SECRICOM

Seamless Communication for Crisis Management

Presentation to BAPCO Conference 2009, London
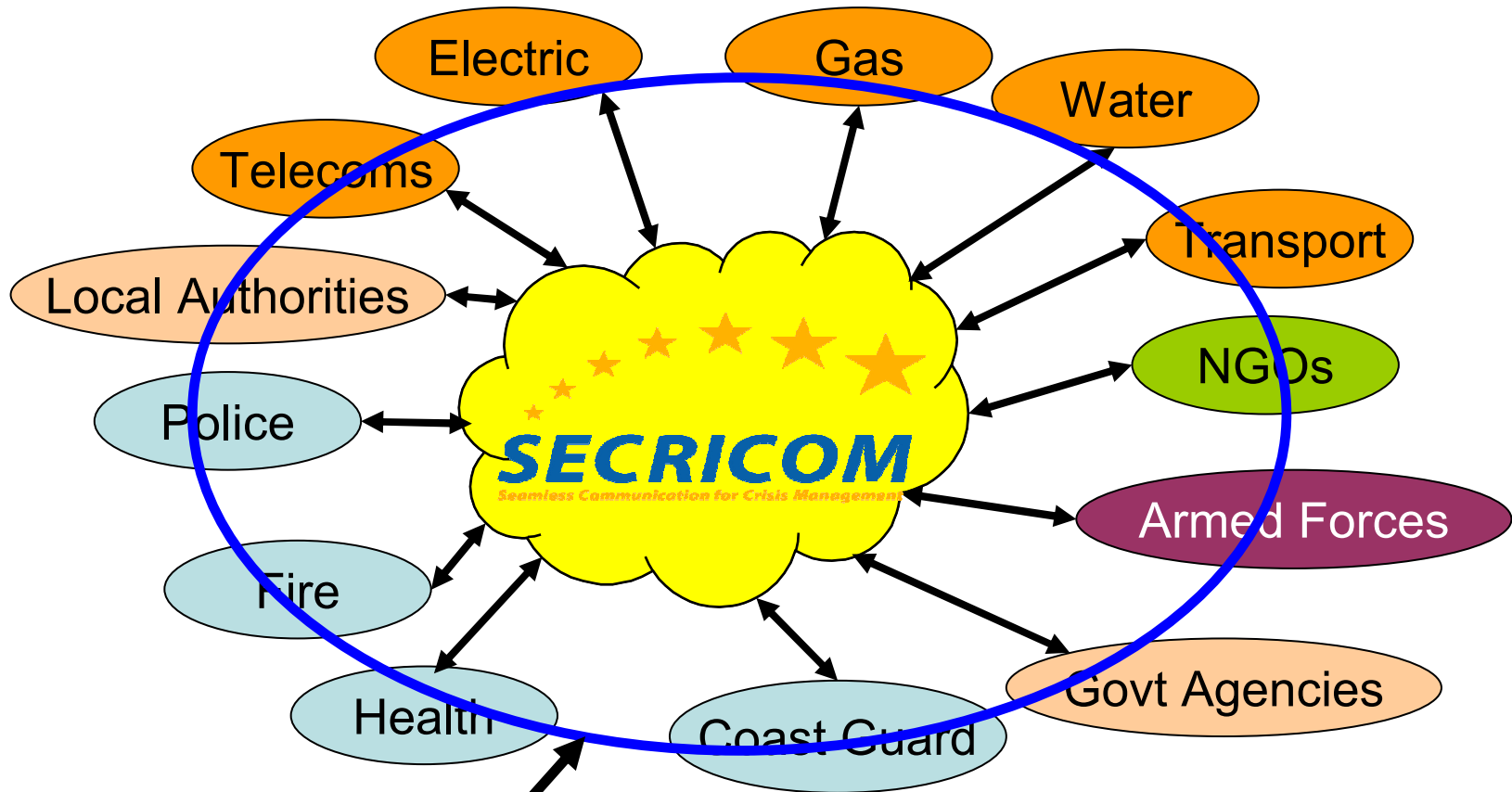
Dr Ahmed Aldabbagh and Rich Edwards

21/4/2009

SEVENTH FRAMEWORK
PROGRAMME

Presentation objectives

- Outline Stakeholder requirements

- Introduce the project
  - Define SECRICOM
  - Vision
  - Programme & Partners

- Introduce the approach taken

- Give examples of architectures and technology

Introduction

Business Stakeholders
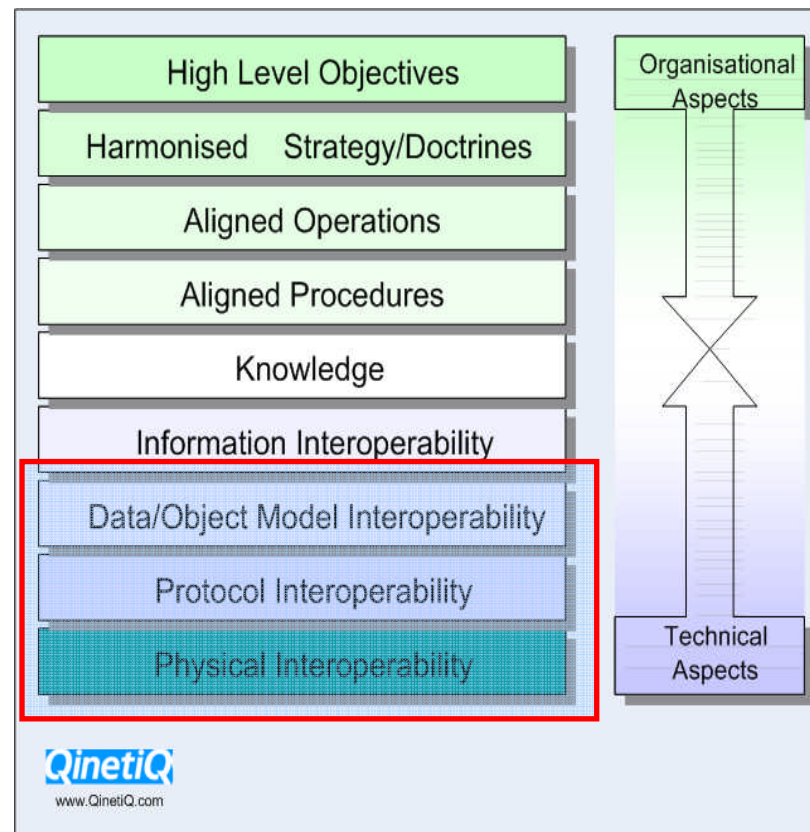

International Border
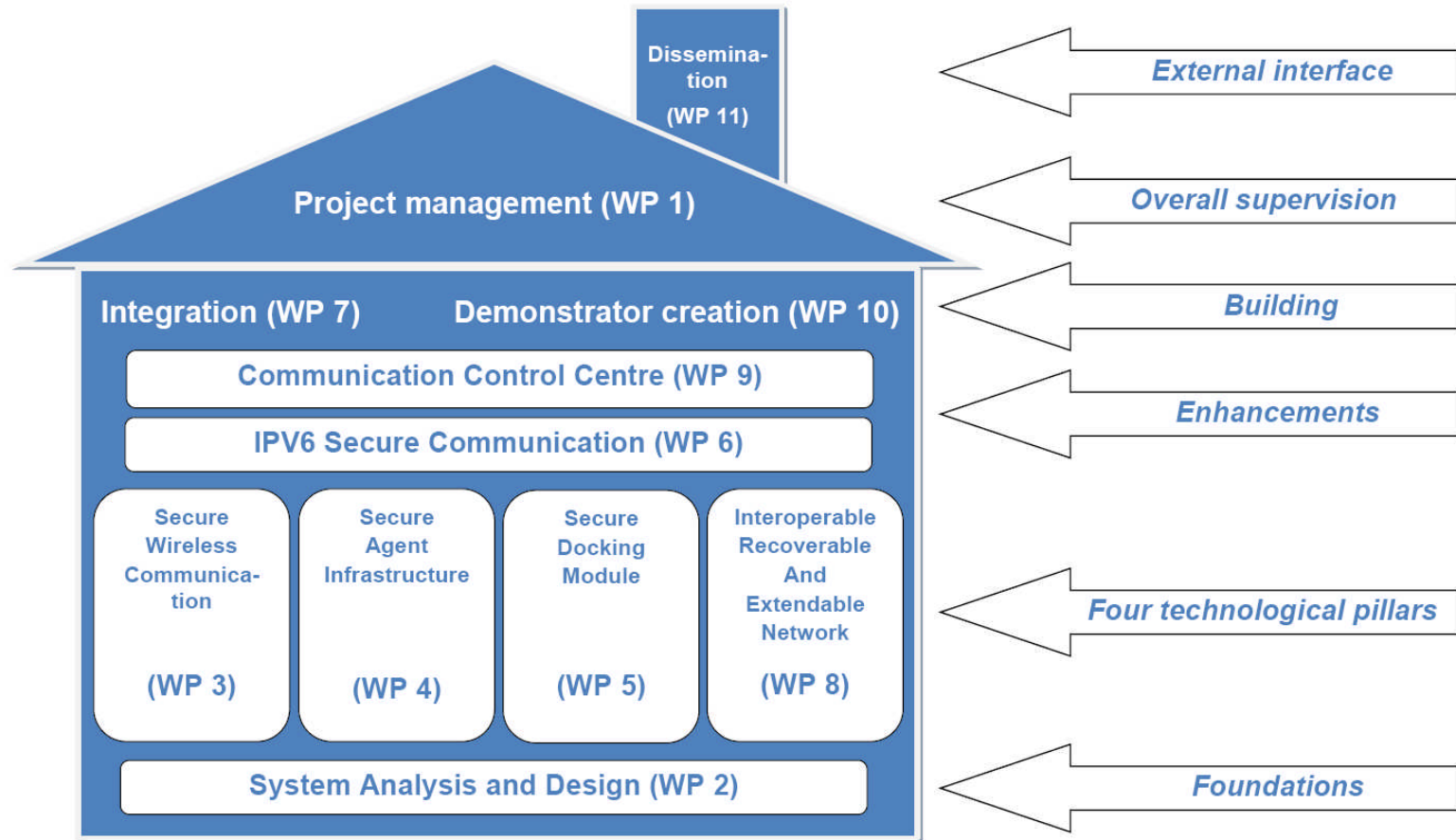
Interoperability

Definition:

The capability of two or more organisations or discrete parts of the same organisation to exchange decision-critical information and to use the information that has been exchanged.

