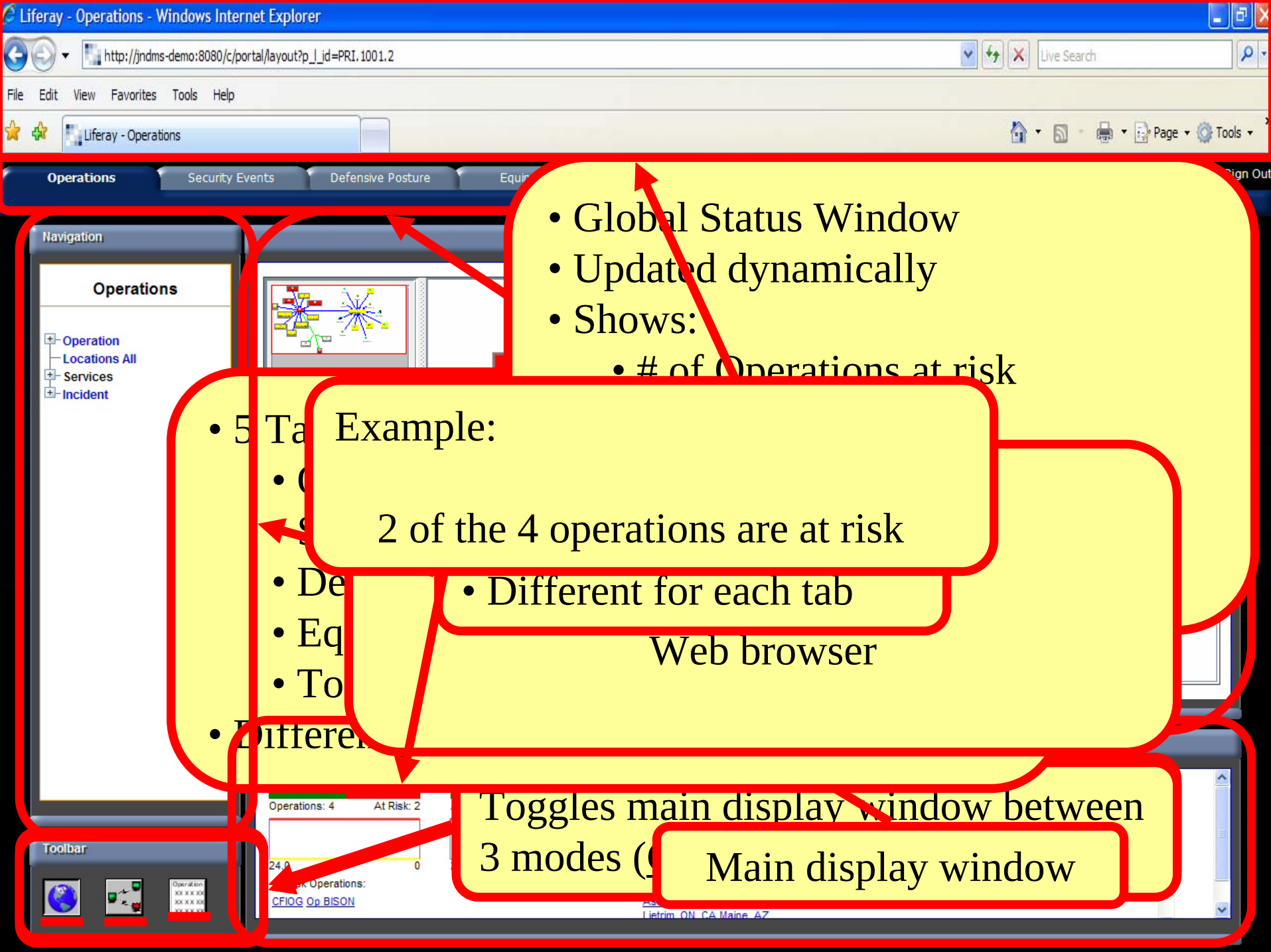


- Envisioned to be part of both the national COP and the overall Coalition COP
- Not necessarily a single identical display of information

Coalition CND COP Architecture



- The Coalition COP & Coalition CND COP are effectively represented by the double-headed arrows and info exchanged through bilateral agreements
- Nations retain control over the CND information they share


Liferay - Operations - Windows Internet Explorer
http://jndms-demo:8080/c/portal/layout?p_l_id=PRI.1001.2
File Edit View Favorites Tools Help
Liferay - Operations
Page Tools
Operations
Security Events
Defensive Posture
Navigation
Operations
Operation
Locations All
Services
Incident
Toolbar
Operations: 4
At Risk: 2
CFIOG Op BISON
• Global Status Window
• Updated dynamically
• Shows:
• # of Operations at risk
• 5 Ta
• De
• Eq
• To
• Differen
Example:
2 of the 4 operations are at risk
• Different for each tab
Web browser
Toggles main display window between
3 modes (
Main display window

