SECRICOM
Seamless Communication for Crisis Management

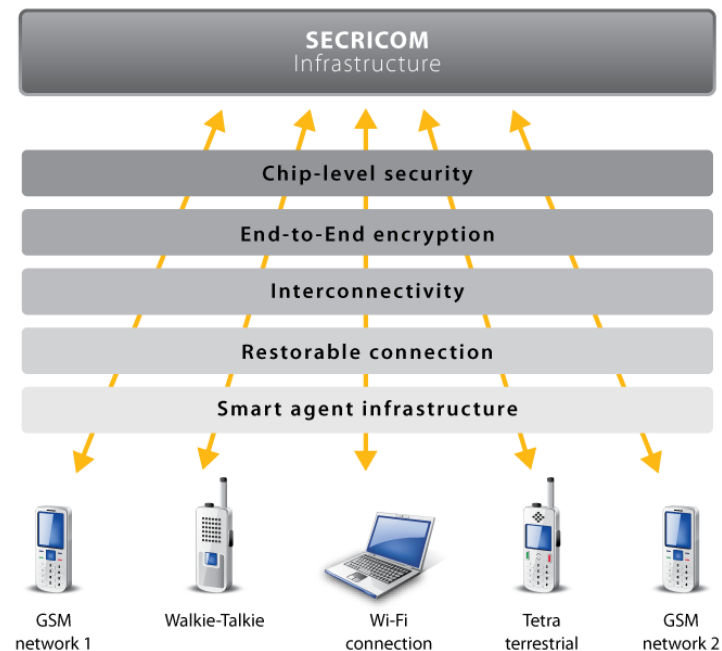Presentation to the
Civil Protection
NATO Conference 2010
Slovakia

Recover
quickly

Keep on

talking

Rich Edwards, QinetiQ
Tomas Kucharik, Ardaco (CEO)

Presentation objectives

- Introduce the Project

- Approach Taken

- Aspects of User Requirements

- Architectures and Technology

- Wrap up

SECRICOM
Infrastructure

Chip-level security

End-to-End encryption

Interconnectivity

Restorable connection

Smart agent infrastructure

GSM network 1   Walkie-Talkie   Wi-Fi connection   Tetra terrestrial   GSM network 2

Terrorism, major industrial accidents, natural disasters...

...unpredictable catastrophic events...

*...require **innovative and affordable communication and situation awareness solutions** for Public Safety Agencies and first responders...*

A key aspect in helping to recover?

Key Project Facts

- Seventh Framework Programme – FP7
- Wireless Communication for Crisis Management
  - Multi-Agency/Multi-National

- 13 Partners
- Start date: 1 Sept 2008
- End date: 30 April 2012
- 44 months duration
- Total cost ~ €12.5M
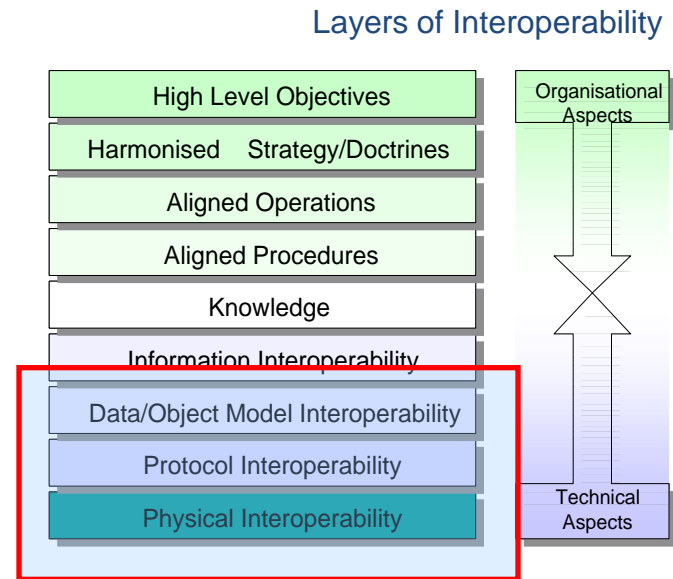- EU contribution ~ €8.6M

Aims

- Provision of secure seamless communications for emergency agencies at times of crisis

- Enhance interoperability among heterogeneous secure communication systems

- Enhance interconnectivity between different networks and User Access Devices

- Exploit existing communication systems

- Interface towards emerging SDR systems in a generic manner

- Mitigate the key capability gaps faced by users of existing systems

User-Directed Objectives

Interoperability is the underlying project theme since it plays an important role in collaborative multi-agency/multi-national crisis management. Areas of Secure Interoperability that are being addressed are

- Between multiple civil protection agencies;

- Across international borders;

- More effective information exchange offering greater scope
  – Vertically along the C2 agency structures,
  – Horizontally between agencies at various C2 levels, and
  – Flexibly for out-of-theatre communication reach;

- Vendor independence for
  – User end devices,
  – Communication systems, and
  – Service providers.

