Presentation Objectives:
1. Project Background
2. User Requirements
4. Interoperability
5. Cognitive Approach
6. Organisation
7. Benefits
8. Achievements
6. Summary

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?

Project SECRICOM Key Facts

- Seamless Communication for Crisis Management
- Multi-Agency and Multi-National Communications for Crisis Management
- EU funded project – FP7
- Start date: 1 Sept 2008
- End date: 30 April 2012
USER REQUIREMENTS

1.2.2.1

hospitals

archive data

Review appropriate

information from

and logs

known specialist

deployed

1.2.6.1.3

IER Exercise - Key Findings

- Voice is predominant (~50%) with Messaging next (~25%)
- More voice at Operational level and decreasing up the CoCmnd
- Data is concentrated at Strategic level and decreasing down the CoCmnd
  - Need for data, image and video capabilities at the Operational level
- Intra-agency communications is key at all levels of command
- Inter-agency communications account for nearly a quarter of all IERs
- Situation Awareness (SA) is the greatest proportion of IERs (~59%)
  - Ratio of C2:SA is approx 3:2 driven by need for audit trail leading to versions of the same IER voice & data
- Voice remains most significant IER data type for both C2 and SA, with SA demands a greater use of data types

Towards User Requirements (Use Case Study)

Command and Control
Situational Awareness

High-Level Business Drivers

- Enabling agencies, when required, to be securely networked using existing and differing legacy communication systems for effective interoperability
  - Including across international borders
- Enhancing resilience in support of business continuity during crisis response
- Enrichment of business information service types for more effective operations (video, imagery, web, etc)
- Cost reduction through convergence of services onto one common IP infrastructure
Aspects of Crisis Management

- Business Aspects
- Technology Aspects
- Environment Aspects
- Organisation Aspects

Business: Stakeholders

- Electric
- Gas
- Water
- Transport
- NGOs
- Armed Forces
- Govt Agencies
- Police
- Fire
- Health
- Coast Guard
- Local Authorities
- International Border

Business

- Multi-Agency
- Multi-National

Cohesive stakeholder collaboration is vital for effective large scale crisis management
Business: Multi-Agency Operations and the Implications

- Different technology maturity levels – non interoperability?
- Different operating procedures – non-compatibility?
- Very vertical CoFcmd – slow information exchange?

Business: Multi-National Operations and the Implications

- Variation in procurement
  - Cycles
  - Time scales and
  - Budgets.
  - Difficult to predict capabilities, and hence forward plan?
- Variation in doctrines & regulations
  - Inefficient business interoperability?

Technical

- Assumption: Networks and comms may be partially or completely destroyed in a crisis zone.
- Need the ability for networks and comms establishment amongst participating agencies and nations
  - Variation in technology amongst agencies?
  - Justification of cost?

Variability in Technology and Procedures and the Implications

Different agencies collaborating during different crisis leads to variability in effective capability from crisis to crisis

Implications on planning and overall effectiveness?
Implications of Multi-National and Multi-Agency Operations on Crisis Management

The variability in technology and business procedures leads to

- Reduced collaboration effectiveness
- Increased risk to life saving operations

Environment

Crisis Type | Impact on the Crisis Zone | Impact on Op's
--- | --- | ---
Earthquake | Open Space with No or Some Communication Infrastructure | • Reduced capability
Large Scale Flood | Open Space with No Communication Infrastructure | • Breakdown
Tunnel Rescue | High Dependency on Choice of RF Frequency and Band | • In-field re-config to achieve some comms capability
Large Scale Fire | Difficult RF Propagation Environment | Costing time and hence life

Organisation: Public Safety & Security

Complex and fragmented landscape
- Many agencies with own local requirements
- Multiple domains
- Fragmented CofCmnd
- New technologies incredibly complex with interoperability issues

EA for Public Safety & Security: OSSAF

The Open Safety & Security Architecture Framework aims to align stakeholders within a PS&S organisation and helps to achieve effective transformation, leading to the following benefits:

- **Agility**: Responsive technology to evolving needs of the user
- **Interoperability**: at the forefront and not an afterthought
- **Cost Reduction**: Investments rationalised across multiple agencies/providers and different generations of systems
- **Decision Support**: Strong support for Programme Management
- **Information Management**: Better distribution of information, throughout the chain of command
- **Higher Mission Effectiveness**: Achieve better access to information and common SOPs
Interoperability is Key

SECRICOM 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.

Interoperability ranges from organisational to technical aspects all of which must be ‘harmonised’ in order to achieve full interoperability.

