

# DRDC Cyber Defence S&T Program

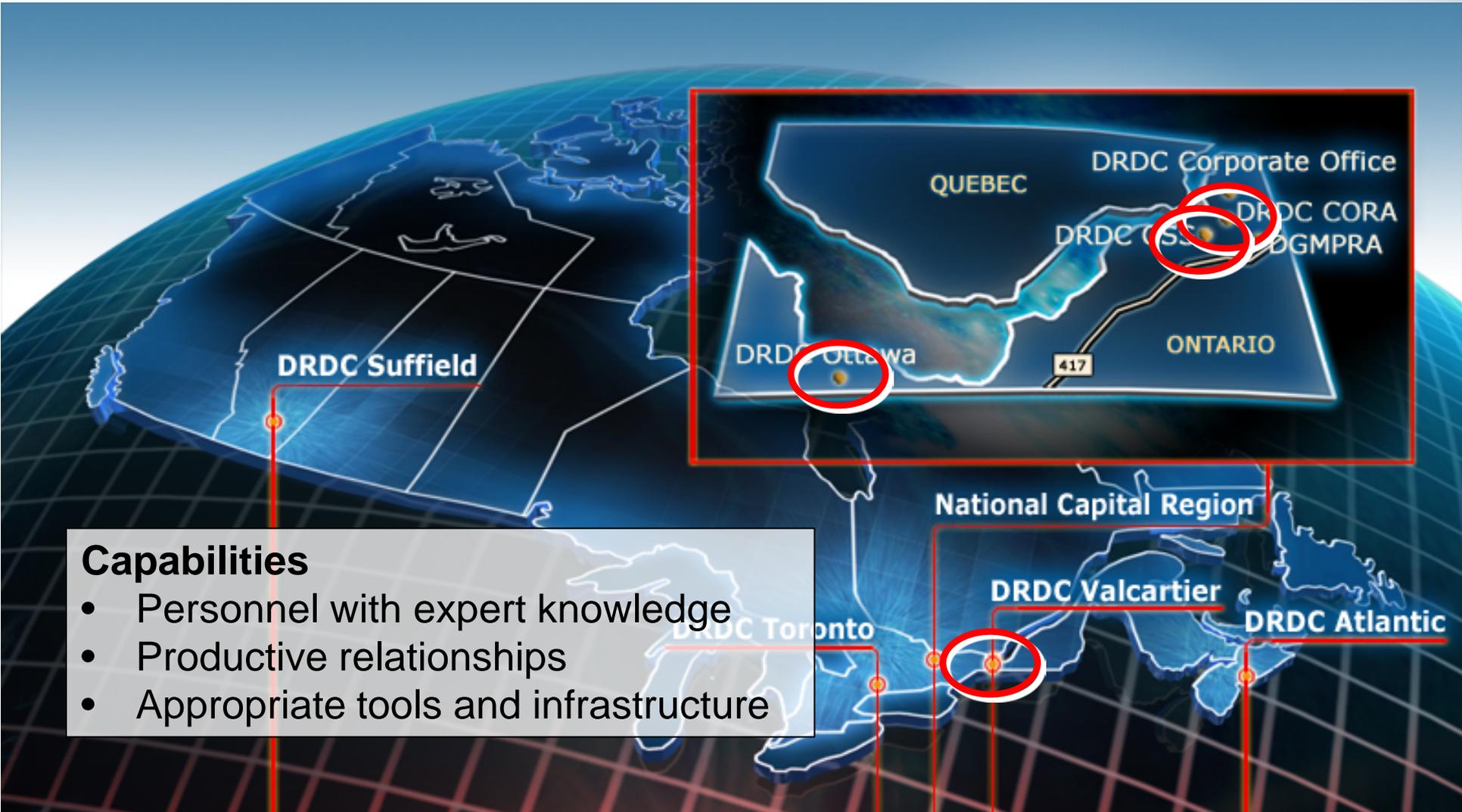
## *An Overview*

Guy Turcotte, Head  
Mission Critical Cyber Security Section  
Defence R&D Canada