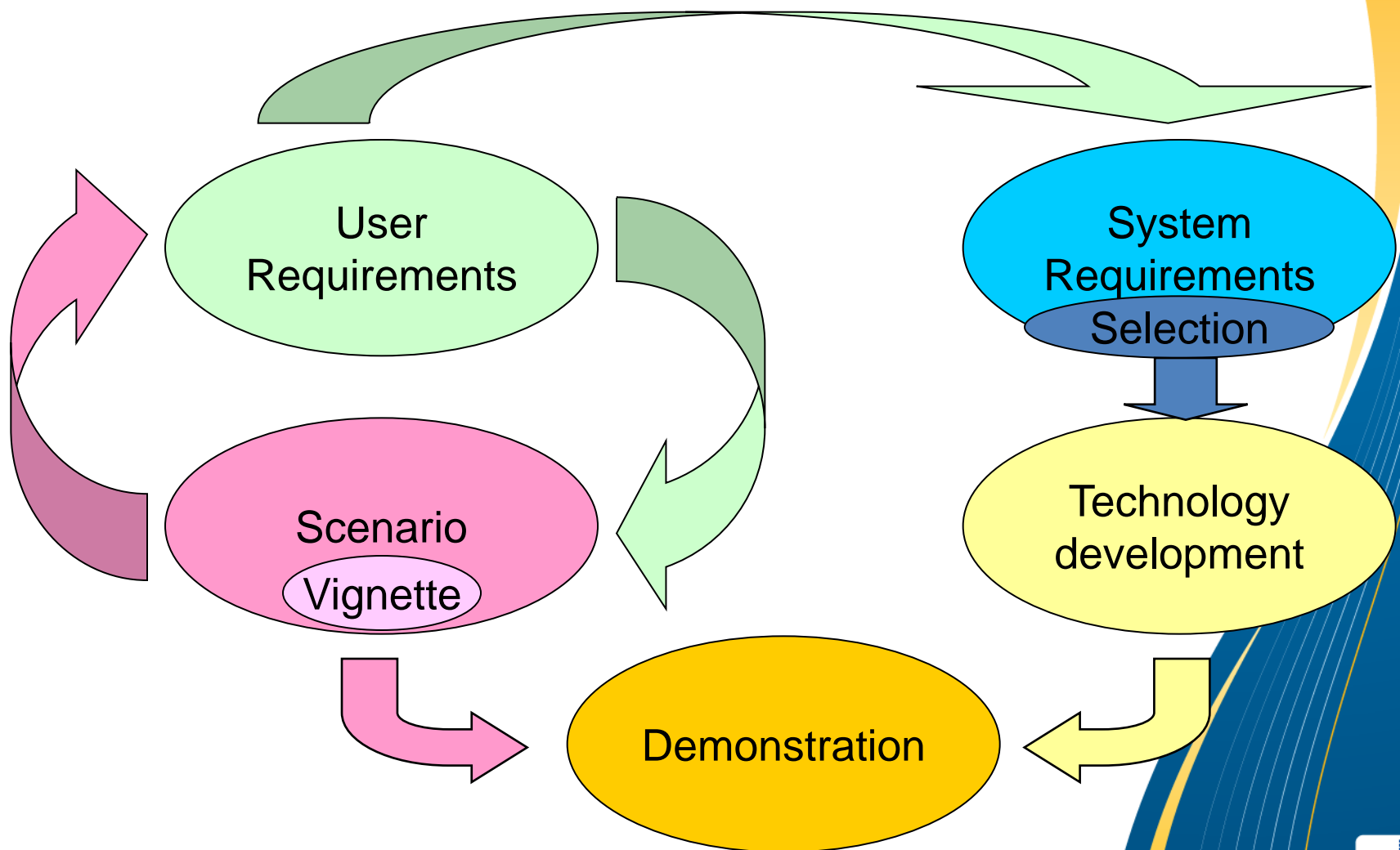| Layers of Interoperability	
High Level Objectives	Organisational Aspects
Harmonised Strategy/Doctrines	
Aligned Operations	
Aligned Procedures	
Knowledge	
Information Interoperability	
Data/Object Model Interoperability	
Protocol Interoperability	
Physical Interoperability	Technical Aspects

