

Roadmap for Future Unlicensed Services Working Group

Chairs: Mark Bayliss, Milind Buddhikot

Vice Chair: John Barnhill

FCC Liaisons: Michael Ha

September 24, 2015



Working Group Members

- WG Co Chairs: Mark Bayliss, Milind Buddhikot
- Vice Chair, John Barnhill
- FCC Liaisons: Michael Ha, Karen Rackley
- Members:
 - John Barnhill, GENBAND
 - Mark Bayliss, Visualink
 - Nomi Bergman, Brighthouse
 - Milind Buddhikot, Bell Labs
 - Adam Drobot, Open Techworks
 - Dick Green, Liberty Global
 - Russ Gyurek, Cisco
 - Jeff Foerster, Intel
 - Theresa Hennesy, Comcast
 - Farooq Kahn, Samsung
 - Jack Nasielski, Qualcomm
 - George Lapin
 - Mark Racek, Ericsson
 - Brian Markwalter CE.org



Roadmap for Future Unlicensed Services

Unlicensed services have played an unexpectedly vital role in the evolution of communication capabilities and in providing a ‘wireless commons’ for innovation. It is critically important for the Commission to understand both the potential pathways for continued evolution of unlicensed services as well as potential threats to the continued viability of the ‘commons’.

Work Group Focus

- (1) Evolving and novel applications
 - (e.g. low power WANS, internet-of-things (IOT), unlicensed LTE).
- (2) New business models
 - (e.g. managed vs. unmanaged vs. private, indoor-only services).
- (3) New candidate spectrum bands to increase available spectrum.
- (4) Voluntary etiquettes for unlicensed service applications that will help protect the commons model
- (5) The potential impact of present EMC limits for consumer and industrial devices on the continued growth and vibrancy of unlicensed services.

Unlicensed Spectrum – The Key Takeaways

Demand

- Increased Traffic
- New Entrants

- Service Providers
- Enterprises
- Consumers

Action

- More Spectrum
- Better Etiquette

- Both Policy and Technology change needed to ensure usability

Results

- Increased Demand
- Better Utilization

- Availability Stimulates Usage and Services

Industry Engagements

Service Providers

verizon^v **T-Mobile**[®]

Sprint 

Associations

atis 

WiFi[™]
ALLIANCE

 **WISPA**
Wireless Internet Service Providers Association

Equipment

QUALCOMM[®]

 **UBIQUITI**[®]
NETWORKS

Standards Bodies

IEEE 
802.15

Key Observations from Industry Interviews

Demand Drivers

- 1 Growth in connected devices from users and things
- 2 Growth as carriers, users, gov, & enterprises add locations
- 3 Communications app growth & Wi-Fi First mobile providers
- 4 Licensed providers shifting traffic to unlicensed
- 5 The economics of unlicensed spectrum

- General Agreement:
 - More Spectrum is needed; licensed and unlicensed
 - Light-touch regulation preferred
- Over subscribed bands –
 - 900 MHz, 2.4 GHz, with concern about 5GHz
- Life-essential services have emerged using unlicensed spectrum
 - E.g. traffic control

4Q Action: Should essential services be prioritized or move to licensed?

Increasing Demand for 5GHz Band Services

- Spectrum will be shared by both Wi-Fi and LTE variants
 - Agreement that mechanisms are needed to ensure fair co-existence
 - Industry Groups engaging with each other and FCC to resolve
- Interested parties responding to commission ET 15-105.
 - Working group will defer specific technical recommendations as this is an open proceeding

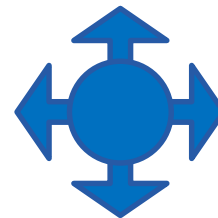


Carrier Wi-Fi Growth

- Improving Coverage with VoWi-Fi
 - By 2018, VoWi-Fi traffic will exceed VoLTE and will account for 53% of mobile VoIP traffic. (Wi-Fi Alliance)
 - VoWi-Fi traffic small vs data
- Mobile data traffic offload is high-value consumer use case
 - 57% mobile data traffic offloaded in 2014 growing to 66% in 2019 (Cisco VNI 2015)
 - Traffic growth CAGR impact is 7%
 - By 2019, Wi-Fi capable tablets and PC's will be 3.5X the number of cellular capable (Wi-Fi Alliance)

Primary Use-Cases

Extended Voice Footprint



T-Mobile – 11M Wi-Fi Calls per day (Infoworld Online 8-27-2015)

Cellular Data Offload



Wi-Fi expected to contribute 20% to mobile data capacity. (Wireless BB Alliance)

Currently 7GHz of spectrum identified above 60GHz.
Commission considering adding an additional 7GHz.

Significant Growth in Real-Time Communications Services over Unlicensed Spectrum

Service Providers
With Plans to support VoWi-Fi



Voice over Wi-Fi Apps
Includes Multi-media/ RTC



Hundreds of apps supporting free or low price real time communications

Wi-Fi-First Carriers



Announced plans are Wi-Fi today, but will include other technologies

More Spectrum + Spectrum Efficiency

- Current unlicensed bands
 - TVWS, 900MHz, 2GHz, 5GHz, and 60GHz (part 15 rules)
 - 3.5GHz (licensed by rule, under part 96)
 - While considering more unlicensed spectrum, identification of additional bands between 5GHz and 60GHz would be useful
- Encourage more sharing between licensed and unlicensed bands
 - Evaluate opportunities for indoor unlicensed use with licensed spectrum bands that are primarily used for outdoor use
 - Specific recommendations targeted for December



How to Manage Increasing Congestion?

- Operating Principle:
Technology neutral
and flexible in
application
- Considerations
 - Duty Cycle &
Bandwidth
 - Spectral/ Capital
efficiency
 - New Entrant support
 - Critical Services –
Special Interests

Etiquette statement from
2014 TAC IoT Work Group

Unlicensed Etiquette Statement

In unlicensed bands, FCC rules provide that unlicensed users must accept interference (and may not cause harmful interference).

Although this regimen has worked well; now may be the right time for the FCC to investigate potential next steps in the evolution of the “digital etiquette”.

Recommendations

- *SDO's should continue to coordinate with each other to facilitate co-existence.*
- *Non-standard wireless solutions should strive to protect the commons in ways that allow the operation of other technologies.*
- *As new frequency bands are allocated there may be significant value in re-examining co-existence techniques for unlicensed spectrum. the FCC should be open to future policy supporting ultra-efficient spectral technologies which may require that some newly allocated bands be restricted to use of specific technologies and or control protocols*
- *The IPv6 network protocol offers several advantages over IPv4 ... and should be used where feasible.*



4Q Work Plan

- Finalize remaining industry engagements
 - Summarize key themes and messages and submit with Final TAC Presentation
- Consider a recommendation to identify additional unlicensed spectrum between 5GHz and 60GHz
 - Evaluate opportunities for unlicensed use
- Re-examine and update etiquette statement
 - Defer specific recommendations regarding Wi-Fi and LTE-U/LAA in favor of active commission proceeding. (ET 15-105)
- Consider a recommendation regarding life-essential services prioritizations in unlicensed bands.
- If necessary, update 2013 TAC recommendation on Terahertz



BACKGROUND



Q32015 Industry Engagement– Sample Questions

Revised June 1

1. What applications and services, both new and future, do you expect to drive demand for the future use of unlicensed spectrum?
 - a. Any quantifiable projections on the potential value or size of these applications and services?
2. Are you aware of any data or market projections on the relative growth of narrow v. wide channels (e.g., white space v. 802.11ac/ad) to better understand future unlicensed spectrum needs?
3. Are you aware of, experiencing, or anticipating heavy congestion in the use of the existing unlicensed spectrum bands which is currently impacting services in those bands or will impact services in those bands in the near future?



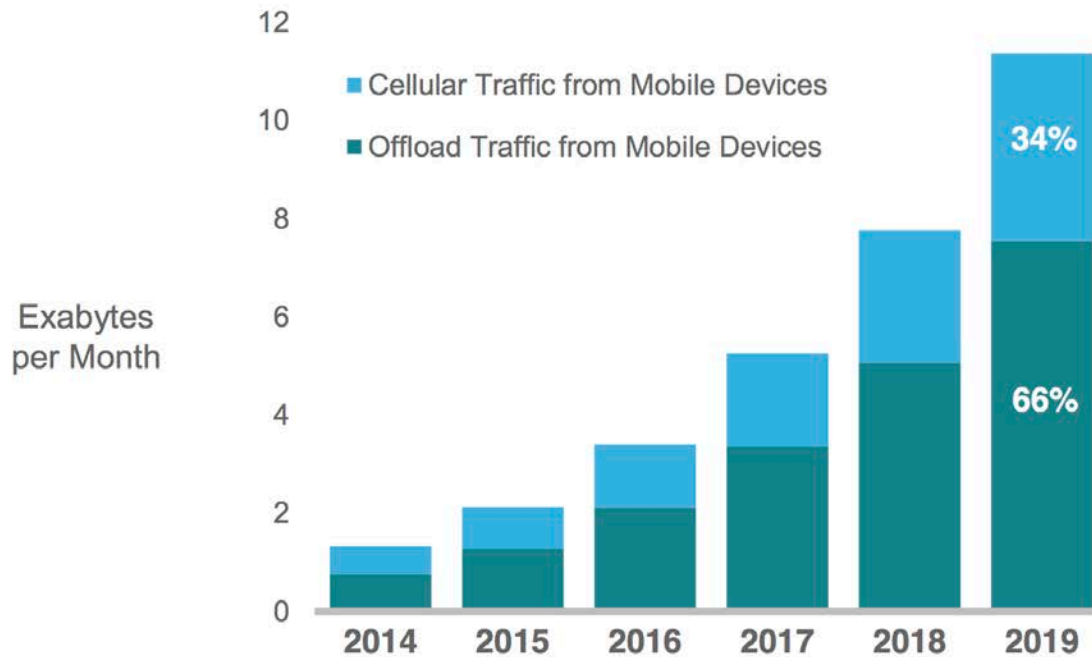
Q32015 Industry Engagement – Sample Questions

4. Are there any existing FCC rules governing the use of the unlicensed bands that are impacting the deployment of existing or future new services? If so, which rules should be revisited and why?
5. If the FCC were to open up new spectrum for unlicensed use, which frequency bands would be the highest priority?
 - a. Given the ongoing 600MHz proceeding, recent adoption of 3.5GHz rules and 5GHz UNII bands, and the Spectrum Frontiers NOI on 60GHz band, what are the potential applications that may be deployed in these bands?
6. Are there new technologies being planned for unlicensed services.



NA Mobile Data Traffic Offload*

66% of Mobile Traffic to be Offloaded by 2019
57% of Mobile Traffic Offloaded in 2014

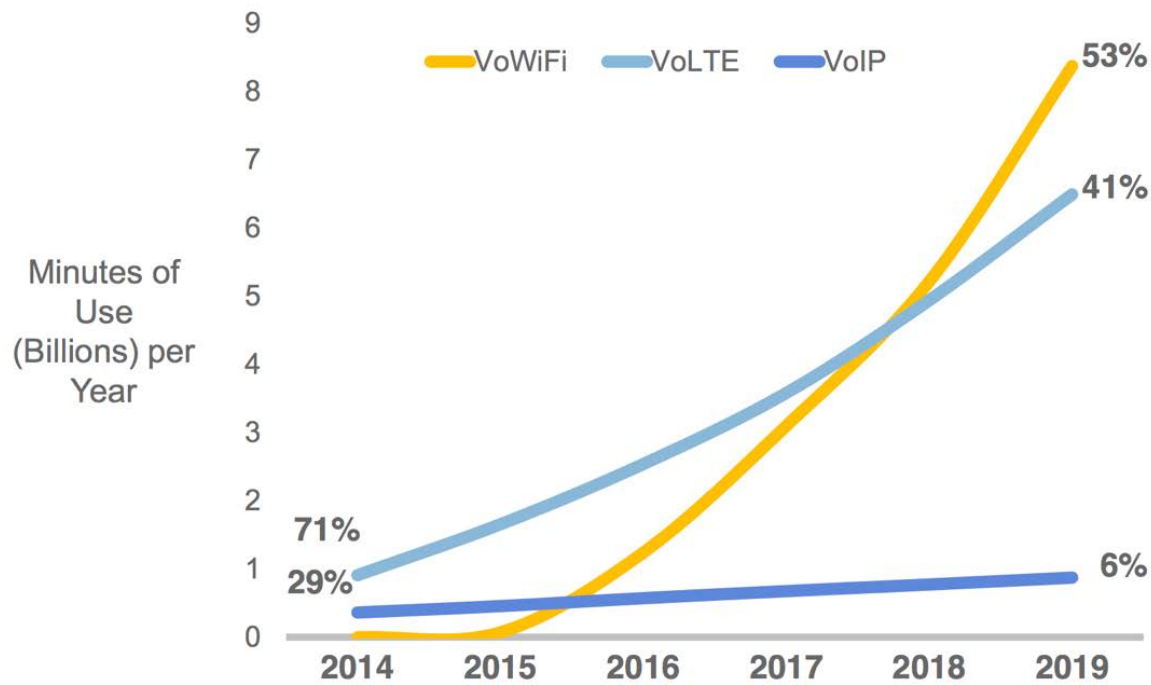


*Offload includes traffic from dual-mode devices (i.e., supports cell & Wi-Fi, excl. laptops) over Wi-Fi/small cell networks

Source: Cisco VNI Global Mobile Data Traffic Forecast, 2014–2019

Wild Card: VoWiFi MoU Exceeds VoLTE by 2018

VoWiFi Accounts for 53% of Mobile IP Voice by 2019



Source: ACG, Cisco VNI Global Mobile Data Traffic Forecast, 2014–2019

Mobile Device Theft Prevention WG Report to the FCC TAC

September 24, 2015



Contents

- Mission
- FCC Request for Further Advice
- Task 1 Update - On-Device Theft Prevention Features
- Task 2 Update - Hardening of the IMEI
- Task 3 Update – Database
- ATIS Best Practices for Obtaining Mobile Device Identifiers for MDTP
- Preliminary Recommendations
- Anticipated Recommendations to the FCC Chairman
- MDTP Plan for Remainder of 2015

WG Participants

- Co-Chairs:
 - Brian Daly, AT&T
 - Rob Kubik, Samsung
- FCC Liaisons:
 - Walter Johnston
 - Charles Mathias
 - Chad Breckinridge
 - Elizabeth Mumaw
- Dennis Roberson, FCC TAC Chair
- Asaf Askenazi, Qualcomm
- Jay Barbour, Blackberry
- Alan Bersin, DHS
- Brad Blanken, CCA
- Jeff Brannigan, DHS
- Matthew Bromeland, Metropolitan DC Police Department
- Craig Boswell, Hobi
- Eric Feldman, ICE/Homeland Security Investigations
- Thomas Fitzgerald, New York City Police Department
- Les Gray, Recipero
- Shelley Gu, Microsoft
- Joseph Hansen, Motorola
- Jamie Hastings, CTIA
- Joe Heaps, National Institute of Justice
- Gary Jones, T-Mobile
- Sang Kim, LG
- Jake Laperruque, Center for Democracy and Technology
- Irene Liu, Lookout
- John Marinho, CTIA
- Samuel Messinger, U.S. Secret Service
- James Moran, GSMA
- Jason Novak, Apple
- Kirthika Parmeswaran, iconectiv
- Greg Post, Recipero
- Deepti Rohatgi, Lookout
- Mark Romer, Asurion
- Mike Rou, eBay
- Matt Rowe, Gazelle
- Christian Schorle, FBI
- DeWayne Sennett, Editor (AT&T)
- David Strumwasser, Verizon
- Maxwell Szabo, City and County of San Francisco
- Ron Schneirson, Sprint
- Samir Vaidya, Verizon Wireless

MDTP WG Mission

- Emphasis will be on longer term initiatives that will combat more sophisticated theft scenarios
 - Developing recommendations on next generation anti-theft features
 - Processes including recommendations for hardening of existing device identifiers and the possible need for new, more secure identifiers
 - Security mechanisms with higher consumer acceptance (e.g. biometrics)
 - More focused analysis of analysis overall theft ecosystem including how stolen devices are re-entered into the marketplace (e.g. recycling industry)
 - Further recommendations on improved reporting mechanisms
- Consideration will also be given to the efficacy of extending theft prevention mechanisms to other classes of devices.
- Provide an assessment of progress made in the area of device theft prevention as some of these recommendations have been applied

FCC Requests for Further Advice

At the initial 2015 meeting of the TAC, the FCC Chairman requested the MDTP WG consider the following tasks (details as provided by the FCC are in the backup material), :

- Task 1 – On-Device Theft Prevention Features Template
- Task 2 – Hardened Device Identifiers
- Task 3 – Database

Tasks 1 and 2 - an interim report was provided May 1

Task 3 feedback is scheduled for October 1

Task 1 Update - On-Device Theft Prevention Features

- CTIA announced on July 1, 2015 the fulfillment of the Smartphone Anti-Theft Voluntary Commitment at no cost to consumers
 - Major commitment of the entire mobile ecosystem including operators, handset manufacturers, and operating system providers
 - Gives U.S. consumers new protections in the event their smartphones are lost or stolen
 - Included are capabilities to remotely lock and wipe missing devices while still enabling 9-1-1 calls even when the phone is locked and providing the consumer a means to unlock the phone when it is recovered
- Chairman Wheeler has asked CTIA to update its voluntary commitment to include "opt out" functionality, as well as all of the MDTP WG's other recommendations
 - MDTP recommendations supports an "opt out" requirement, under which the theft-prevention features would be activated on all phones by default, and consumers would need to take affirmative steps to disable them
 - Also requested improving the availability of data on device theft and loss
 - CTIA is developing a response to Chairman Wheeler's request

Task 2 Update - Hardening of the IMEI

- GSMA Device Security Group will revisit the entire IMEI security topic in 2015 as it has already identified this topic as being a priority for next year and the work will, at a minimum, involve a review of the technical design principles and reporting and correction process
 - GSMA's North American Regional Interest Group will provide North American-specific concerns
 - As a result of the study, ATIS and/or 3GPP may be involved if standardization efforts are required.
- GSM Association's North American Regional Interest Group "North American Fraud Forum & Security Group" liaison to the GSMA Device Security Group:
 - Conduct a study to better understand the duplicate IMEI landscape and to what extent IMEI reprogramming is an issue today
 - Review the technical security design principles to assess if they remain fit for purpose or if they need to be updated
 - Consider how the IMEI changing ecosystem can be monitored and reported on going forward
 - Study if IMEI implementation security requirements could be defined in the industry standards and if there is merit to such an approach

Task 3 Update - Database

- MDTP WG asked to study database systems that effectively track stolen items and develop a spec sheet for an effective stolen phone database that might be focus on North America
- Issues under study include:
 - Law Enforcement related:
 - Across the US, law enforcement officers may not be aware of the significance of the device identifier (IMEI, MEID, etc.)
 - Procedures to obtain the IMEI or ESN on devices vary among manufacturers and this complicates law enforcement abilities to acquire that information. Also, if the device will not power-on, this further complicates abilities.
 - Across the US, law enforcement officers are not fully aware of how to access information that is in the GSMA IMEI Database.
 - Consumer related:
 - A fragmented system of consumer outreach exists in which no single government agency, group, manufacturer, or carrier providing a uniform and comprehensive outreach program or source for information.
 - Consumers don't always report the theft of their devices to law enforcement and/or carriers.
 - Consumers need instructions and clarity of the process and procedures for the reporting of stolen devices.

