Policy Implications for Better Communications and Interoperability for Public Safety

March 4, 2004

Dr. Paul Kolodzy, Director

Nancy Jesuale, Public Safety Program Manager

Outline:

- Part One: Emerging National Trends (Paul)
- Part Two: Local and Regional Policy Issues (Nancy)
- Part Three: Policy Response (Paul)

Part One: Emerging National Trends

SAFECOM: Key Challenges for Public Safety Interoperability

1. Incompatible and Aging Equipment
2. Limited and fragmented budget cycles and FUNDING
3. Limited and fragmented planning and coordination
4. Limited and fragmented radio spectrum
5. Limited equipment standards

Technology trends: mobility and connectivity

- Cellular Service moving toward broadband services
- Wi-Fi and Wireless Broadband Deploying more places
- Meshed Networking
- Spectrally Adaptive, Aware Radios/End-User Devices

Industry Trends:

- Competition vs. Mergers and Acquisition
  - We may start with vigorous entrepreneurial involvement, but consolidation eventually rules!
- Momentum is behind the IP standard
- Coverage and Availability (the winners have to have network access available everywhere)
- Quality of Service -- It’s an afterthought still! Price, not quality rules the marketplace
- Security is still an afterthought

The Market Trends:

- From wired to unwired services
- Mobility is Key to consumers
- Demand moving from narrowband to broadband uses
- Investment is continuing in new infrastructure, new access devices, technologies and services

Part Two: Local and Regional Policy Issues

Communications is the primary weapon for public safety

- Most urban police vehicles and fire apparatus contain over $10,000 of communications equipment (MDT, modem, multiple radios). It’s all narrowband.
- Future requirements are for broadband voice, data, video and image: video on board, wearable computers, cyber-crime, nano technology, geo-spatial data, database access, etc.
- The bottom line is, public safety needs better, or at least equivalent access to technology as the “perps”

Public safety is about 10 years behind the military --how are we going to catch up?

Communications is the primary weapon for public safety

- For firefighters, the high-rise environment of steel and concrete is a no-transmit zone
- Underground environment -- light rail, tunnels, parking lots
- Chemical hazards
- Density issues (suburban wildfires)
- Immediate and future need for wearable computers, geo-spatial data for hazmat, directions, and on-the-fly interoperability (meshed networks)

Public Safety Spectrum Policy State and Local Level-

unchain infrastructure and access

- Local approaches are widely divergent on “shared” infrastructure, resources and control.
- Fire-fighting is largely a volunteer effort in this country.
- Decisions on spectrum policy made at the “platoon” level.
- American system of government requires a great deal of <u>local autonomy</u>--local approaches can NOT be easily dictated from a central “top down” approach.
- There is no cookie-cutter for local public safety spectrum

The Status Quo is not adequate

We need to promote the regional utility model for public safety communications infrastructure

- Locals have long recognized the need to “regionalize” utilities (water, sewer, transportation)
- Local, regional and State government simply have no funding mechanism for planning, building or maintaining communications infrastructure (We need the equiv. of the Federal Dept of Transportation to funnel funds on a regular and predictable schedule)
  - Currently rely on bond measures
  - Local tax base won’t support the dedicated infrastructures
- Locals don’t have engineering and technical resources necessary for planning, engineering, operations and maintenance
- The dominance of a single vendor has hurt public safety

What will shape future spectrum policy?

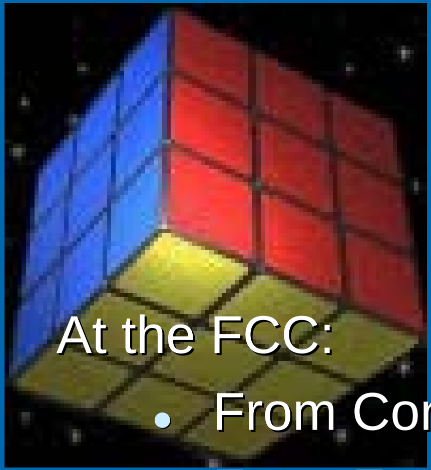
Can the 10-year paradigm change to put local public safety in a top seat?

Places to look:

- Assuming adaptive ("cognitive") radios--why can't we devise a policy scheme that provides advantage to public safety?
- How could interruptible spectrum advantage public safety?
- Who are the secondary and who are the primary users going forward?
- How much spectrum is there? Is it limited? Or unlimited for priority public benefit?
- Whose paradigm changes? Just public safety's? What about cellular's spectrum paradigm? What about the broadcasters?

Part Three: Policy Response

The Communications Policy Paradigm is Changing



At the FCC:

- From Command and Control to Commons Spectral Rights
- From Frequency and Space Dimensions to Time Dimension
- Development of secondary spectrum markets
- Eventual movement toward "put and call" spectrum access

At Congress:

- Privacy Issues
- Spam
- Identity Theft
- Digital Divide
- Homeland Security

Spectrum Policy Task Forces (FCC and NTIA)-- Reexamining Paradigms

- Separation between commercial, public safety and military spectrum authority
- Delegation of licensed and unlicensed spectrum
- Interference Issues and the concept of Interference Metrics/Temperature
- Rights of Spectrum Holders

Old Policy + New Technology = Collision!