SECRICOM Scope:
The technical aspects of Interoperability

Business Stakeholders
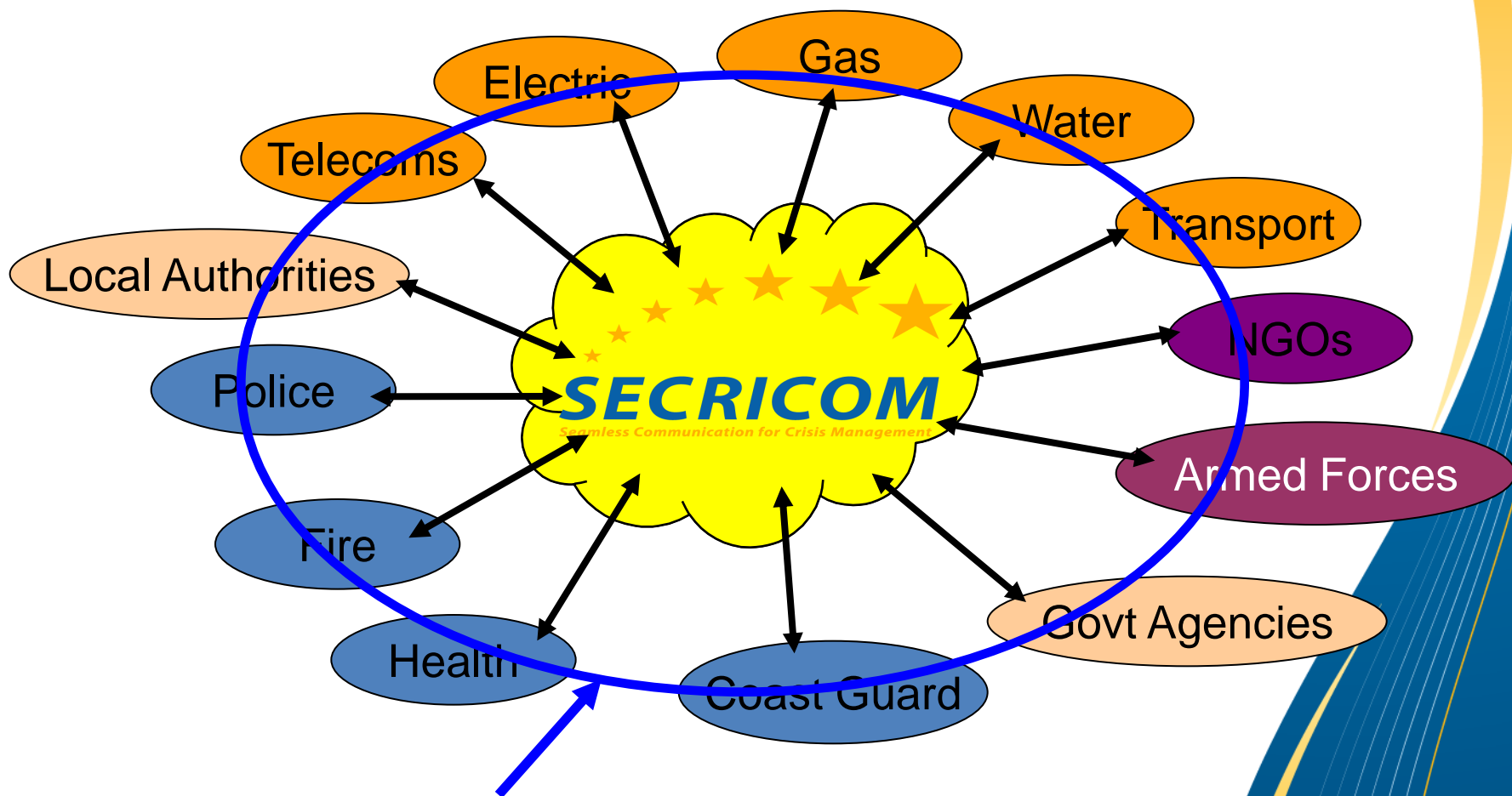
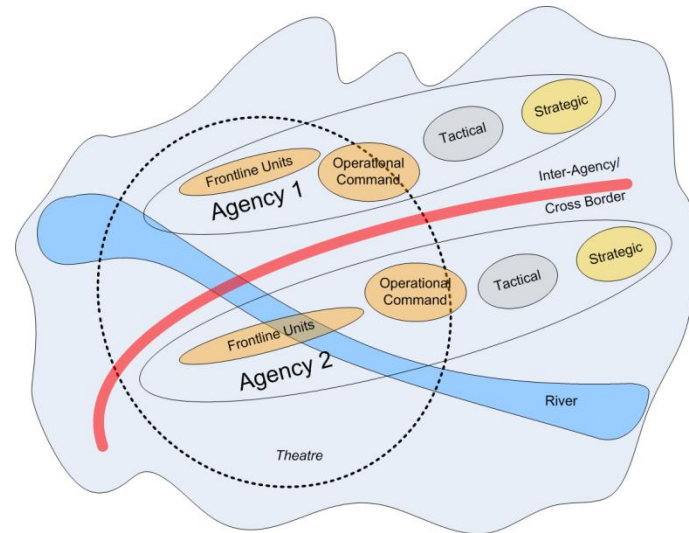**International Border**