Task 3 Update – Database (continued)

- Topics identified include:
 - Mobile device information is dispersed across different stakeholder databases such as local/global blacklists, insurance databases, OEM device check services, MEID/IMEI databases, etc.
 - A lookup across more than one database is required to get comprehensive information.
 - Potential buyers of smartphones do not have access to a complete information to verify that the smartphone is not a stolen mobile device
 - Potential buyers of smartphones may not understand the importance of identifiers and how to identify their smartphones
 - Some mobile network operators in other countries are not using the GSMA IMEI Database, or do not use data from other carriers or regions
 - Some US mobile network operators, especially the smaller mobile network operators, do not utilize the GSMA IMEI Database or have the technology to deny stolen handsets service on their networks

Task 3 Update – Database (continued)

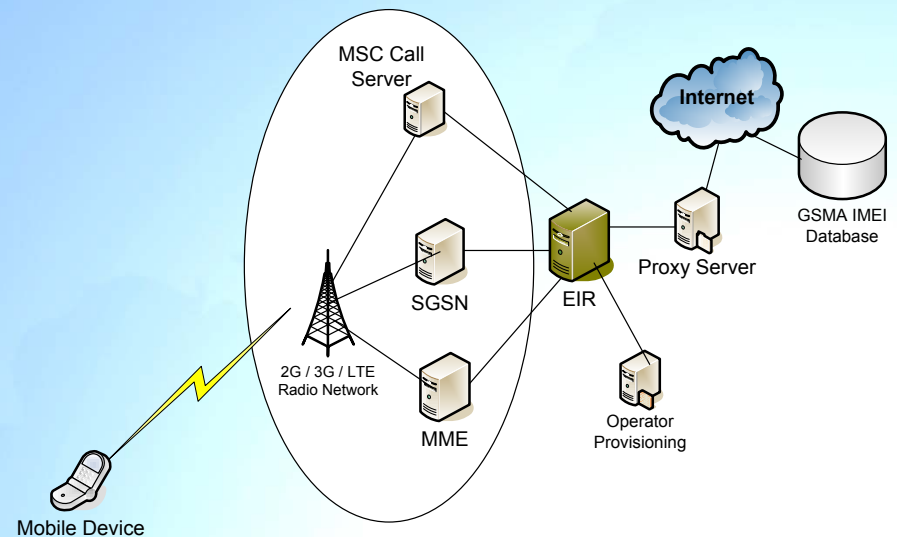
- Database solutions may be characterized into the following categories:
 - Databases used by network operators containing device identifiers which are used to deny access to known stolen devices on their networks
 - IMEI/MEID Database provided by the GSM Association to facilitate the sharing and distribution of stolen device identities between mobile network operators
 - Some OEM/OS vendor databases which specify the enrollment state of the on device theft prevention solution
 - Aggregator databases which provide device checking services and/or portals to network operator and OEM/OS vendor databases

Task 3 Update – Database (continued)

- Network Operator Databases
 - Network operator databases are specifically targeting and denying use of known stolen devices on the network
 - These network operator databases provide the identities of devices stolen from their customers to the GSMA's IMEI Database for distribution to other network operators and they are independent of the subscriber-initiated enrollment status of their chosen on-device theft prevention solution
- GSM Associations North American Regional Interest Group “Analysis and Recommendations for Stolen Mobile Device Issue in the United States” provides example implementations that can be used by the network operators to deny services for stolen mobile devices on their networks
 - Equipment Identity Register
 - CDR Analysis
 - Network Transaction Trigger

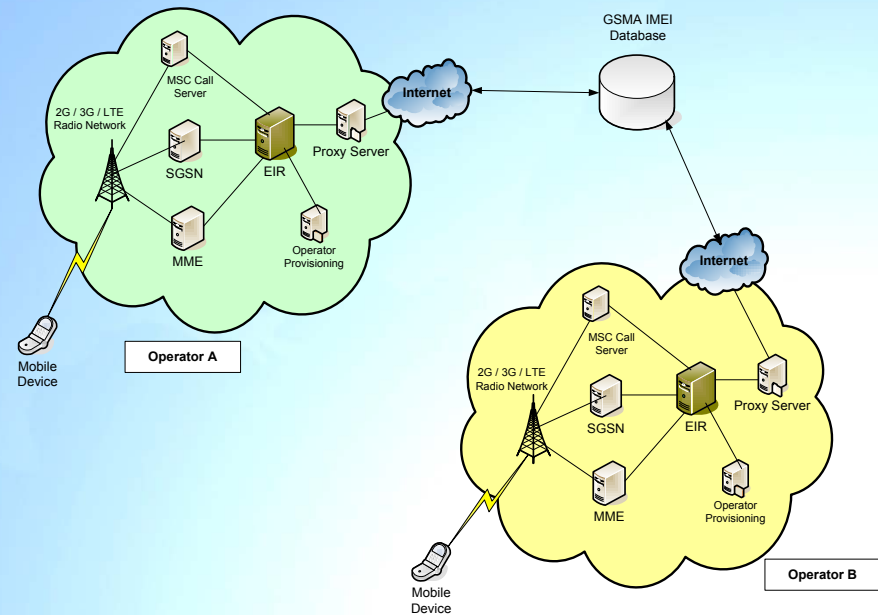
Task 3 Update – Database (continued)

- Equipment Identity Register (EIR) by a wireless operator is the most common network-based implementation to identify and prevent the use of stolen mobile devices
- EIR is a standards-based network infrastructure implementation that has been defined by the 3rd Generation Partnership Project (3GPP), the global standards development organization for the GSM family of technologies



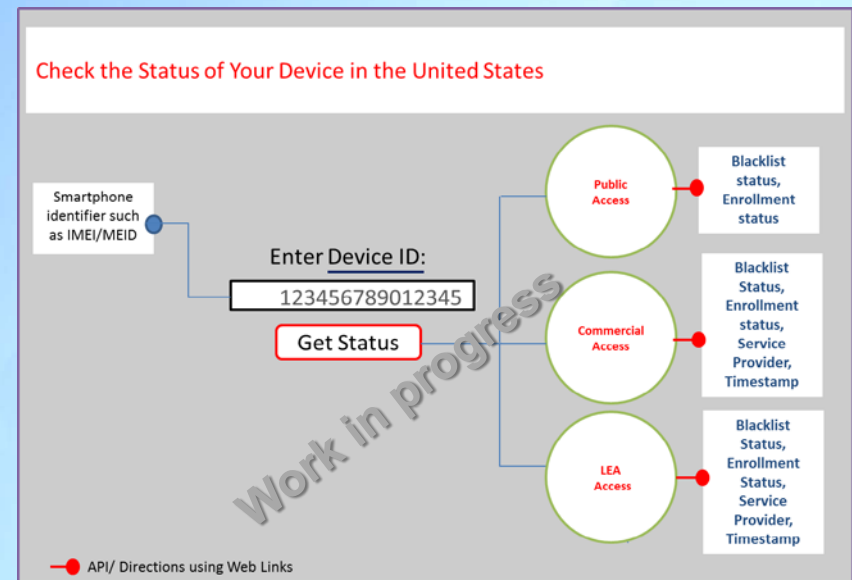
Task 3 Update – Database (continued)

- GSMA's IMEI/MEID Database is based on a data platform run and maintained by the GSM Association
- Designed to share stolen device data between network operators to enable them to prevent known stolen devices from being used on any operator network that subscribes to the Database and that has the necessary technology in place within its network to check for and deny service to blacklisted devices



Task 3 Update – Database (continued)

- Device Information Portal (Conceptual View)
 - Enables stakeholders to get information on how to determine the status of a device using a portal
 - Could be utilized as a platform to provide instructions on how to obtain information about a device and aggregate available device information across different solutions (GSMA, Operator, OEM platform, OS platform and other aggregators) to enable credible, synthesized information to all stakeholders in the mobile ecosystem



ATIS Best Practices for Obtaining Mobile Device Identifiers for MDTP

- ATIS standards effort resulting from TAC MDTP WG recommendation in December, 2014:
 - Recommendation 1.5: The FCC TAC recommends that ATIS in coordination with other appropriate industry groups (e.g., GSMA-NA Regional Interest Group) be tasked with developing standards, methods and procedures to obtain device identifiers from smartphones including those which are locked or rendered inoperable.
 - Expected out for ballot this month, and targeted for publication in October

ATIS Best Practices for Obtaining Mobile Device Identifiers for MDTP

- Device Disabled By Owner Initiated MDTP Procedures
 - Recommended that upon disabling of a mobile device the mobile device display screen show the device IMEI
- IMEI Display on Disabled or Locked Devices
 - Objective is to provide a method where access to the device IMEI does not require specific knowledge of a proprietary user interface
 - Examples could include:
 - When an emergency call is initiated from a device locked screen or a device disabled screen, a pre-call window (emergency dialogue box) appears asking the user if they really want to make an emergency call. In that dialogue box the IMEI can be displayed
 - The IMEI could always be displayed on the device locked or device disabled screen
- IMEI Display on Unlocked Devices
 - Enter `*#06#` into the mobile phone

GSMA-NA Device Blocking and Data Sharing Best Practices

- Document is under development, and will address:
 - **INSTALLATION OF NETWORK ACCESS CONTROL CAPABILITY**
 - EIR or a solution or process having the effect of EIR functionality
 - **ACCESS TO IMEI DATABASE**
 - Establish connections to access the IMEI DATABASE for the purposes of uploading and downloading Device identity data
 - **BLOCKING OF LOST AND STOLEN DEVICES**
 - Agreement on what devices are subject to network blocking i.e. anything with an IMEI
 - Blocking on network plus delivery of the IMEI to the IMEI Database to be placed on the GSMA Blacklist
 - Agreement on what to block – lost, stolen or lost and stolen
 - **EXCHANGE OF DATA ON LOST AND STOLEN DEVICES**
 - Investigating Blacklist entries to be submitted to the IMEI DATABASE on an hourly basis and Blacklist entries downloaded on an hourly basis.
 - **DATA FORMAT**
 - Ensure that the Data exchanged shall be in accordance with the requirements specified by the GSM Association

Preliminary Recommendations

- The FCC TAC recommends a deeper investigation by industry into the causal factors for the increase in consumer use of on-device solutions that could be used for determining how to optimize further efforts to incentivize greater consumer use of anti-theft features, if necessary
 - Recommend completion by EOY2015
- The FCC TAC recommends an industry-led investigation into whether the increased availability of anti-theft functionality on new smartphones, as well as the upcoming initial device setup prompts that will be required by California legislation after July 2015, have the effect of further increasing consumer use of these features.
 - Such a study should be undertaken after the July 1, 2015 date to allow for a sufficient number of devices with these features to have been placed into circulation
 - CTIA committed to include in its on-going consumer research investigation into adoption of anti-theft functionality

Anticipated Recommendations to the FCC Chairman

- Continued studies to determine whether implementations post July have the desired affect on mobile device theft
 - Refers to the planned recurring survey effort for continued monitoring of improvements
 - FCC should work with CTIA in defining survey
 - Better tracking of actual phones stolen – investigate as part of the MDTP working group task 3 deliverable
- FCC voluntary framework for a set of on-device capabilities to guide industry
 - Based on the “working group view” column of the Best Practices Template: Comparison of Anti-Theft Tools
- FCC to work with industry on developing effective outreach initiatives to educate the consumer
- Identify key technological areas where the FCC should seek further information from industry
 - IMEI
 - Requirements and Use of databases
 - Future theft prevention opportunities

MDTP Plan for Remainder of 2015 – Conclude Reports & Finalize Actionable Recommendations

- Task 1 - On-Device Theft Prevention Features Template
- Task 2 – Hardened Device Identifiers (IMEI)
- Task 3 – Database

BACKUP

Task 1 - On-Device Theft Prevention Features Template

- Password protection, Remote lock/wipe/restore functionality
- Most effective only if they are part of a package of practical solutions that consumers actually use, and today the majority of U.S. consumers don't
- WG asked to explore developing a proposed template approach that would ensure wider and easier use
- The template should cover:
 - A relatively uniform approach to these features (from the end user perspective) so that consumers do not need to re-educate themselves whenever they change devices
 - An “automatic on” approach, or something similar, under which consumers can set up a new device only if they select a screen-saver password (whether digits, biometric, or something else) and activate lock/wipe/restore features
 - A feature making it easier for consumers to report thefts to providers and/or police, including reporting the device's IMEI
 - General consideration of the implications of Wi-Fi only connectivity.

Task 2 - Hardened Device Identifiers (IMEI)

- Reliable IMEIs are critical not only for theft prevention, but also for improving the integrity of the wider provisioning system that uses the identifiers
- GSMA and 3GPP have begun discussions in this area, we need more urgency
- The WG was asked to assess rapidly whether there are any constraints that would prevent 3GPP and/or GSMA from developing a standard for a hardened IMEI by the end of this year
 - Note it is recommended that the WG work through ATIS as the North American 3GPP Organizational Partner

Task 3 - Database

- The WG is asked to study database systems that effectively track stolen items (phones, cars, funds) and develop a spec sheet for an effective stolen phone database that might be focus on North America
- GSMA already hosts a configurable stolen phone database which is facilitating pan operator blocking and information distribution. There is an opportunity for ecosystem participants to make greater use of this resource through optimized configuration and adoption
- The WG should finalize the proposed spec sheet by October 1

Cybersecurity Working Group

Chairs: Shahid Ahmed, Paul Steinberg
Vice Chair: Ramani Pandurangan
FCC Liaisons: Jeffery Goldthorp, Padma Krishnaswamy,
Ahmed Lahjouji

24-September-2015



Working Group Members

- WG Chair: Shahid Ahmed, Accenture / Paul Steinberg, Motorola Solutions
- Vice Chair: Ramani Pandurangan, XO Communications
- FCC Liaisons: Jeffery Goldthorp, Ahmed Lahjouji, Padma Krishnaswamy
- Members:
 - John Barnhill, Genband
 - Mark Bayliss, Visualink
 - Nomi Bergman, Brighthouse
 - Mike Bergman, CEA
 - John Brzozowski, Comcast
 - Ken Countway, Comcast
 - Brian Daly, AT&T
 - Renato Delatorre, Verizon Wireless
 - John Dobbins, Earthlink
 - Martin Dolly, AT&T
 - Dale Drew, Level 3 Communications
 - Adam Drobot, Open Tech Works
 - Amit Ganjoo, Ocusnetworks
 - Dick Green, Liberty Global
 - Craig Greer, Samsung
 - Russ Gyurek, Cisco
 - Theresa Hennesy, Comcast
 - Farooq Kahn, Samsung
 - Dr. Prakash Kolan, Samsung
 - Tom McGarry, Neustar
 - Paul Misener, Amazon
 - Jack Nasielski, Qualcomm
 - George Popovich, Motorola Solutions
 - Katrin Reitsma, Motorola Solutions
 - Christoph Schuba, Ericsson
 - S Rao Vasireddy, Alcatel Lucent
 - Jack Waters, Level 3 Communications
 - Brian Witten, Symantec
 - David Young, Verizon Wireless
 - Lim Youngkwon, Samsung



Agenda

- **Summary**
- **Working Group Reports**
 - 1. Simplifying Smartphone Security**
 - A. Requirements for Consumer-friendly Interface/Wizard for Security Configuration (Leaders: Martin Dolly, Renato Delatorre)**
 - B. Requirements for Smartphone Security Checker (Leaders: Amit Ganjoo, Katrin Reitsma)**
 - 2. Applying security to IoT Consumer Products (Leaders: Tom McGarry, George Popovich)**
 - 3. Securing SDN (Leaders: Ramani Pandurangan, Rao Vasireddy)**

1. Simplifying Smartphone Security

(1a: Requirements for Consumer-friendly Interface/Wizard for Security Configuration)

- **Scope and Approach**

- Proposed scope/direction
- Develop platform agnostic baseline security controls, recommended settings and common vernacular for reporting on device security and application permissions.

