



Communications  
Research Centre  
Canada

An Agency of  
Industry Canada

Centre de recherches  
sur les communications  
Canada

Un organisme  
d'Industrie Canada

# Wireless Communications – Ubiquitous Networked Devices, Systems and Warfighters

(Wireless communications  
disruptive technologies)

Luc Boucher,  
Communications Research Centre (CRC)  
Luc.Boucher@crc.ca, 998-2050

Canada

CENTRE DE RECHERCHES SUR LES

COMMUNICATIONS

RESEARCH CENTRE

CRC

# A Glimpse at CRC

- Primary federal government laboratory for advanced communications R&D
- Agency of Industry Canada
- Major clients: Industry Canada, National Defence, Canadian Space Agency, Canadian industry
- \$40 M annual budget
- 200 research staff
- Landlord of 600-hectare research campus, shared with DND, CSA, SITT, NCIT



# Continuing the Military Tradition



- National Defence remains a major client of CRC
  - 25% of R&D effort
- Meeting requirements for R&D on higher-capacity, secure, interoperable, global military communications
  - Wireless communications – terrestrial & satellite
  - Network technologies for quality-of-service-based, seamless, heterogeneous networks
  - Communications surveillance technologies
  - Antennas & electronics

# Shirleys Bay Campus



CENTRE DE RECHERCHES SUR LES

COMMUNICATIONS

RESEARCH CENTRE

# CRC Research Branches

- Terrestrial Wireless
- Satellite Communications and Radio Propagation
- Broadcast Technology
- Broadband Network Technologies





# WISELAB

Wireless and Inter-Networking Systems Experimentation Laboratory

Laboratoire expérimental de systèmes de communication sans fil et d'interconnexion de réseaux



<http://www.crc.ca/wiselab>

CENTRE DE RECHERCHES SUR LES

COMMUNICATIONS

RESEARCH CENTRE

# Four Wireless Communications Disruptive Technologies According to the Economist \*

- **“Four disruptive technologies are emerging that promise to render not only the next wave of so-called 3G wireless networks irrelevant, but possibly even their 4G successors”**
  - **Smart Antennas,**
  - **Mesh networks,**
  - **Ad-Hoc architectures,**
  - **Ultra-wideband transmissions**
- **CRC & DRCD Ottawa => conduct research in all these areas**
- **These technologies are derived from military research**
- **They will be described in this presentation, but first let’s look at the trends**

\* Jun 20th 2002

[http://www.economist.com/printedition/displayStory.cfm?Story\\_ID=1176136](http://www.economist.com/printedition/displayStory.cfm?Story_ID=1176136)

# Trends

- Surge in popularity of mobile phones—their number will **overtake that of fixed phones** during 2002/03—has prompted both established firms and start-ups to investigate ways to make phones more efficient and versatile.
- At the same time, the **Internet is going wireless**, driving a separate wave of innovation as the Internet's legendary ability to disrupt traditional ways of doing things enters a new arena.
- One Goal is to be able to connect (voice and data) from **anywhere**, mobile or fixed.
- Another Goal is to be able to roam from one network to another without any communication interruptions (**seamless communications**).





# Trends (cont.)

- **Multiple interfaces** in a single unit – support both 2.5G networks (long-range, but capable of only a few hundred kilobits per second) and the popular Wi-Fi wireless networks (“hot-spots” - short-range, and capable of 11 megabits per second).
- A move towards **merging fixed and mobile** infrastructure - providing fast mobile-data access, and also a wireless solution to the “last mile” problem of providing high-speed broadband access to the home.
- Within the past few years the field has seen a **rapid expansion** of visibility and work due to the proliferation of inexpensive, widely available wireless devices and the community's interest in mobile computing.
- Innovation is supported by **technical advances** such as: Increasing processing power of DSP, Evolution of network protocols, miniaturization of electronics and of network components (routers), supported by low costs.

# Trends (cont.)

- If the current pace of innovation in the field is anything to go by, wireless technology is **still in its infancy**.
- Difficulties surrounding the deployment of “third generation” (3G) networks in particular could be taken as evidence that **existing ways of doing things** are reaching their limits, and that some radical **new ideas** are needed.



# New Technologies

- Hence, it is in this context that four emerging technologies show much promise:
  - Smart antennas,
  - Mesh networks,
  - Ad hoc architectures, and
  - Ultra-wideband transmission.
- Smart antennas and mesh networks have been around commercially for a couple of years, while ad hoc architectures and ultra-wideband are starting to appear on the market.
- Each challenges existing ways of doing things; each, on its own, or in combination with others, could shake up the wireless world.



# Smart Antennas

- Wireless antennas, in their simplest form, are inefficient: A base-station on a cellular telephony network, for example, typically communicates with nearby handsets by **broadcasting in all directions**.
- Base-stations use only a fraction of the radio spectrum available (to avoid interference with adjacent cells) but the use of **directional antennas** enables radio frequencies to be reused more **efficiently**, thus boosting capacity.
- So instead of one omni-directional antenna, many base-stations now use **three-directional** antennas pointing in different directions, each of which covers a 120° sector.



# Smart Antennas (cont.)

- Smart antenna systems go a step further, using multiple antennas to provide more accurate **directional targeting** and additional improvements in efficiency.
- The base-station **finds out where you are** from the relative signal strengths at multiple antennas and then **direct its transmission to you** (some systems, at the power level that you need).
- Adding this technology to a base-station typically **boosts capacity** by a factor of three to seven. Some new schemes claim even higher improvement of efficiency.
- The plunging cost of processing power (DSP) means that smart antennas, which started out as an expensive military technology, are now **a cheaper way to increase network capacity than building new base-stations**.