Project Approach
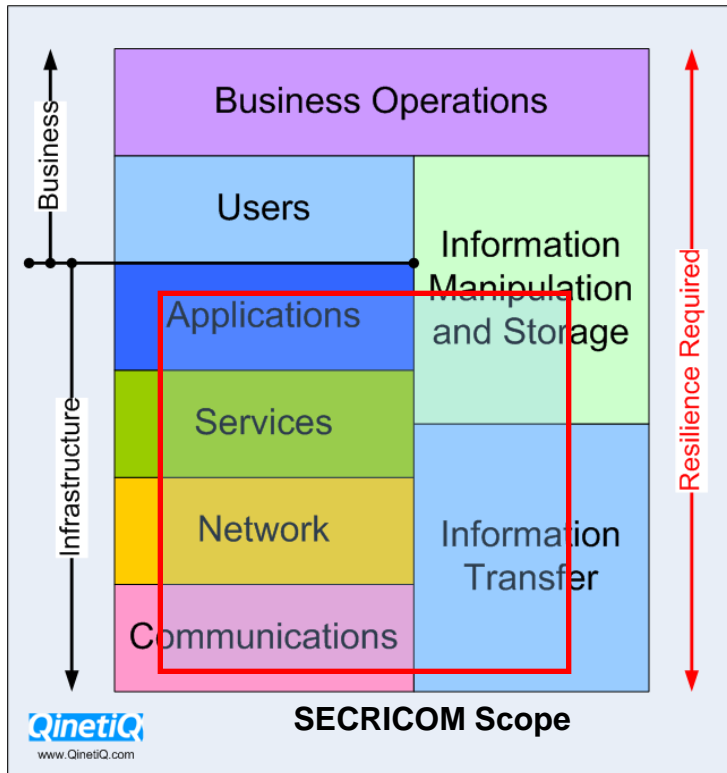
Chain of Command (C2) in Demonstration

Overlaid Chain of Command

Strategic Command

Inter-Agency/ Cross Border

Tactical/ Coordination Command

Operational Command

Operation

Agency No1

Agency No2

Agency No1

Agency No2

Frontline Units

Frontline Units

Out of Theatre

Adjacent Theatre

In Theatre

Provided by Internet over SatComms

Provided by Emulated Bearers

Provided by WiFi
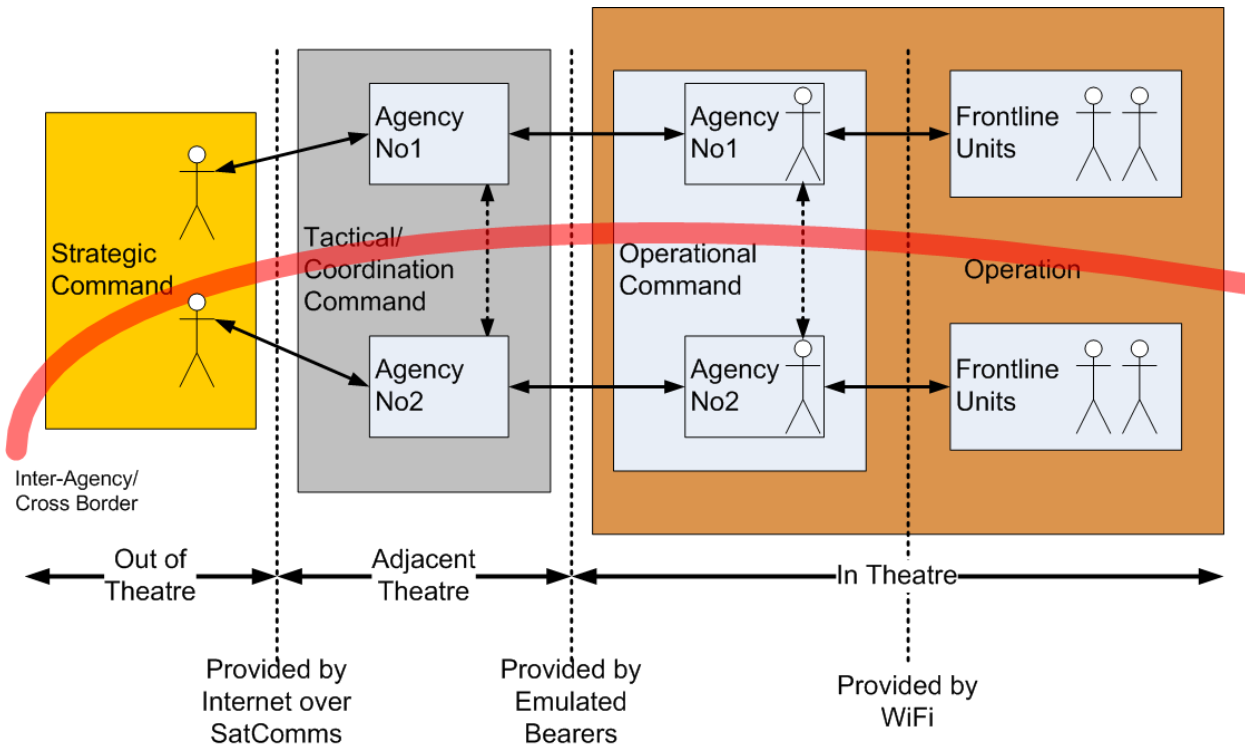
Critical Communications Infrastructure

