

Presentation to NSTAC RDX 2006

Communications Research Centre's Cyber Security and Public Safety Program

Dr. Veena Rawat
President, CRC

September 22, 2006



Communications Research Centre

Shirleys Bay Campus



About CRC

CRC Mission

- To be the federal government's Centre of Excellence for communications R&D, ensuring an independent source of advice for public policy purposes.
- To help identify and close the innovation gaps in Canada's Communications sector by:
 - Engaging in industry partnerships
 - Building technical intelligence
 - Supporting small and medium sized high-technology enterprises

CORE Competencies

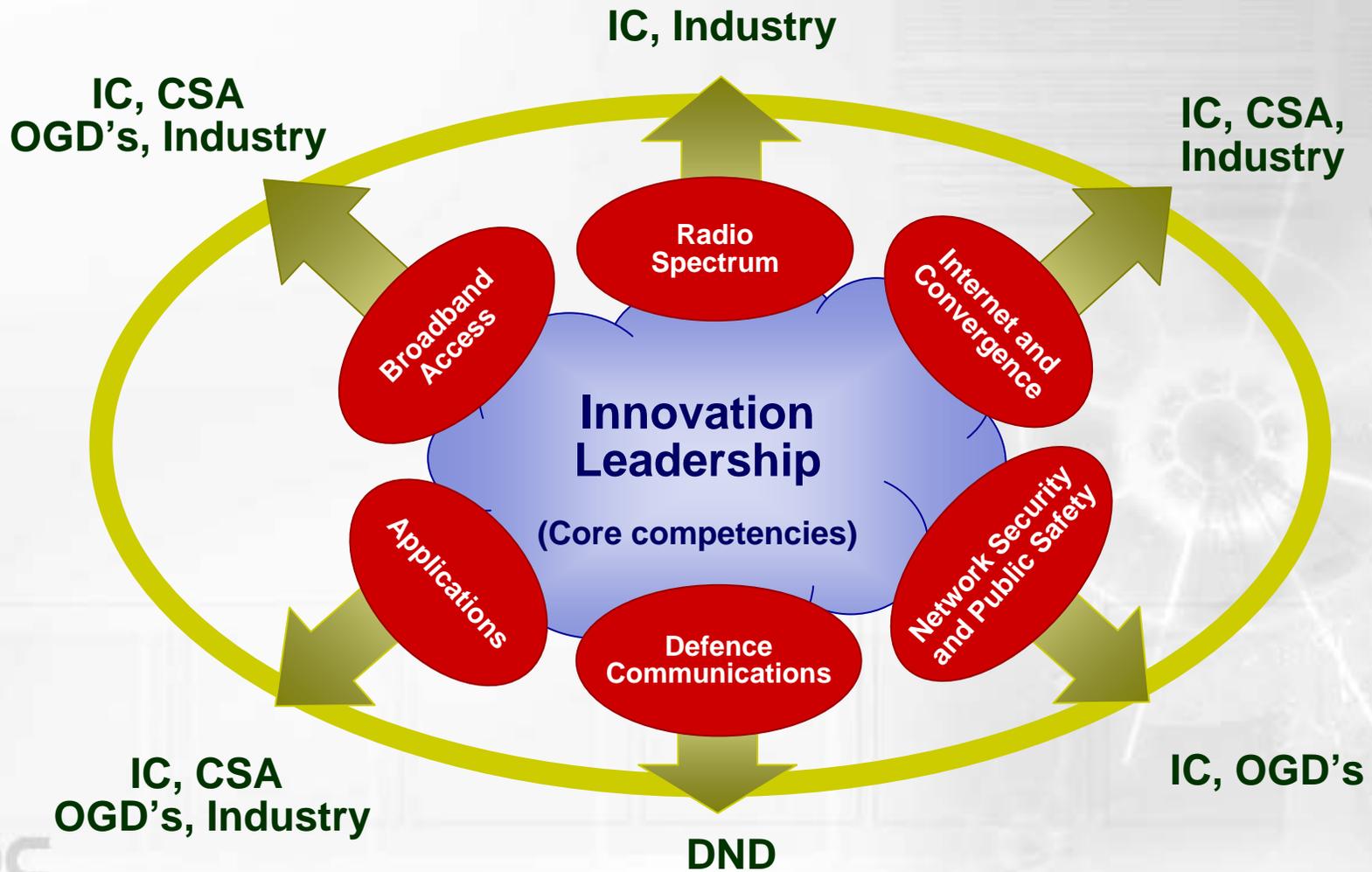
- Wireless Systems
- Communications networks
- Radio Fundamentals
- Interactive Multimedia
- Photonics (Optical Communications)

Strategic Research Priorities (2004-2007)