Clearly, interoperability ranges from organisational to technical aspects all of which must be 'harmonised' in order to achieve full interoperability.

Layers of Interoperability

- High Level Objectives
- Harmonised Strategy/Doctrines
- Aligned Operations
- Aligned Procedures
- Knowledge
- Information Interoperability
- Data/Object Model Interoperability
- Protocol Interoperability
- Physical Interoperability

Organisational Aspects

Technical Aspects

QinetiQ
www.QinetiQ.com

Project Overview

Consortium

Manufacturers & NGO

Research & SMEs

**Universities**

SEVENTH FRAMEWORK PROGRAMME

Vision / Aims

- Ability for responders to operate across different European emergency services/responder agencies as one cohesive unit at the time of crisis

- Exploit the existing communications systems
- Enhance interoperability
- Enhance interconnectivity
- Reduce the disadvantages faced by users of Existing Systems

Approach
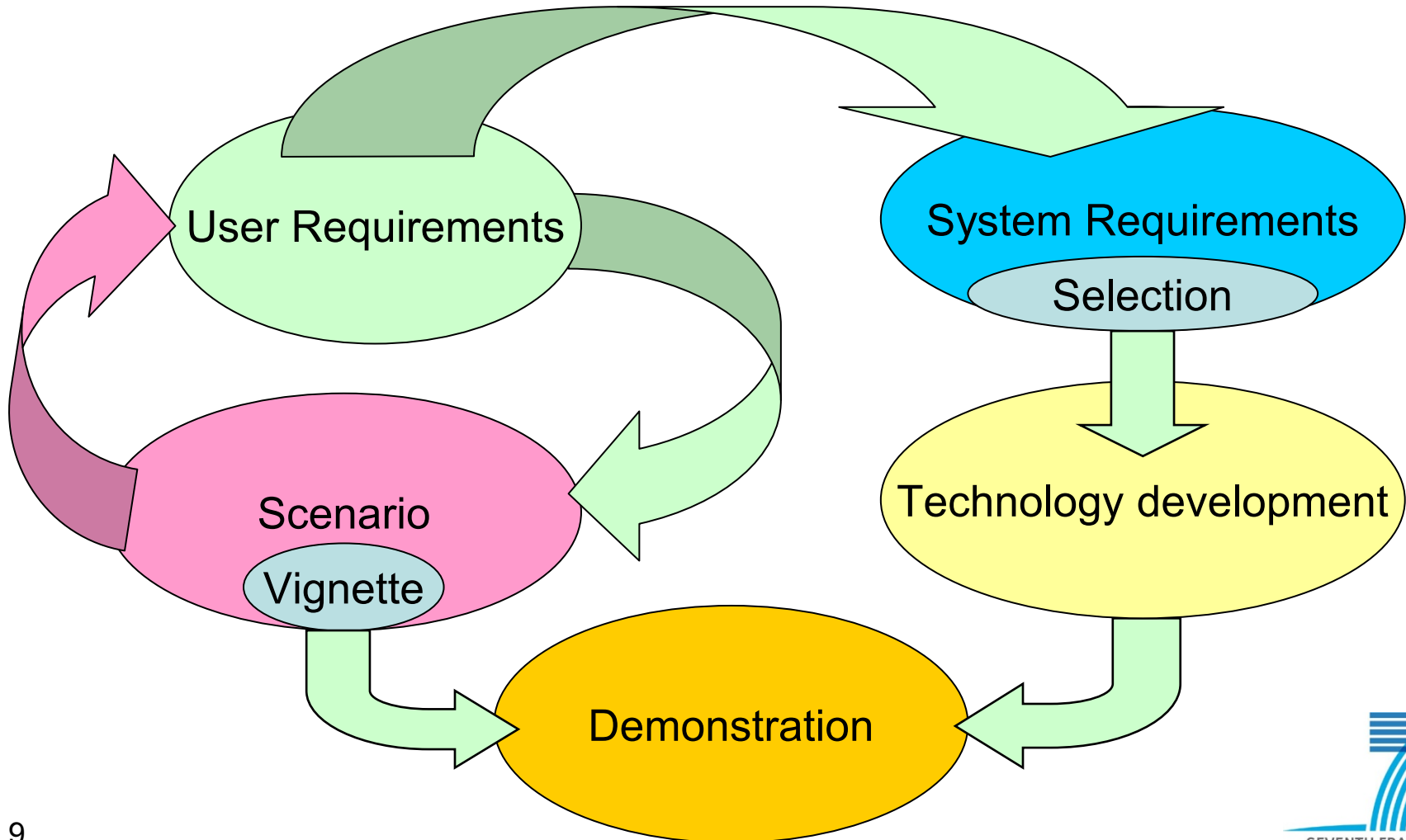
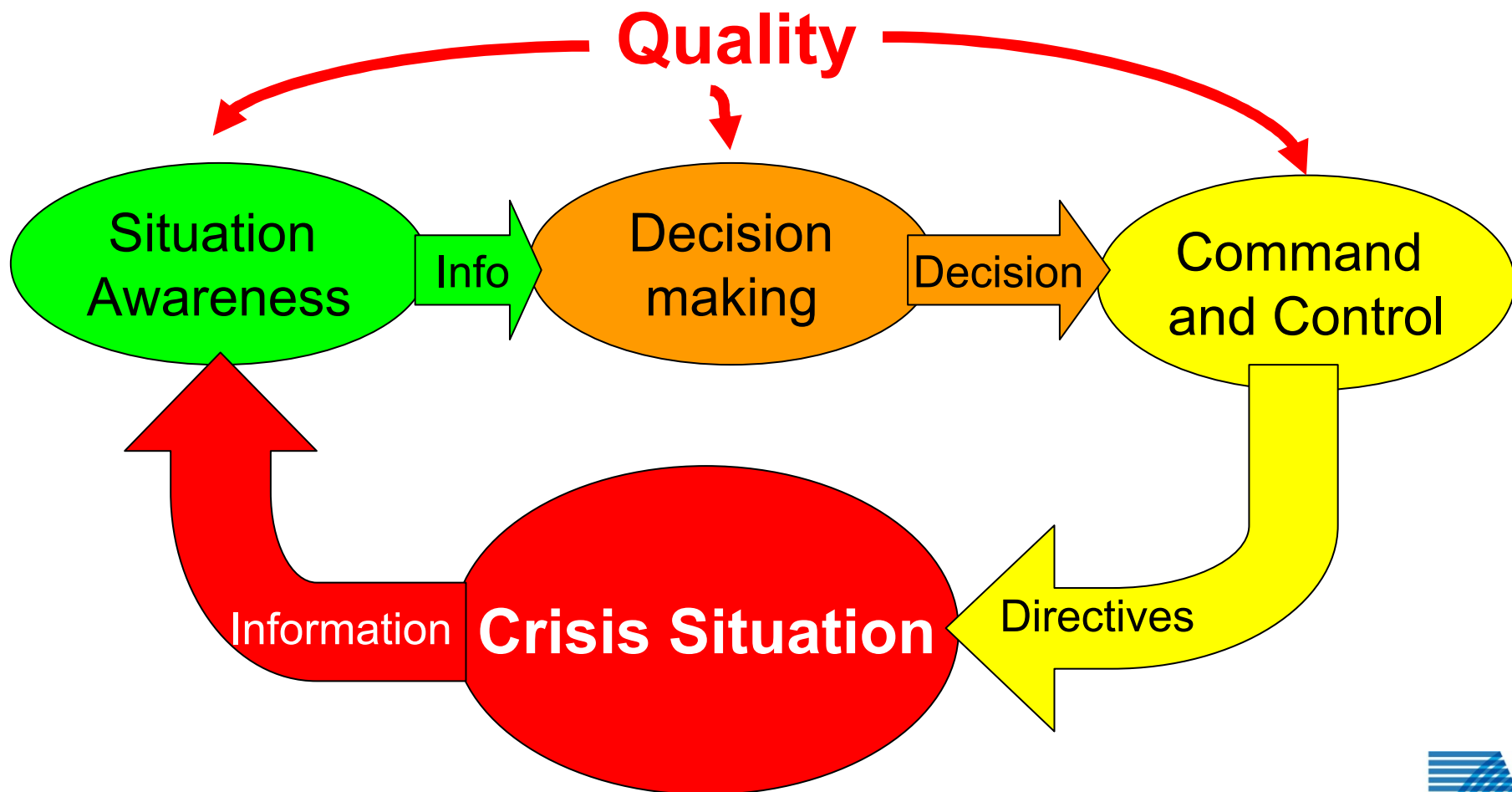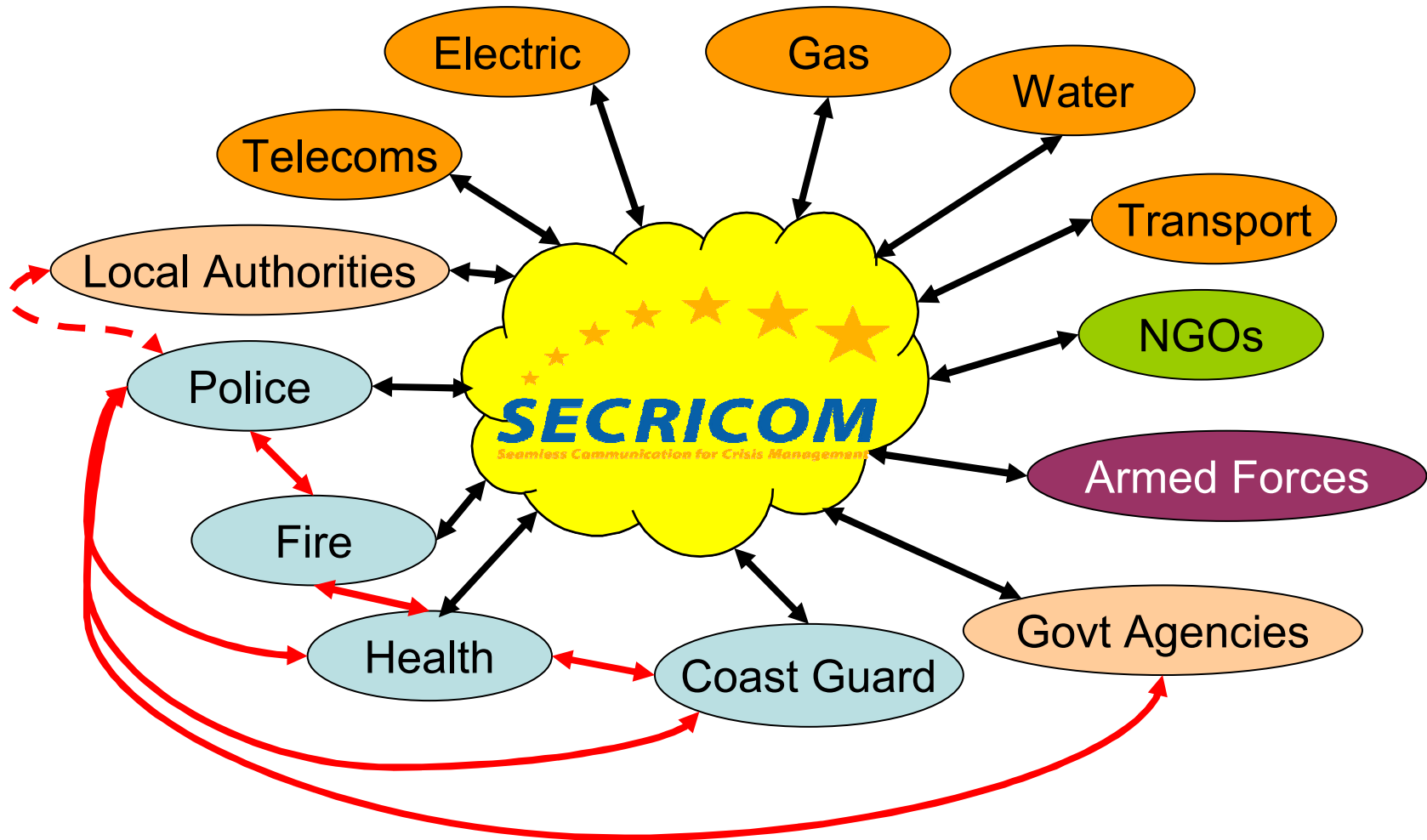# User Requirements