# Mesh Networks

- For Mesh networks, the neighborhood is first “seeded” by the installation of a “neighborhood access point” (NAP)—a radio base-station connected to the Internet via a high-speed connection. Homes and offices within range of this NAP install wireless access points of their own, enabling them to access the Internet at high speed.
- Then, each of those homes and offices can also act as a relay for other homes and offices beyond the range of the original NAP. As the mesh grows, each node communicates only with its neighbors, which pass Internet traffic back and forth from the NAP. It is thus possible to cover a large area quickly and cheaply.



# Mesh Radio Technology

## Conventional Base Station Approach



## Mesh Radio Approach (wireless router)



- Each radio not only provides internet access for attached users, but also becomes a part of the network infrastructure (relay the signal of other users)
- No need for initial expensive infrastructure implementation (build as needed)
- Increased coverage - Reach non line-of-sight users

# Mesh Networks (cont.)

For providing fixed-wireless access, the mesh approach is technically superior to the traditional “point-to-multipoint” radio approach in a number of ways:

- Reduce needed RF power significantly.
- No need for tall antennas.
- Reduced problem of interference with adjacent cells. Mesh networks use rooftop antennas.
- Mesh systems are self-configuring so that, like the Internet, traffic is sent by the quickest route.
- Also like the Internet, mesh networks are robust and can be scaled up easily
- Because of reduced power needs = can use unlicensed spectrum (no license costs)
- Implementation = radios based on 802.11 hardware + mini wireless router = low costs



# Nokia Rooftop Mesh Radio

- A number of firms are now pushing mesh network technology as a fast and easy way to provide broadband Internet access, e.g.
  - Nokia's system, called **RoofTop**, is being rolled out by more than 50 operators in the US, mainly small Internet service-providers (**ISPs**).
  - The ISP installs an AirHead unit (Nokia's name for a NAP) to seed a neighbourhood, and a small, weatherproof pod with an omni-directional antenna is fixed to the outside of each subscriber's home or office.
  - Each pod costs around **\$800 (US)**.
  - ISPs charges around \$200 for installation, and then a monthly fee of \$50 for broadband Internet access (competitive to cable modem and DSL).



# Nokia Mesh Radios

- Uses the 2.4 GHz unlicensed band (next generation will use the 5.8 GHz).
- 1-3 km Range, more with directional antennas
- Characterization was done by Wiselab (to identify its potentials and its operational limitations) e.g.
  - the number of users that can be cascaded before the network encounters interference or throughput limitations,
  - non line-of-sight advantages,
  - the robustness of the network's TCP/IP and scheduler algorithms,
  - security protection, etc.



# Other Mesh systems

- SkyPilot (California) are using **smart antennas** to beam data back and forth in their mesh implementation, enabling frequencies to be reused more efficiently and increasing capacity.
- Radiant Networks (UK) has implemented mesh technology for the **LMCS/LMDS** bands (25 to 40 GHz).
- MeshNetworks (Florida) are developing a wireless mesh-network that **supports mobile devices**. In addition, when two or more devices are beyond the range of a “neighborhood access point” (NAP), they spontaneously form their own local network. MeshNetworks' technology thus combines the mesh architecture with the approach of “**ad hoc**” networking.



# Ad- Hoc Networks

- In an ad-hoc network, stations **cooperate to build the network** and communicate using a common wireless channel.
- Each station **can communicate directly** with one or more of the other stations in the network.
- To reach stations further away, radios on the network **act as relays**. Data is carried through from source to destination by being passed from one relay to the next.
- Each station **maintains a list** of the stations with which it can directly communicate.
- Connectivity information is built up and **distributed** by each station.



# Ad- Hoc Networks (cont.)

- An ad-hoc network may be **integrated** with a wider network by one of the stations on the ad-hoc network acting as a **gateway**.
- Ad hoc networks are well suited for use in situations where infrastructure is either not available, not trusted, or can not be relied on in times of **emergency**. A few examples include:
  - mobile military units in the field;
  - sensors scattered throughout a city for biological detection;
  - an infrastructure-less network of notebook computers in a conference or campus setting;
  - temporary offices such as campaign headquarters, etc.
- Rescue workers in an earthquake zone, for example, could use handheld radios, each of which also acts as a relay for other nearby radios.



# Ad- Hoc Networks (cont.)

- Recently interest in this field has **increased as commercial** possibilities have started to emerge. “**Bluetooth**”, a short-range wireless protocol that enables mobile devices to talk to nearby handheld computers, printers and phones, is a simple form of ad-hoc networking, though it supports only single “hops” between individual devices.
- The advent of **Wi-Fi (802.11b)** networking equipment has also provided a foothold. With the **right software**, it is possible to allow WI-FI-equipped laptops to act as relays for other nearby machines, letting packets make multiple hops from machine to machine to get to and from the Internet.
- Ad hoc networks can be built around any wireless technology, including **infrared and radio frequency (RF)**.



# Differences Between Mesh and Ad-Hoc Networks

- Getting very similar.
- Traditionally Mesh was mostly for fixed applications (not mobile).
- In Mesh the emphasis is on communications **from the user to the infrastructure gateway** (e.g. internet), where with ad-hoc networks the emphasis is on establishing a **self-configurable network** that allows all devices **to talk to each other**.
- More on ad-Hoc networks and their applications for military communications **to follow**. For now, a short description of the last disruptive technology: **UWB**



# Ultra Wideband (UWB) Communications

- Ultra Wideband (UWB) systems transmit signals across a **much wider frequency** than conventional systems and are usually very **difficult to detect**.
- The amount of spectrum occupied by a UWB signal, i.e. the bandwidth of the UWB signal is at least 25% of the center frequency. Thus, a UWB signal centered at 2 GHz would have a minimum bandwidth of 500 MHz and the minimum bandwidth of a UWB signal centered at 4 GHz would be 1 GHz.
- The most common technique for generating a UWB signal is to **transmit pulses** with **durations** less than 1 nanosecond
- Such pulses pass unnoticed by conventional radio receivers, but can be detected by a UWB receiver.