- **Key actionable deliverables**

- Step 1: Options (low hanging fruit) to connect the published security questions (CAC) published online into the mobile experience (not automation)
- Step 2: Requirements for a 'wizard' approach to facilitate mobile device security configuration for users

- **Contributors**

- Brian Daly, AT&T
- Martin Dolly, AT&T
- Renato Delatorre, Verizon
- Amit Ganjoo, Oceusnetworks
- Dr. Prakash Kolan, Samsung
- Katrin Reitsma, Motorolasolutions
- Lim Youngkwon, Samsung



1. Simplifying Smartphone Security

(1a: Requirements for Consumer-friendly Interface/Wizard for Security Configuration)

- Recommendations Summary *(Final)*

- Recommendation 1: Follow up with other key stakeholders

- Device Vendors – Samsung, Sony, HTC, Apple, LG, etc.
- Mobile OS representation – Google / Android, Apple / iOS, RIM / Blackberry, Microsoft / Windows Phone, alternative mobile OSs – e.g. FireOS, Sailfish, Firefox OS, Ubuntu, Tizen
- Carriers – AT&T, Verizon
- Security Solution providers – Lookout, NQMobile, Symantec, Intel
- Device OEMs– Broadcom, AMD, Qualcomm, TI, Freescale, Marvell



Agenda

- **Summary**
- **Working Group Reports**
 - 1. Simplifying Smartphone Security**
 - A. Requirements for Consumer-friendly Interface/Wizard for Security Configuration (Leaders: Martin Dolly, Renato Delatorre)
 - B. Requirements for Smartphone Security Checker (Leaders: Amit Ganjoo, Katrin Reitsma)
 - 2. Applying security to IoT Consumer Products (Leaders: Tom McGarry, George Popovich)**
 - 3. Securing SDN (Leaders: Ramani Pandurangan, Rao Vasireddy)**

1. Simplifying Smartphone Security

(1b: Requirements for Smartphone Security Checker)

- **Scope and Approach**

- Derive and document requirements and development guidelines for a security checker application. The app helps consumers to configure security settings on their personal smartphones in a quick and user-friendly way according to best industry practices and reflecting individual security needs . The app is first launched during device setup and can be re-visited to make changes to security settings or view the current security status of the device.
- Target audience is FCC and OS vendors as well as any party involved in the development, provisioning/hosting, and maintenance of the security checker app

- **Contributors**

- Amit Ganjoo, Oceus Networks
- Katrin Reitsma, Motorola Solutions
- Alex Abey, Lookout
- Andrew Hoog, Now Secure
- Andy Banks, Citrix
- Youngkwon Lim, Samsung
- Martin Dolly, AT&T
- Renato Delatorre, Verizon



1. Simplifying Smartphone Security

(1b: Requirements for Smartphone Security Checker)

- Key Findings

- app launched during initial on boarding and can be revisited later (both to modify security configurations or view the current device security status)
- Two possible app architectures 1) fully native or 2) client/server
- Intro questionnaire desirable for exploring user's security needs
 - results used by security checker to recommend configurations
 - proposed design guidelines should be followed to ensure a good user experience (leading to a wider user adoption)
- Use 4-tier security levels (no/low/medium/high) for easier/faster configuration as well as easier overview of current device security status
 - OS-based and 3rd-party security features
 - enforceable security features can be configured by app
 - non-configurable security features; status can be viewed in the app
 - we provide examples for each level for every covered security feature
 - app calculates security score and expose it to other apps using underlying OS communication framework



1. Simplifying Smartphone Security

(1b: Requirements for Smartphone Security Checker)

- **Recommendations Summary for FCC** *(Proposed)*
 - Recommended immediate actions:
 - Get mobile OS vendors involved for feedback and help with the execution & deployment of the security checker app
 - Recommended next steps:
 - Recommend a focus group to develop an intro questionnaire and derive more detailed guidelines e.g., based on user research, in terms of what would be an acceptable user experience for various security levels (none, low, medium, high). This approach will decrease the initial setup time and improve overall user experience
 - Form group to investigate whether recommendations are technically feasible, i.e., can be supported by considered mobile OS versions
 - Define a vetting process for entities to become trusted app stores.
 - Implement a two pronged approach, 1) a security checker and 2) a web based or native app acting as an educational tool which is constantly refreshed with latest recommendations
 - Create a validation team to ensure design guidelines and security requirements as outlined in this document are met



1. Simplifying Smartphone Security

(1b: Requirements for Smartphone Security Checker)

- **Recommendations Summary for Mobile OS Vendors** *(Proposed)*
 - This section summarizes suggestions for mobile OS vendors that would allow for a more effective security checker
 - For a better user experience for security conscious end users, automatic app updates should come with an option, such that end users are only prompted when an app update requests additional permissions.
 - Assist with the development & deployment of the security checker app, by enabling the security checker to 1) access the status of the security settings and features listed in this document and 2) expose a security score (or something similar) that app developers can use and leverage to control app behavior without the need to create new APIs
 - If not already supported, OS vendors should incorporate FIPS compliant crypto libraries on the device
 - If not already supported, enable users to select whether they want to share GPS or cellular/WiFi network based location information as separate items



1. Simplifying Smartphone Security

- **Deliverables**

- 1a: Final Wizard Requirements
 - Draft (limited circulation): September 24, 2015 (complete)
 - Final version imminent (contingent upon CAC engagement)
- 1b: Report with App Requirements & Design Guidelines and Final Recommendations
 - Draft (limited circulation): September 24, 2015 (complete)
 - Final version including agreed upon recommendations (due Dec 2015)



1. Simplifying Smartphone Security

- **Discussion Topics / Issues**

- Lack of Mobile OS vendor engagement
- Identification of a sustainable business model and suitable partners for the development, deployment and maintenance of the wizard and security checker
- Collaboration with the CAC to design the ‘front end’ User-Friendly questions that drive the wizard and security checker configuration



Agenda

- **Summary**
- **Working Group Reports**
 1. **Simplifying Smartphone Security**
 - A. **Requirements for Consumer-friendly Interface/Wizard for Security Configuration (Leaders: Martin Dolly, Renato Delatorre)**
 - B. **Requirements for Smartphone Security Checker (Leaders: Amit Ganjoo, Katrin Reitsma)**
 2. **Applying security to IoT Consumer Products (Leaders: Tom McGarry, George Popovich)**
 3. **Securing SDN (Leaders: Ramani Pandurangan, Rao Vasireddy)**

2. Applying Security to Consumer IoT Devices

• Scope and Approach

- The WG will examine the special cybersecurity challenges posed by the emerging Internet of Things, and suggest actionable recommendations to the FCC with particular focus on the security and protection of IoT consumer products.
- WG 2015 phasing
 - Q2: IoT security initiatives industry scan
 - Q3: Gap analysis, recommendations preview, and progress on the categories of **1) communication networks, 2) IoT devices, 3) best practices**
 - Q4: Recommendations addressing the takeaways and identified gaps from the Q3 update

• Contributors

- Mike Bergman, CEA
- John Brzozowski, Comcast
- Renato Delatorre, Verizon Wireless
- Martin Dolly, AT&T
- Craig Greer, Samsung
- Russ Gyurek, Cisco
- Tom McGarry, Neustar (co-lead)
- George Popovich, Motorola Solutions (co-lead)
- Christoph Schuba, Ericsson
- Brian Witten, Symantec
- Peter Davis, Neustar



2. Applying Security to Consumer IoT Devices

- Work breakdown

- In order to run in parallel to address the FCC's questions around IoT security, the IoT team has broken up into 3 sub-teams
 - The **communications networks** team will look to address the FCC's question around the underlying technologies for IoT, along with their vulnerabilities and challenges
 - The **devices** team will focus on the state of the art and gaps around IoT device security, including any technical solutions that help with resource constrained IoT devices
 - The **best practices** team will continue to build our understanding of the state of the industry on how stakeholders are looking to address IoT security concerns



2. Applying Security to Consumer IoT Devices

• Status on the FCC's questions around IoT security

1. What are the underlying technologies (e.g., WiFi, ZigBee, GPRS, LTE) that dominate the IoT space? and what security vulnerabilities and challenges do they present in the IoT environment?
 - **In process within the communications networks team** – some technologies have been looked at in more detail than others – see the IoT communications networks matrix slide in the appendix as a representation of our status
2. What other security challenges face IoT consumer products? For example, to what extent does lack of physical security pose a threat to unsupervised IoT devices? Explain.
 - **In process across all 3 IoT security teams** – we list our current take on security challenges on the “key findings” slide. We are also in the process of leveraging the information from the Cloud Security Alliance IoT team (who recently joined our TAC WG)
3. What is the industry doing to secure and protect battery-operated and resource- constrained (i.e., minimum computing power and memory) M2M devices, which cannot encrypt its data?
 - **We are finding examples of progress within the devices team effort** – some examples of lower-resource IoT nodes have been identified, and it is also suggested that resource issues will be alleviated over time with technology advances (Moore's Law).
Examples - devices like <http://www.ti.com/product/cc430f5137> and battery saving LoRa (Long Range) equipped devices
4. How are the IoT/M2M stakeholders addressing those security challenges and vulnerabilities, and what are the gaps?
 - **We are nearly complete on the best practices front**, but still need more study on devices – we do see industry momentum toward addressing common security gaps but challenges remain. See the “key findings” and “best practices” slides for details.
5. What is the potential impact of these security challenges on the future of IoT/M2M industry, the end user and the economy, especially when IoT devices become fully integrated in all of our systems, including our critical infra.?
 - **In process – TBD, likely challenging to list out all the potential impacts. We still have much thinking to do on this question.**
6. What role could the FCC play in facilitating positive changes in the security, privacy and resiliency of M2M/IoT devices and systems?
 - **In process – We are currently wrestling with the concept of an industry led IoT security certification program in an attempt to raise the security bar through voluntary industry actions.**



2. Applying Security to Consumer IoT Devices

- Key findings thus far

- There are numerous IoT related industry consortiums, but many are early in their charters and thus have not produced publically available security standards or specifications
- It is clear that IoT-type devices are being compromised through multiple paths—the attackers have gotten ahead of the defenders. However, industry is increasingly treating security as a priority, and producing security-hardened devices, communications links and lifecycle best practices.
- There is no current industry certification program for IoT security
 - Something like a “UL certification” for consumer IoT could bring about greater motivation for vendors to provide minimal sets of security capabilities. *The value of such a program is currently being debated within the sub-group.*
 - There is some recent movement in this space.
 - In July it was revealed the White House is working with Underwriters Laboratories on a IoT security certification program (<http://www.darkreading.com/endpoint/underwriters-laboratories-to-launch-cyber-security-certification-program/d/d-id/1321202>)
 - The Open Interconnect Consortium and the Online Trust Alliance have both expressed interest in IoT security certification programs as well.



2. Applying Security to Consumer IoT Devices

- **Deliverables:** Status around our analysis of IoT related communications networks and protocols
 - FCC Question - What are the underlying technologies (e.g., WiFi, ZigBee, GPRS, LTE) that dominate the IoT space? and what security vulnerabilities and challenges do they present in the IoT environment?
 - Evaluated the following wireless technologies
 - Mobile/WAN – LTE, GPRS, UMTS, CDMA
 - WAN – LoRaWAN, Weightless-N/W
 - LAN – 802.11, 802.15.4, ZigBee, Thread, Z-Wave, 6LoWPAN, Sigfox
 - PAN – Bluetooth, Bluetooth LE, NFC, WAVE (1609), ANT/ANT+, DASH7
 - Identify responsible organization
 - Notes on the technology and organization
 - Identified security issues



2. Applying Security to Consumer IoT Devices

IoT Communication networks – preliminary findings summary

- Most technologies are managed by membership organizations
 - Therefore it is difficult to identify actual security requirements and capabilities
 - Some are well known with strong TAC member expertise
 - Many are not well known with little to no TAC member expertise
 - However some of these have publicly known security issues
 - IETF 6LoWPAN is only publicly available spec
- Most specs allow for various implementations
 - For example, they could allow for different types of encryption, some stronger than others
 - Backwards compatibility may allow for technologies with known security issues
- Recommendation to FCC will be the best security practices for:
 - Confidentiality – preventing unauthorized use of or disclosure of information
 - Integrity – safeguarding accuracy and completeness of information
 - Authentication – confirming the user's (device's) identity

2. Applying Security to Consumer IoT Devices

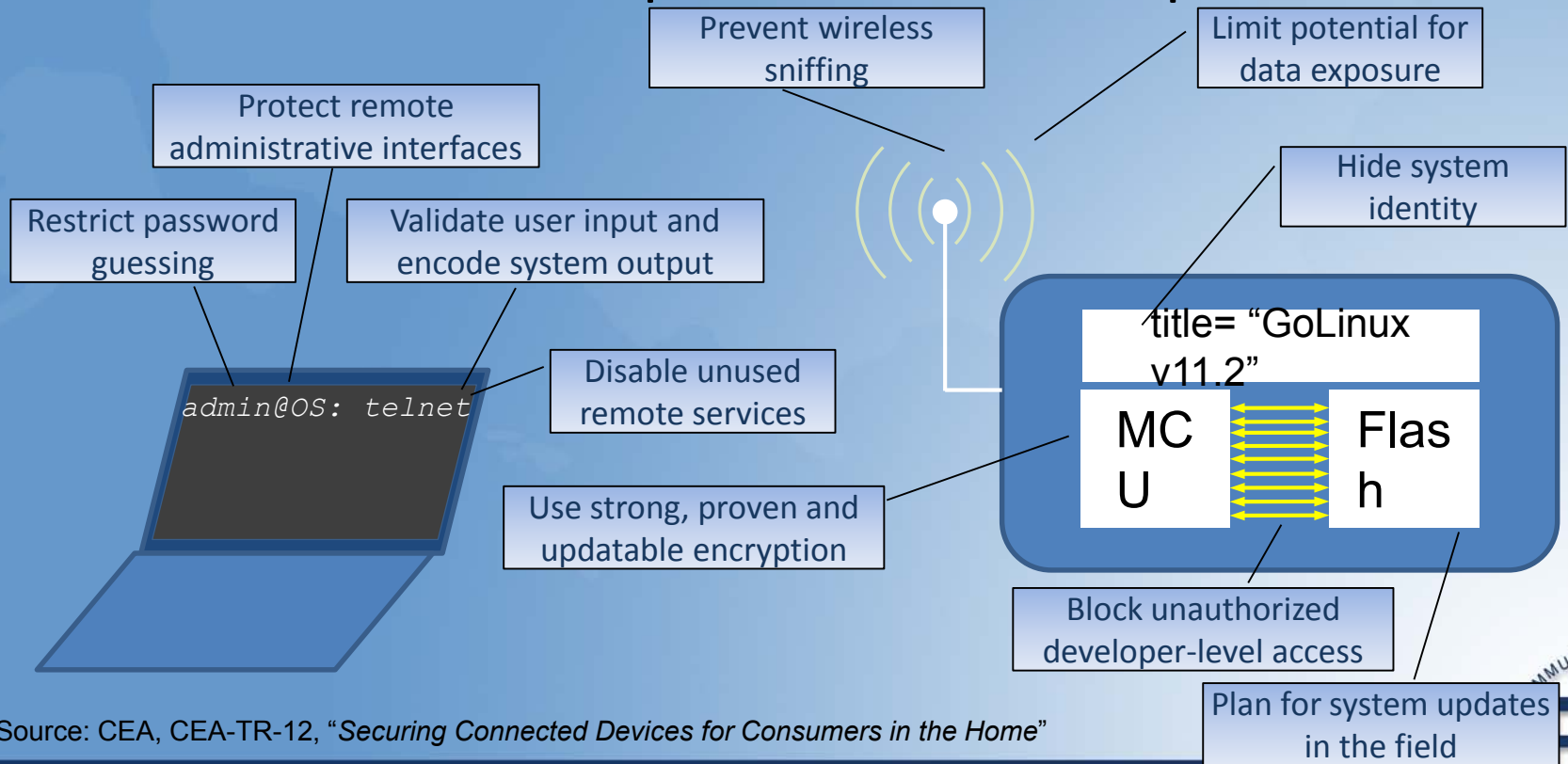
IoT Devices – preliminary findings summary

- Security-Hardened Device Architectures
 - For low-level systems (sensors, controls, other single-function elements)
 - Currently limited in resources
 - There are best practices with existing systems
 - Moore's Law will help over time
 - For OS-capable systems (web cams, smart TVs, routers)
 - Security is increasingly a priority
 - Suppliers are hardening the OS and chip levels (32-, 64-bit SoC's)
 - Security-hardened solutions are available



2. Applying Security to Consumer IoT Devices

Best Practices: Developer Actions For Improved Security



Source: CEA, CEA-TR-12, "Securing Connected Devices for Consumers in the Home"



2. Applying Security to Consumer IoT Devices

IoT security best practices – preliminary findings summary

- When examined as a whole, the landscape of the most popular “best practices” documentation provides very good coverage across a large scope of security topics
- The CSA IoT Guidance paper stands out due to its broadness of scope (covers processes as well as technologies), therefore **we are starting collaboration efforts with CSA IoT members for our TAC WG**
- We are on the lookout for additional best practices references for IoT device security, especially when addressing challenges around resource constrained devices



2. Applying Security to Consumer IoT Devices

- Contentious discussions Summary

1. At this point we have been unable to reach consensus around any preliminary recommendations
2. We are currently studying the pros and cons of a recommendation around an industry led IoT security certification program. The study items for this could include:
 1. Determining what are the key technical cyber issues to contemplate for consumer IoT (a purely technical study aligned with the spirit of the TAC)
 2. Examining existing testing/certification mechanisms as potential examples of how such a certification program could be orchestrated (e.g. from voluntary to an open source project to some form of industry group)
 3. Looking for opportunities to engage more industry stakeholders
3. We are soliciting clarification from the rest of the TAC and the FCC on how best to proceed and to spend our energy in the last quarter.



Agenda

- **Summary**
- **Working Group Reports**
 - 1. Simplifying Smartphone Security**
 - A. Requirements for Consumer-friendly Interface/Wizard for Security Configuration (Leaders: Martin Dolly, Renato Delatorre)**
 - B. Requirements for Smartphone Security Checker (Leaders: Amit Ganjoo, Katrin Reitsma)**
 - 2. Applying security to IoT Consumer Products (Leaders: Tom McGarry, George Popovich)**
 - 3. Securing SDN (Leaders: Ramani Pandurangan, Rao Vasireddy)**

Definition: Topic 3 – Securing SDN/NFV

Questions:

1. What are the key security challenges that SDN architectures present? And how is the telecom industry addressing them?
2. What measures could be employed to make networks deploying SDN applications resilient and secure?
3. What is the trust model that should be applied between devices and controllers, and between controllers?
4. What, if any, high-assurance approaches may apply to SDN?
5. What specific lessons can we extract from the long running efforts to secure existing control plane protocols -- such as BGP and DNS – to benefit SDN-based networks?
6. What are the pros and cons of embedding security within the network, as opposed to embedding it in servers, storage and other computing devices?
7. What are the strengths and weaknesses of Software Defined Security (SDSEC)?
8. What role could the FCC play in facilitating positive changes in the security, privacy and resiliency of SDN?