Client Support

Strategic Goals

Strategic priorities



Research Branches

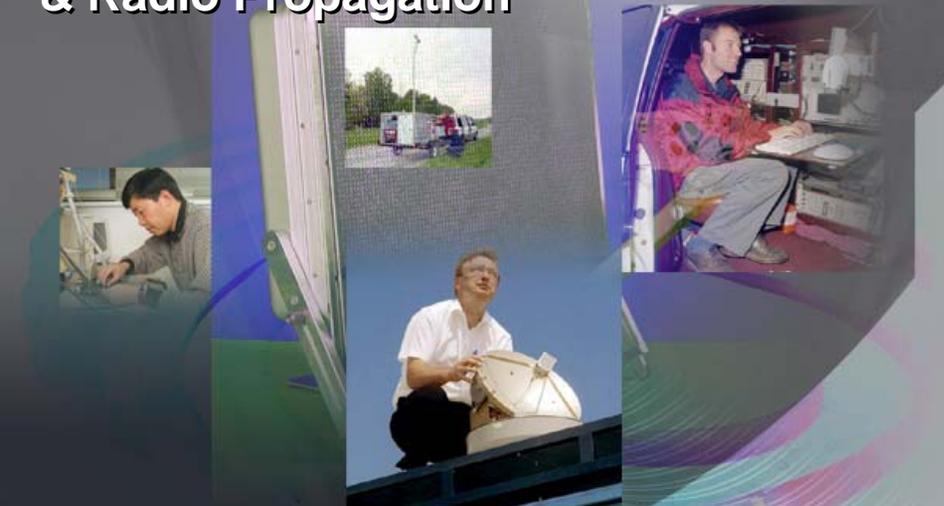
Terrestrial Wireless



Broadband Network Technologies



Satellite Communications & Radio Propagation

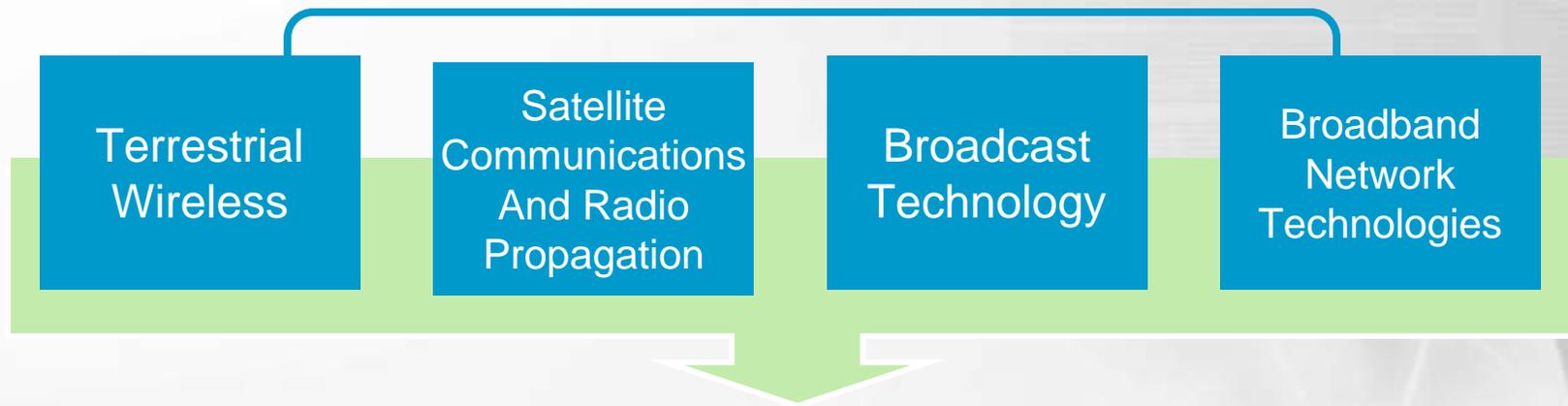


Broadcast Technologies



S&T Linkages

Research Branches



Linkages

Major Federal Partners

e.g. Industry Canada and portfolio (incl. Technology Partnerships Canada, Canadian Space Agency, National Research Council), National Defence

Industrial Partners

e.g. Telesat, Telus Mobility, Wavesat, MDA, Dragonwave, Alcatel, ComDev

Academia

e.g. University of Manitoba, McGill, Carleton, McMaster, UNB, UBC

International Organizers

e.g. NATO, European Space Agency, International Telecommunications Union (ITU), Institute of Electrical and Electronics Engineers (IEEE), C-Dot (India), CPQD (Brazil), NSC (Taiwan), EU-ITS

Others

e.g. CANARIE Inc., OCRI, National Capital Institute of Telecommunications (NCIT), Canadian Photonics Consortium

Linkages: Industry Canada

Examples:

- Spectrum R&D
- S&T for ICT sector in Canada
- Telecommunications policy and standards
- BRAND and NSI
- S&T strategy, integration and related intramural activities
- Human Resources, Finance, IM/IT

Linkages: The Defence Communications Program

- On behalf of Defence R&D Canada (DRDC)
- Applying CRC's expertise to niche areas of defence communications

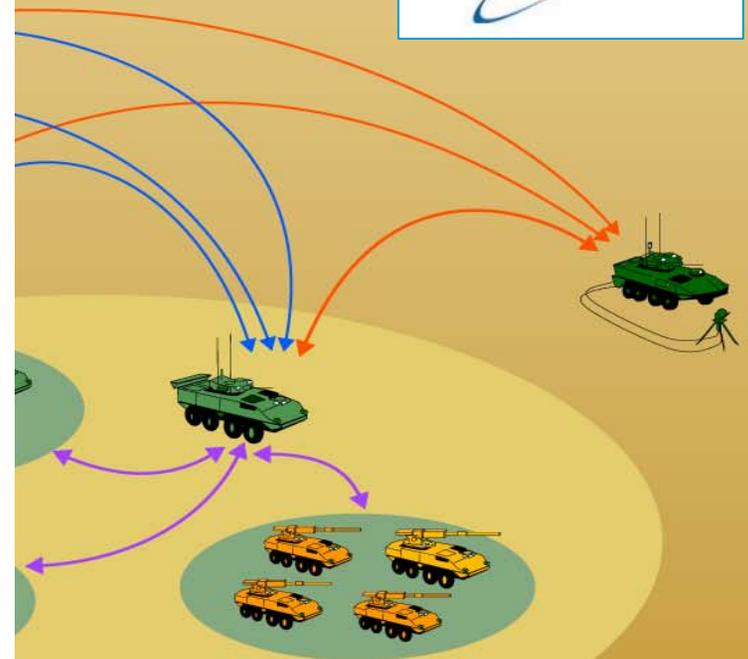
R&D Focus

Robust Network Systems

- Architectures, protocols
- Network management
- Interoperability
- Security
- Sensor networks