# UWB Applications

- Communications - High Speed WLANs, Mobile Ad-Hoc wireless networks, Groundwave Communications, Handheld and Network Radios, Intra-home and Intra-office communication. **Stealthy communications** provide significant potential for military, law enforcement, and commercial applications.
- Sensor Networks - Ground penetrating Radar that detects and identifies targets **hidden** in foliage, buildings or beneath the ground. Intrusion Detection Radars, Obstacle Avoidance Radars, and Short-range motion sensing.
- Tracking/Positioning - Precision Geolocation Systems and high-resolution imaging. Indoor and outdoor tracking down to less than a centimeter. Good for emergency services, inventory tracking, and asset safety and security.



# Regulatory aspects of UWB

The Federal Communication Commission (FCC) adopted in February 2002 a First Report and Order that permits the marketing and operation of certain types of new products incorporating ultra-wideband (“UWB”) technology. Subject to **power and frequency limitations**:

- Ground Penetrating Radar and Wall Imaging Systems: must be operated below 960 MHz or in the frequency band 3.1-10.6 GHz.
- Wall-imaging systems and Through-wall Imaging Systems: must be operated below 960 MHz or in the frequency band 3.1-10.6 GHz.
- Medical Systems (“see” inside the body): operated in the frequency band 3.1-10.6 GHz.
- Surveillance Systems (“security fences”): operated in the frequency band 1.99-10.6 GHz.
- Vehicular Radar Systems: operated in the 24 GHz band.
- Communications and Measurement Systems: operated in the frequency band 3.1-10.6 GHz.

# Regulatory aspects of UWB (cont.)

- The FCC ruling limits the **range** of UWB transmissions to about **ten metres**, although longer ranges may be allowed in future once the question of interference has been sorted out. However, UWB is capable of a data rate of at least **100 megabits** per second over such distances.
- UWB devices can be used for a variety of communications applications involving the transmission of very high data rates over short distances **without suffering the effects of multi-path interference**.
- These devices (with **higher power**) could also be utilized by police, fire, and rescue personnel to **provide covert, secure communications** devices.



# UWB and Ad-Hoc Networks

- Together, UWB and ad hoc architectures are a natural fit, since the UWB devices will have to locate each other and start communicating automatically, tasks that ad hoc networking readily facilitates. The two technologies have been used together in military applications. UWB pulses, emitted apparently at random, are very difficult to detect or intercept, and are ideal for battlefield transmissions.
- At this time only the US (FCC) has put in place regulations to allow the commercial use of UWB, but other countries are studying the technical aspects and may update their spectrum policies to allow UWB use.



# Future US Communications and Networks

- **Why** are these technologies so **important** to military?
- Let's look at **future battlefield scenarios** and US military communications and networking **plans**:
  - During the 1990's, the DoD published a number of "vision" documents, all of which depicted a future Warfighter scenario where heavy dependence on **Information Dominance** is a central feature.
  - **Wireless connectivity and wireless information networks** are the only practical means for **achieving** the end objective: a force which is based on equipment that inherently provides the ability to command Information Dominance in every situation.
- Very strong Need for secure and reliable communications



# Objective Force Communications and Information Architecture

- Multi-Layered Communications/Information Network
  - Space Layer
  - Airborne Layer
  - Terrestrial Layer
- Network-Centric “Infosphere”
  - “In network-centric warfare, sensors and shooters are connected by a ubiquitous network through which weapons can engage targets based on a situational awareness that is shared with other platforms”
- Distributed and Redundant