Securing SDN/NFV – Approach

- As the industry’s adoption is still evolving there may not be a set of established practices but will capture the industry landscape with respect to security challenges and opportunities
- Conduct research using industry resources (vendors, SPs, SDOs, Communities)
- Consulted 10 industry practitioners to date - SDN / NFV Security SMEs from vendors and communities (e.g. OPNFV, OpenDayLight) - see slide “Consulted Industry Practitioners”
- Leverage the architecture work done by FGCT Architecture group on SDN / NFV
- Contributors
 - Ken Countway, Comcast
 - Brian Daly, AT&T
 - Martin Dolly, AT&T
 - Mike Geller, Cisco
 - Dr. Prakash Kolan, Samsung
 - Padma Krishnaswamy, FCC Liaison
 - Ahmed Lahjouji, FCC Liaison
 - Ramani Pandurangan, XO Communications (Lead)
 - Christoph Schuba, Ericsson
 - S Rao Vasireddy, Alcatel Lucent (Co-lead)

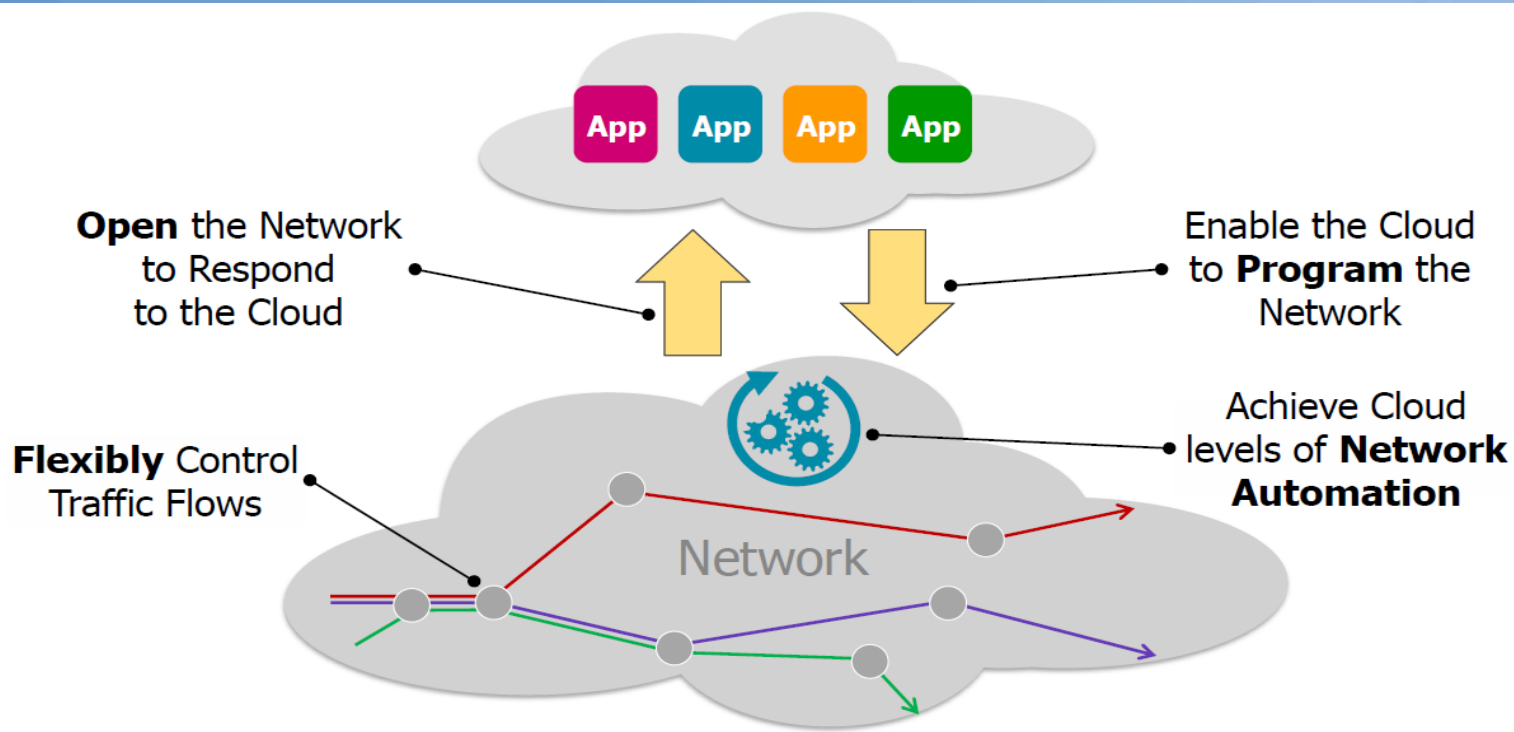


Securing SDN/NFV - Deliverables

- **September 2015**
 - Status of SDN / NFV in the Industry as researched by the SWG and as provided by speakers from 10 industry and standards organizations.
 - Gathered information on SDN TAC questions 1 through 7.
 - Identified challenges and opportunities
 - This presentation summarizes work to date
- **December 2015**
 - Final report and recommendations
 - White Paper



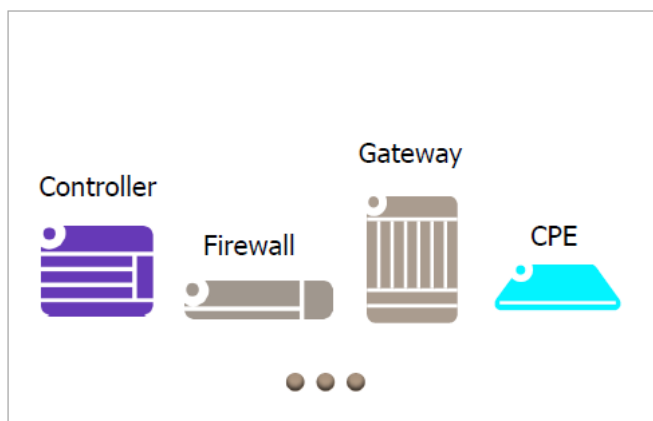
Software Defined Networking (SDN)



Making the network programmable and adaptive to applications

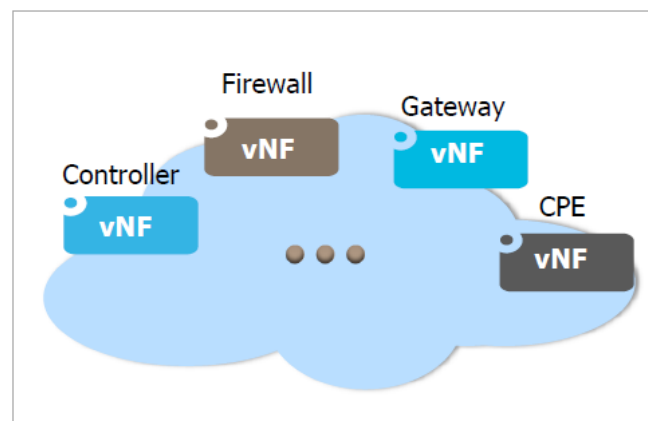
Source: Kevin Sparks, TAC FGCT Architecture

Network Function Virtualization (NFV)



Specific appliance/hardware for each network function

NFV



General purpose x86 server hardware for one or more virtualized network functions

Scalability ++

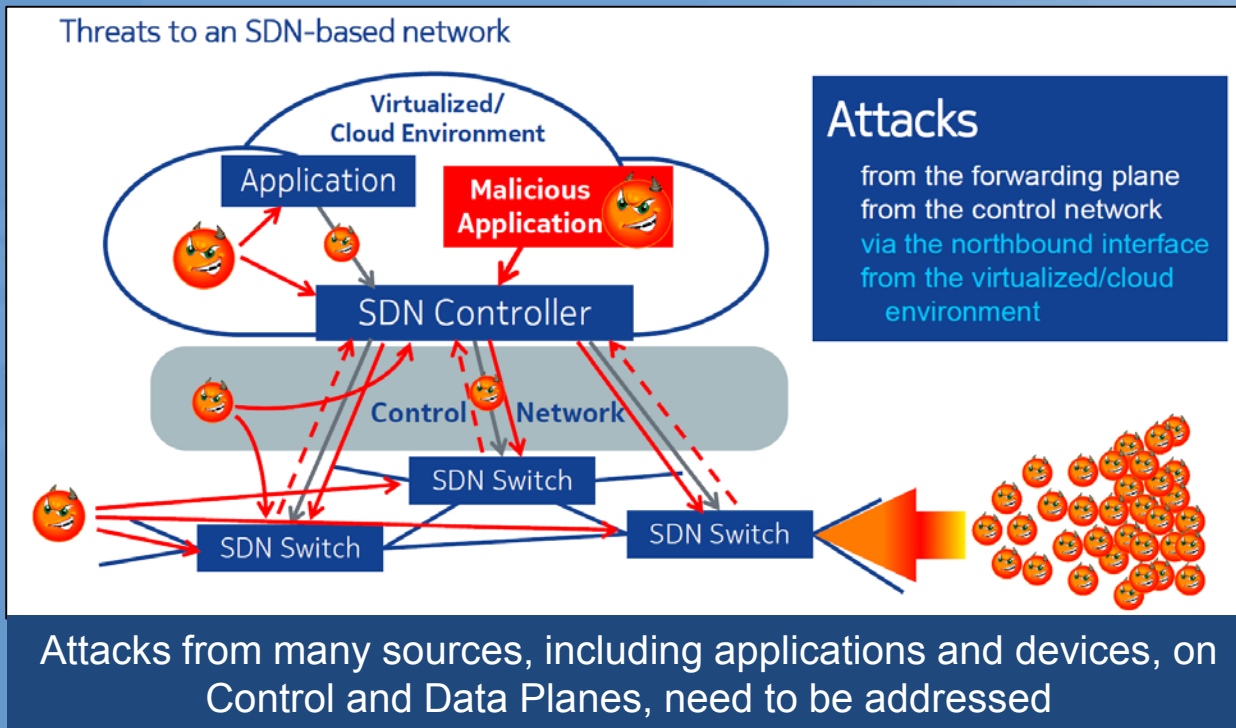
Adaptability ++

Economics ++

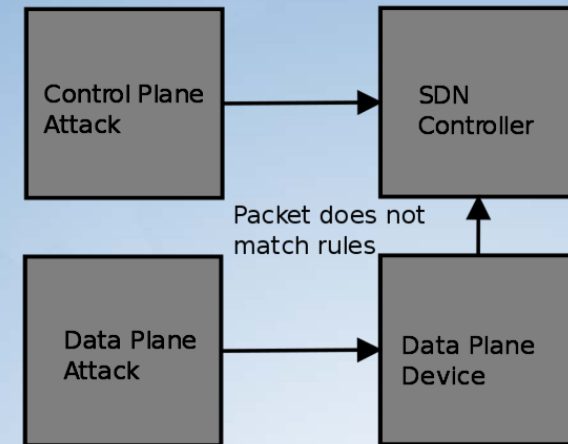
Source: Kevin Sparks, TAC FGCT Architecture



SDN/NFV Security Challenges



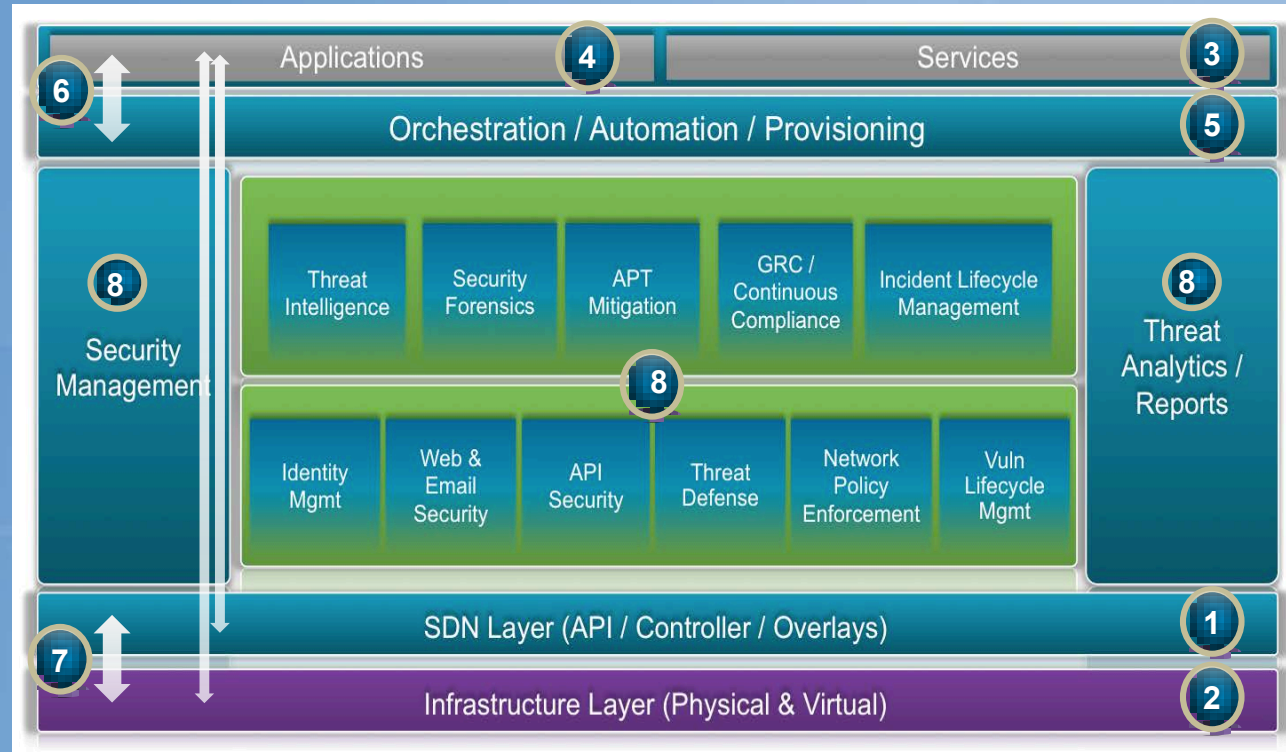
Source: Peter Schneider, Nokia



Source: David Jorm, Open DayLight

Multiple Layers of Security for the SDN

1. Securing Controller
2. Securing Infrastructure
3. Securing Network Services
4. Securing Application
5. Securing Management & Orchestration
6. Securing API
7. Securing Communication
8. Automation of Security Technologies



Source: Mike Geller, Cisco



SDN / NFV Challenges and Opportunities (1/3)

SDN/NFV Attribute	Challenges	Opportunities	Possible security approaches
Logical centralization of Control 1. Controller 2. Infrastructure 3. securing network services	Single target of high value <ul style="list-style-type: none"> successful attack can impact the entire network under control span of the controller. may be taken over by the attackers; attack can come from devices, applications, into controllers or through communication channel Resiliency and scaling challenges potentially impacting availability 	<ul style="list-style-type: none"> Centralization enables network level control and optimization resulting in: scalability, flexibility and cost savings. Dynamic control of resources can enable flexible security architecture Effective security measures for centralized networking assets. 	Architecture options for Controller and underlying OS security: <ul style="list-style-type: none"> Active / active, active / standby, clustering, geo-redundancy deployment alternatives available Limited scope with federation may be possible Network elements may be designed to operate with the last-good-state if controllers are down
Disaggregation - Separation of control and data planes 1. Controller 2. Infrastructure 4. Applications 5. Management & orchestration 6. API 7. Communications	Increases attack surface; <ul style="list-style-type: none"> multiple devices need be protected; communication channels and protocols must be secured a compromised device may attack SDN controller State of device security is non static; a compromised device may remain undetected In Telemetry, compromised device may send false or fabricated data to the SDN controller; securing telemetry presents a significantly harder challenge* 	<ul style="list-style-type: none"> Each layer can scale and evolve independently; provides vendor independence to SPs. 	Security for application s, underlying platform, orchestration, automation and Provisioning: <ul style="list-style-type: none"> Clearly Define Security Dependencies and Trust Boundaries, Assure Robust Identity, Build Security based on Open Standards, Protect the Information Security Triad – Confidentiality, Integrity and Availability (CIA), Protect Operational Reference Data, Make Systems Secure by Default, Provide Accountability and Traceability

* Source: Dr. Kireeti Kompella, CTO, JDI, Juniper



SDN / NFV Challenges and Opportunities (2/3)

SDN/NFV Attribute	Challenges	Opportunities	Possible security approaches
<p>Abstraction - Programmability</p> <ul style="list-style-type: none"> 1. Controller 2. Infrastructure 5. Management & orchestration, 8. Automation of Security Technologies 	<p>Abuse of control functions, exploiting vulnerabilities, compromising controllers. Semantic consistency between messages to a single device may be solvable; Semantic consistency between messages among multiple devices is harder to solve*</p>	<ul style="list-style-type: none"> ○ Facilitates deployment of agile, fine-grained security solutions running as applications and Software Defined Security approaches 	<p>Securing of all communication (Northbound, Southbound, East - West) channels and messages; Authentication between communicating entities, continuous attestation, not just at the time of spawning, of functions, audits and anomaly detection may be needed . Multiple layers of security would be needed</p>
<p>Multiple Trust Domains</p> <ul style="list-style-type: none"> 1. Controller 2. Infrastructure, 5. Management, & orchestration 8. Automation of Security Technologies 	<p>New types of threats arise due to the explicit programmatic access SDN offers to clients that are typically separate organizational or business entities. Not unique to SDN is the fact that insiders represent a significant security threat, and that operator error threatens system integrity</p>	<ul style="list-style-type: none"> ○ Provides openness to allow customer self-service and different business models 	<p>Requires strong authentication and robust security at all interfaces. Should include strong identity and credential management functions that secure all entities and their associated state.</p>

* Source: Dr. Kireeti Kompella, CTO, JDI, Juniper



SDN / NFV Challenges and Opportunities (3/3)

SDN/NFV Attribute	Challenges	Opportunities	Possible security approaches
<p>Virtual Network Functions (VNF) running in virtual machines and replace / supplement physical network functions</p> <ul style="list-style-type: none"> 2. Infrastructure 3. securing network services 4. Applications 8. Security Technologies 	<p>Union of generic threats from virtualization / cloud, threats specific to previous physical network functions and new threats from the combination</p>	<p>Provides elastic capacity and automated provisioning. Service Chaining allows micro services to be properly sequenced to provide great flexibility and granularity and as and when needed; operating efficiencies and rapid service innovation. Recognizing the need for more holistic solution, Server / Endpoint security vendors are integrating with Network Security vendors by correlating network and server / endpoint threat data</p>	<p>Best Current practices of cloud (e.g. NIST, CSRIC, CSA, previous work of TAC) available. TPM and Virtual TPM for higher level of assurance. Trusted Computing practices start being used in commercial shipments ; expected to become more common in the future (e.g. Trusted Platform Module (TPM) chip on HP-UX Integrity servers, Intel Trusted Execution Technology (TXT), industry is also developing Virtual TPM for virtualized environment. It is not either network security or security embedded in hosts / servers; both are needed; significant work ongoing in ETSI – see GS NFV-Sec documents</p>
<p>Use of Open Source</p> <ul style="list-style-type: none"> 8. Security Technologies 	<p>Being open source subject to attack</p>	<p>The more participants examine the code, the faster will the vulnerabilities be detected and fixed. Several vendors are enhancing Open Source and making them more rugged.</p>	<p>Carrier grade , including security, is work in progress in the various communities. Community is working on security areas (e.g. OpenStack Trusted Compute Pools); significant work ongoing in ETSI – see GS NFV-Sec documents</p>

Securing SDN/NFV – Summary of Findings

- SDN is an evolving technology and several innovations are occurring at a fast clip.
- So far, SDN has been deployed only in specific applications/ use cases such as data centers, WAN connecting data centers ; All the more reason to build-in security now instead of bolting-on security into a massive installed base
- Key attributes of SDN open up new threat surfaces and challenges, and also opportunities
- Industry recognizes that SDN/NFV increases threat surface; as industry gains more deployment experience supplemental security and new strategies may be needed beyond what has been learnt from building and operating existing networks. Industry is working on
 - adoption of bidirectional device – controllers – applications authentication *
 - forums and standards starting to address issues and promote awareness
- What is under discussion in the SWG
 - Develop use cases
 - Create SDN/NFV security best practices and recommendations



Appendix 1

(Simplifying Smartphone Security)

Definition: Topic 1 - Simplifying Smartphone Security

Today, configuring a device to minimize security and privacy risks can be can be confusing and requires consumer education so that the impacts are not well understood by most consumers. Last year, the Commission asked the Consumer Advisory Committee to recommend a series of questions that could be presented to consumers by way of their smartphones. The answers to these questions would be used by an app resident on the device to configure the device's security and privacy settings to the user's liking. We originally had in mind that the Smartphone Security Checker could be a platform for presenting the questions to users, but we have turned our attention to apps produced and on the market. We recommend that the TAC be asked to provide us with a set of recommended generic requirements that we could seek comment on, thereby promoting the availability of features in such apps that converge on a set of common security and privacy concerns.