9<sup>th</sup> October, 2012



# DRDC Centres Involved in Cyber Security S&T

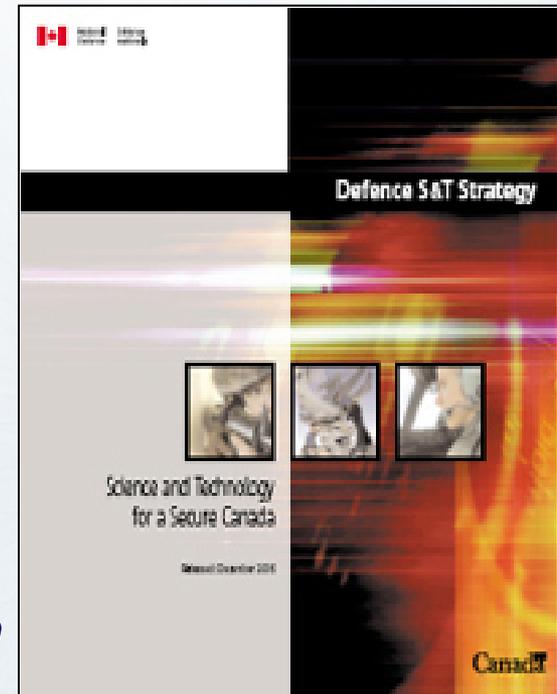


Defence R&D Canada (DRDC) operates eight research centres across Canada, each with a unique combination of expertise and facilities to carry out world-class science and technology research.

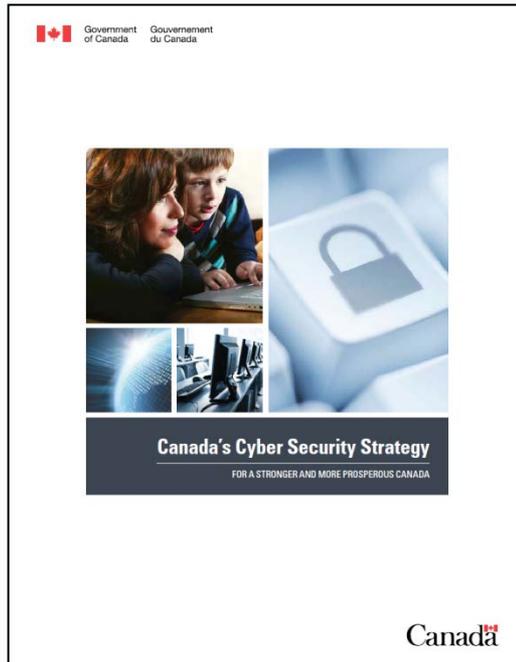
### Overarching Objective

To ensure that the Canadian Forces are technologically prepared and operationally relevant

- *Provide expert S&T knowledge for informed decision making.*
- *Contribute to the success of military operations.*
- *Enhance the preparedness of the Canadian Forces.*
- *Help to create and maintain a Canadian defence S&T industrial capability.*
- *Conduct projects for external clients, to assist the Agency to develop and maintain its capabilities.*



# High Level Requirements: Canada's Cyber Security Strategy\*



## Three pillars:

1. *Securing government systems*
2. *Partnering to secure vital cyber systems outside the federal government*
3. *Helping Canadians to be secure online*

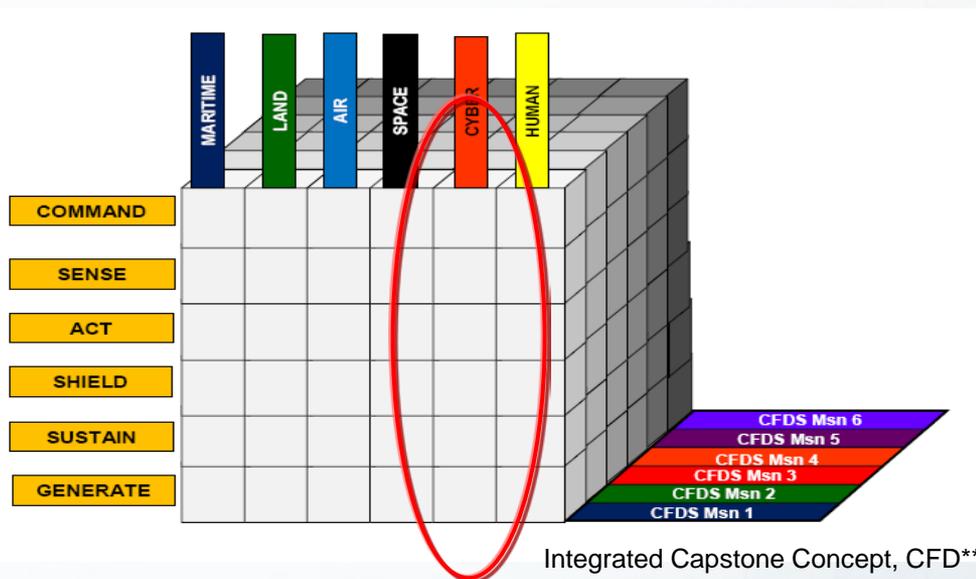
## “The CF and DND will:

1. ***strengthen their capacity to defend their own networks, will work with other Government departments to identify threats and possible responses, and will continue to exchange information about cyber best practices with allied militaries; and***
2. ***work with allies to develop the policy and legal framework for military aspects of cyber security, complementing international outreach efforts of Foreign Affairs and International Trade Canada.”***

\*<http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx>

# High Level Requirements: Canada First Defence Strategy\*

*“Canada needs a modern, well-trained, and well-equipped military with the core capabilities and flexibility required to successfully address both conventional and asymmetric threats, including terrorism, insurgencies, and **cyber attacks**.”*

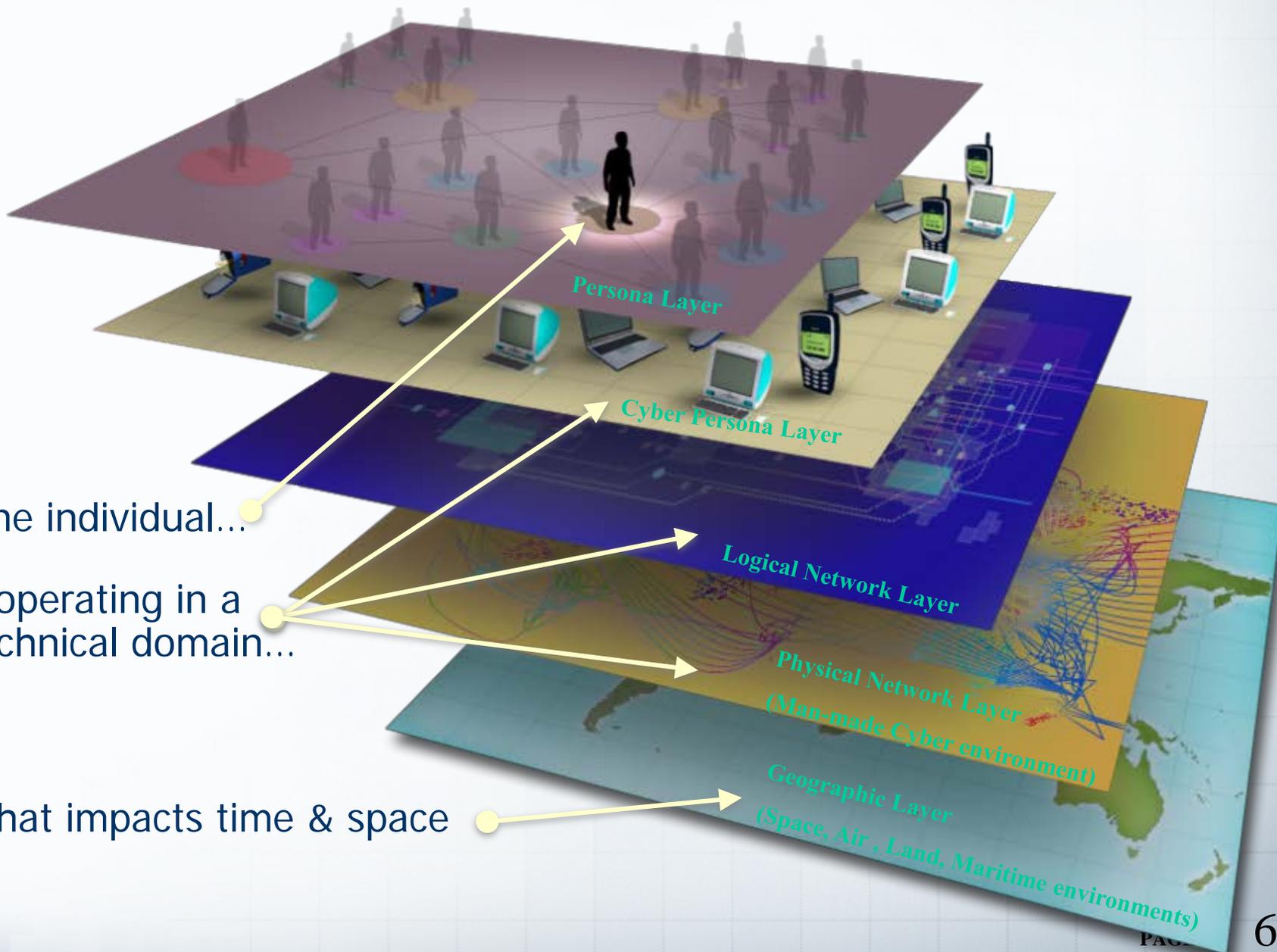


The Canadian Forces have set up a Cyber Task Force (CTF) to **conceive and design a coherent integrated approach to cyber operational capabilities with DND/CF.**