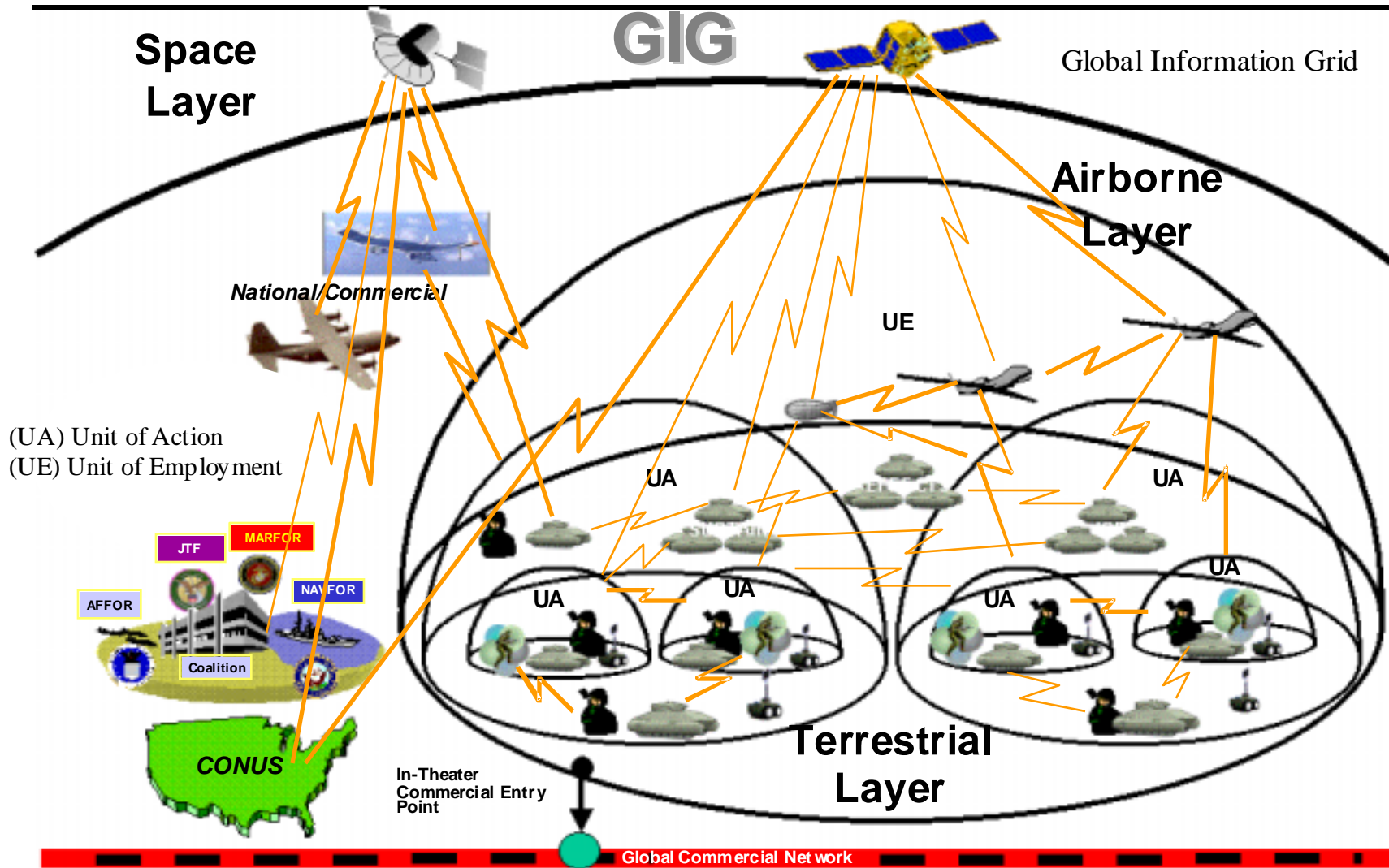
# Information Dominance - The Communications “Infosphere” Concept

- The “Tactical InfoSphere” around battlefield will **carry** among other things: voice, data, messaging, sensors data, and control information.
- It is a combination of **C4ISR\* capabilities** organized to support Army or Joint forces in the accomplishment of a mission.
- It consists of a **large number** of sensors, a robust command and control system, rules for rapid distribution of information through the InfoSphere, and all the communication nodes of the tactical units assigned to the force concerned.
- It may be linked to organizations and resources which will support the operations **outside** the Tactical InfoSphere, for example logistic organizations charged with providing supplies.

\* command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR)