Layers of Resilience — Business Operations, Users, Applications, Services, Network, Communications; Information Manipulation and Storage; Information Transfer; Resilience Required; SECRICOM Scope; QinetiQ, www.QinetiQ.com

Critical communications require *resilience* to support business continuity during critical and non-critical business operations:

– Robustness during stressed periods and in stressed environments;

– Robustness against equipment failures; and

– Graceful degradation: by <u>design</u> <u>and</u> <u>not</u> <u>luck</u>..!

Behind Every Resilient IT-Reliant Business is Resilient Data Networks/Communications

Ubiquitous Services to Support End User

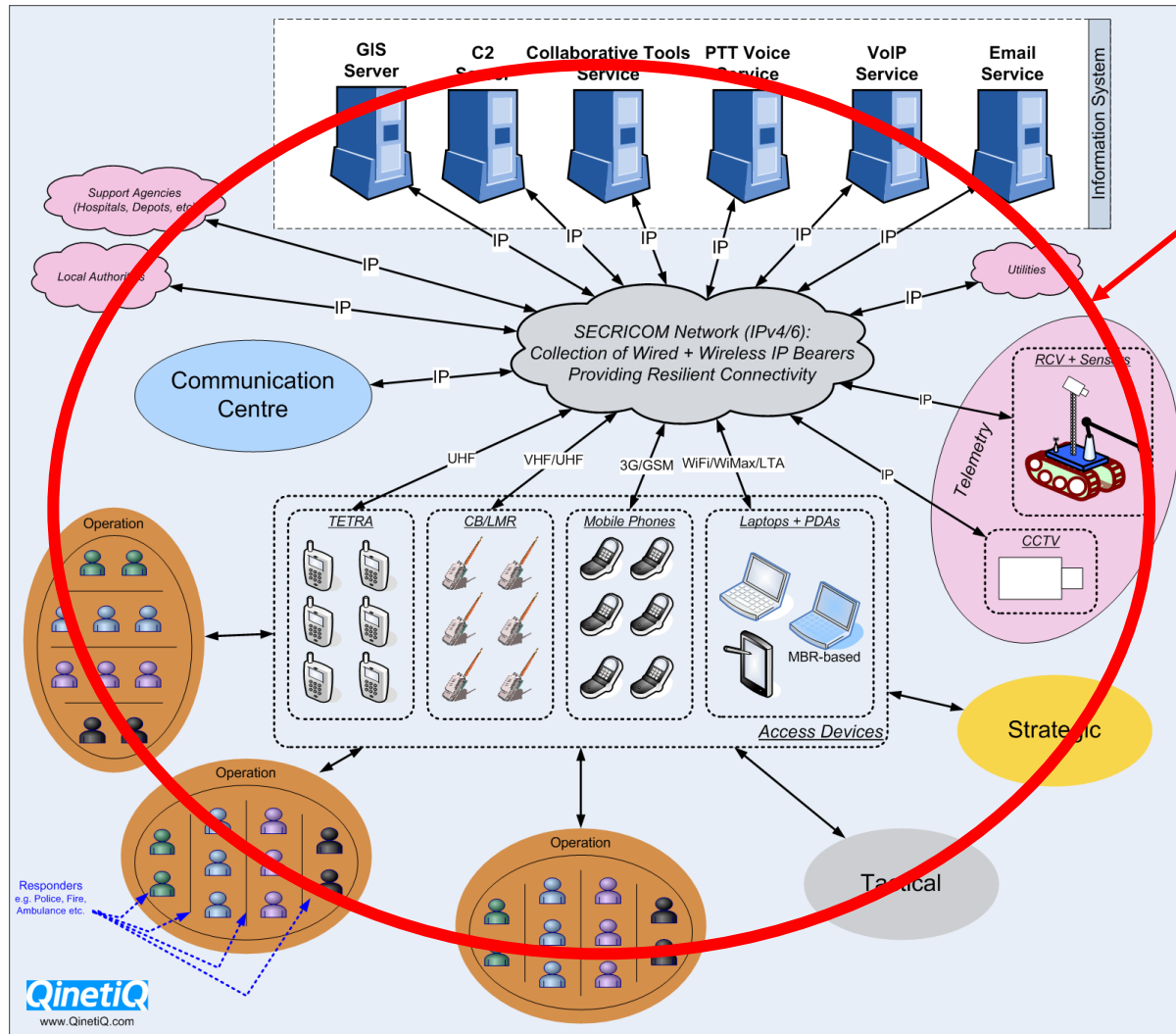Avoidance of reliance on a single comms system or provider