\* [http://www.forces.gc.ca/site/pri/first-premier/June18\\_0910\\_CFDS\\_english\\_low-res.pdf](http://www.forces.gc.ca/site/pri/first-premier/June18_0910_CFDS_english_low-res.pdf)

\*\*[http://publications.gc.ca/collections/collection\\_2012/dn-nd/D2-265-2010-eng.pdf](http://publications.gc.ca/collections/collection_2012/dn-nd/D2-265-2010-eng.pdf)

# Understanding the Cyber Environment



One individual...

...operating in a technical domain...

...that impacts time & space

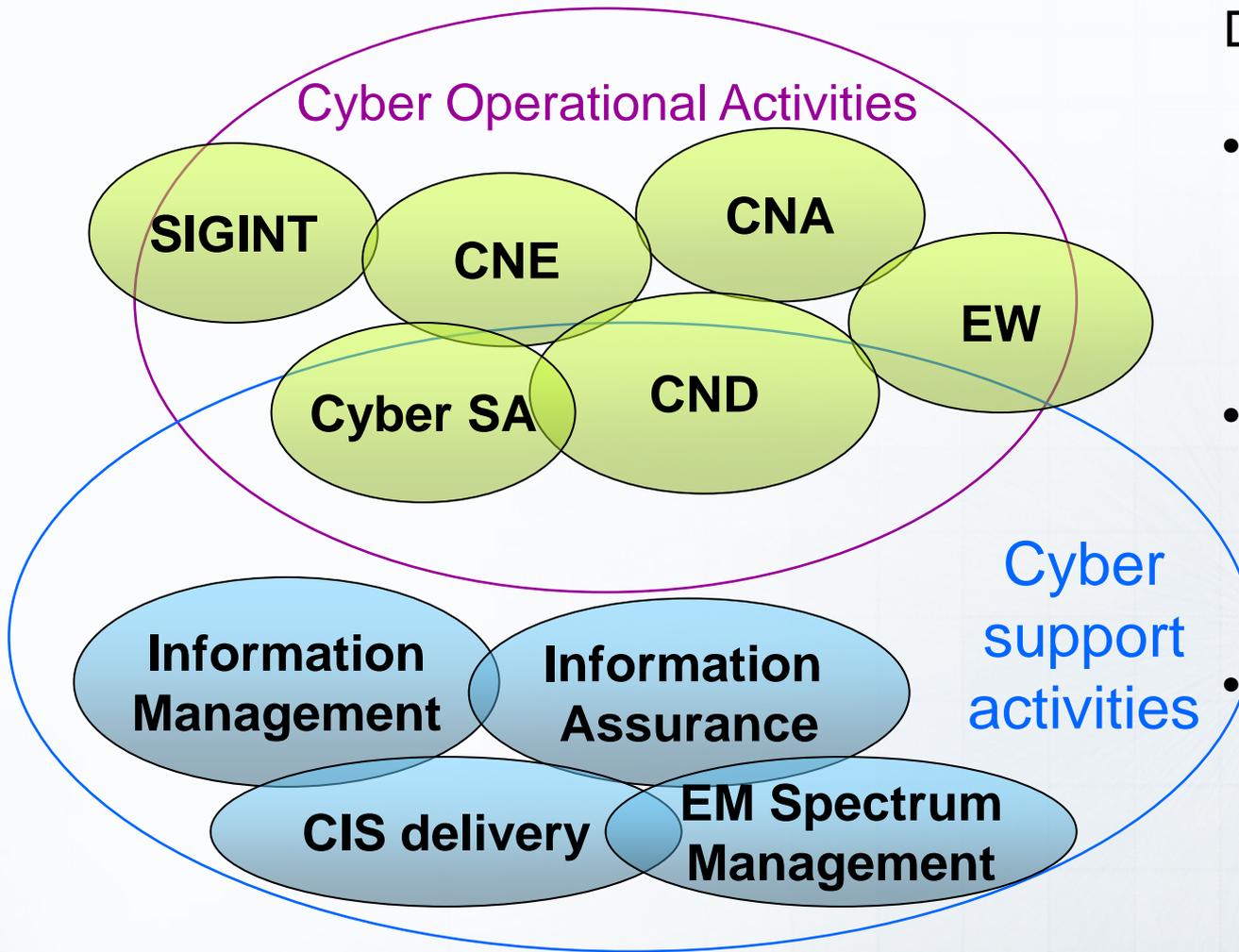
# Complexity of the Cyber Environment

## A short list ...

- Tempo – *activity in seconds*
- Distance – *router hops*
- Non-physical – *software weapons*
- Non-geographic – *logical view*
- Complexity – *software and connectivity*
- Terrain – *continually changing*
- Attribution – *anonymous transactions*
- Threat – *asymmetric, persistent*
- Roles & responsibilities – *unclear*
- Legal – *challenging*



*A strong S&T component will always be required to ensure that CF and DND capabilities remain current.*



## DRDC Focus Areas

- Capabilities for operating in the cyber environment
- Trust and confidence for conducting operations in the cyber environment
- Resilient networks and systems in a contested environment

# Thank You!

Guy Turcotte  
Head / Mission Critical Cyber Security Section

Defence Research & Development Canada – Valcartier  
2459 Pie XI North  
Quebec City (QC)  
Canada

Tel: (418) 844-4000 x 4354  
eMail: [guy.turcotte@drdc-rddc.gc.ca](mailto:guy.turcotte@drdc-rddc.gc.ca)