# US Army's CONOPS for Network Centric Signal Support

## The Multi-Layered Comm/Info Network





# The Multi-Layered Comm/Info Network

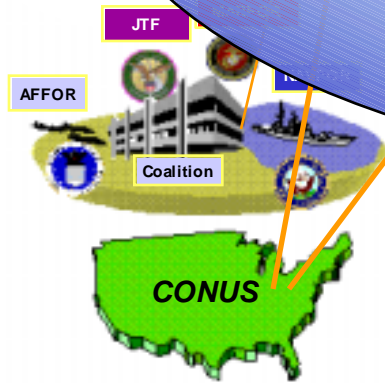
Space  
**The Goal...**

**GIG**



**Move the switching and routing backbone into the sky**

Airborne

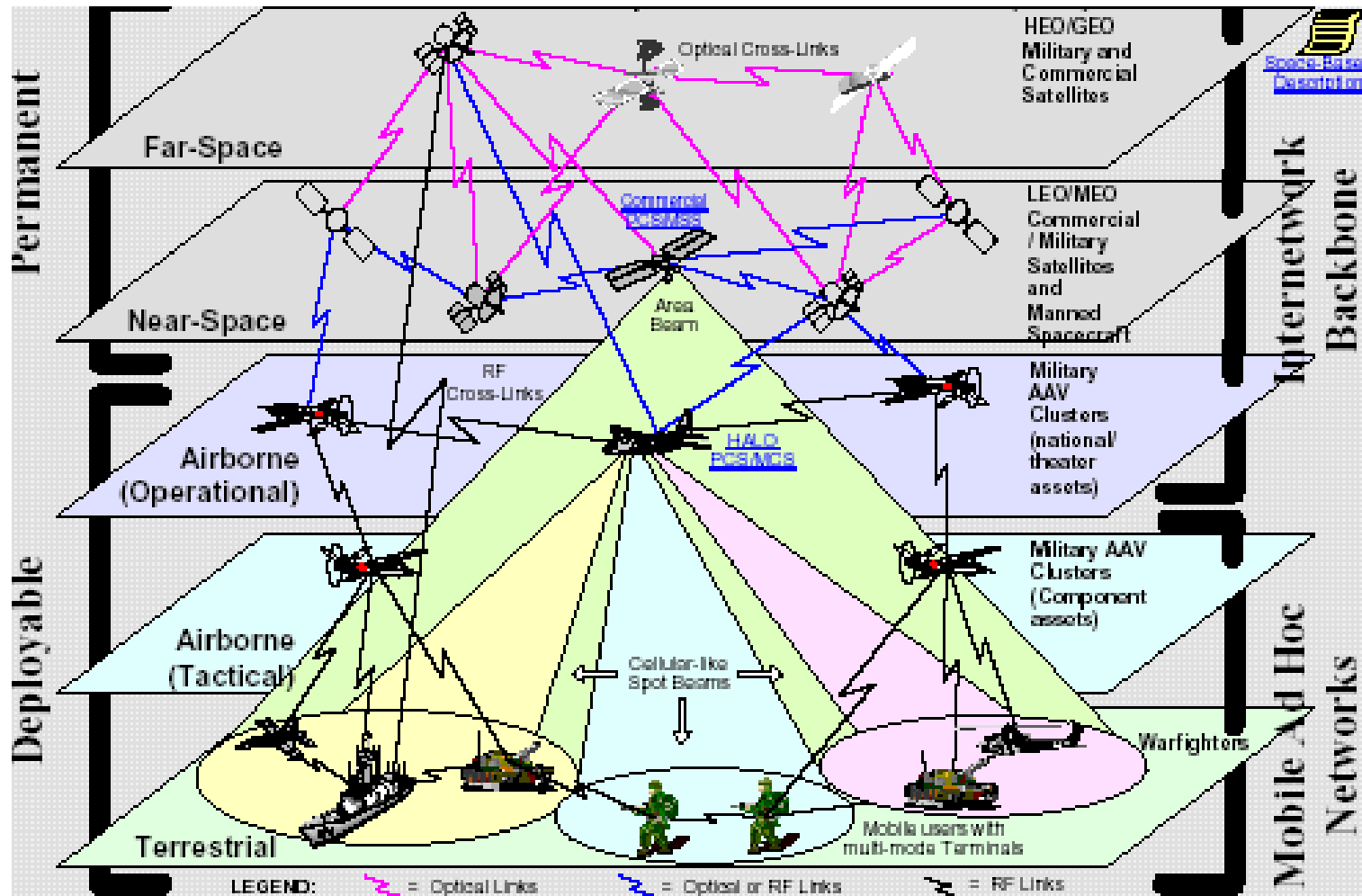


In-Theater  
Commercial Entry  
Point

- Easier to deploy
- Connects widely dispersed forces
- Covers fast-paced operations
- No ground backbone to maneuver

Global Comm. Network

# Levels of Warfighting Operations



An important means for providing this level of connectivity will be the incorporation of multiple layers of airborne rebroadcast using aircraft, UAVs and satellites  
 Note: Mobile Ad-Hoc Networks layers

# Other Studies showing the importance of Ad-Hoc networking

**ARMY SCIENCE BOARD**

**2001 AD HOC STUDY**

**FINAL REPORT**



DEPARTMENT OF THE ARMY  
ASSISTANT SECRETARY OF THE ARMY  
(ACQUISITION, LOGISTICS AND TECHNOLOGY)  
WASHINGTON, D.C. 20310-0103

**ADAPTING FUTURE WIRELESS  
TECHNOLOGIES**

**November 2001**

**Distribution Statement:  
Approved for public release; distribution is unlimited**

CENTRE DE RECHERCHES SUR LES

**COMMUNICATIONS**

RESEARCH CENTRE

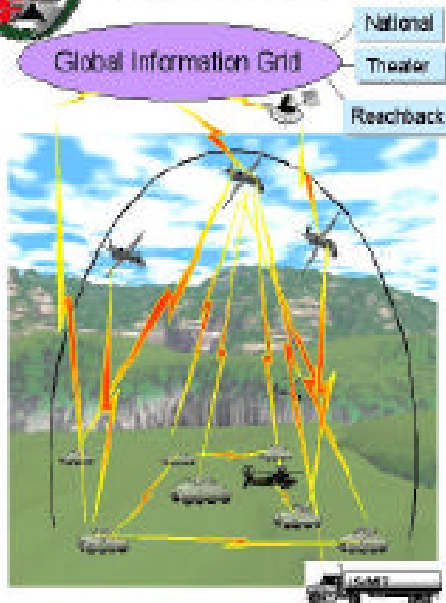


# Information Dominance

- Mobile Army of the Future is heavily dependent upon wireless communications.
- Need connectivity from all echelons to Tactical Infosphere **and** GIG.
- Reliable, Robust, Mobile comm is essential!



## Objective Force Tactical InfoSphere



### Comprised of:

- Platforms equipped with radios, sensors, processors, routers, Pos Nav, communicating via a tactical internet
- A family of dedicated UAVs for Assured Comm and ISR
- Distributed Processing and Information Management

### That Provide:

- Real-time, precision situational awareness and targeting
- Connectivity with Joint, Theater, and National sources and Reachback Assets on the GIG
- Decision Dominance by Tactical Commanders

Technical and Tactical Opportunities for Revolutionary Advances in Network Centric Warfare Joint Chiefs of Staff, 2005-2015

DoD Copy, No. 1. It is published without permission from the Army Research Office (ARO) or the Secretary.

Page 8  
06/05/2011 10:11

- What Technologies are needed?
- How many satellites and UAVs?
- Imperative to have mobile ad hoc network!