– Make simultaneous use of TETRA, 3G, GSM, WiFi, WiMax, Satellite, SDR, etc
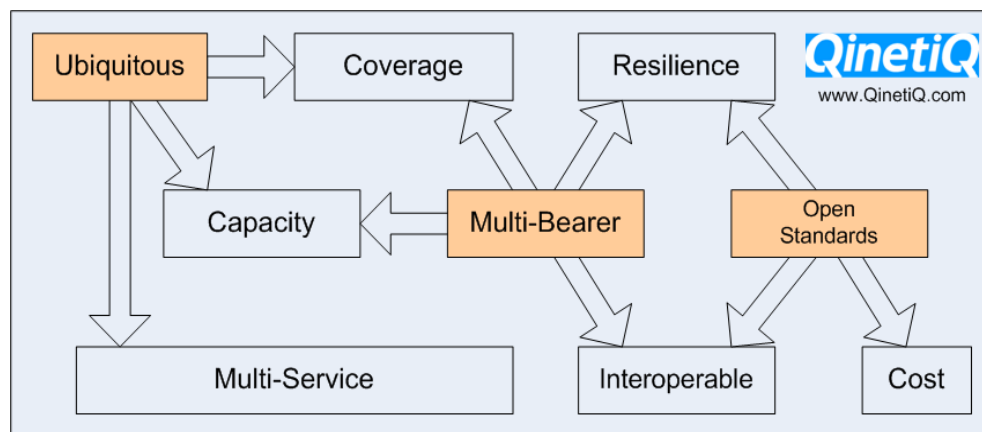
Usage of open/non-proprietary standards

– Network: IPv6 as the principle standard for networking

– Wireless: 3G, GSM, WiFi, WiMax, TETRA, Satellite, etc

– Fixed: Ethernet

SECRICOM Technical Plan

MBR

Multiple Bearer Router

Research leader: **QinetiQ**

Ahmed Aldabbagh, QinetiQ (Principal Engineer)

Introduction to the MBR

The MBR

- An intelligent adaptive routing device;
- Enables seamless inter-networking in a multi-bearer, multi-node, mobile environment;
- Enables a flexible, affordable and scaleable network solution; and
- Designed to optimise network performance wherever users operate in environments where connectivity is poor.

MBR Benefits + Features

| Benefits	Features
Low Cost	• Exploits existing investment in network infrastructure; • Operated by non-skilled user – "configure-and-leave-alone";
High Speed	• Changes operation policies in accordance with business needs; • Exploits whatever bandwidth is available in support of business;
High Availability	• Opportunistic use of bearers maximises availability; • Makes best use of all available bandwidth; • Detects and automatically responds to network changes;
Ease of Use	• Requires minimum configuration post-installation; • Delivers benefits without operator intervention;
Flexibility to Expand	• Supports a large range of government and civil bearers; • Simplifies process to add support for new bearers; and • Interoperable with COTS IP routing solutions.