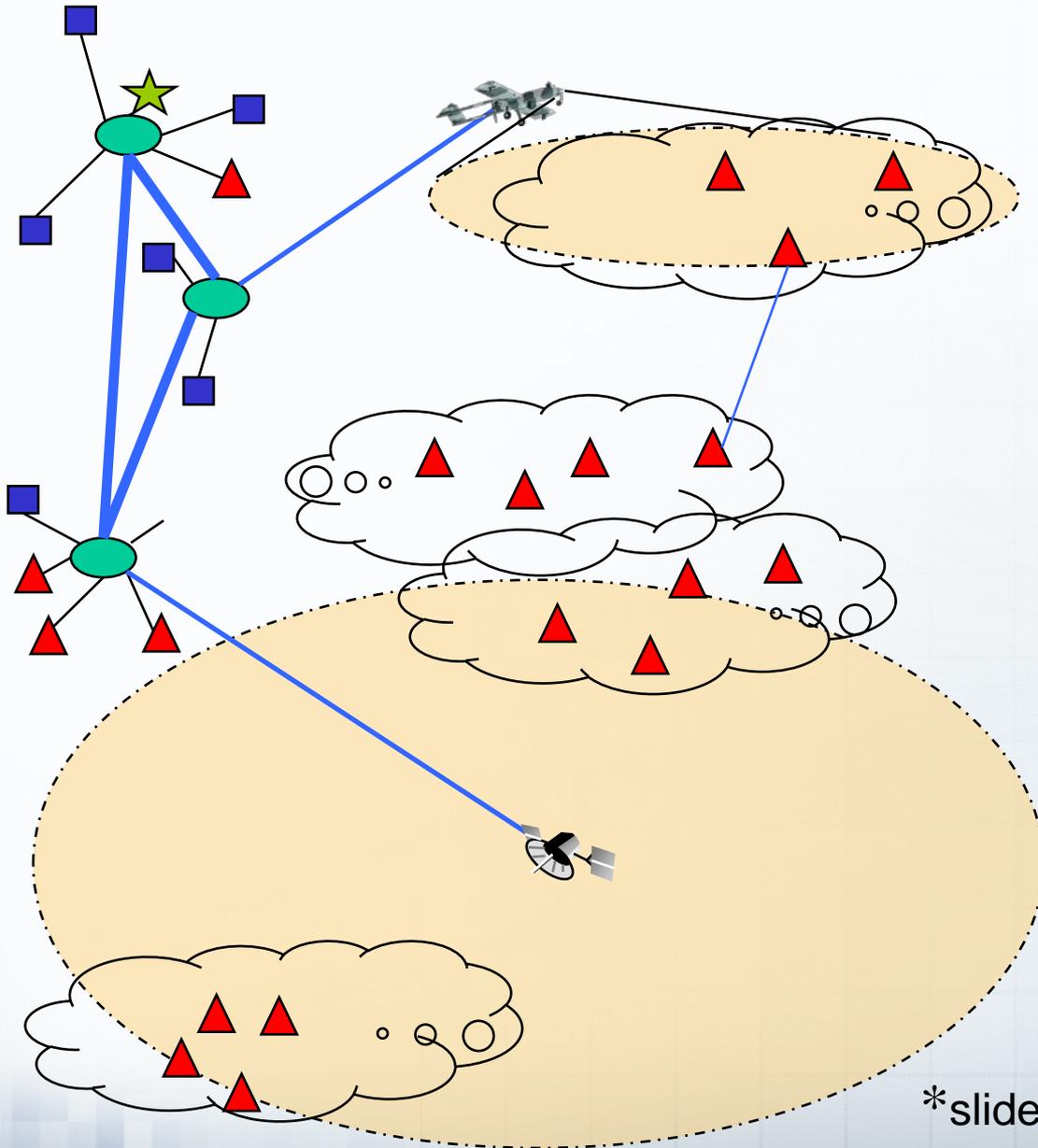
**DEFENCE**



**DÉFENSE**

# Mobile Ad Hoc Networks (MANETs)

## Example of a Complex Cyber Terrain



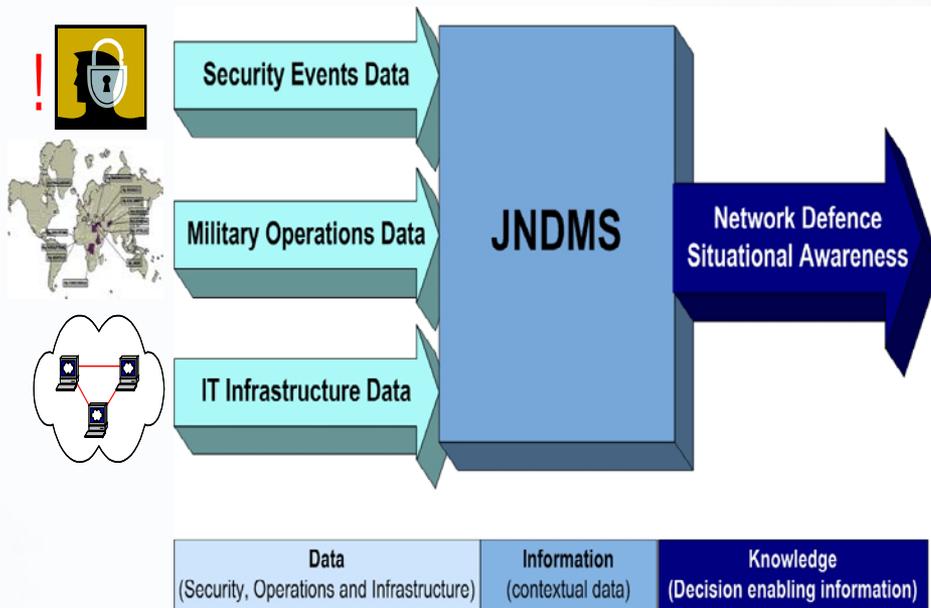
- System of autonomous stations
  - No set infrastructure
  - No single control authority
  - No pre-designated routers
  
- Defending MANETs is a challenge

	Management node
	Backbone node
	Mobile User node
	Host/User node

\*slide courtesy of (lifted from) CERDEC