Robust Wireless Systems

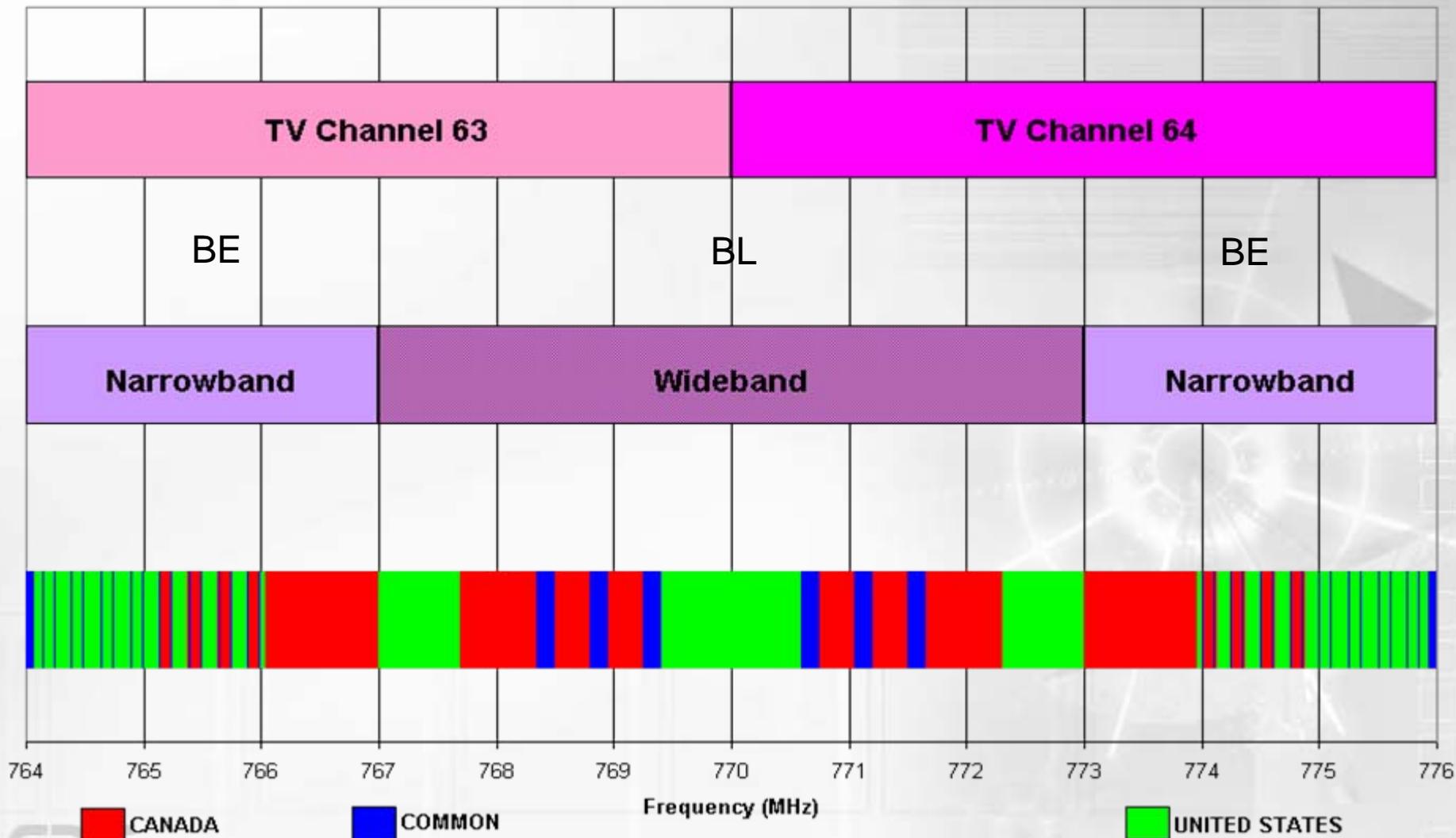
- Terrestrial/satcom
- Highly-adaptive systems (cognitive, software radio)
- Antennas and electronics



Spectrum Activities in Public Safety

- Support to Industry Canada (IC)
 - 700MHz Band
 - 4.9 GHz Public Safety Band
 - 5.9 GHz Intelligent Transport Systems Band
- Support to PSEPC on radio communication interoperability
 - Deploy communication interoperability pilots
 - Conduct technology reviews, testing, and evaluation
 - Develop testing capacity
 - Determine interoperability requirements (technical, functional, procedures)
 - Determine training requirements
 - Conduct research and development on longer-term solutions

Division of Spectrum for Public Safety - 700MHz Band



CANADA

COMMON

UNITED STATES

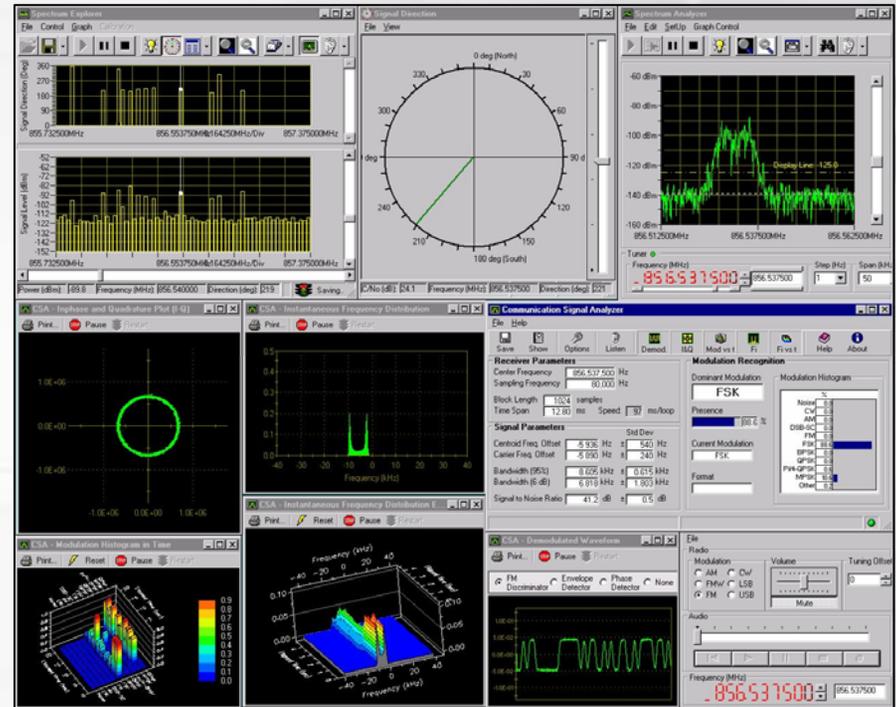
Spectrum Explorer / MiDAS

Wideband radio spectrum surveillance system

- Spectrum Explorer developed at CRC for civil applications
- In collaboration with DRDC Ottawa, extended for military applications - MiDAS