Variability in Technical and Operational Capabilities; and Interoperability

Convergence is a key efficient enabler of Interoperability

Technical Interoperability

From an agency perspective, new systems should provide for:

- “Intra-agency interoperability”
  i.e. new technology works with the agency’s:
  -- Current technology, and
  -- Future technology

- “Inter-agency interoperability”
  i.e. new technology works with other agencies’:
  -- Current technology, and
  -- Future technology
Cognitive Approach

Convergence as the Approach

Need for Flexible, Business-focused IT Solution Capable of Delivering Diverse Business Applications over Different Communication Systems, Devices and Standards with Resilience to support Business-continuity during Critical and Non-critical Business Operations

Cognitive Networking

• IP Network-of-networks combines together wired, wireless, fixed, ad hoc and mobile networks
• Multi-bearer edge
• Multi-bearer capable end equipment

Cognitive

• Management of the
  – Business demand to support operations, and
  – Supply of the communication resource
• Business continuity is the goal
Cognitive IP Network-of-Networks

- Self-planning
- Self-configuration
- Self-optimising
- Self-testing
- Self-healing
- Self-maintenance

- Management of business demand and supply of communication resource

- Minimise Cost
  - CAPEX
  - OPEX

Cognitive Radio

- Ability to pass IPv4/6 traffic, preferably ‘natively’
- Ability to operate over any infrastructure: mobile, fixed, satellite and in the following modes:
  - Single bearer, and
  - Multi-bearer: key for interoperability with other agencies
- Ability to manage user traffic in dynamic multi-bearer availability
- Ability to operate independently of any infrastructure

- Ability to use multiple frequencies/bands to match to the operational environment
  - Tunnels, caves and corridors: Waveguide effect
  - Fires: evidence of fire blocking RF needs to be investigated
- The ability to use repeaters at key points with CR capability between the WAN (i.e. with repeaters and also IP Network-of-Networks) and user equipment

Cognitive Radio Architecture (IP)

- Policy
- Cognition: Managing the Demand vs. Supply Balancing Process
- Information Source/Sink

SECRICOM CR/SDR Testbed

- Extensible
- Re-Configurable
- Based on
  - Layer 3 model
  - Server-client
- Supports infrastructure and infrastructure-less modes
SECRICOM’s Benefits

• Increased number of first responders
  – Trusted use of Mobile Telephony
  – Voice communication/instant text messaging
  – Exchange of imagery and hand-drawings

• Enhanced information for better operation
  – Faster info gathering accessible from mobile devices
  – Intelligent resource management

• No eaves-dropping
  – Chip-based security
  – End-to-End encryption
  – Network monitoring centre

• Resilient communication service
  – Multi-bearer based for resilience
  – Network monitoring centre

SECRICOM: Access Devices, Bearers and Services

Any Secure Service from Any Agency over Any Bearer via Any Access Device

Achievements within a User Framework
Achievements to Date

• Multi-national and multi-agency information exchange over multi-bearers over commercial networks and COTS products

• SECRICOM capabilities proven to function effectively in a multi-agency and multi-national live Civil Protection Exercise (CBRN)

• Resilient PTT voice over IP using a network-of-networks underpinned by SECRICOM’s multi-bearer router

• Use of commercial networks: PTT voice calls conducted between a Tablet/PCs in the UK and mobile Smart Phones on a Slovak Mobile network

Achievements to Date

• Range of integrated user devices
  – Legacy radios (UHF/VHF): Walkie-Talkies and Citizen-Band Radios
  – PCs, Laptops, Mobile Phones, PDAs, Tablets

• Range of integrated/converged information services
  – Real-time: PTT Voice, Telephony, Video, Mapping
  – Data: Imagery, Chat, Web, File Transfer, etc.

• Range of integrated communication systems
  – Satellite and deployable networks
  – Internet, wireless (WiFi, 3G and GSM) and wired technologies (Broadband, LANs).

• Vendor independence through the integration of different devices: PCs, Laptops, Mobile Phones, PDAs and Tablets

Summary

• User requirements
  – Multi-agency and multi-national
  – Impact on business, technical, environmental, organisation

• Convergence and flexibility are key enablers for interoperability

• Cognitive networking
  – Management of demand & supply for business continuity
  – Cognitive IP network-of-networks
  – Cognitive IP radio and its architecture

• Benefit: towards any secure service from any Agency over any bearer via any access device

• Project achievements

Demonstration/Exercise Activities

• UK 2010

• BAPCO 2010

• CP NATO 2010

• BAPCO 2011