# The importance of Ad-Hoc networking for future military communications

- Quoted from the Army Science Board report “Adapting Future Wireless Technologies”:
  - “During our study of terrestrial wireless technologies, one key technology area that stood out was the utilization of mobile **ad-hoc networks** within tactical military networks.”
  - “To implement the Objective Force C4ISR and maintain reliable, versatile communications through and across all echelons requires integration of **ad hoc networks** with layered hierarchical networks (land, air, and space segments) **in an IP environment.**”
- Advanced **research programs on ad-hoc** networking in the US:





# Findings - Terrestrial

## **Mobile Ad Hoc Network continued...**

- What we found in DoD/Army
  - DoD (DARPA) Programs supporting ad hoc networks: Glo Mo, SUO/SAS, survivable Ad Hoc Routing Protocol (TBRPF), FCS, Ad Hoc networks with directional antennas
  - CECOM MOSAIC
    - Self-healing, mobile ad hoc networks, vertical routing optimization
    - Adaptive self-configuring protocols
    - QoS across the network
- What we found in Commercial
  - Commercial primarily addressing mobile users, but not mobile infrastructure

# Challenges

- Many challenges remain in order to be able to provide reliable, robust and mobile communications for the Armed Forces, among them:
- **Robust and secure** ad-hoc network **protocols**:
  - Need to set up networks quickly in a deployment => efficient ad hoc protocols
  - Need to support mobile and highly transient environments
  - The use of wireless-networking protocols creates new vulnerabilities, making interruption possible not only by jamming but deception.



# Mobile Networks

- The thrust for wireless communications systems developments in both the military and civilian sectors clearly indicate that **Internet Protocol (IP)** service will become a standard service model for tactical RF networks. A move to Internet Protocol version 6 (**IPv6**) will be needed to support mobility, and **improvements to it** will be needed to support highly transient and secure environments
- The military must develop methodologies for **QoS** adaptation (management of routing, priorities, bandwidth, power consumption, frequency) and information assurance with adaptive response based on perceived level of attacks.
- **Scalability** - the network must be able to provide an acceptable level of service to packets even in the presence of a large number of nodes in the network.





# Encryption

- Implementation of **mobility**, particularly wireless mobility, has **implications for the management of encryption keys**. It will be necessary to provide either a common key for use across the whole network or to provide mobile users keys for use in different parts of the network, imposing difficulty in guaranteeing the security of such widely distributed keys.



# Software Radio

- The use of software radio technology will see some **convergence** of equipment in the various subsystems of the tactical communications system, especially between the trunk and CNR subsystems. Software radio technology will be a **key enabler of the battlefield communications network**, allowing previously separate communications systems to cooperate in forming the network.
- Software radios offer the **flexibility suitable for ad hoc networks**.
- There are a number of key **technologies requiring development** for software radio, including antennas, receiver RF processing and down-conversion, analog-to-digital conversion, signal processing technology and general-purpose processors.

# Future Electronic warfare (EW) Challenges

“Future combat system and the Objective Force feature a concept for employing **unattended** missiles or munitions at **unmanned** remote locations”

- **Network protection**: The key change in the nature of EW on a future digitized battlefield will be its orientation towards the **network**, leading to a proliferation of opportunities for EW. The focus will change **from** being primarily on the **physical layer** to focusing on attacks on **network security and the security services** that protect against these attacks.
- **Information protection and assurance**: Particular emphasis will have to be directed to the security issues such as confidentiality, authentication, integrity, non-repudiation, access control and availability.



# UAV

- Reach-back capabilities encompasses satellite and UAV-based communications to link the theater of operations with information assets. There are a number of issues with UAV communications/operations that need to be developed/solved.

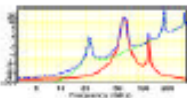



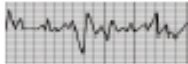

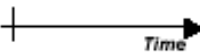


# USE of COTS

- The extensive use of commercial off-the-shelf (COTS) equipment in modern tactical communications systems is also a **source of increased vulnerability**. Much of this equipment does not conform to military standards. Furthermore, commercial wireless-network protocols are not designed to operate in a hostile electromagnetic environment, and are vulnerable to a variety of attacks, especially interruption. In general, **COTS equipment will be more vulnerable to jamming, deception and neutralization**.
- Hence, additional research and development needed to use COTS for military applications.