- Enable the user to clearly understand their objectives and/or command directives

- Expressed in terms of **what** the user wants to achieve

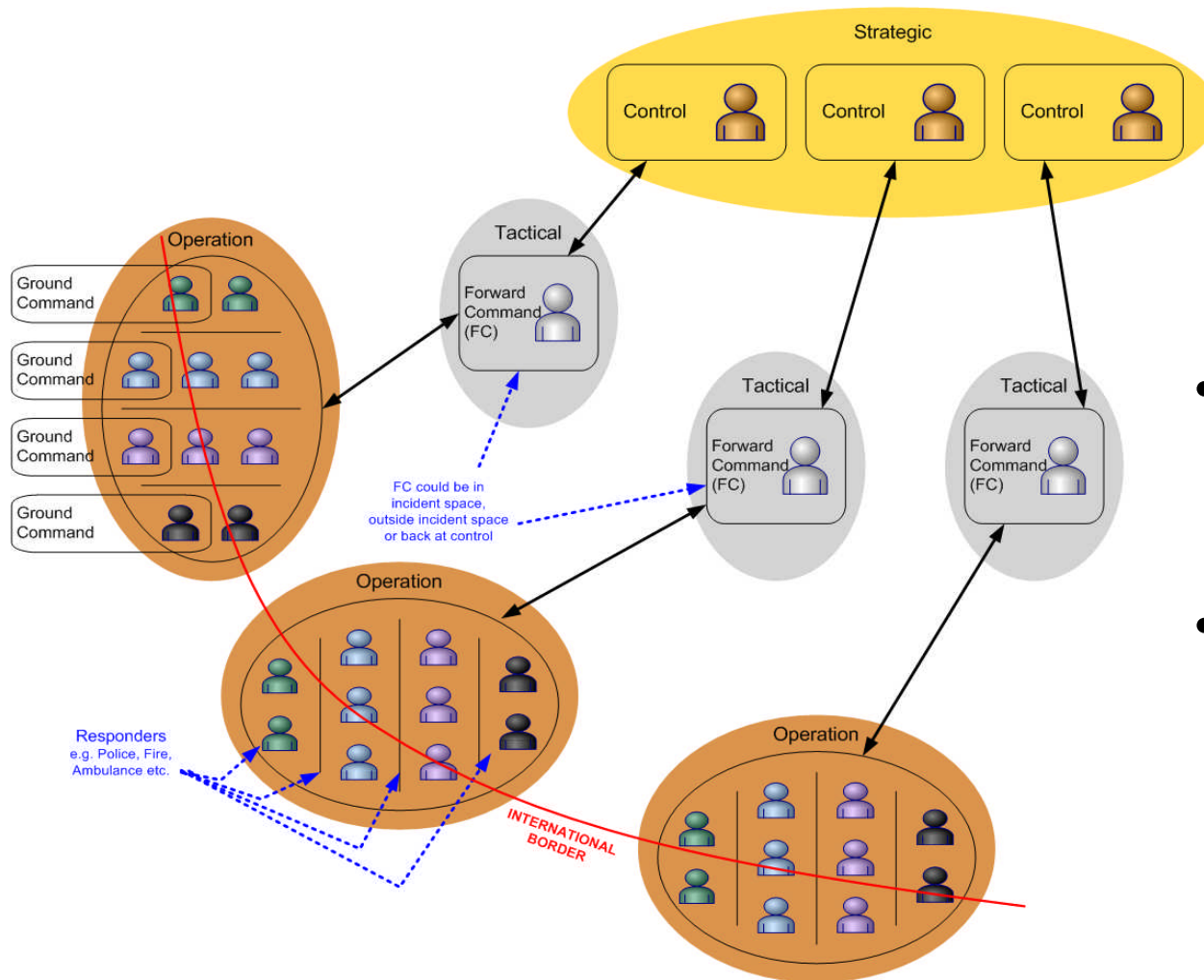- Discourages users from being seduced by technology