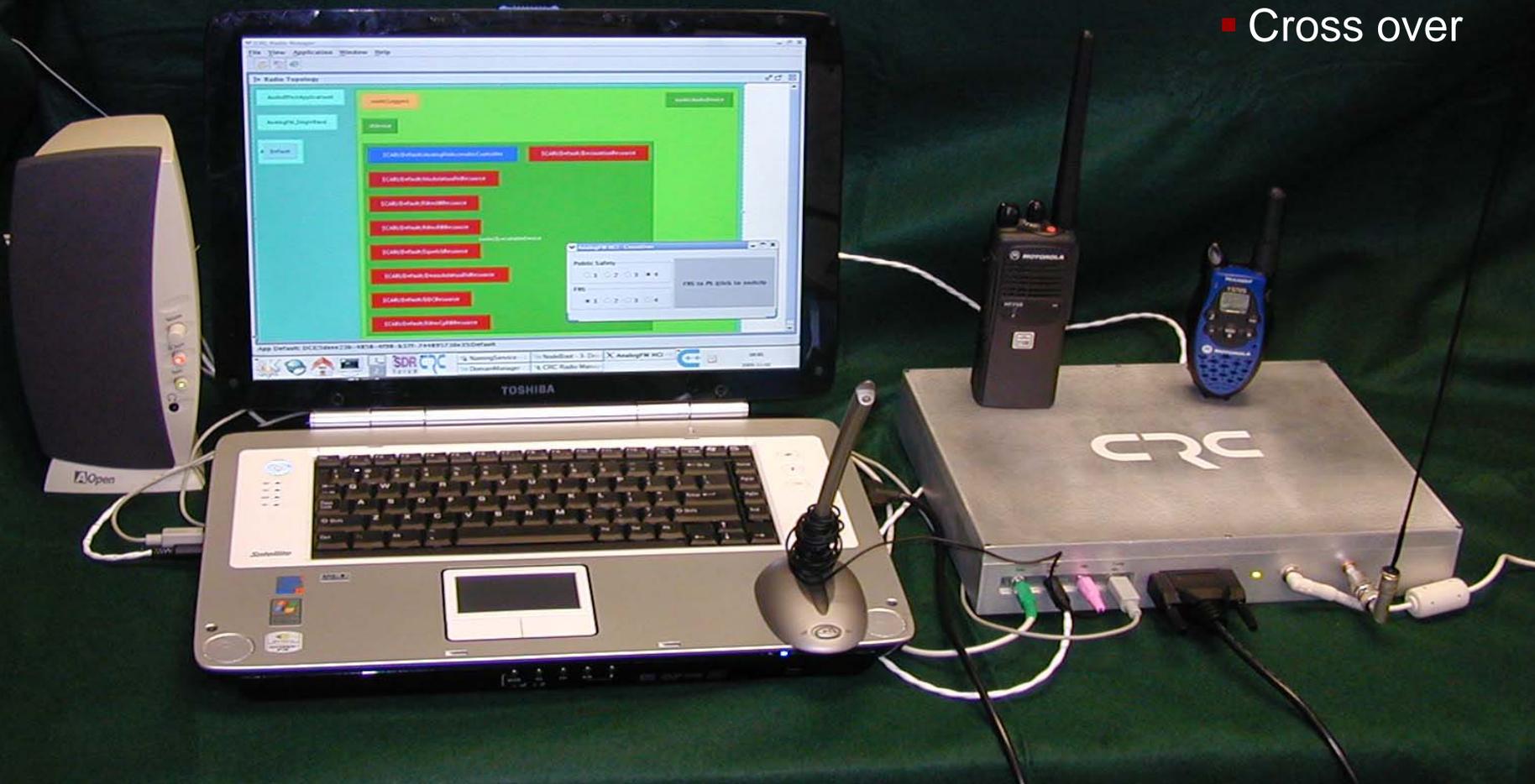
Signal capture (20 MHz - 6 GHz)
Direction-finding and localization
Signal and modulation recognition