1. Simplifying Smartphone Security

(1b: Requirements for Smartphone Security Checker)

- **Appendix A: Covered Security Features**
 - Screen lock mechanisms & Screen lock timeout
 - Security Policy Updates & Automatic App Updates & OS Updates
 - Disk Encryption & SD Card Encryption
 - WiFi, Bluetooth, NFC
 - Remote Lock, Wipe, Locate and Alarm (LWLA)
 - Developer Mode
 - Portable WiFi Hotspot
 - Access to Location Information
 - Locking bootloader
 - Malware Protection
 - root/jailbreak status

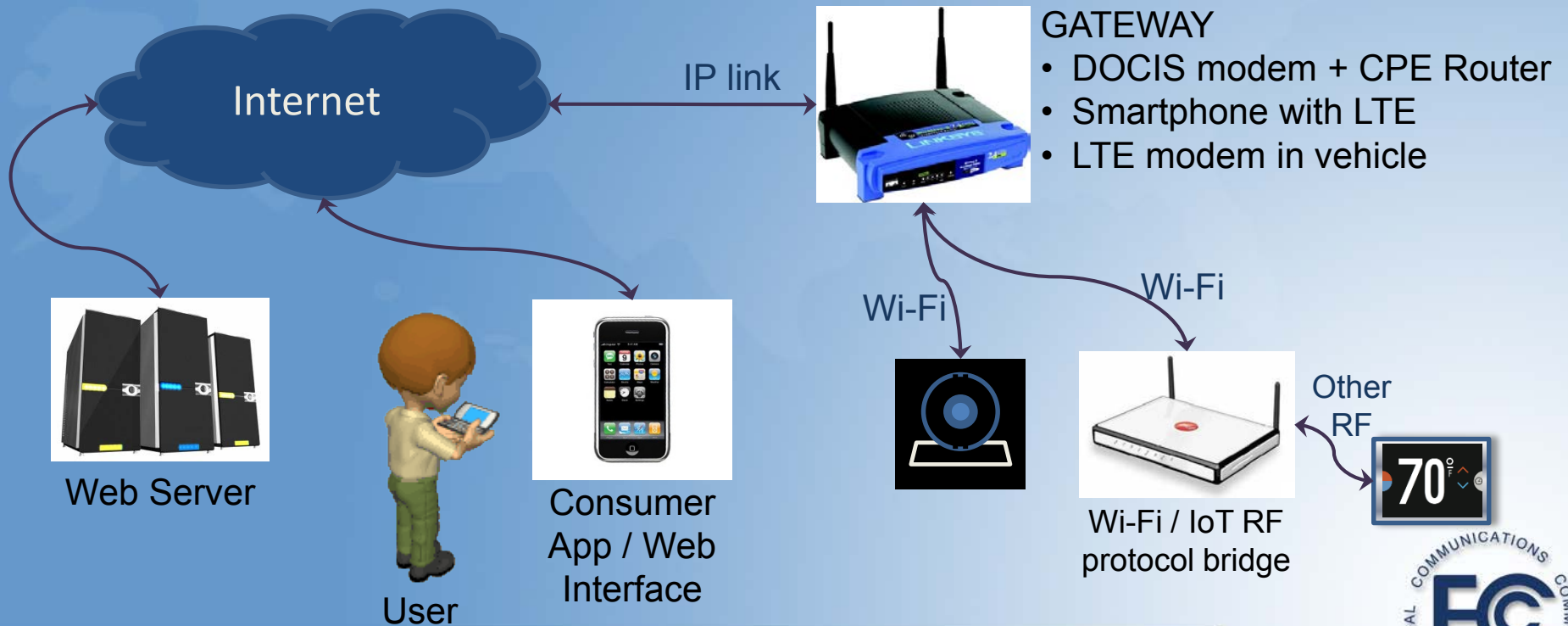


Appendix 2

(Applying Security to IoT Consumer Products)

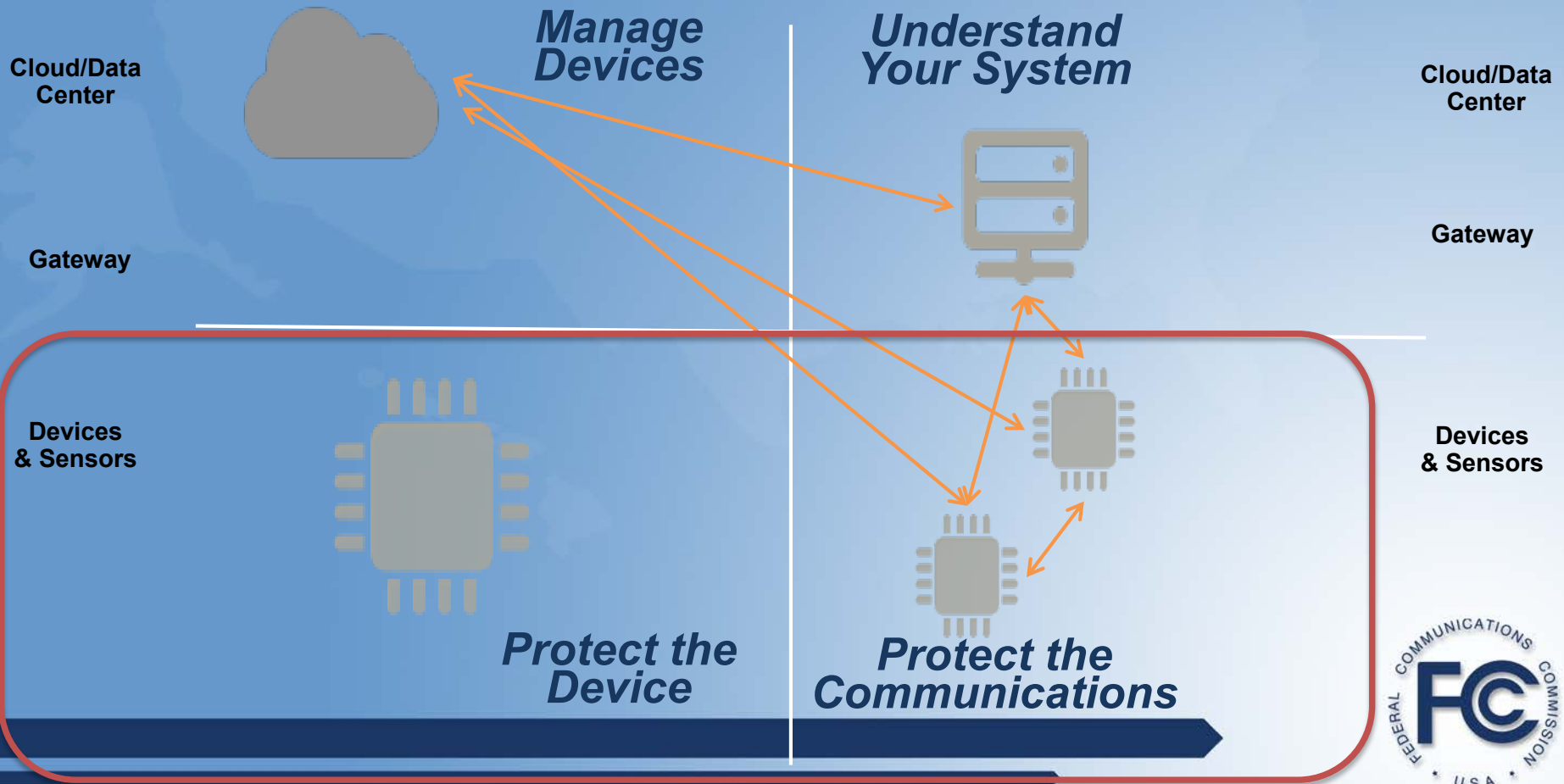


Examples of IoT In Use



Cornerstones of Security for the Internet of Things (IoT)

IoT Security Reference Architecture



Work in progress communication network analysis

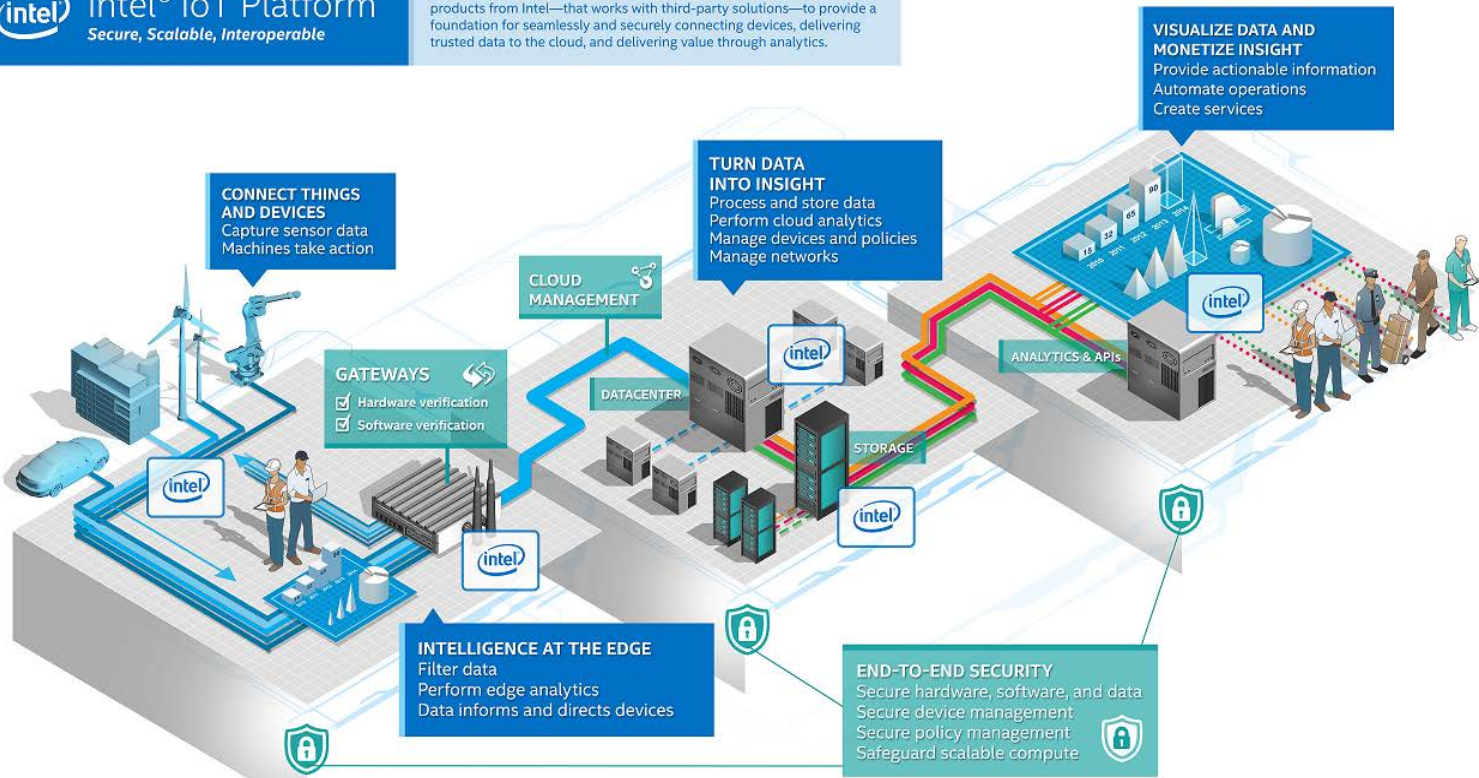
Technology	Organization	Category	Note	Known Security Gaps
LTE	3GPP	Mobile/WAN		
GPRS	3GPP	Mobile/WAN		
UMTS	3GPP	Mobile/WAN		
CDMA	3GPP2	Mobile/WAN		
LoRaWAN	LoRa Alliance	WAN	Originally developed by Cycleo, acquired by Symantec	
Weightless - N/W	Weightless SIG	WAN	Developed by Neul, acquired by Huawei	
802.11	IEEE	LAN		Early versions allow for technology with known security flaws
802.15.4	IEEE	LAN		
6LoPAN	IETF	LAN	Based on 802.15.4	
ZigBee	ZigBee Alliance	LAN	Based on 802.15.4	Temp. exposure of keys required for provisioning new devices
Thread	Thread Group	LAN	Based on 802.15.4	Human passphrase that unlocks stronger key during provisioning
Z-Wave	Z-Wave Alliance	LAN	Focused on home automation	
Sigfox	Proprietary	LAN	Developed and managed by Sigfox	
Bluetooth	Bluetooth Alliance	PAN		Manufacturers often use same password for all devices, noted in instructions
Bluetooth LE	Bluetooth Alliance	PAN		
NFC	NFC Forum	PAN	Focused on proximity, 10cm or less	
WAVE IEEE 1609	IEEE	PAN	Focused on vehicular environment	
ANT/ANT+	ANT+ Alliance	PAN	Developed by Garmin, focused on health sector	
DASH7	DASH7 Alliance	PAN		



Device Architectures – Intel IoT Platform

intel Intel® IoT Platform
Secure, Scalable, Interoperable

The Intel® IoT Platform is an end-to-end reference model and family of products from Intel—that works with third-party solutions—to provide a foundation for seamlessly and securely connecting devices, delivering trusted data to the cloud, and delivering value through analytics.



Device Architectures –TPM



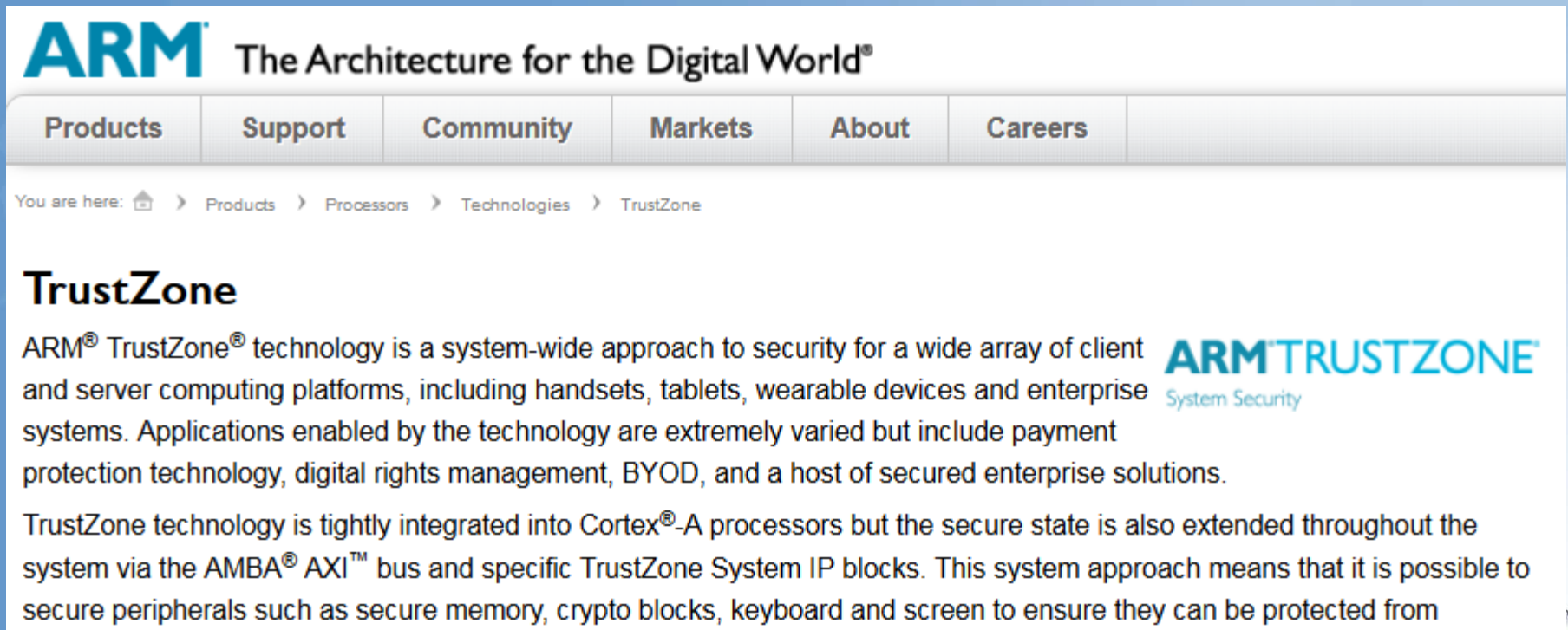
ARCHITECT'S GUIDE: CYBERSECURITY

October 2013

Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97006



Device Architectures – ARM TrustZone



The image is a screenshot of the ARM TrustZone website. At the top left is the ARM logo with the tagline "The Architecture for the Digital World®". Below this is a navigation bar with links for Products, Support, Community, Markets, About, and Careers. A breadcrumb trail indicates the current location: "You are here: Home > Products > Processors > Technologies > TrustZone". The main heading is "TrustZone". The text describes ARM TrustZone as a system-wide security approach for various devices and enterprise systems, listing applications like payment protection and digital rights management. It also mentions integration with Cortex-A processors and AMBA AXI bus. The ARM TrustZone logo with "System Security" is on the right. A dark blue arrow points from the text towards the bottom right corner.

ARM The Architecture for the Digital World®

Products Support Community Markets About Careers

You are here: [Home](#) > [Products](#) > [Processors](#) > [Technologies](#) > [TrustZone](#)

TrustZone

ARM® TrustZone® technology is a system-wide approach to security for a wide array of client and server computing platforms, including handsets, tablets, wearable devices and enterprise systems. Applications enabled by the technology are extremely varied but include payment protection technology, digital rights management, BYOD, and a host of secured enterprise solutions.