Principle of Crisis Management
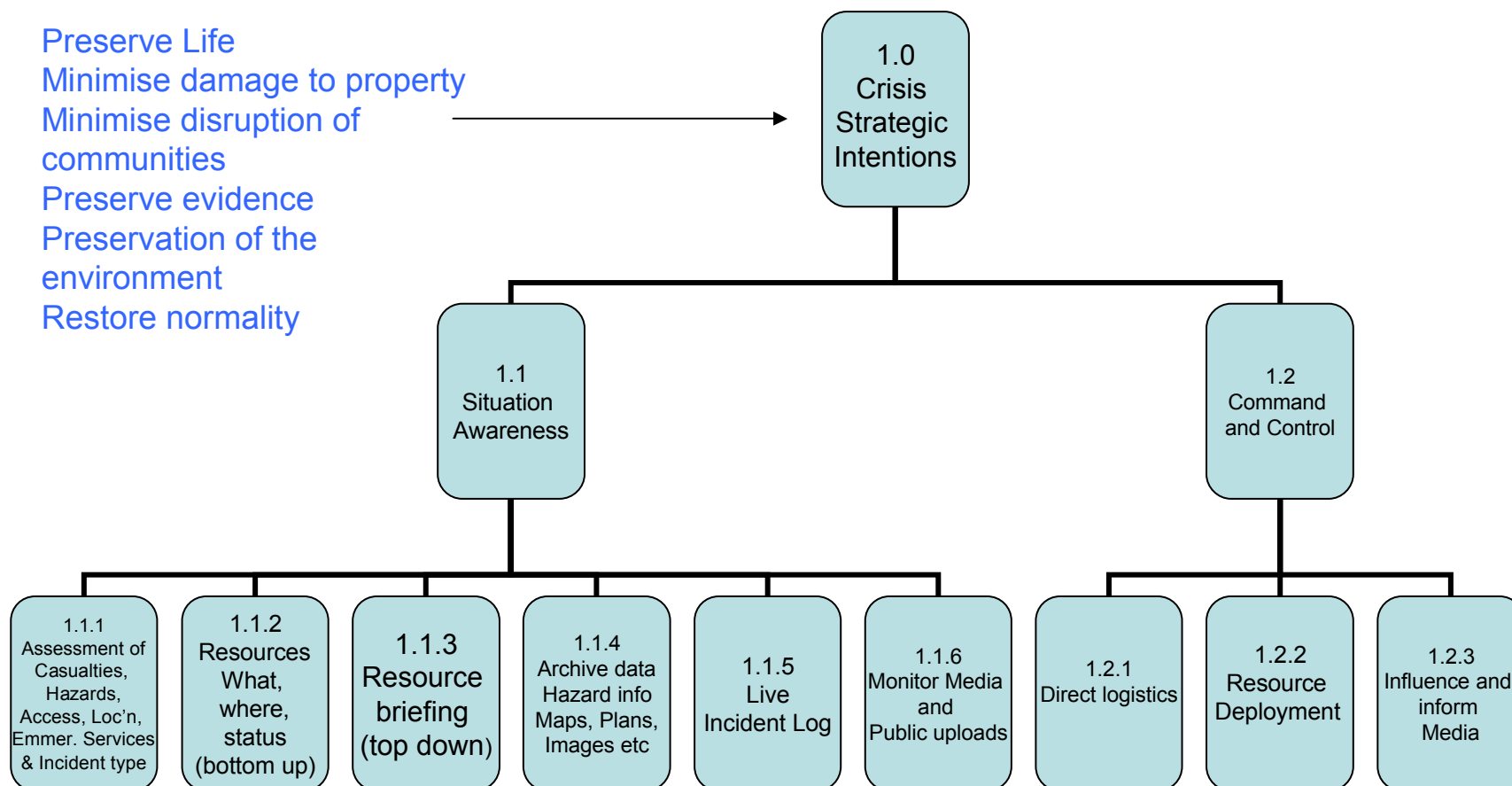
Typical Information Exchange

Typical C2 for the Emergency Services

- Extends across international borders
- Extends across different agencies

High Level User Requirements

Preserve Life
Minimise damage to property
Minimise disruption of communities
Preserve evidence
Preservation of the environment
Restore normality

```
                          ┌──────────────┐
                          │     1.0      │
                          │    Crisis    │
                          │  Strategic   │
                          │  Intentions  │
                          └──────────────┘
              ┌──────────────────┴──────────────────┐
      ┌──────────────┐                        ┌──────────────┐
      │     1.1      │                        │     1.2      │
      │  Situation   │                        │   Command    │
      │  Awareness   │                        │ and Control  │
      └──────────────┘                        └──────────────┘
```

| 1.1.1 Assessment of Casualties, Hazards, Access, Loc'n, Emmer. Services & Incident type | 1.1.2 Resources What, where, status (bottom up) | 1.1.3 Resource briefing (top down) | 1.1.4 Archive data Hazard info Maps, Plans, Images etc | 1.1.5 Live Incident Log | 1.1.6 Monitor Media and Public uploads | 1.2.1 Direct logistics | 1.2.2 Resource Deployment | 1.2.3 Influence and inform Media |

Core Functions


```
                          2.0
                        Perform
                      Core System
                       functions

2.1         2.2         2.3         2.4         2.5         2.6         2.7         2.8
Provide     Secure      Seamless    Maintain    Quality of  No impact   Resilient   Provide
Audit trail (Confiden-  Interoper-  Integrity   service     on          (Avail-     Risk Flags
            tiality)    ability –   of message  (Timeli-    operations  ability)
                        Intra                   ness)
                        Agency,
                        Inter
                        Agency &
                        Inter State

2.1.1                                                       2.5.1       2.5.2
Provide                                                     Intuitive   No
Decision log                                                to users    requirement
                                                                        to
                                                                        configure
                                                                        In the field
```