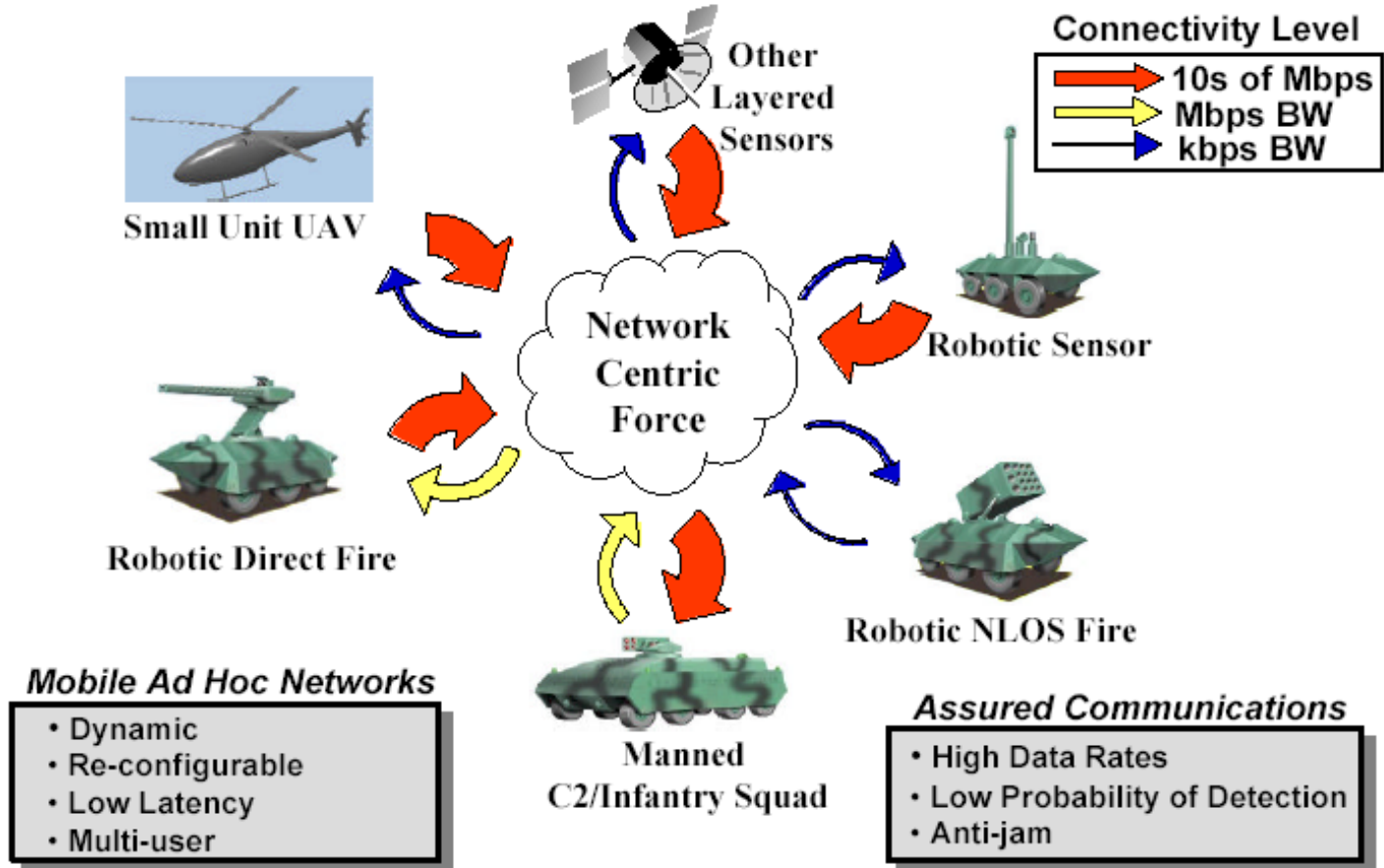
# Wideband Technology Components

		Commercial Thrust	Additional Defense Thrust
Frequency		Microwave to Wideband	Mobility
Waveforms		Multiple Access	Low Probability of Detection
Coding		Bandwidth Efficiency (Turbo Codes)	Featureless Waveforms
Multipath		Diversity Exploitation	Mobility
Interference		Spatial & Symbol Processing	Anti-Jam
Networks		IP	Mobility, Adhoc, and Assurance
Latency		QoS	

# Future Combat Systems vision (DARPA)



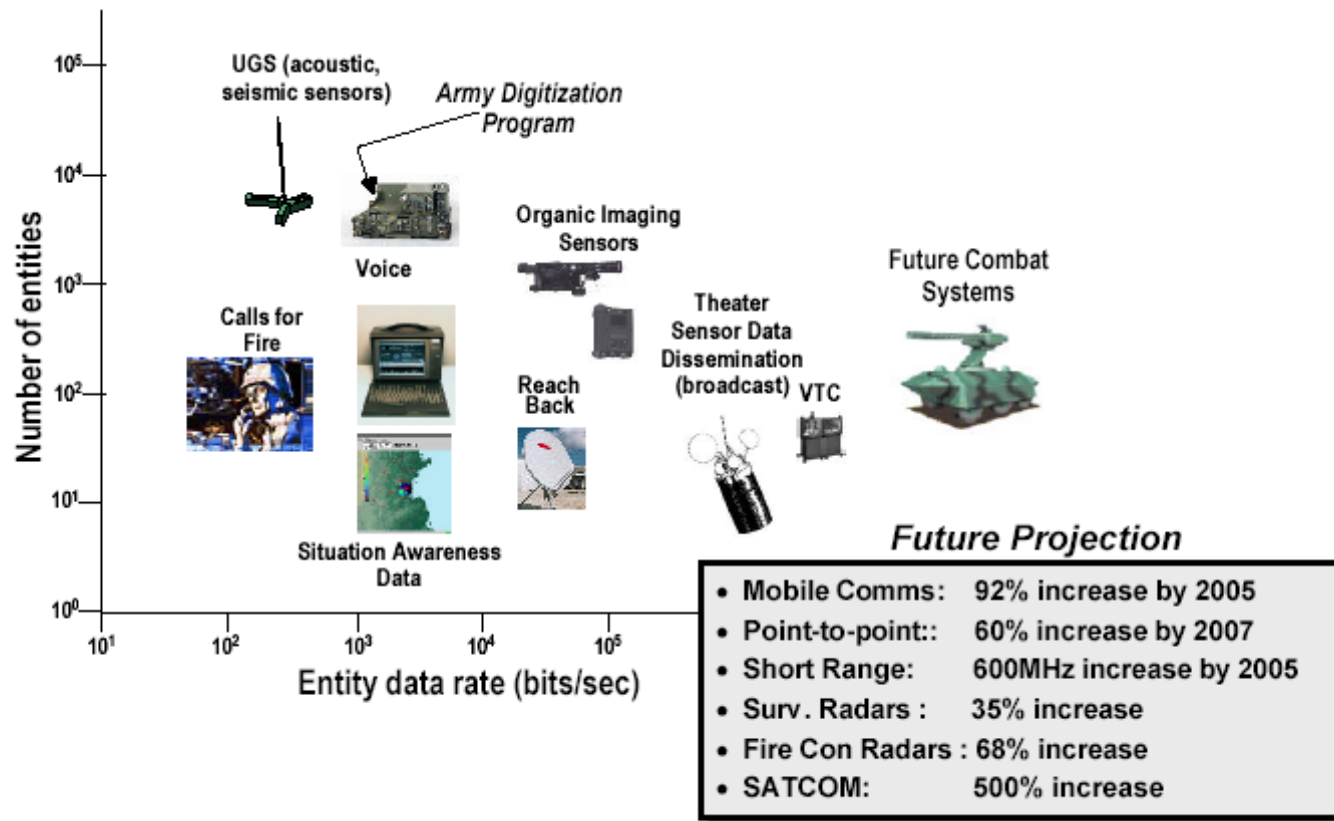
## Future Combat Systems - Assured Real-time Connectivity