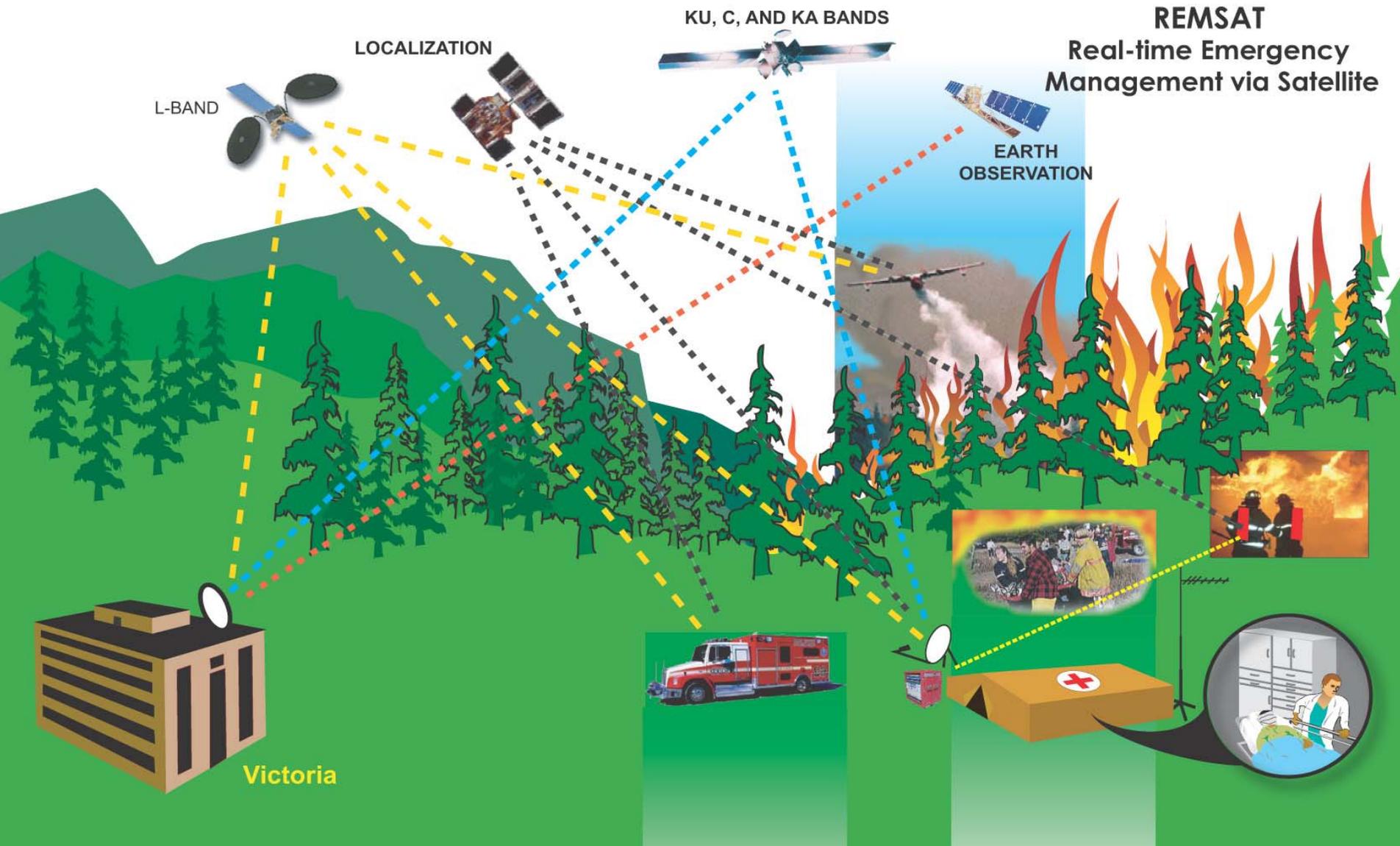
Software Defined Radio (SDR) for Public Safety

Prototype SDR for Public Safety

- 150 MHz – 460 MHz
 - FM and AM
 - Cross over



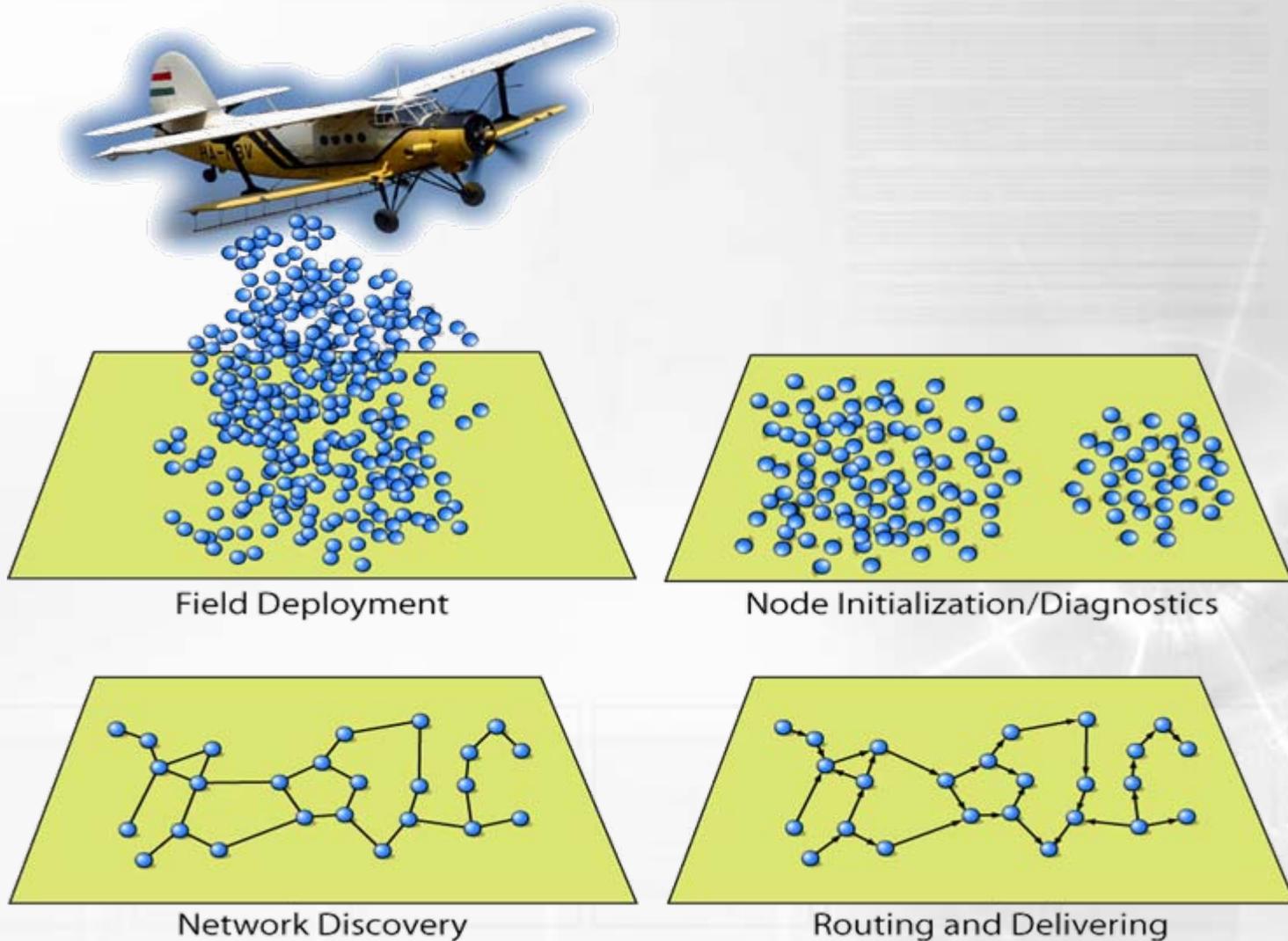
Remote Emergency Management via Satellite (REMSAT)