# Joint Network Defence and Management System (JNDMS) Technology Demonstrator

Demonstrate integrated, operation-centric, enterprise-wide network situational awareness for Computer Network Defence.

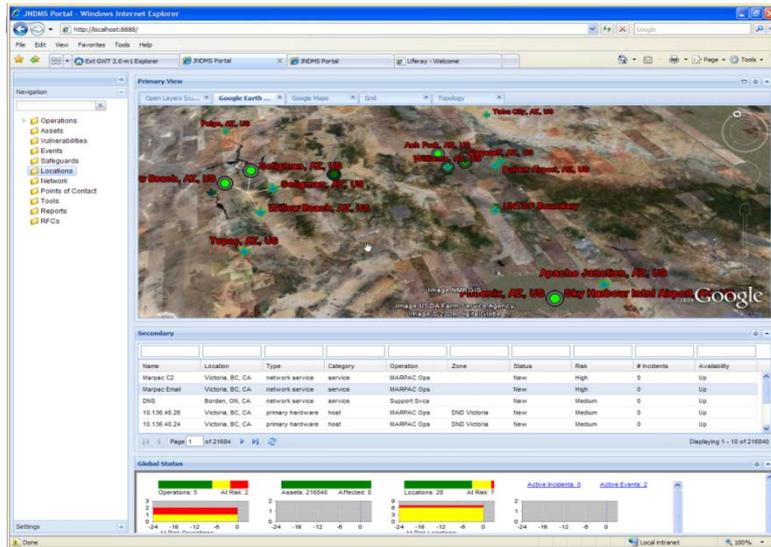


**Start-End:** Apr 03' – June '10

## Outcomes

- cyber defence situational awareness data model.
- prototype system deployed on the DRDC network
- results used in the definition phase of the Canadian Forces NetC2 Integrated Situational Awareness Capability