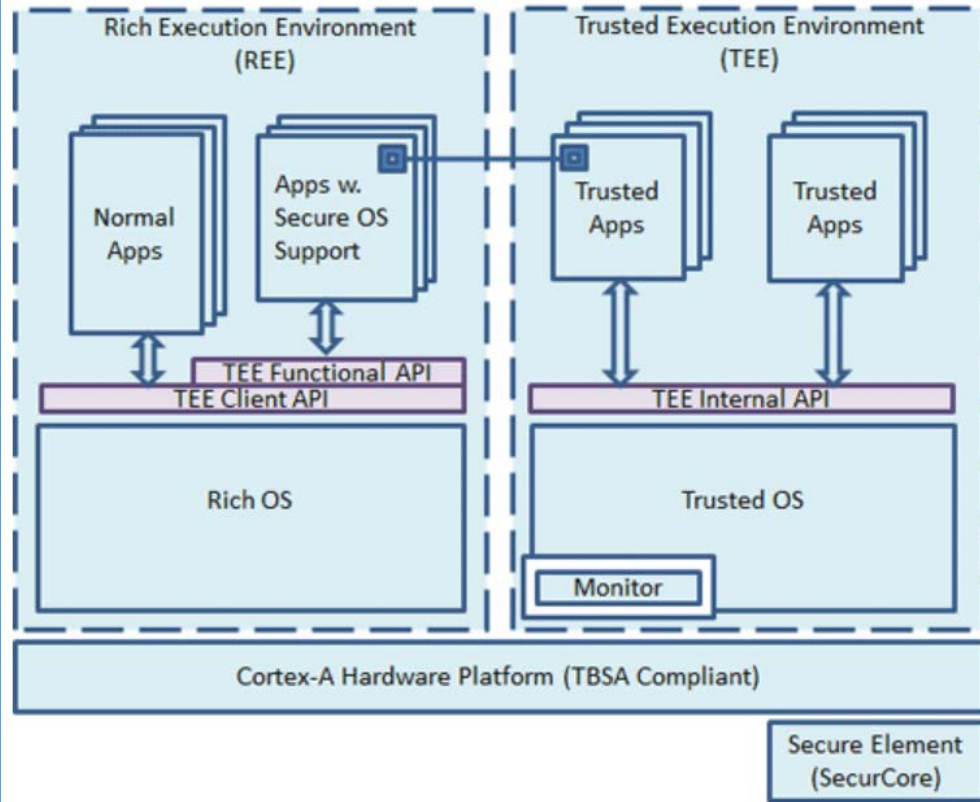
TrustZone technology is tightly integrated into Cortex®-A processors but the secure state is also extended throughout the system via the AMBA® AXI™ bus and specific TrustZone System IP blocks. This system approach means that it is possible to secure peripherals such as secure memory, crypto blocks, keyboard and screen to ensure they can be protected from

ARM TRUSTZONE
System Security



ARM The Architecture for the Digital World®

Development of TEE and Secure Monitor Code



2. Applying Security to Consumer IoT Devices

- **Deliverables:** Status around our analysis of IoT related security best practices
 - **OWASP Internet of Things Top Ten Project**
(https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project)
 - Analysis:
 - Good coverage on security topics relating to the back end servers and cloud deployments, along with solid guidance on how to address the top 10 identified issues
 - Less emphasis on device security best practices, although there is discussion of insecure firmware updates and physical IO ports



2. Applying Security to Consumer IoT Devices

- **Online Trust Alliance IoT Trust Framework**
(<https://otalliance.org/initiatives/internet-things>)
- **Analysis:**
 - Short but informative list of 23 proposed requirements to seed future certification programs, covering such topics as disclosing of privacy policies, forcing the update of default passwords, use of HTTPS as the default, the need for penetration testing, digital signature on firmware updates, and the ability to perform remote SW updates,
 - As with the OWASP Top Ten project, there is less coverage on device security and IoT specific access technology topics



2. Applying Security to Consumer IoT Devices

- **Cloud Security Alliance (CSA) Mobile WG**

[\(<https://cloudsecurityalliance.org>\)](https://cloudsecurityalliance.org)

- **Analysis:**

- Fairly extensive coverage overall on both processes and technologies, with plenty of detail (document is 53 pages – fairly long in comparison to other IoT security best practices documents)
- The document covers topics such as good engineering processes, perceived security challenges, privacy considerations, threat modeling, life cycle security controls, layered security protections (defense in depth), and authentication/authorization frameworks



2. Applying Security to Consumer IoT Devices

- **Symantec “Insecurity in the Internet of Things” paper**
(https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/insecurity-in-the-internet-of-things.pdf)
- **Analysis:**
 - The report’s main goal is to sensitize folks around the current vulnerabilities in the smart home market
 - The report summarized the analysis of 50 smart home devices that are available today.
 - Issues were identified around password usage, the lack of mutual authentication, or protected accounts against brute-force, lack of protection of data in transit, and the existence of several other common vulnerabilities
 - The “mitigation” section is short (one page) but provides a laundry list of topics to be considered by Smart Home product vendors



2. Applying Security to Consumer IoT Devices

- DHS “**DRAFT Security Tenets for Life Critical Embedded Systems**” (<http://www.dhs.gov/information-technology-sector>)
- Analysis:
 - Purpose: *“provides core technical principles that serve as a starting point for industry-specific consortia and government groups to consider in developing standards and norms and for system developers to use in building or updating life critical embedded systems.”*
 - It enumerates a list of tenets that cover general security topics, communications, boot/run time security, secure device management, back end system security, and advanced threat monitoring
 - Because of the life critical focus, it may serve as guidelines for higher tiers of consumer IoT, such as medical devices
 - It may be less applicable to low cost, resource constrained devices



Appendix 3

(Securing SDN)



Definition: Topic 3 – Securing SDN/NFV

There are clear signs that the telecommunications market is standing at the cusp of a significant paradigm shift in how computer networks of the future will be designed, controlled, and managed. One of the key technologies at the heart of this transformation is called Software Defined Networking (SDN) architecture. According to ONF, this new approach to designing, building, and managing networks make it possible for enterprises and carriers to gain unprecedented programmability, automation, and network control, enabling them to build highly scalable, flexible networks that readily adapt to changing business needs. The way this is accomplished is by decoupling the control and data planes, logically centralizing network intelligence and state, and abstracting the underlying network infrastructure from the applications.

SDN is sometimes considered to carry significantly more cyber risk than traditional network architectures. Therefore, the need to secure both SDN's centralized network's control plane and distributed dataplane seem essential. It would be worthwhile considering how to build in security as opposed to retrofitting it, and seeking to apply lessons learned from the long running efforts to secure existing control plane protocols such as BGP, and DNS.

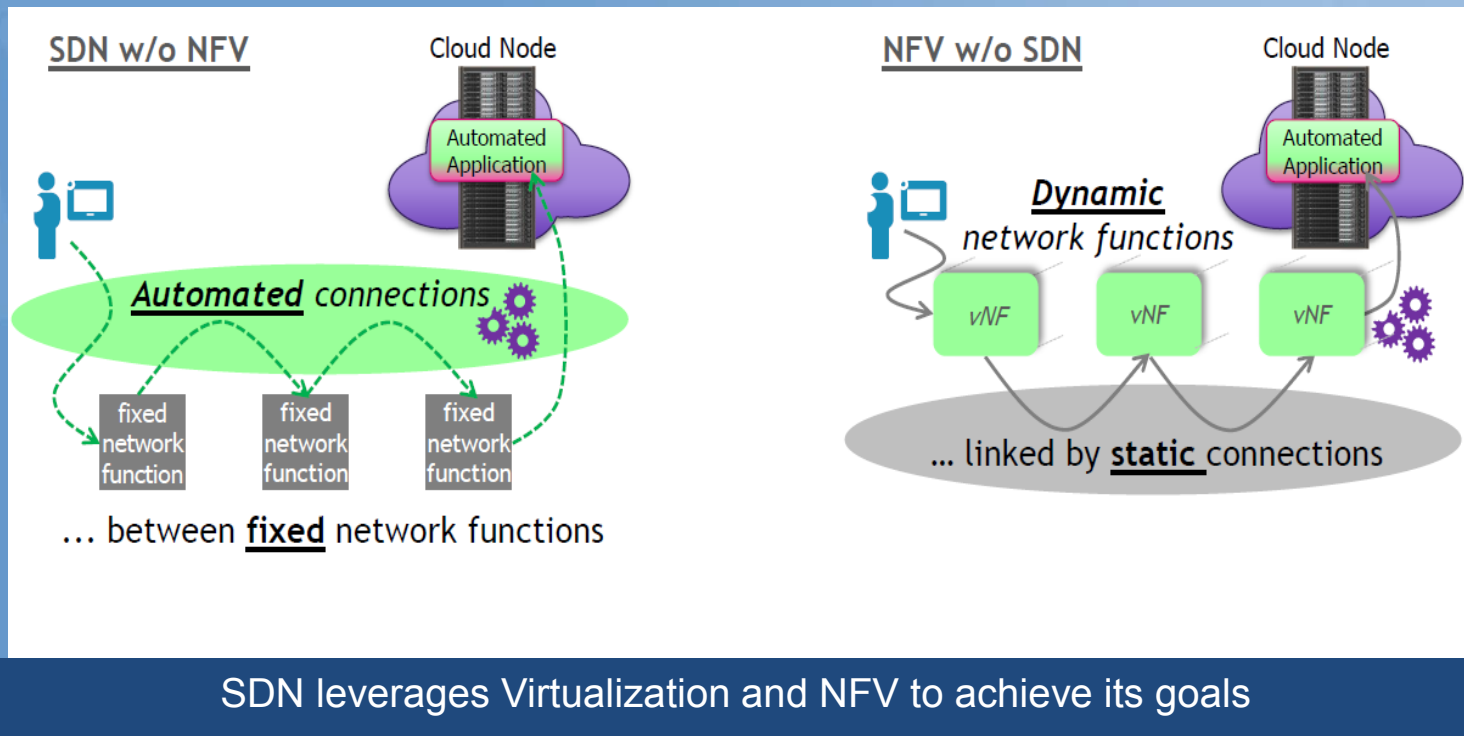


Securing SDN/NFV: Consulted Industry Practitioners

1. Torsten Dinsing, “Virtualizing the Network”, Ericsson
2. Dr. Igor Faynberg , Dr. Hui-Lan Lu , Alcatel Lucent
3. Luke Hinds, Security Architect, Nokia, OPNFV Security Group Project, Team Lead
4. Deepak Manjal, HP
5. Alastair Johnson, Diego Garcia Del Rio and Furquan Haq, Alcatel Lucent
6. Dr. Dilip D. Kandlur, IBM
7. Mike Geller, Cisco
8. David Jorm, Open DayLight
9. Kireeti Kompella, CTO, Juniper
10. Andrew Crawford, VP Service Provider Strategy, Brocade
11. Brian Daly, AT&T, SDN and NFV in Mobile Networks (To Be Scheduled)



How are SDN and NFV Complementary



SDN leverages Virtualization and NFV to achieve its goals

Source: Kevin Sparks, TAC FGCT Architecture



Technological Advisory Council

Spectrum and Receiver Performance

Working Group

September 24, 2015



2015 Mission

- **Make recommendations in areas focused on improving access to and making efficient use of the radio spectrum from a system and receiver perspective**
- **Provide support as the Commission considers TAC recommendations related to the statistical aspects of interference**
- **Conduct analysis and make recommendations related to enforcement issues in a rapidly changing RF environment**



Working Group

- **Chair:**

- Lynn Claudy, NAB
- Greg Lapin, ARRL

- **FCC Liaisons:**

- Julius Knapp
- Uri Livnat
- Bob Pavlak
- Matthew Hussey

- **Participants / Contributors:**

- Dale Hatfield, University of Colorado
- Pierre de Vries, Silicon Flatirons
- Brian Markwalter, CEA
- David Gurney, Motorola Solutions
- Steve Kuffner, Motorola Solutions
- Geoff Mendenhall, GatesAir
- Robert Dalgleish, Ericsson
- Kumar Balachandran, Ericsson
- Robert Miller, incNetworks
- Bruce Judson, Qualcomm
- Dennis Roberson, IIT
- Dave Pehlke, SkyWorks
- Scott Burgett, Garmin



Working Group Areas of Focus

- **Develop recommendations about statistics of interference and risk-informed decision making**
- **Recommend strategies for interference resolution and enforcement in a changing RF environment**
- **Propose methods for characterizing the operational impact to receiver performance from interference**

Risk-Informed Interference Assessment

- **Focusing on MetSat/LTE interference as test case: build on analysis done by CSMAC WG-1**
- **Testing the 3-step method recommended last year:**
 1. Inventory of hazards: Analyzed MetSat / LTE data required for assessment
 2. Consequence metrics: Exploring mapping from RF to service metrics. Mostly done for MetSat, in progress for public safety and broadcasting
 3. Assess likelihood & consequence using Monte Carlo modeling

Interference Resolution and Enforcement

- **Deliverables for TAC Meeting on December 9, 2015:**
 - Updated straw-man proposal for dealing with aggregate interference and enforcement architecture
 - Preliminary recommendations for immediate and specific actions to support enforcement
 - Detailed research plan / statement of work for future system engineering study, to be carried out by government or under government auspices

Interference Resolution and Enforcement

▪ Updates and Progress

- Updating straw-man proposal to include *inter alia* transmitter identifiers, emission designators, and PIM; some risk due to personnel constraints
- Preparing preliminary recommendations for comprehensive system engineering study
 - Objective: Use modern system engineering tools, analysis, and techniques, to develop and justify a comprehensive national program for interference detection, classification-identification, location, resolution, reporting and enforcement

Principles for Assessing New Band Allocations

- The Commission can benefit by applying fundamental principles when allocating new services adjacent to existing ones
- Basic principles have been developed
- Deliverable for TAC meeting on December 9, 2015:
 - White paper discussing the principles and their application to band allocations

Themes Underlying the Principles for Assessing New Band Allocations

- Interference is due to characteristics of both transmitters and receivers
- Interference is unavoidable, dynamic, and should be planned for
- Responsibilities of: receivers, systems, & transmitters
- Benefits of disclosing operating characteristics to the FCC
- Use of interference limits to distinguish harmful interference
- Quantitative analysis of interaction between services

THANK YOU



DRAFT

Technological Advisory Council

**Proposed RF Noise Floor and
Interference Study Ad Hoc Group
September 24, 2015**



Background

- RF noise floor is an issue for numerous wireless communications services
- Anecdotal evidence suggests RF noise floor has been steadily rising; assessment methodologies and quantitative studies are lacking
- Topic was addressed in June 2014 white paper from Spectrum Working Group: “Introduction to Interference Resolution, Enforcement and Radio Noise”--white paper recommended focused study by the TAC
- Interest sought at last TAC meeting by TAC FCC liaisons for forming ad hoc group
- Mission statement developed by interested parties for formation of an ad hoc group to study the issue
- Requesting authorization of ad hoc group

Mission of Proposed Ad Hoc Group

- Research literature on RF noise floor changes from 500 kHz to 2 GHz
- Research FCC rules on RF emission limits from licensed and unlicensed services
- Research literature on manufacturing and testing of unlicensed RF emitting devices
- Compare available test data relative to current emission limits
- Research require noise floor for wireless communications bands and assess unlicensed service contributions to noise floor



THANK YOU



Future Game Changing Technologies Working Group

Chairs: Nomi Bergman, Adam Drobot
FCC Liaisons: John Leibovitz, Nnake Nweke,
Walter Johnston

24-September-2015



Working Group Members

- WG Chair: Nomi Bergman, Bright House Networks
Adam Drobot, OpenTechWorks

- FCC Liaisons: John Leibovitz, Nnake Nweke, Walter Johnston

- Members:
 - Kumar Balachandran, Ericsson
 - John Barnhill, Genband
 - Mark Bayliss, Visualink
 - John Chapin, SGE
 - Lynn Claudy, NAB
 - Brian Daly, AT&T
 - John Dobbins, Earthlink
 - Jeffrey Foerster, Intel
 - Dick Green, Liberty Global
 - Ramani Panduragan, XO Communications
 - Thyagarajan Nandagopal, NSF
 - Jack Nasielski, Qualcomm



Working Group Members Cont'd

- Members:
 - Mark Gorenberg, Zetta Ventures
 - Russ Gyurek, Cisco
 - Farooq Kahn, Samsung
 - Gregory Lapin, ARRL
 - Brian Markwalter, CEA
 - Tom McGarry, Neustar
 - Paul Misener, Amazon
 - Bruce Oberlies, Motorola Solutions
 - Lynn Merrill, NTCA
 - Mark Richer, ATSC
 - Marvin Sirbu, SGE
 - Paul Steinberg, Motorola Solutions
 - Lisa Guess, Juniper Networks
 - Kevin Sparks, Alcatel-Lucent
 - Sanjay Udani and David Young, Verizon
 - Steve Lanning, Viasat



Working Group Members Cont'd

- **Sub-Working Group Chairs:**

1. Demand and New Business Models – Brian Markwalter, CEA
2. Capacity Impacting Technologies – Jack Nasielski, Qualcomm
3. Drivers for Architecture Changes – Kevin Sparks, Alcatel-Lucent



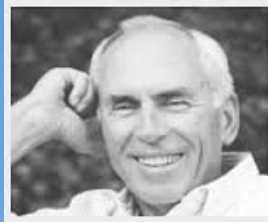
Future Game Changing Technologies Working Group Charter

The workgroup will seek to **identify technologies with the potential to radically change communication infrastructure and business models** across a broad range of fronts. The intent is to identify seminal technologies and concepts that the Commission should understand and possibly include in its considerations. The workgroup will seek to identify these catalysts and assess their potential impact. The group will be chartered to **scan across a wide breadth of technical areas**, identify areas of potential promise, and organize them in the context of synergies and potential impacts.



FGCT WG – What’s on the Horizon

- Amara’s Law



Two way wrist Radio 1946
Two way wrist TV 1964

“We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.”

- Amara, Roy; Institute for the future (1972). A framework for national science policy analysis (Report). Menlo Park, California: Institute for the Future. OCLC 4484161. P-18. Reprinted from IEEE transactions on systems, man, and cybernetics, v. SMC-2, no. 1 January 197

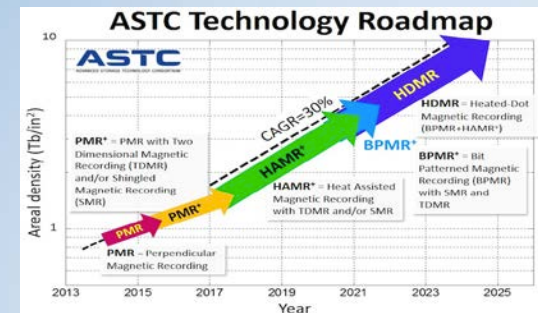
FGCT WG – What’s on the Horizon

- A few additional Laws

"Moore's law" is the observation that, over the history of computing hardware, the number of transistors in a dense integrated circuit has doubled approximately every two years.