Capability Gaps - illustrative

SECRICOM added value

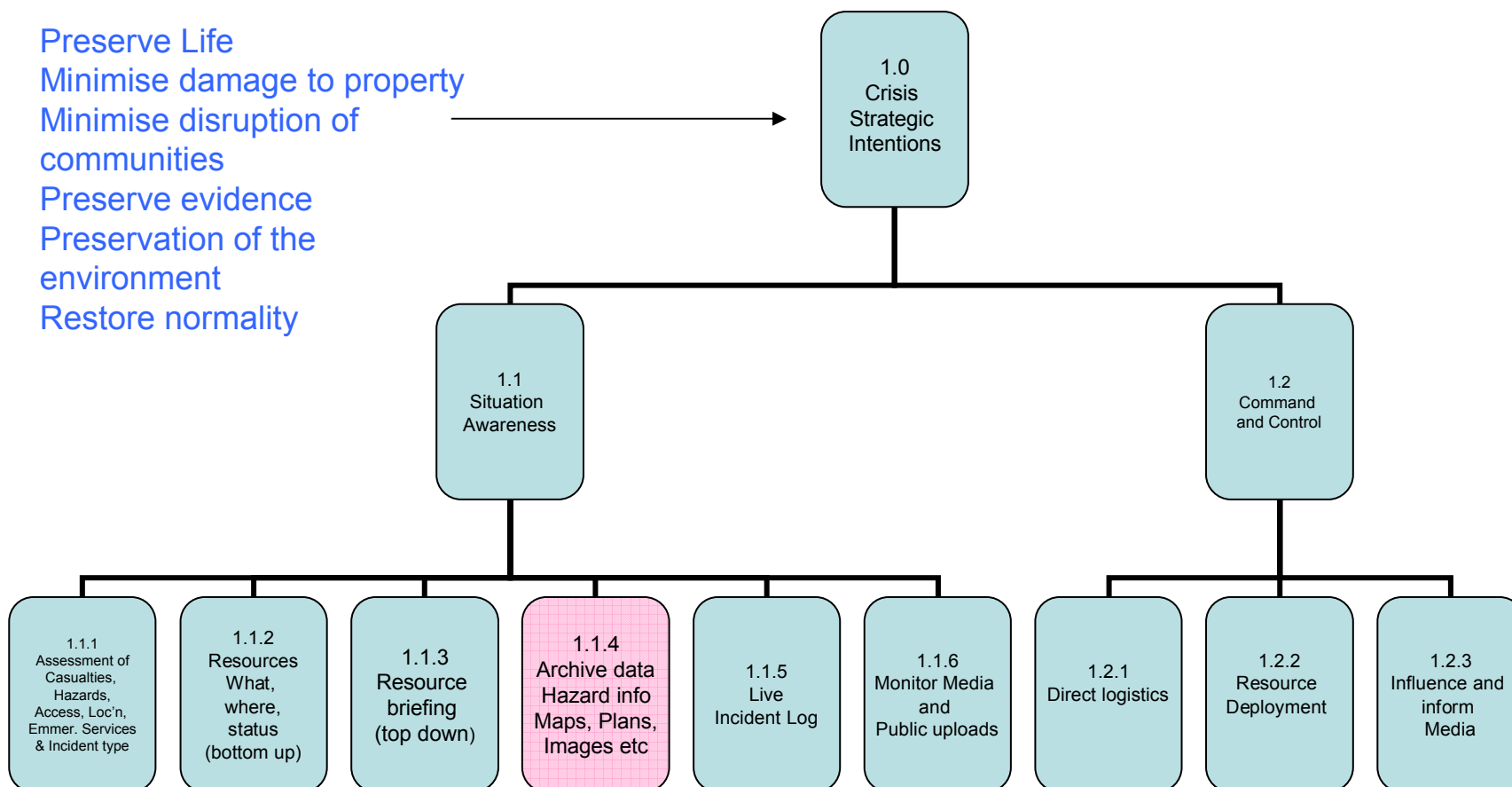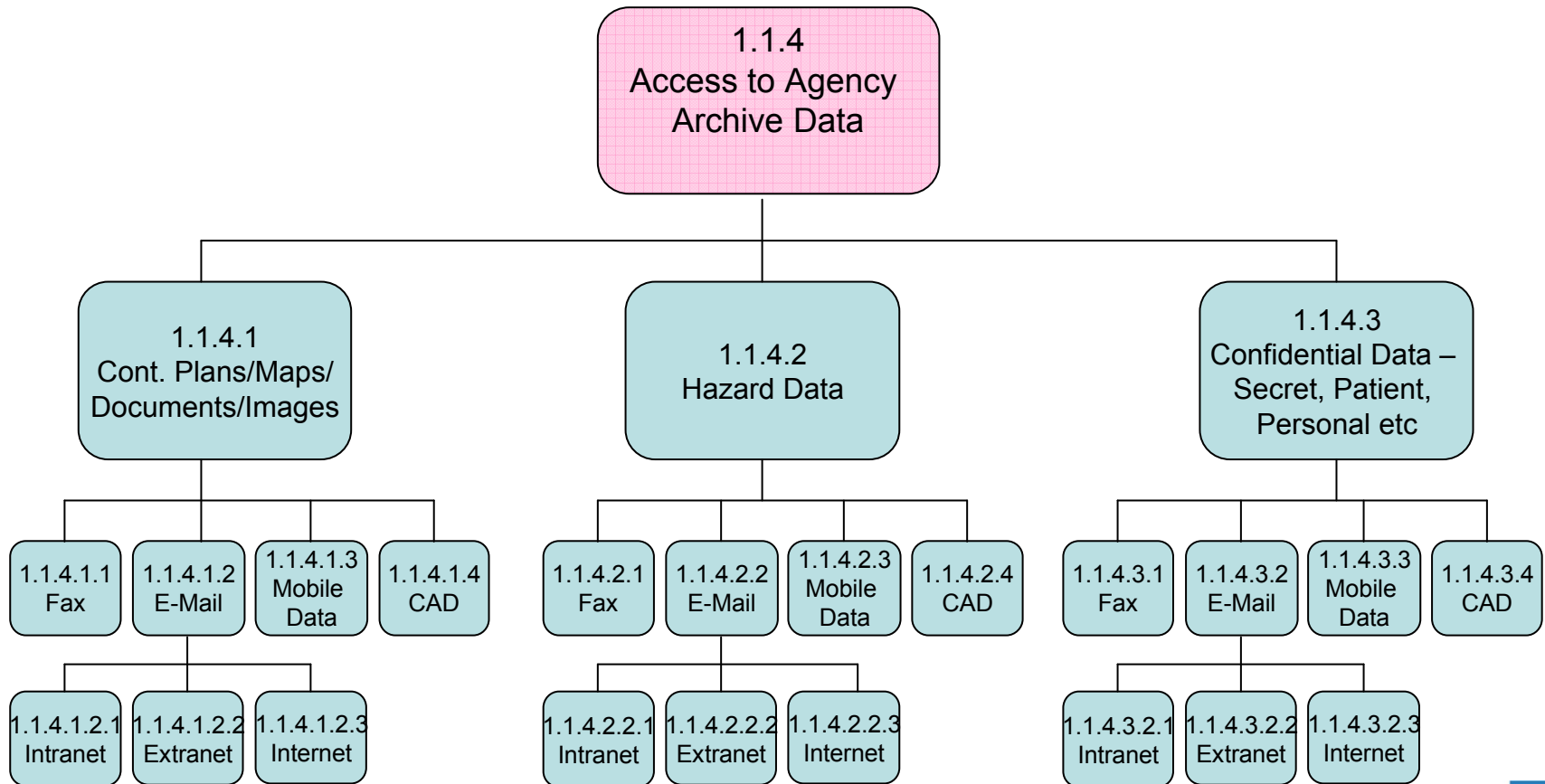|	
Scope of User Requirements	Security
	Resilience
	Seamless Interoperability
User Requirements met by Existing Infrastructure / Systems	Audit trail
	Real time inventory tracking
	Rapid deployment
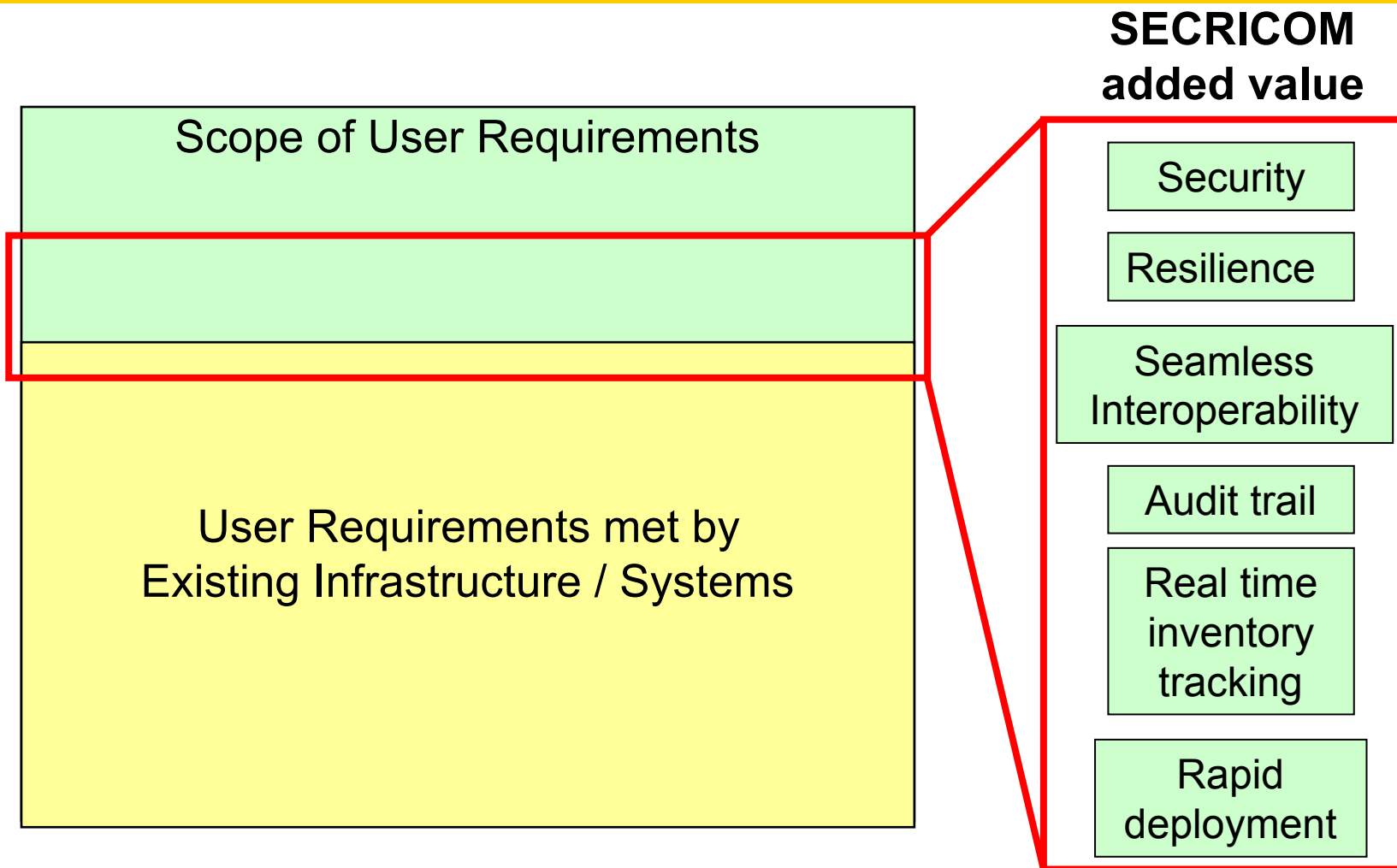
System Requirements

- Derived from the user requirements

- Concerned with the minimum required functionality necessary to meet the user requirement

- Expressed in an appropriate fashion, e.g. tree and/or architecture diagrams

- Must take existing systems into account
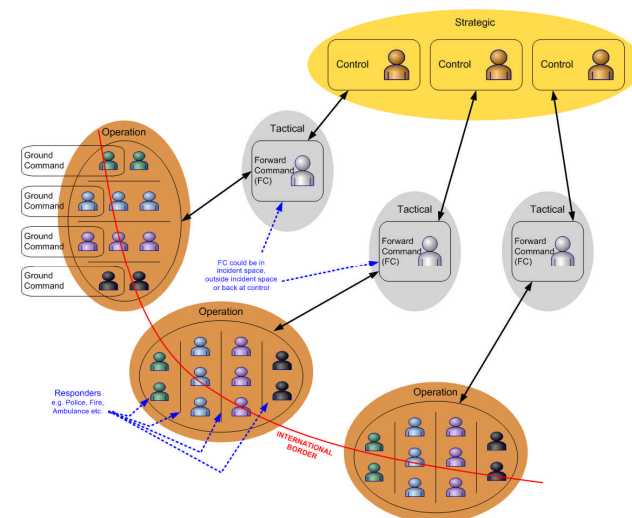
Example of Procedure

Preserve Life
Minimise damage to property
Minimise disruption of communities
Preserve evidence
Preservation of the environment
Restore normality

1.0
Crisis Strategic Intentions

1.1
Situation Awareness

1.2
Command and Control

1.1.1
Assessment of Casualties, Hazards, Access, Loc'n, Emmer. Services & Incident type

1.1.2
Resources What, where, status (bottom up)

1.1.3
Resource briefing (top down)

1.1.4
Archive data Hazard info Maps, Plans, Images etc

1.1.5
Live Incident Log

1.1.6
Monitor Media and Public uploads

1.2.1
Direct logistics

1.2.2
Resource Deployment

1.2.3
Influence and inform Media

Derivation of System Requirements

```
                        ┌─────────────────────┐
                        │        1.1.4        │
                        │  Access to Agency   │
                        │    Archive Data     │
                        └─────────────────────┘
```

1.1.4 Access to Agency Archive Data

1.1.4.1 Cont. Plans/Maps/Documents/Images

1.1.4.2 Hazard Data

1.1.4.3 Confidential Data – Secret, Patient, Personal etc

1.1.4.1.1 Fax
1.1.4.1.2 E-Mail
1.1.4.1.3 Mobile Data
1.1.4.1.4 CAD

1.1.4.2.1 Fax
1.1.4.2.2 E-Mail
1.1.4.2.3 Mobile Data
1.1.4.2.4 CAD

1.1.4.3.1 Fax
1.1.4.3.2 E-Mail
1.1.4.3.3 Mobile Data
1.1.4.3.4 CAD

1.1.4.1.2.1 Intranet
1.1.4.1.2.2 Extranet
1.1.4.1.2.3 Internet

1.1.4.2.2.1 Intranet
1.1.4.2.2.2 Extranet
1.1.4.2.2.3 Internet

1.1.4.3.2.1 Intranet
1.1.4.3.2.2 Extranet
1.1.4.3.2.3 Internet

System Architecture and Solution Technologies

Clear Need for Communications that can be relied upon, that is both *Ubiquitous and Interoperable*