Operational Scenario: Network Vulnerability Assessment Team (NVAT) Cooperation

Scenario Overview:

- Nations share human resources to deal with a new vulnerability
- Vulnerability release occurs in normal working hours in two nations and night hours in a third nation with on-call personnel only
- Nations share a watch list of applications
- Pre-established information sharing relationships exist

NVAT Cooperation – Event Sequence

1. A new buffer overflow vulnerability in Vendor X type firewalls is released
2. A notification is automatically produced through the national CND COPs and risk level is assessed
   - Nations A and B CND COPs produce notifications at watch desks
   - On-call duty personnel are notified in Nation C

Nation	Risk Level
A	Low
B	High
C	High

3. Nation C requests to work with Nation B instead of waking staff

Text highlighted in red indicates information shared through the Coalition CND COP

NVAT Cooperation – Event Sequence

4. Nations B and C request that A focuses intelligence gathering on exploits from hacker groups
   - Sources indicate that there may be a potential exploit within two days
5. Nations determine means of dealing with the vulnerability and begin to develop workarounds based on their security architectures
6. Nation B develops an IDS signature to detect exploit attempts until a patch is developed and rolled-out
7. Vendor X releases a patch for the vulnerability
   - Nation C tests the patch in their lab during the night to identify and address issues with implementation

NVAT Cooperation Outcomes

- Sharing simple information has benefits
  - Automatically sharing watch list and threat information results in clearer SA
- Coalition collectively benefits from sharing human resources
  - Nation A focuses on data mining, Nation B develops an IDS signature, Nation C tests patch
  - Leverage strengths and times zones of nations

Operational Scenario: Virtual Machine (VM) Migration

VM technology allows systems to run on a software-simulated hardware platform instead of actual hardware

Scenario Overview:

- Deployed coalition uses virtual machines (VMs) for C4ISR applications
- Coalition members have compatible VM infrastructures
- Physical attack results in destruction of some of one nation's servers hosting VMs

VM Migration – Event Sequence

1. Mortar attack on Nation A base destroys a vehicle containing C4ISR application servers
2. Nation A's CND COP automatically correlates loss of multiple C4ISR VMs as being on physical servers in a single vehicle
3. Nation A determines new VM configuration on remaining C4ISR application servers and time to repair
   - Nation A doesn't have enough server capacity to run all VMs
   - Coalition commander decides to stop low-priority VMs and restart lost high-priority VMs from recent backup

VM Migration – Event Sequence

4. Coalition operations result in some stopped low-priority VMs becoming mission critical
   - Nation A requests VM server resources from coalition members
5. Nations B and C have spare physical server capacity and agree to house the coalition VMs
   - Firewalls and VPNs are configured to backhaul the remote VMs to Nation A's network for VM migration
6. Nations B and C restart VMs with their VPN network connections backhauled to Nation A's network and full operations capability is restored

VM Migration Outcomes

Automation helps in dealing with the volume and complexity of information

- Nation A's CND COP determined that apps were offline and housed in a single vehicle
- Automated detection allowed coalition members to get near real-time notification
- Complex IT configuration information exchanged as part of the COA (VPN specifications, firewall rule adjustments, etc.)

VM Migration Outcomes

Scenario demonstrates the efficient use of coalition resources

- Knowledge of coalition needs allows for correct prioritization of VMs
- Efficient sharing of server capacity means coalition operations are minimally impacted
- Scenario could be extended to allow for more optimal deployment of IT resources among coalition members

Coalition CND COP Benefits

Obvious benefits:

1. Clearer SA
   - Better insight into the defensive posture of national and coalition network
2. More efficient use of resources
   - Automated sharing of information reduces human resource requirements
   - Sharing of IA workloads among coalition members
3. More effective CND action
   - Rapid, high volume, complex data exchanges without errors and omissions due to human processing
   - Enhances coordinated CND activity

Areas Requiring Research

1. Information Requirements for Coalition CND SA
   - Specifying information to be shared
   - Integrating network management and network security
   - CND information fusion
2. CND Information Sharing Issues
   - CND information classification
   - Influencing CND information sharing policies
   - Sanitizing CND information

Areas Requiring Research

1. Information Requirements for Coalition CND SA
   - Specifying information to be shared
   - Integrating network management and network security
   - CND information fusion
2. CND Information Sharing Issues
   - CND information classification
   - Influencing CND information sharing policies
   - Sanitizing CND information

Areas Requiring Research

3. Implementation of a Coalition CND COP
   - CND data model
   - CND information visualization
   - Integrating CND COPs into C2 systems

Conclusion

- The proposed Coalition CND COP:
  - Automates the exchange of both network management and security information
  - Is part of the overall C2 system
  - May become an operational necessity when coalition cyber operations become more prevalent
- The vision and research gaps can serve as a starting point for developing a capability

DEFENCE R&D DÉFENSE