Broadcasting and Emergency Warning

- Broadcasting is the most effective way to alert Canadians of an imminent danger
- Advantages of the analog Broadcast systems (AM, FM, NTSC TV) are:
 - Ubiquitous receivers,
 - Low cost portable, battery operated receivers
 - Large coverage area
 - No overload of the transmission system
 - Instantaneous transmission of the information and simultaneous reception
- Digital Broadcasting systems offer new features and functions
 - As an example, CRC has developed and proposed a new position location technique using the DTV transmitters
- Transition to Digital Broadcasting must take into consideration the impact this will have on the governments' ability to reach citizens and alert them of emergencies

Sensor Network Communications for Public Safety



Network Security R&D Program

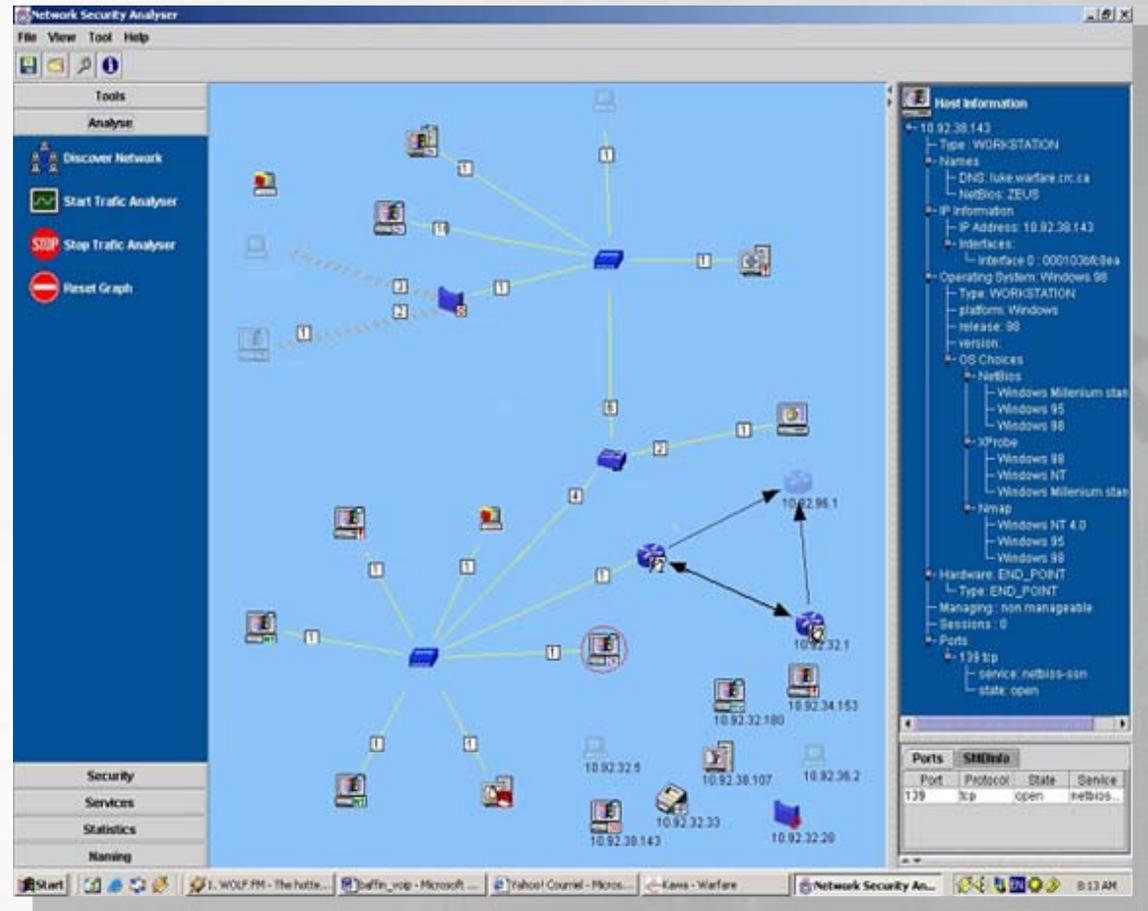
- New **algorithms and advanced techniques** to identify and mitigate future network based attacks
- Covers both **wireless** and **wired networks**
- Aligned with Industry Canada S&T programs and policies
- Technology and experience shared across Branches

Network Security R&D Themes

- Detection of **Next Generation** of Attacks
- Detection of **Disguised** Malicious Activities
- Next Generation of **network management systems** and tools
- Development of advanced **Test Strategies and Facilities**

Discovery, Identification and Monitoring Prototype

- Tools that help managers know what is happening on the network
- **Passive** and **active** techniques (tools) for network discovery and event identification