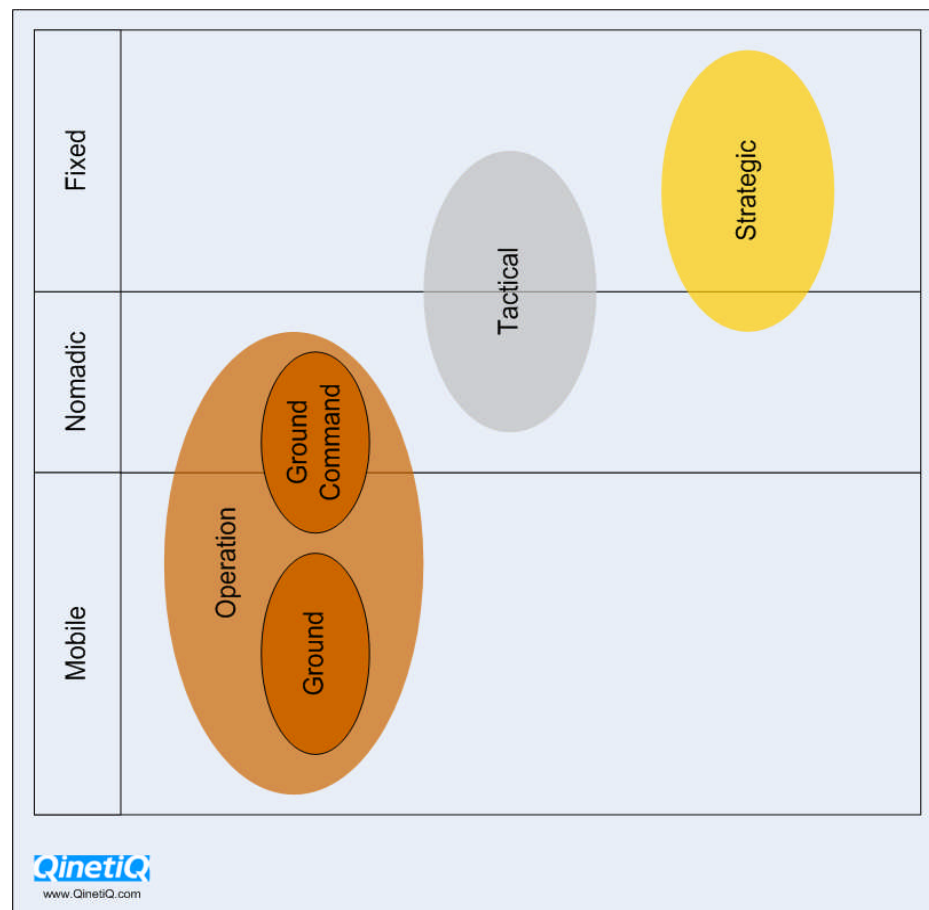# Communications System Architecture

- <u>Ubiquitous</u> communications requires usage of as many communications, and avoidance of reliance on a single system

  - Make simultaneous use of 3G, GSM, WiFi, WiMax, Satellite, SDR, etc

  - Aim for seamless switch over with minimal impact to user/business

- <u>Interoperable</u> communications requires usage of open/non-proprietary standards for system, hardware and software

  - Network: IPv6 as the principle standard for networking: future-proof

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

  - Fixed: Ethernet

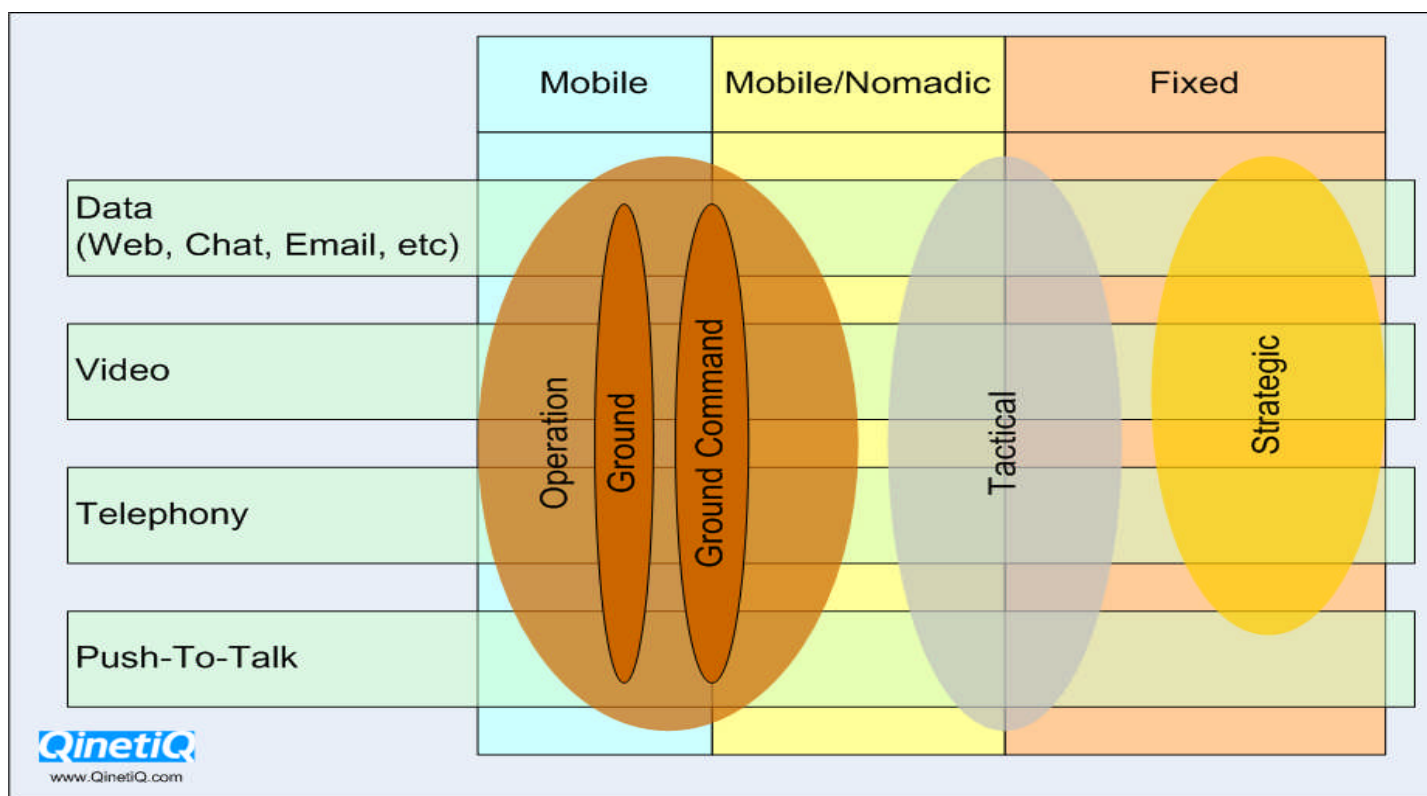# Communications System Features for SECRICOM
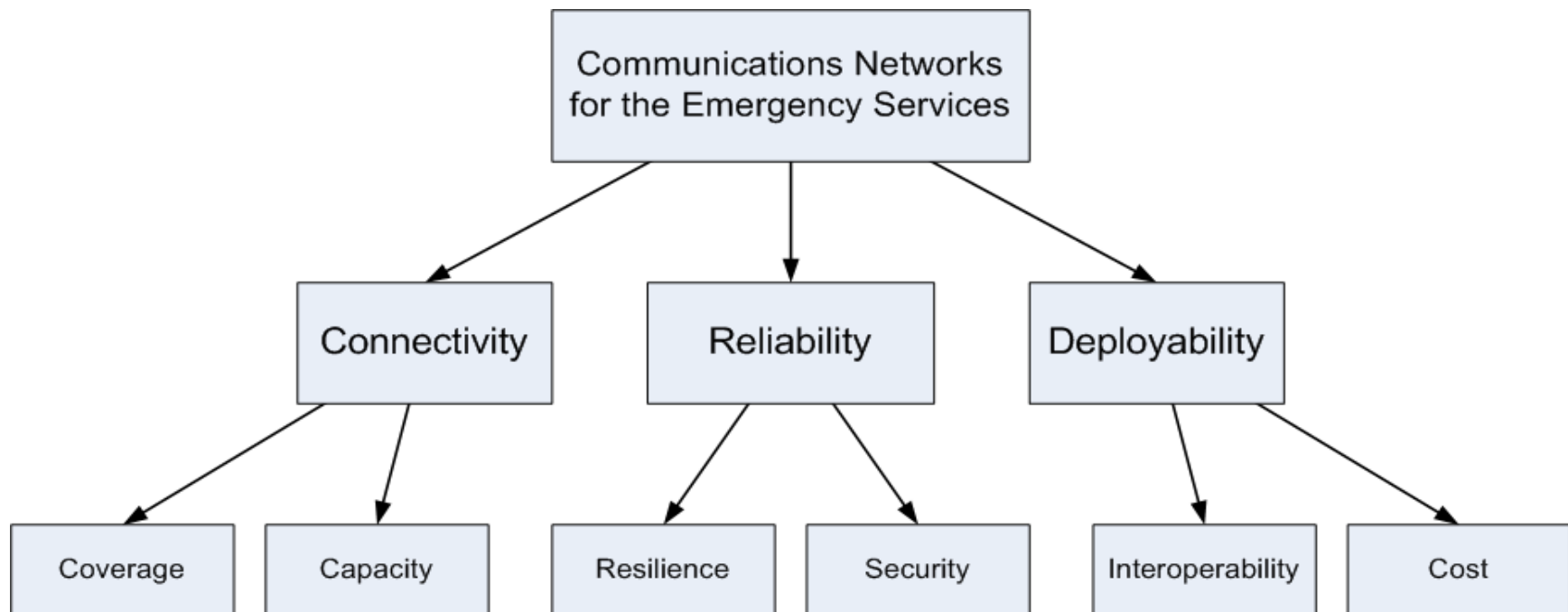
Type of Users