# Military Broadband Requirements (DARPA)



## Military Broadband Requirements





# The Need for More Spectrum

- **Wireless** connectivity and wireless information networks are the only practical means for achieving Information Dominance in every situation.
- Since the radio frequency spectrum is going to host this wireless explosion, it is clear that the Armed Forces will **need access to more spectrum** than it currently has.
- Using higher frequency bands (mmw) may provide some alternatives (e.g. 90 GHz) – but expensive.
- Since it may be difficult to re-assign **existing** allocated frequency bands, the way spectrum is accessed must change.
- Deploying **adaptive**, flexible systems anywhere in the world requires that those systems be able to access the spectrum in adaptive, flexible ways, anywhere, anytime.



# Spectrum Sharing Schemes

- To increase the use of already allocated spectrum, various solutions are possible. Several technological advances can provide cost-efficient ways to share the allocated spectrum.
- This includes spectrum sharing schemes such as:
  - Dynamic frequency allocation,
  - Adaptive modulation,
  - Ultra wideband,
  - Higher modulation schemes, i.e. spectrum efficient air interfaces (e.g., CDMA, QAM, OFDM).
  - Smart Antennas, spatial reuse



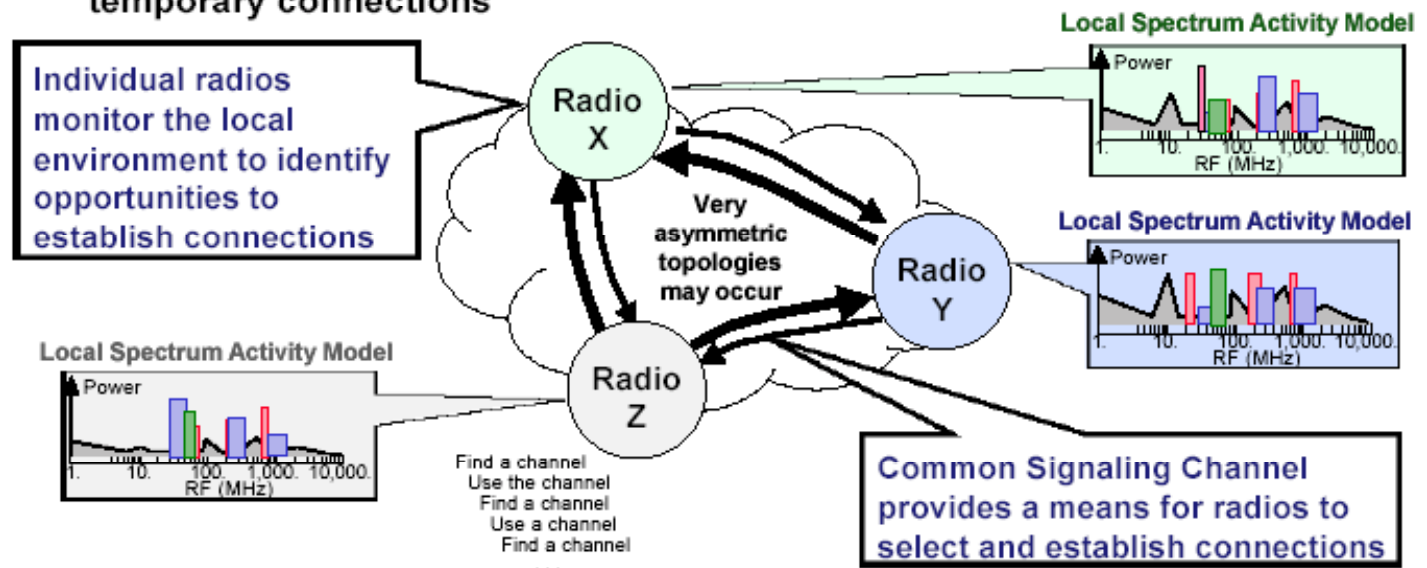
# Adaptive Spectrum Schemes (DARPA)



## Adaptive Spectrum Utilization

### • Concept:

- Adaptive Spectrum Sharing - employ unused spectrum (frequency, time and power) when and where available using special waveforms, protocols and etiquette to overlay and underlay frequencies without interference
- Tactical Adaptation- adapting locally, at the individual link level, for temporary connections



**Spectrum Adaptation can be done locally, without interference, and be stealthy**

# Conclusions

- With command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) becoming one of the most important element of military operations, its systems **must work reliably** to ensure that the future armed forces can function efficiently in a lighter and more mobile form. This will require an infrastructure that will **interconnect all systems** from the ground, air and space domains. In order to maintain all facets of information exchange in the highly mobile, rapidly changing battlefield, these systems will **depend heavily on advanced wireless communications**.
- The vision developed to support these goals includes many new technologies, one of them, **Ad Hoc wireless** networking is seen as an essential ingredient of the Tactical Infosphere.



# Conclusions

- But many challenges remain to make this vision a reality. Our research organizations (CRC, DRDC, CFEC, etc.) are working at evaluating and advancing the latest communications technologies, and at identifying how they can contribute to successfully build the wireless connectivity that meets the Canadian Armed Forces' future communication needs.