- VOIP: Telephone, or NOT?
- Cable modems: Cable service or NOT?
- Broadband Network Access: Utility or NOT?
- Taxation: universal service (who pays?) franchise fees (why me?), carrier access billing (not fair?)
- Regulation or NOT? (unbundled network elements, mandated wholesale access, government provided networks)
- Privacy, Identity Theft, Foreign Ownership, Cybercrime, Cybersecurity….
- Spectrum Scarcity vs. Spectrum Access

So, in light of emerging technology, policy and industry trends;

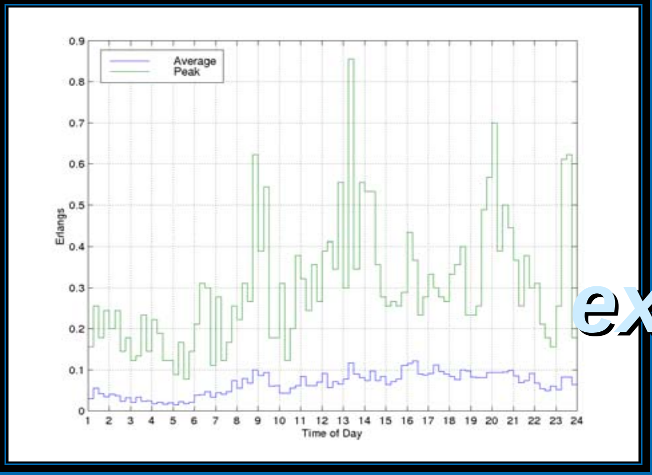
How Does Public Safety Win?

Technology Pieces

- Adaptive radio is nearly a reality
- Commercial infrastructure (cellular, Wi-fi and fiber) build-out creates more access opportunities for public safety (Physical and Network-Level)
- Security, reliability and authentication on commercial networks still an issue today
- Public safety future uses very different from today's narrowband uses. (real-time video, image, GIS, wearable computers, augmented reality--we will need broadband data, not just voice)

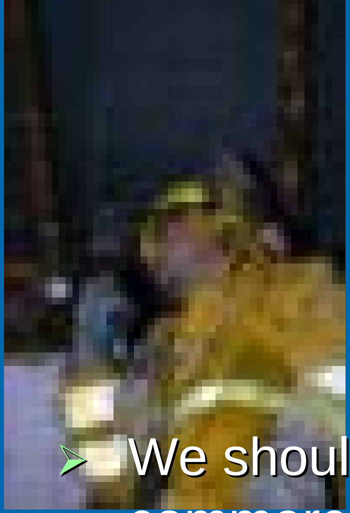
Exploit emerging technology

WiNSeC
Wireless Network Security Center



Big gains for Public Safety if we *exploit emerging technology*

- "Lights and sirens" access -- The investment made in commercial infrastructure can be leveraged to provide public safety access
- Accordion spectrum -- Adaptive radios can be leveraged to provide flexible spectrum usage
- Adaptive radios -- agility can be leveraged to create seamless interoperability between dissimilar frequency bands.
- Put and call authentication -- Roaming, permissioning and carrier access billing systems can be leveraged to create secure mechanisms for public safety access to commercial networks
- More COTS -- Encourage development of adaptive receiver technologies that are affordable, ubiquitous and standardized

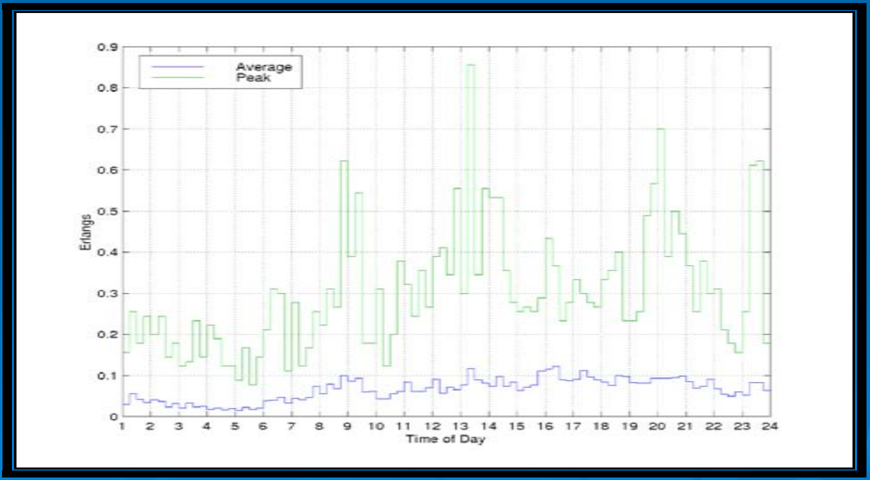


How should we proceed?
Some specific research issues

- We should measure the impact pubic safety access would have on commercial network capacity (measure and then model the demand dynamics)
- We should develop the models and subsequent standards for put and call (interruptible) access (authentication, permission, release)
- We should define the reliability and security augmentation necessary to make commercial infrastructure and networks meet public safety grade-of-service requirements (99.999% reliability)
- Find the proper trade-offs between wireless and wireline technology
- Examine asset re-use at the RF level, network level, system level and software level

Public Safety Policy Strategy--

- Build the policy case with facts and research results,
- Look long over a long horizon
- Develop R&D capability dedicated to public safety requirements
- Commercial and military infrastructure are an untapped national assets for public safety interoperability



Pkolodzy@stevens-tech.edu
njesuale@winsec.us

Thank You