- <u>Fixed</u>, e.g. office

- <u>Nomadic</u>, e.g. deployable office
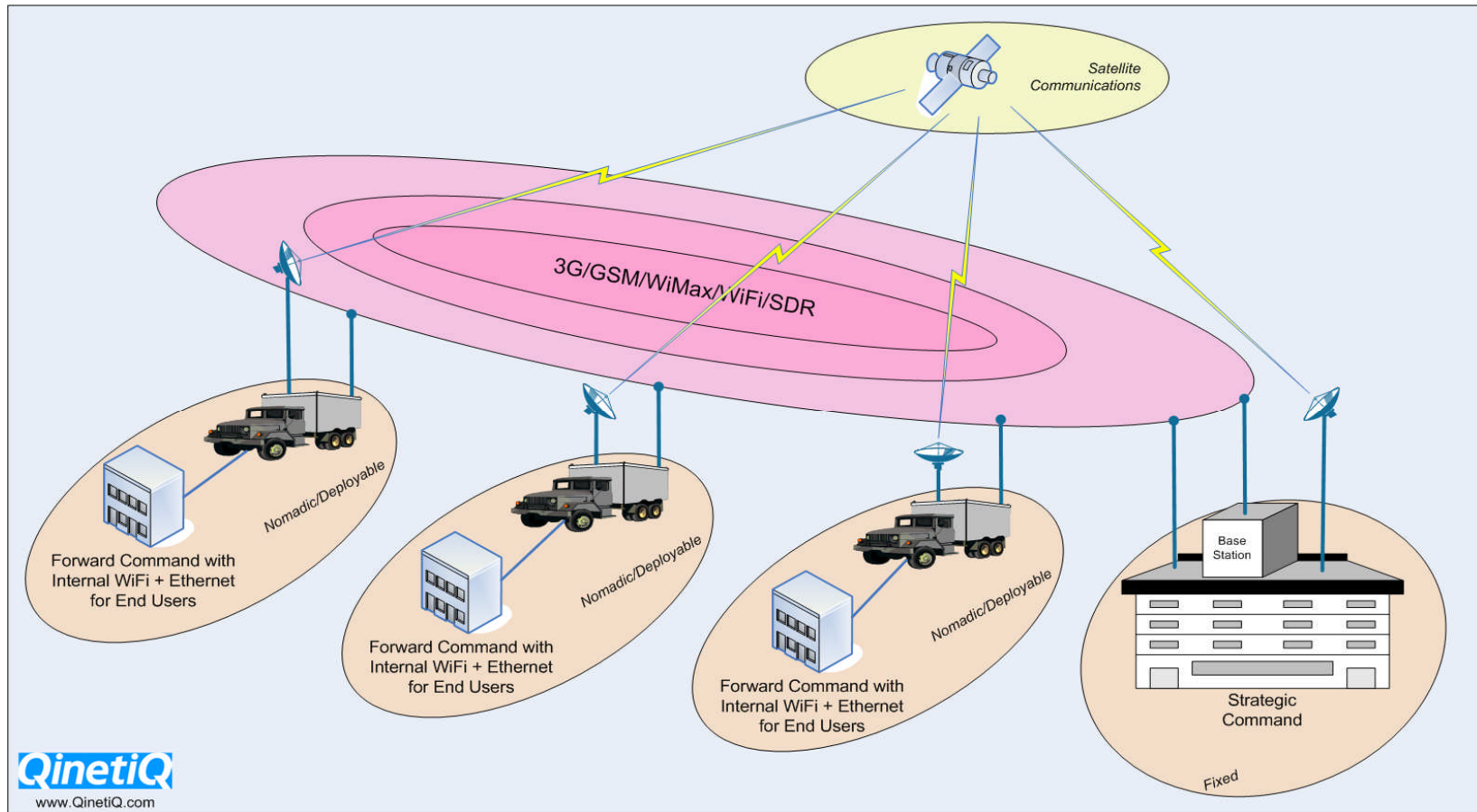
- <u>Mobile</u>, e.g. land/air/water transport or on-foot

# Type of Traffic

1.1.4
Access to Agency Archive Data

- **1.1.4.1** Cont. Plans/Maps/Documents/Images
  - **1.1.4.1.1** Fax
  - **1.1.4.1.2** E-Mail
    - **1.1.4.1.2.1** Intranet
    - **1.1.4.1.2.2** Extranet
    - **1.1.4.1.2.3** Internet
  - **1.1.4.1.3** Mobile Data
  - **1.1.4.1.4** CAD
- **1.1.4.2** Hazard Data
  - **1.1.4.2.1** Fax
  - **1.1.4.2.2** E-Mail
    - **1.1.4.2.2.1** Intranet
    - **1.1.4.2.2.2** Extranet
    - **1.1.4.2.2.3** Internet
  - **1.1.4.2.3** Mobile Data
  - **1.1.4.2.4** CAD
- **1.1.4.3** Confidential Data – Secret, Patient, Personal etc
  - **1.1.4.3.1** Fax
  - **1.1.4.3.2** E-Mail
    - **1.1.4.3.2.1** Intranet
    - **1.1.4.3.2.2** Extranet
    - **1.1.4.3.2.3** Internet
  - **1.1.4.3.3** Mobile Data
  - **1.1.4.3.4** CAD

Type of Traffic for Users
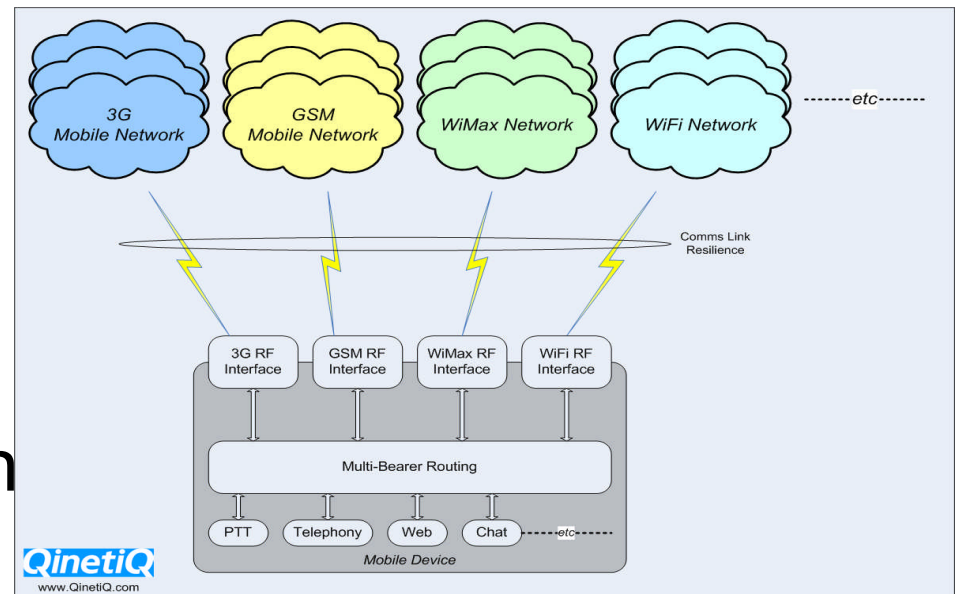
Strategic/Forward Command Communications