Kryder's Law is the assumption that disk drive density, also known as areal density, will double every thirteen months.

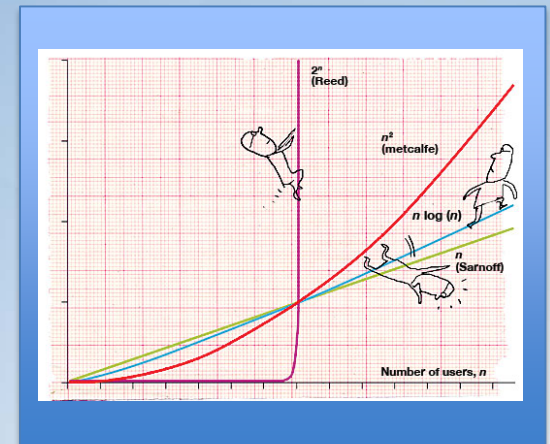
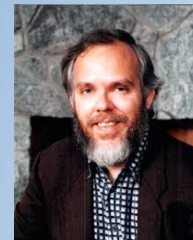


FGCT WG – What's on the Horizon

- A few additional Laws

Metcalfe's law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2).

Reed's law is the assertion of David P. Reed that the utility of large networks, particularly social networks, can scale exponentially with the size of the network.



FGCT WG – What's on the Horizon

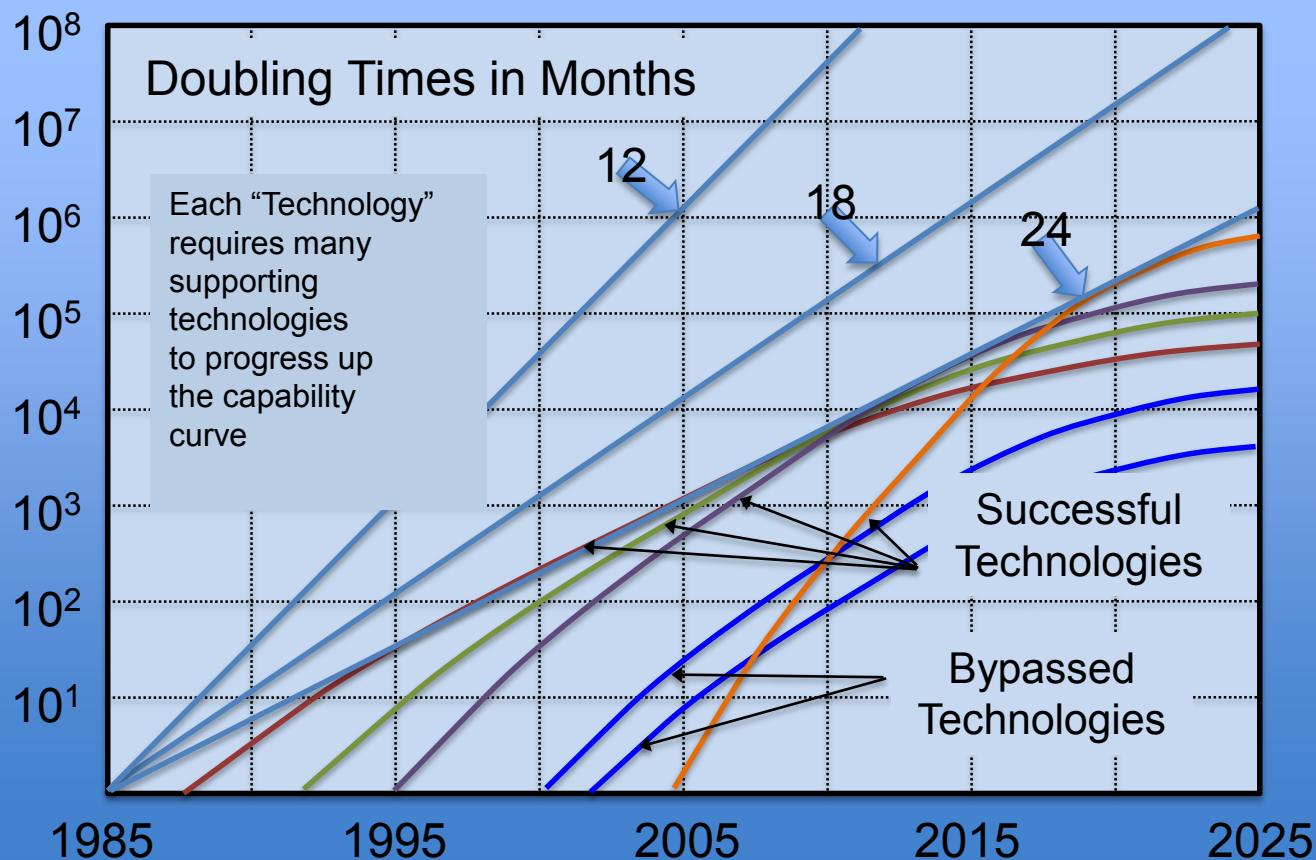
Basic Technologies

- Computing
 - Storage
 - Communications
 - Sensors
 - Actuators
 - Interfaces
 - Software
-
- Power

Important Enabling Technologies

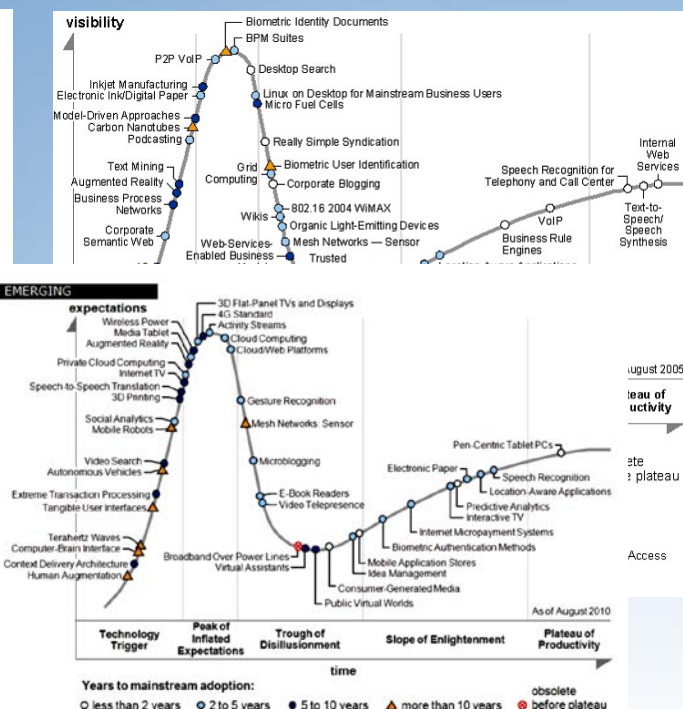
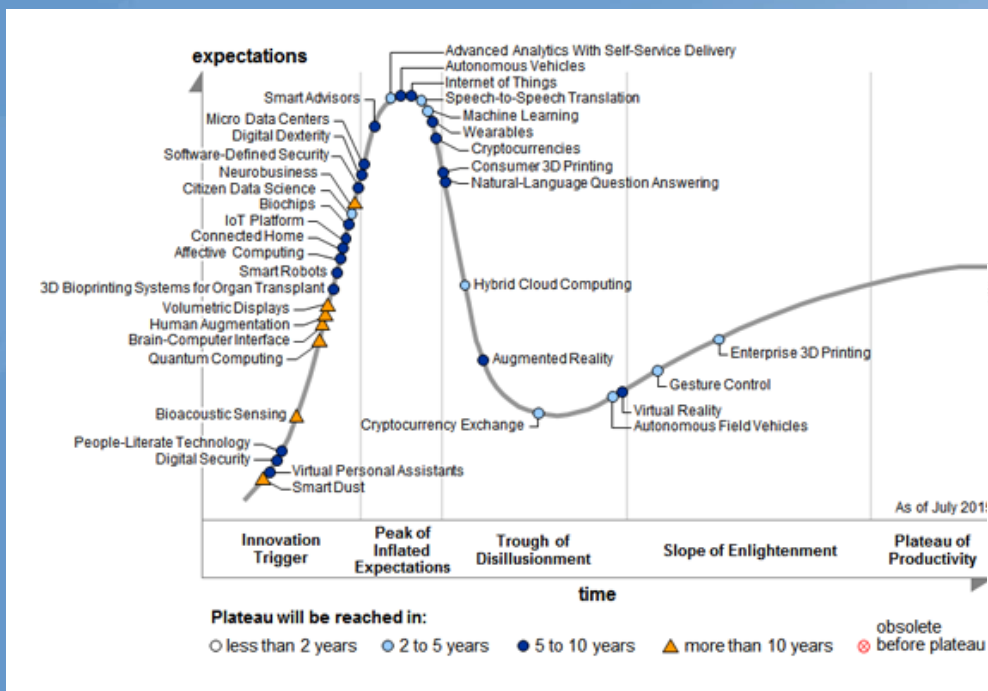
- Cloud Computing
- Mobility
- Analytics
- Artificial Intelligence
- Autonomy
- Software Defined Functionality

FGCT WG – What's on the Horizon



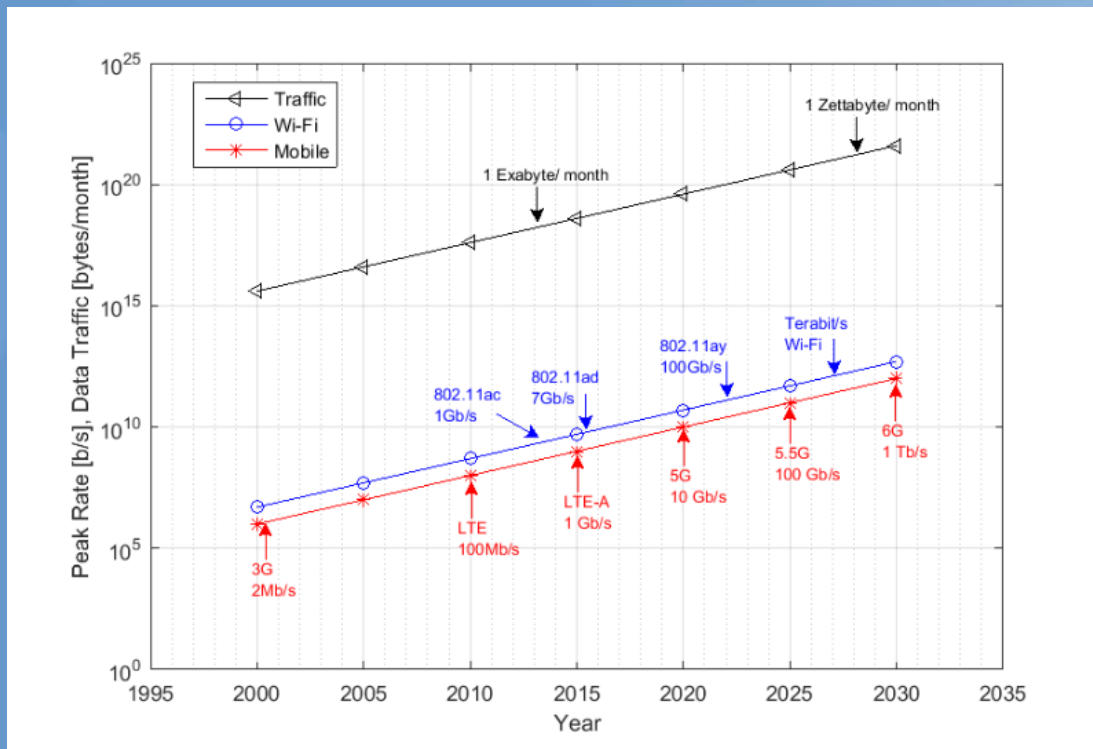
Characteristics
of
Exponential
Technologies

FGCT WG – What's on the Horizon



* Source: Gartner Hype Cycle 2015, 2010, 2005

FGCT WG – What’s on the Horizon



An example
of one basic technology
Area
Projected
Into the Future

* Source: Farooq Khan, Samsung

FGCT WG – What’s on the Horizon

- **Implications for the FCC**
 - **The National ICT infrastructure has deep penetration and is built from components that are evolving rapidly.**
 - **Consequently, expectations and user experiences in 5-7 years will be considerably different from what we have today!**

FGCT WG – In Progress Report

- **Completed Broad Call for Ideas and Technologies**
- **Began Analysis to identify most impactful Technologies**
 - **That affect Demand and Business Models**
 - **Technologies that are likely to significantly improve capacity (In several different dimensions)**
 - **Developments that may cause major Architectural Changes in the way Networks are Designed and Built**
- **Arranged for a full schedule of talks and presentations from SMEs**
- **Initiated discussions on observations and recommendations**

FGCT SME Speakers

- May 15 – 5G Requirements and Use Cases - Jack Nasielski, Qualcomm
- May 29 – **Massive MIMO** - Tom Marzetta, Bell Labs
- June 5 – **Cloud RAN/vRAN**, Kumar Balachandran, Ericsson
- June 26 – **RF Full Duplex** – Yang-Seok Choi, Intel Labs
- July 10 – **ATSC 3.0** – Mark Richer, Luke Fay, Rich Chernock, ATSC
- July 24 – **RF Mirror Worlds**, high res RF models from sensors & supercomputing – Pierre de Vries, Silicon Flatirons
- July 31 – **Hybrid satellite/cellular broadband** – David Lerner, ViaSat
- August 7 – **UAVs** - Ravi Jain, FAA
- August 14 – **Satellite Access** – Alexander Gerdenitsch, EchoStar



FGCT SME Speakers - Continued

- August 21 – **NG DSL and PON Access Technologies** – Peter Vetter, Bell Labs and John Dickinson, Bright House Networks
- August 28 – **SDN, NFV and Programmable Networks** – Kevin Sparks, ALU
- September 18 – **100G RF Program** - Ted Woodard, DARPA
- September 18 – **Smart Cities**, Roberto Saracco, IEEE Initiative
- September 18 - **Sensors**, IoT, and Swarms - Prof. Jan Rabaey, UC Berkeley
- September 25 – **Virtual Reality**, Phil Lelyveld, USC Entertainment Technology Center
- October 2 – **Public Safety** Ed Parkinson and TJ Kennedy, First Net
- October 16 – **Drones and Airspace**, Tavis Mason, Google

And more speakers in the works



Future Game Changing Technologies

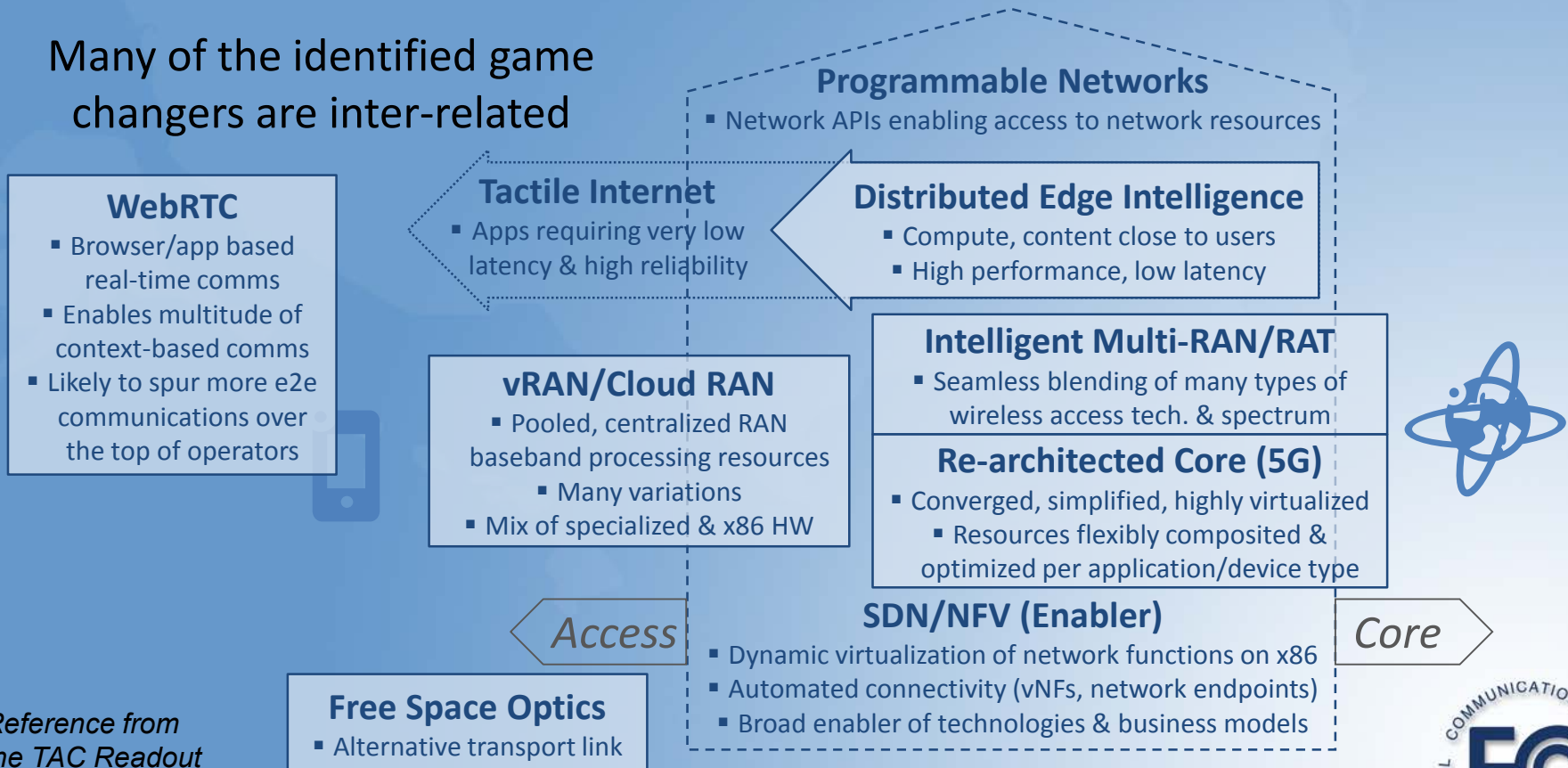
Architecture SWG

Kevin Sparks - Chair



Architecture Impacting Game Changing Technologies

Many of the identified game changers are inter-related

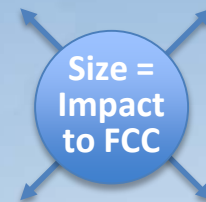
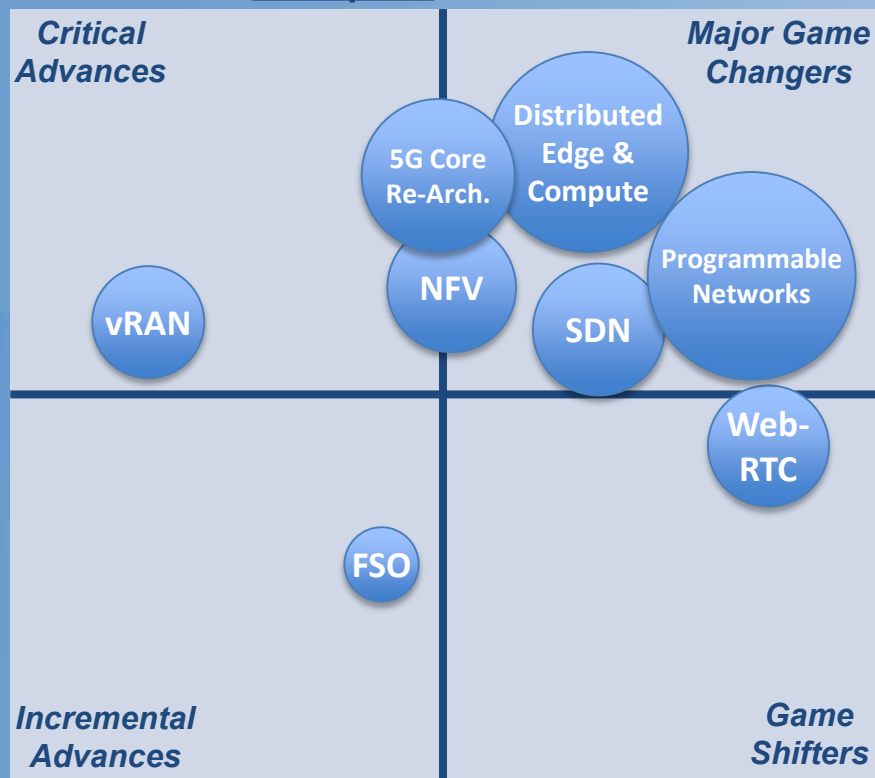