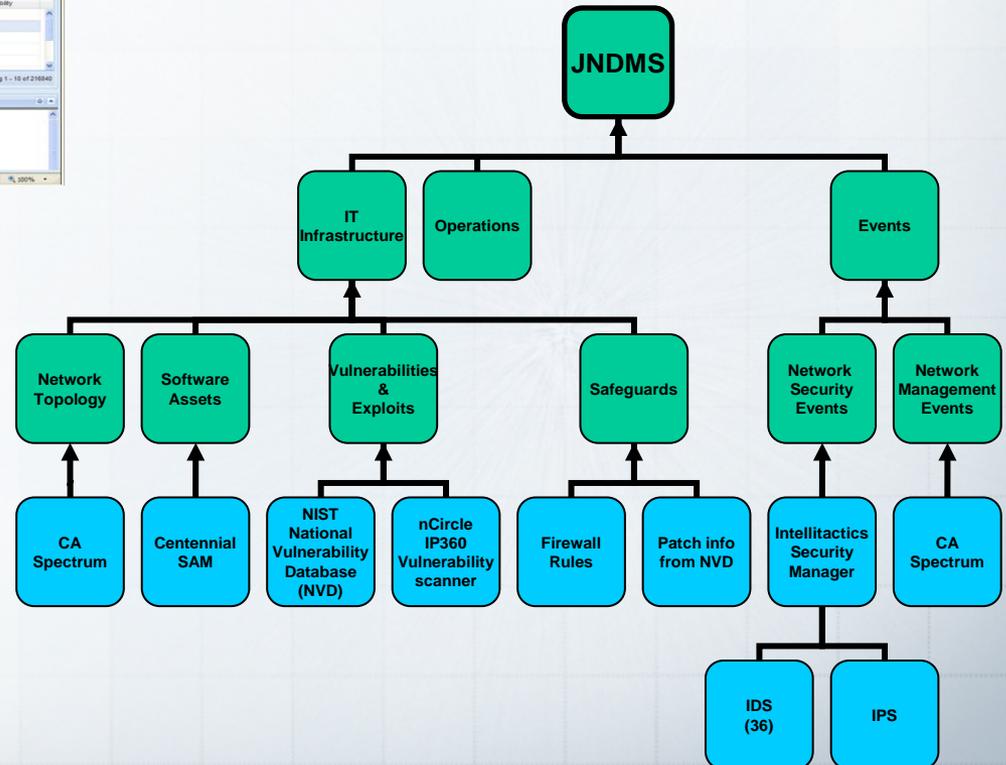
# JNDMS Results



- No single commercial tool could provide the information required for cyber defence SA.

## R&D gaps:

- Real-time mapping of the dependency of operations on the IT infrastructure.
- Measures and metrics for cyber defence situational awareness (e.g. risk, defensive posture, damage)
- Visualization



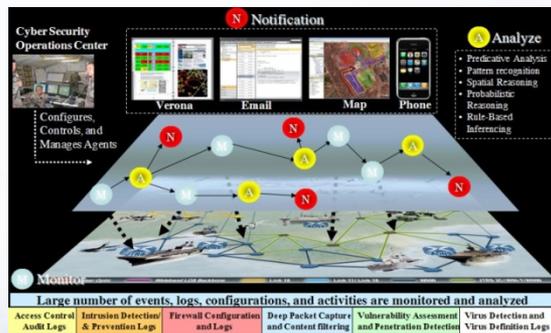
# Coalition Cyber Defence Requires (more) Information Sharing



## IMPEDIMENTS:

- Legal challenges
- Limited personnel resources
- Need for training
- Procedural challenges
- Higher priorities
- Trust issues