Forward-Command/Operations Communications
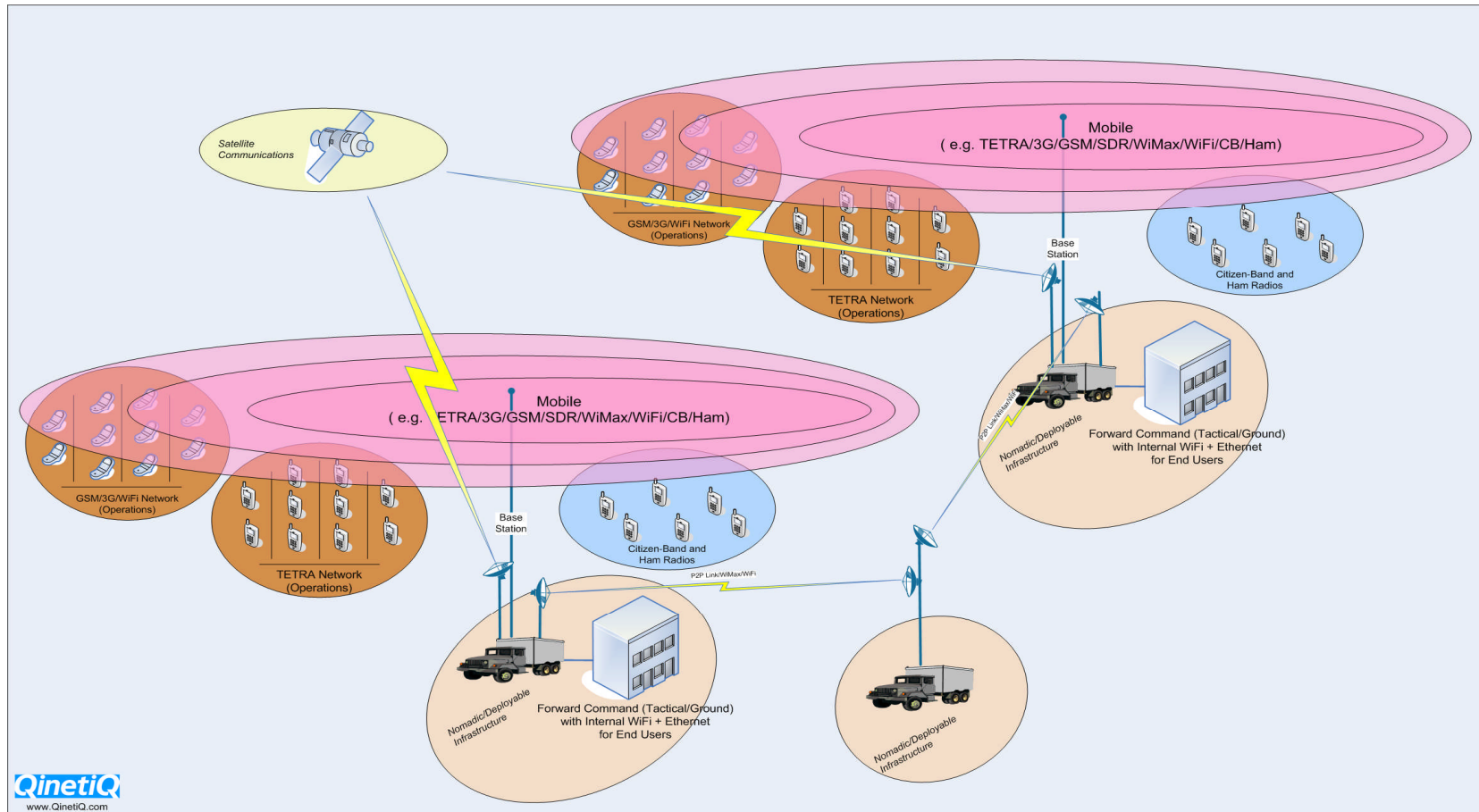
Delivering Resilience

Resilience can be best carried forward to the frontline and into the operations space by the use of mobile communication devices which are
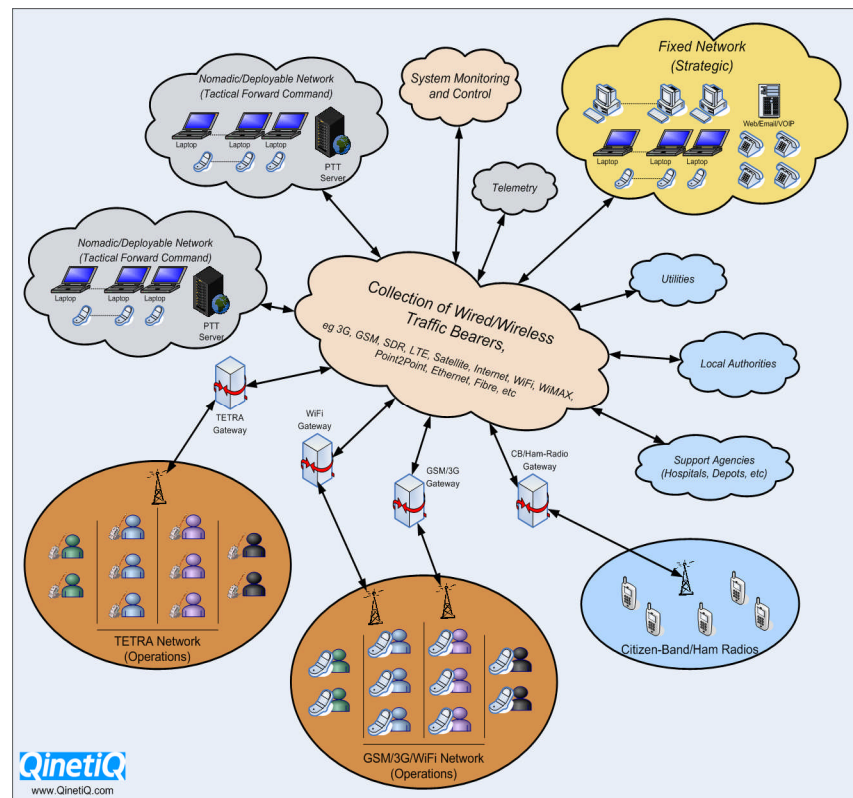
– Open
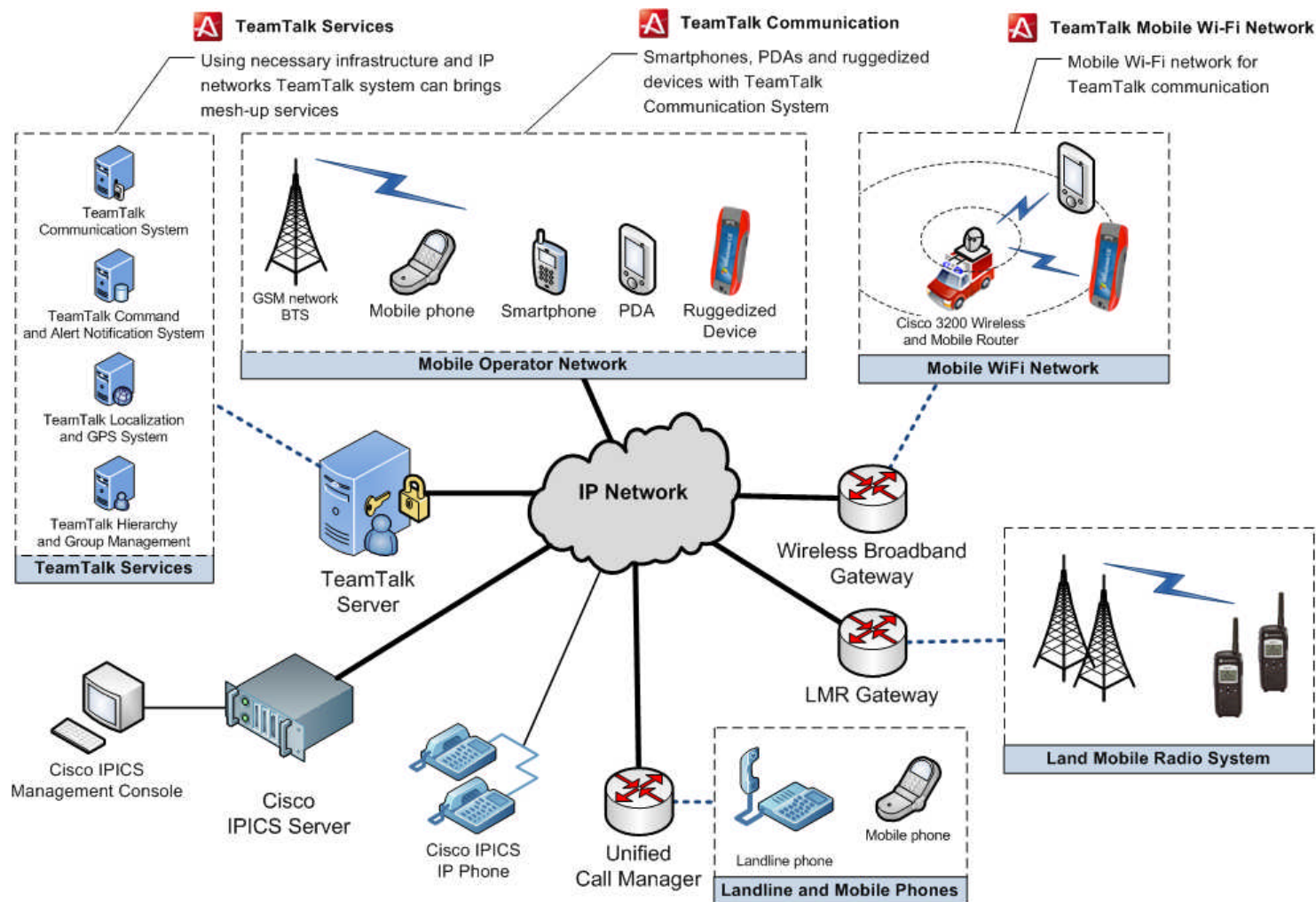– Capable of communicating using multiple standards

Holistic High Level View

The communications system architecture allows:

- – Technical interoperability: Able to extend comms across different agencies and countries.

- – Service expandability: Able to extend comms into areas of poor coverage.

System Convergence

Contributions from Partners

- User Requirements

- Infrastructure

- Applications

Questions ?

Contact

- SECRICOM Website (www.secricom.eu)

- Presenters:

Dr A Aldabbagh
Portsdown Technology Park
QinetiQ, UK

Tel: +44 (0) 2392 31 2107
Fax: +44 (0) 2392 31 2852
E-mail: aaldabbagh@qinetiq.com

Mr R Edwards
Portsdown Technology Park
QinetiQ, UK

Tel: +44 (0) 2392 31 2259
Fax: +44 (0) 2392 31 2852
E-mail: raedwards1@qinetiq.com