Complex Attack Detection

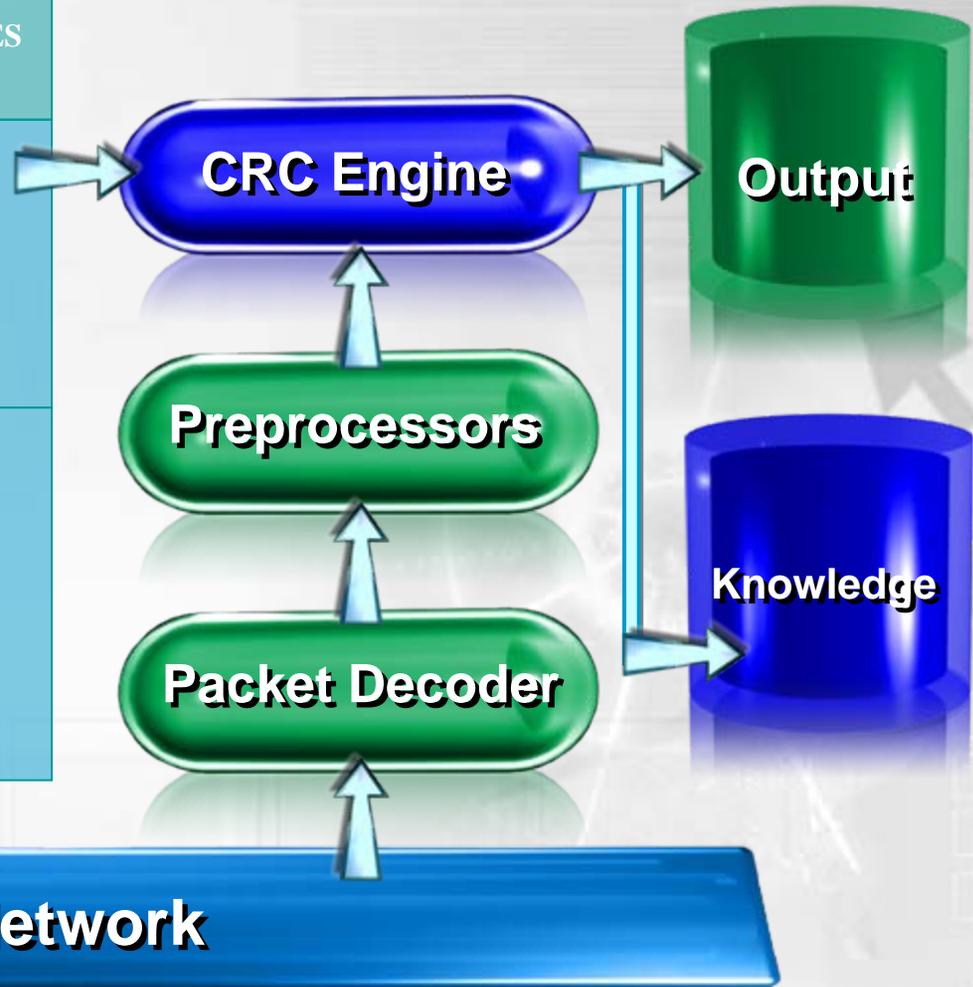
- Attack language scenario for Intrusion Detection Systems
- Multi-packet, multi-source attacks
- Correlation of security events and network information

Complex Attack Detection Prototype

```
alert tcp $HTTP_SERVERS $HTTP_PORTS ->  
  $EXTERNAL_NET any (msg:"ATTACKRESPONSES  
  index of /cgi-bin/ response")
```

```
step syn1 : tcp (flags :S ;  
step syn2 : tcp (flags :S ;  
timeout : syn1.timestamp + 2sec  
step syn3 : tcp (flags :S ;  
Output : assert(alert(portscan,[syn1.sip],[syn1.dip])).  
timeout : syn1.timestamp + 2sec
```

```
step arpreply : arp (opcode=2 ;  
step anyip : ip  
match : arpreply.dmac=anyip.smac ;  
        anyip.sip=arp.sprotoadr ;  
arpreply.tprotoadr !=anyip.dip ;  
output : assert(gatewayfor(anyip.sip,arpreply.tprotoadr).  
timeout : arpreply.timestamp + 2 ;
```



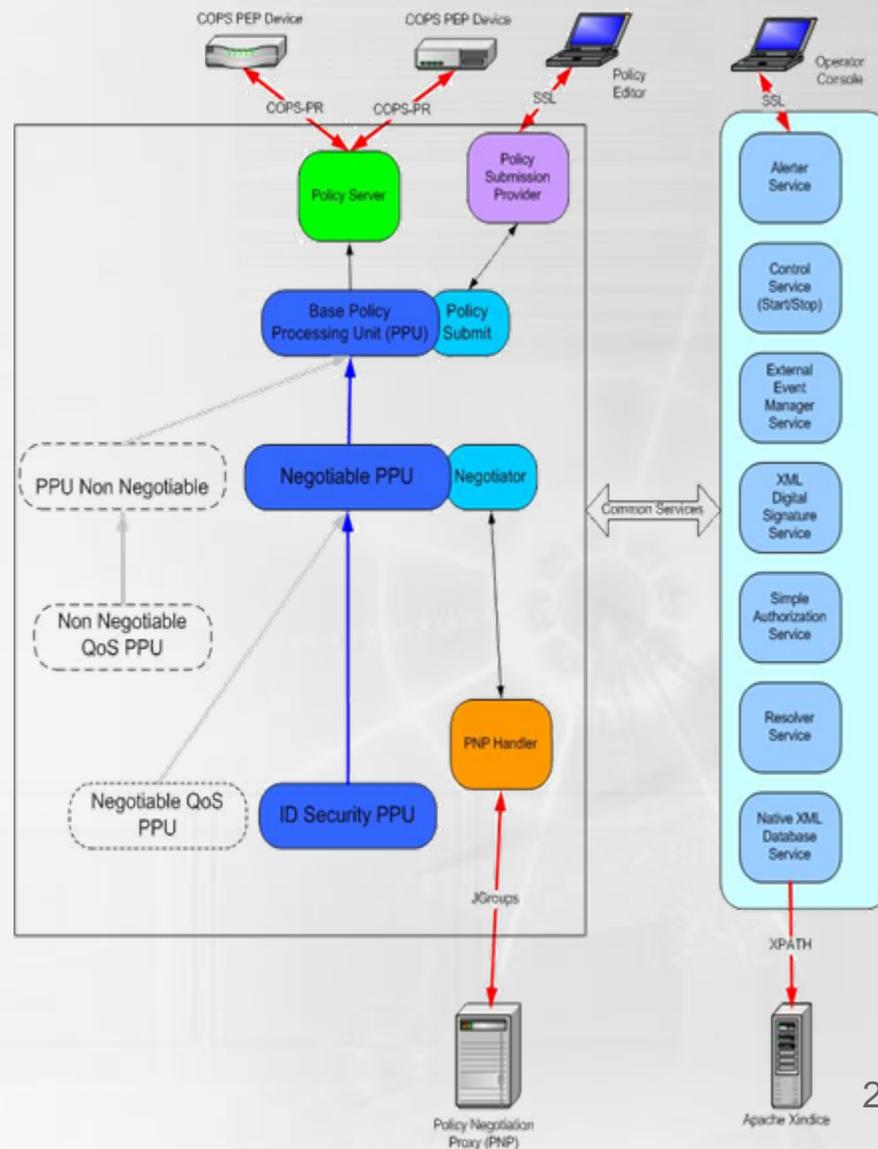
Information Flow Analysis

- Passive tools to help network managers **identify disguised malicious activities** on the network
- Light weight techniques
- Characterizes commonly used protocols and services
- Proof of concept completed