Coalition  
Network



# ARMOUR: Automated CND TDP

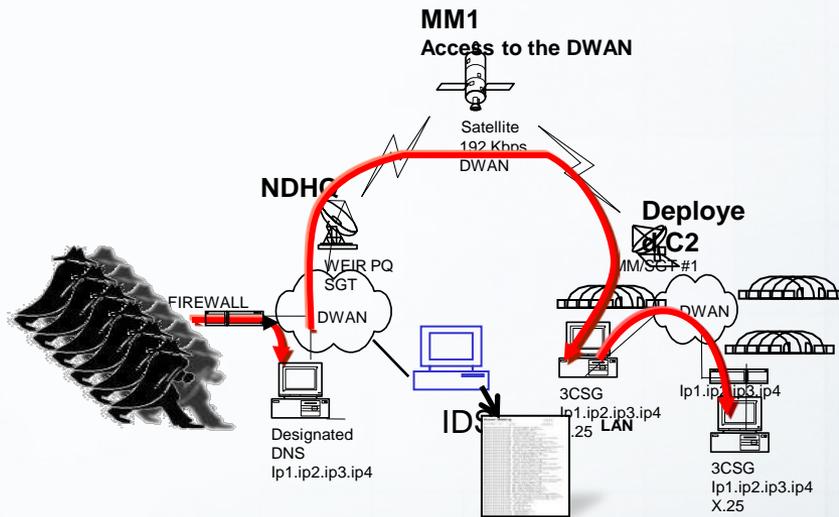
Demonstrate semi-automatic to fully automatic cyber defensive action to defend from network threats.

- Compute defensive courses of action.
- Prioritize defensive courses of action to minimize impact.
- Proactively and reactively respond.
- Compute system security metrics over the entire system.

**Start-End:** April '10 – Mar '15

**Key Outputs:**

- Delivery of openly shared demonstration system software project;
- Technical specifications, CONOPS;
- Identification of ongoing force development needs; and
- Build knowledge, identify technology risks and cost drivers for future Capital acquisition projects.



# ***ARMOUR TDP – Leveraging***

- *Requirements specification for a DND Capital Project:*
  - results anticipated to be used in the definition phase of the DND NetC2
- *Leveraging and Partnering with Academia, Industry and Allies:*
  - by providing an integration framework that enables incremental, interoperable, distributed development by academia, governments, and industry.
  - NATO Research Task Group on Cyber Defence and Information Assurance Research Framework (NATO IST-096) ARMOUR integration framework as the basis of its Cyber Defence Prototyping Environment Description.
  - Integrated the DRDC MulVal/AssetRank system into the NC3A Dynamic Risk Assessment system to demonstrate an automated CND risk assessment capability. MOU with NC3A

***Coming up Next ... Cyber Operations in a Contested Environment***

# Cyber Incident Integrated Rapid Response

- An integrated rapid-response capability to cyber-attacks
- A plan for the short-term transition of this capability to the Canadian Forces



**Start-End:** Apr 11' – Mar 14'

## Outcomes

- An assessment of DND/CF current capability to respond to cyber-attacks
- A customizable process for cyber-attack rapid response that is compatible with DND/CF current practices
- An advanced prototype of a software system to support the rapid-response process

# Cyber Attack Protection of DND/CF Information Systems

Develop an integrated capability for software architectural risk analysis, software vulnerabilities analysis, endpoint protection evaluation and systems penetration testing.

**Start-End:** Apr 11' – Mar 14'

## Outcomes

- An assessment of current practices for software vulnerabilities analysis, endpoint protection and systems penetration testing.
- The state of the art on best practices in SOA and cloud computing security.
- An integrated capability for information systems cyber attack protection with a process for its operation

```

// ----- OTHER METHODS -----
/**
 * acceleration for a given band. Tokens need to be rendered
 * for a given band.
 * @param r clip region to be rendered.
 * @return firstTokenNeedToRender.
 */
private int firstTokenNeedToRender( Rectangle r )
{
    int top;
    // pick a band.
    int firstTokenNeedToRender;
    // home
    int band;
    int firstBaseline;
    if ( band < 0 )
    {
        // cannot insert point to the band below.
        int band;
        band = bandCount - 1;
    }
    // As s
    startAtBaseline = baselines[ band ];
    // startAtLineNumber is 1-based.
    startAtLineNumber = firstLineNumbersToBand[ band ];
    return
}
/**
 * acceleration for a given bandCount. Tokens need to be rendered
 * for a given bandCount.
 * @param r clip region to be rendered.
 */

```

Architectural Risk Analysis

Software Vulnerabilities Analysis

Endpoint Protection Evaluation

Penetration Testing Tools Characterization