SEVENTH FRAMEWORK PROGRAMME

SECRICOM MBR for Communication Resilience
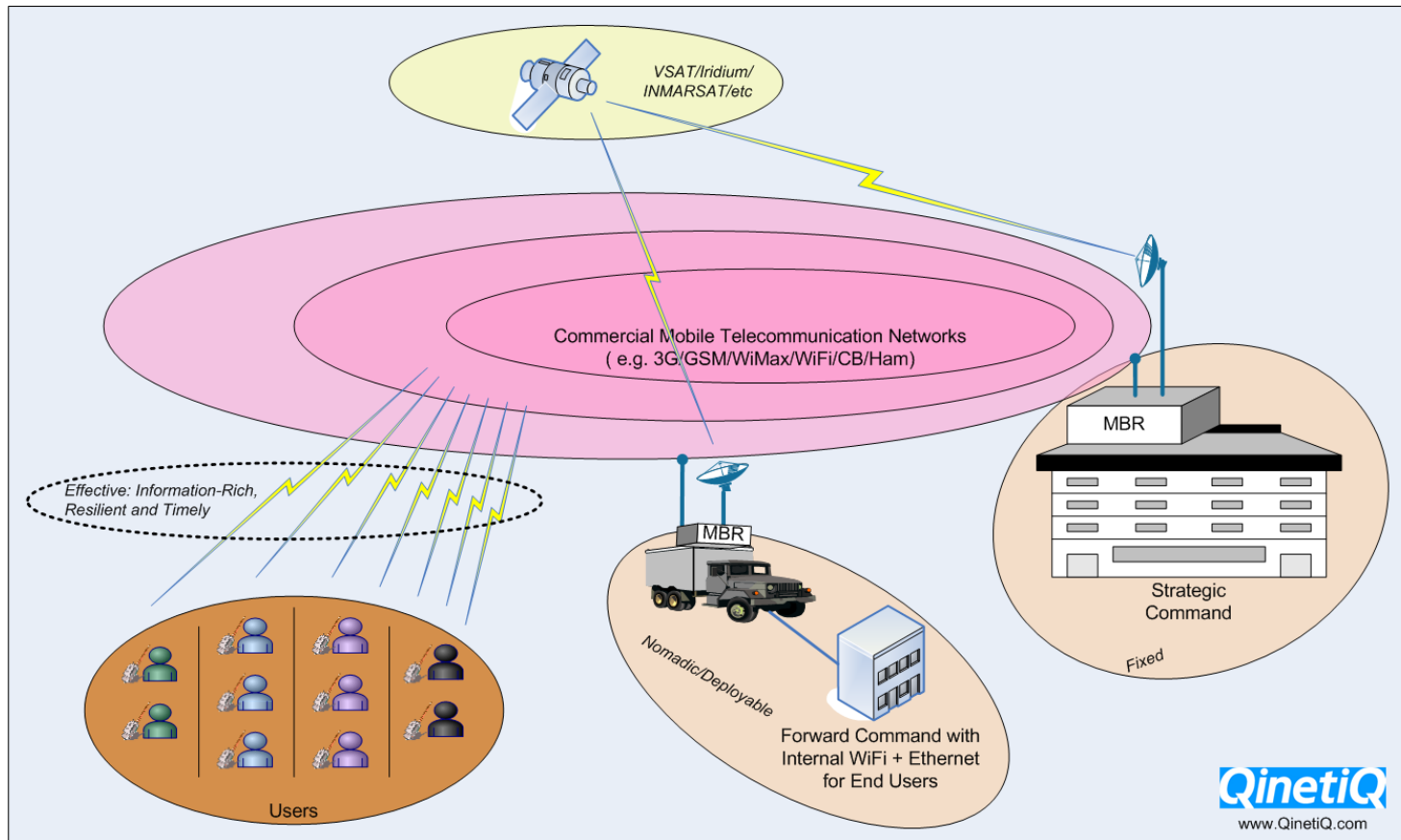
Secure PTT

Secure Seamless Wireless Communication

Tomas Kucharik
Chairman and CEO
tomas.kucharik@ardaco.com

ARDACO

Main Objectives for Secure PTT

★ Provide feature rich and affordable system

   ★ Opposite to private, closed and expensive systems

   ★ Based on latest standards

★ Reuse already made investments into the infrastructure

   ★ Do not throw away anything existing

   ★ Make it hw vendor independent

★ Integrate with existing systems

   ★ Tetra, Satellite, GSM, Military, Police, … networks

★ Security as integral part not an afterthought

   ★ Security according to the NATO required standards

User Requirements for Secure PTT

★ Reliability, Back up (why not just GSM, why not just Tetra, why combination of networks is important)

★ Secure Confidentiality for certain Groups

★ Provide Audit Trail (demand for logged inn communication, 7 years record, ….)

★ Intuitive to users, easily manageable, immediate response

  ★ Easy and immediate creation/removal of communication groups (sometimes policeman should not talk to the other policeman without Control & Command Room knowing it)

User Requirements for Secure PTT

★ Seamless, Interoperable, Inter Agency, Inter Country

  ★ No interruption in communication

  ★ Connect all – Control & Command Room, Police, Military, Navy, Fire Brigade, Hospitals, Ambulances, City Council, Health and Safety, Utilities, Press, Media, ..

★ Integrity, Confirmation of information delivery, Knowing status of users

  ★ Showing the status - reachable, do not disturb, …

★ Speed, Timeliness for information delivery

  ★ For some information time is critical

 ★ Some information might be delivered within few seconds or minutes

Secure PTT Smart functions 1

★ Voice communication in different modes (one-to-many, one-to-one)

   ★ All, including persons selections, with a press of single button on standard mobile phones

★ Operator easily and intuitively managing contact lists and communication groups through Multi Touch Screen Operator Studio

★ Showing User Presence/activity status information (present, out of reach, ….)