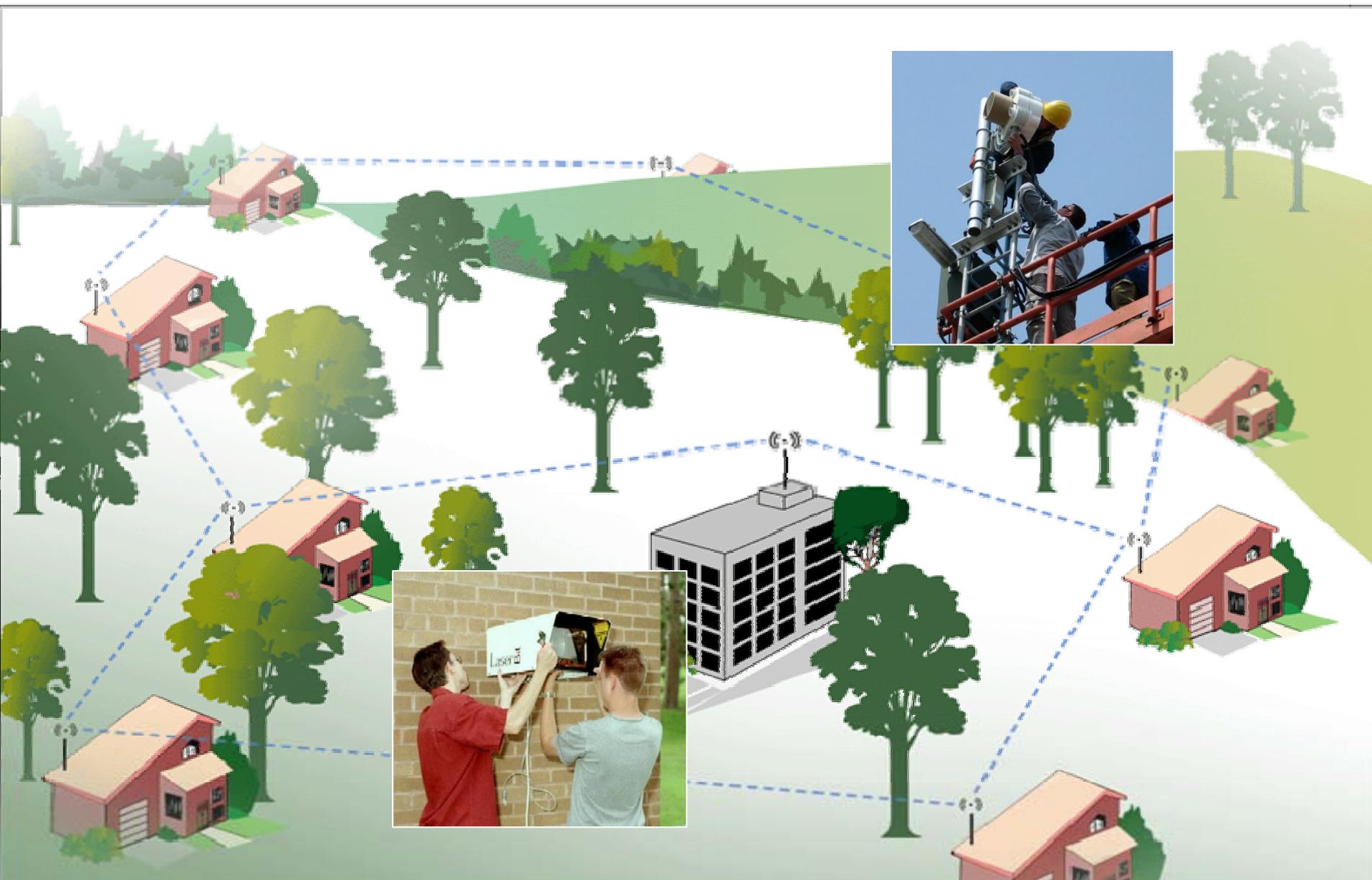


Policy Based Network Management

- Prototype implementation of **policy management** including Security Policy, Quality of Service, Routing
- Cooperative effort with **DRDC Ottawa** and others (international)
- Focus on **trust among peer** organizations
- Multi-use system



WiseLab: Wireless Security



Wireless Security

- **Secured Mobile Network test-bed (support to DRDC)**
 - Testing, evaluation, and experimentation
 - Wi-Fi security (WPA, Wireless VPN, 802.11i, RADIUS)
- **Industry and International research collaboration**
 - Telus Mobility
 - Dependability and Security by Enhanced Reconfiguration (DESEREC), European Community Framework 6 Project
- **Wireless security applications**
 - Protection for Public Safety Ad-Hoc Network
 - Multimedia Over Secure Network and QoS
 - Secure Voice over IP
- **Wireless transmission security**
 - Radio fingerprinting
 - Beamforming

Summary

- **Outcome of CRC's R&D supports:**
 - Policy, regulatory and standards development
 - Prototype development and testing
 - Protocol test and evaluation
 - Spectrum Management
 - Federal government programs
- **CRC contributes to commercialization through:**
 - Research collaboration
 - Technology transfer
 - Access to our test-beds and facilities
 - Incubation Facilities



Communications
Research Centre
Canada

Centre de recherches
Sur les communications
Canada

An Agency of
Industry Canada

Un organisme
d'Industrie Canada

www.crc.ca

Canada 