★ Taking and Sending pictures, hand-drawings or photos
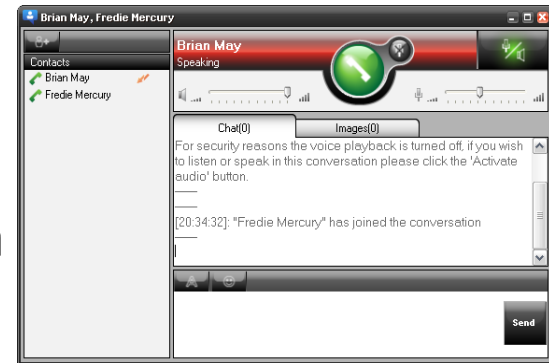
Secure PTT Smart functions 2

★ User location information and mapping (GPS), with user defined time updates and "emergency button"

★ Instant Text Messaging with immediate information delivery

★ Smart Text Messaging (for long messages including delivery and read receipts)

★ Integration with radios and other CS

★ Coverage, guarantied coverage on whole Globe (no white spots any more)

★ For all transferred information secured confidentiality
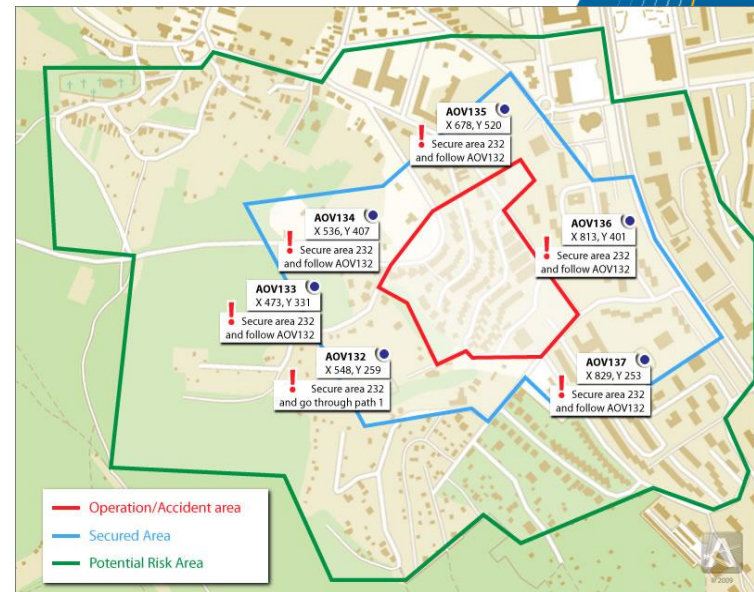
For whom is Secure PTT

★ Control & Command Room, Police, Military, Navy, Fire Brigade, Hospitals, Ambulances, City Council, Health and Safety, Utilities, Press, Media, ..

  ★ Different levels of Decision Makers and Commanders, Government representatives, Mayors and other civilian officials, Communication operators, Experts from all over the world

  ★ Red Cross, Sanitary operations, Voluntaries, ….

★ Situation today – accident in one country, chemical analysis in other country and health analysis with expertise in other country

Why using also Standard Mobile Phones

★ The best available technology

  ★ Only up to '70s it was military leading the communication

  ★ Billions of investment into consumer R&D (size factor, battery life)

★ In today's phones all is integrated

  ★ GPS, Video, Camera, Text, Forms, …

★ Service, Maintenance and Training costs are fraction of the cost of private communication systems

  ★ Network build up and maintenance, phones service and maintenance, training of administrators and users

★ You make users happy
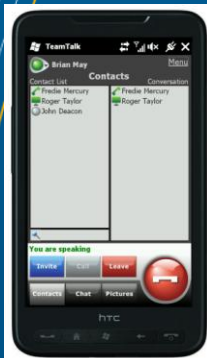
Today and Future Communication Systems

★ Civil, Military, Police, Health, Government and all other sectors working together

★ Communication system must be able to connect all

★ Must work anywhere in the world

★ Must be reliable and secure

★ Affordable for low budget institutions

★ Scalable - could be stand alone for small operations or easily integrated for large organizations and operations

★ The users can use the equipment they are used to

★ Easy to use and user friendly

★ There is not such a thing as "The one communication system for the future"

The main objective of any crises management operation is to preserve lives, health and assets.

Timely reliable communication securing confidentiality is one of key components of the crises management operation.

Secure PTT and MBR are made to help you to achieve these objectives. Please visit us in our stand.

Tomas Kucharik
Chairman and CEO
tomas.kucharik@ardaco.com

ARDACO