Reference from
June TAC Readout

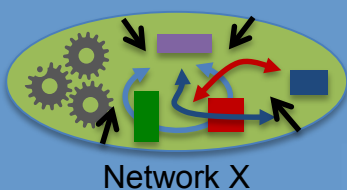
FGCT Architecture SWG – Technologies Assessment

Disruptive Innovation

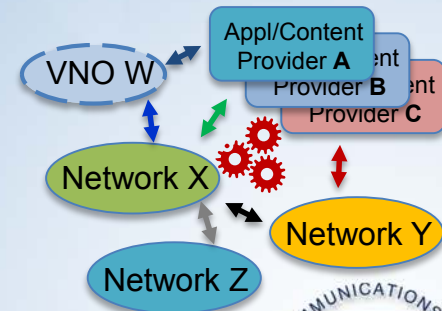
Analysis:
Long Term Impact



Internal Network Impact



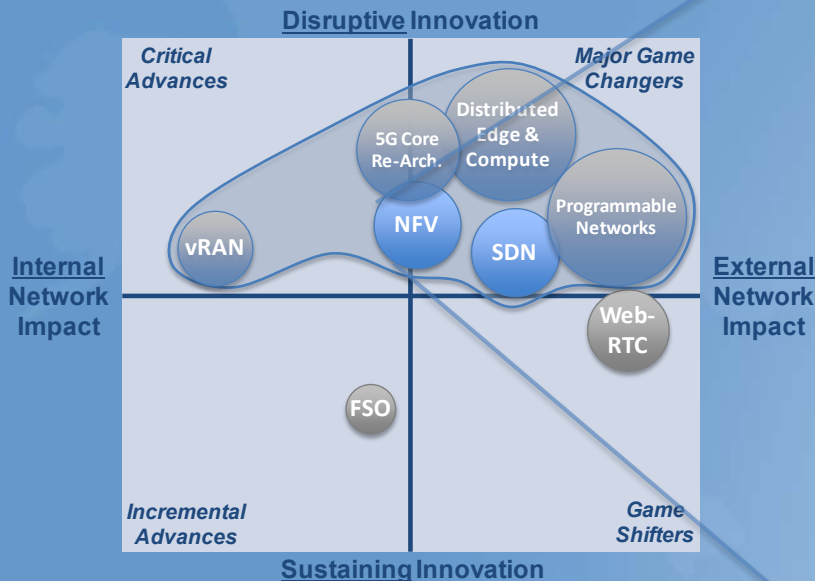
External Network Impact



Sustaining Innovation



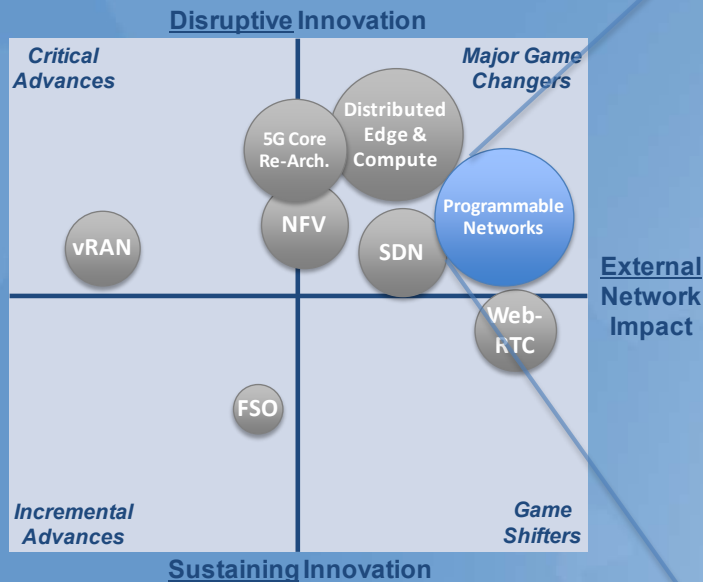
SDN & NFV (Underlying transformative enablers)



- NFV (Network Functions Virtualization)
 - Implementation of network mgmt-, control-, and data-plane functions on pools of virtualized commodity (x86) servers
 - Allows network functions to be rapidly scaled up/down (more/less capacity) and out/in (geographically distributed)
 - SDN (Software-Defined Networking)
 - Separation of control and data planes (classic definition)
 - Centralization & integration of control and resource mgmt.
 - Abstraction & API exposure for programmable services
- FCC impact:* Brings many new degrees of freedom to networks; enabler for key game changing technologies
- Timeframe:* DC & early WAN use now; full e2e network deployment: ~4-8 yr (existing networks)

SDN and NFV are foundation enablers driving many aspects of NG network transformation.

Programmable Networks



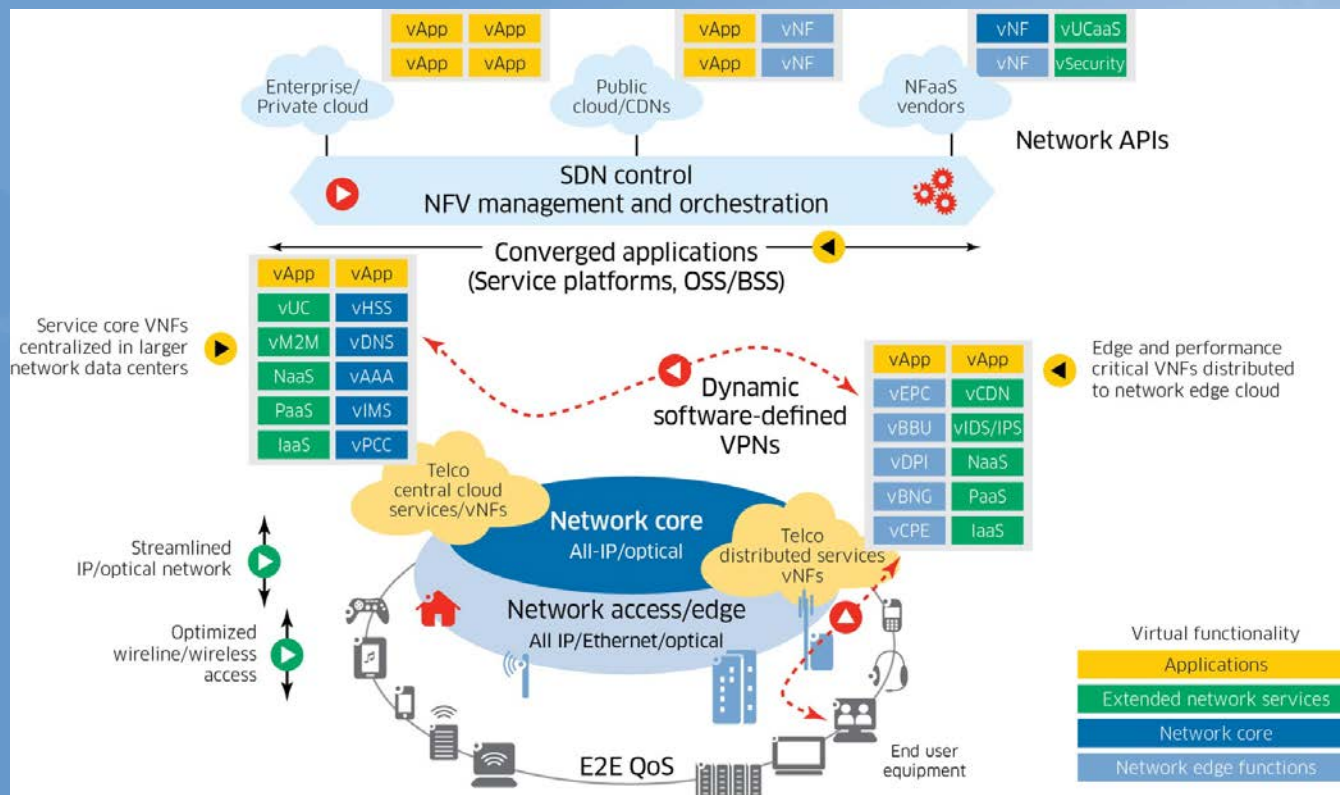
- Dynamic on-demand services, fit for cloud timescales
 - “API consumable” connectivity & network functions
- Enables new forms of virtual network operators, and mixed network operator/service provider models
- Fundamentally enabled by SDN and NFV, and enhanced by edge computing and 5G advances

FCC impact: Facing new forms of dynamic services and optimizations, potentially more complex ecosystem of physical/virtual network & service providers

Timeframe: Some dynamic connectivity services already commercialized; complex NaaS forms will likely take 5 or more years to mature to be widely available

A broad sweeping transformation of networks that will build up over many years.

A View of an SDN/NFV Programmable Network



"Reshaping the future with NFV and SDN, The impact of new technologies on carriers and their networks", Report by Arthur D. Little and Bell Labs Consulting, May 21, 2015; <https://www.alcatel-lucent.com/press/2015/european-telecoms-could-realize-eu39-billion-re-imagining-network>



SDN, NFV, & Programmable Networks: Dimensions of Impact

Network CapEx Efficiency

- GPP (x86) commodity hardware riding Moore's Law curve (gain or not depends on type of function being virtualized)
- GPP hardware pooling/reuse
- Automated multi-layer optimization of network drives higher network utilization (less 'headroom' overhead required)

Business Model Innovation

- APIs and NaaS opens up possibility for many new types of virtual operators
- Highly optimized customization can enable previously infeasible business models
- Automated global service needs may drive consortiums and federated BW markets

Virtual Edge Advances

- Lowers cost of distributing cluster of IP edge functions close to users
- Enables distribution of compute & storage close to users
- Edge computing w/very low latency enables new classes of services (AR, VR, tactile Internet)
- Positions network for low latency 5G

Network OpEx Efficiency

- Economy of scale of operations & maintenance on common GPP hardware
- Auto self-service cuts provisioning costs
- Reduction in non-deferrable maintenance

Service Velocity

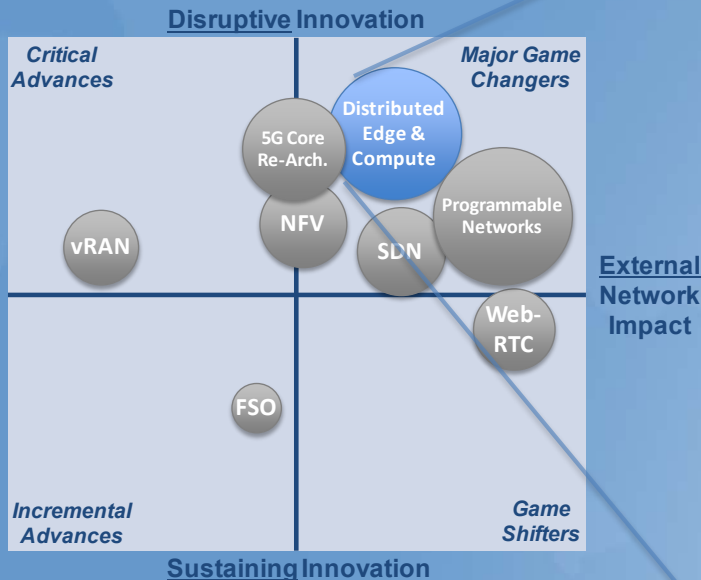
- Rapid service instantiation
- New service development/test time (& cost) reduced
- Automated service scaling (network scaling like cloud)

Automated Cloud-Optimized Services

- Elastic 'BW-on-demand' & 'BW calendaring' services via APIs
- Automated software-defined overlay VPNs
- Virtual network slice services (Network-aaS)
- Many opportunities for network-cloud partner mashups

SDN/
NFV

Distributed Edge & Compute

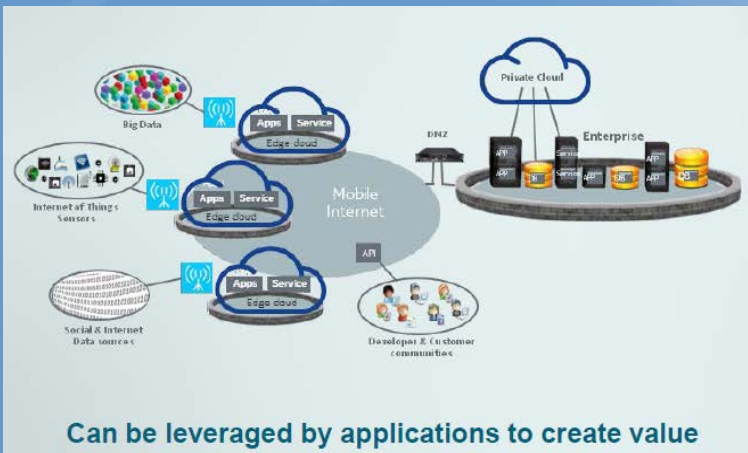
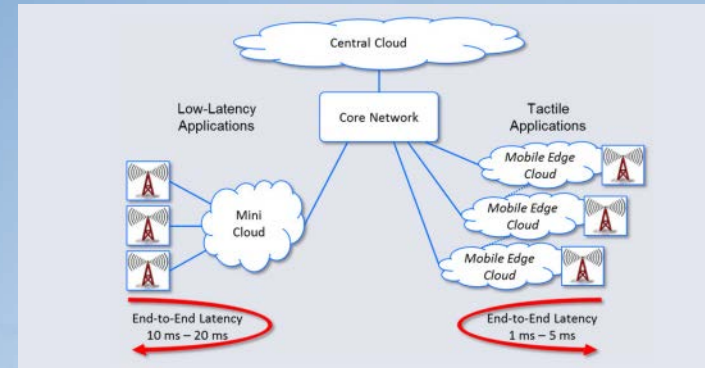


- Distribution of IP service edge and virtualized cloud infrastructure close to end users
 - highly efficient, high quality video distribution from CDNs
 - very low latency for highly interactive applications & vNFs
 - Will enable new classes of high performance cloud applications (AR, VR, 5G IoT, “Tactile Internet”, ...)
 - Efficient distribution made possible by NFV (and SDN)
 - allows array of virtualized edge functions, at any scale
- FCC impact:* Blurs line between network & cloud; many new opportunities for emerging technology markets
- Timeframe:* IP Edge/CDN distribution under way, fully virtualized edge clouds in ~3-5 years, with applications exploiting ultra low latency expected to follow closely

Intelligent virtual edge will be the focal point for SDN/NFV network transformation.

Tactile Internet & Distributed Intelligent Network Edge

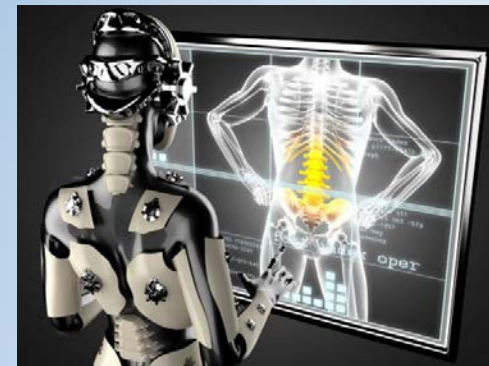
- Tactile Internet
 - Extremely low latency in combination with high availability, reliability and security
- Distributed Intelligent Network Edge
 - Moore's law driving Si cost down, enabling distribution of functions and intelligence to the edge of the network (and into devices).



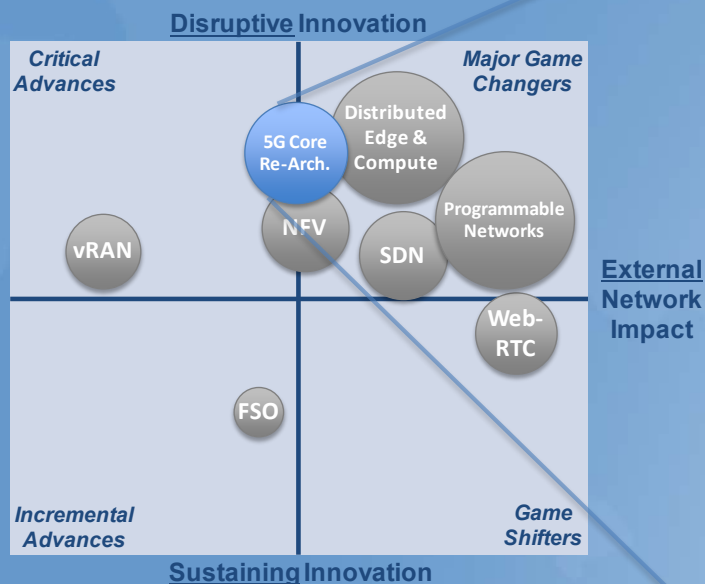
Offers application developers and content providers cloud-computing capabilities and an IT service environment at the edge of the mobile network

This environment is characterized by:

- Proximity
- Ultra-low latency
- High bandwidth
- Real-time access to radio network information
- Location awareness



5G Core Re-Architecture

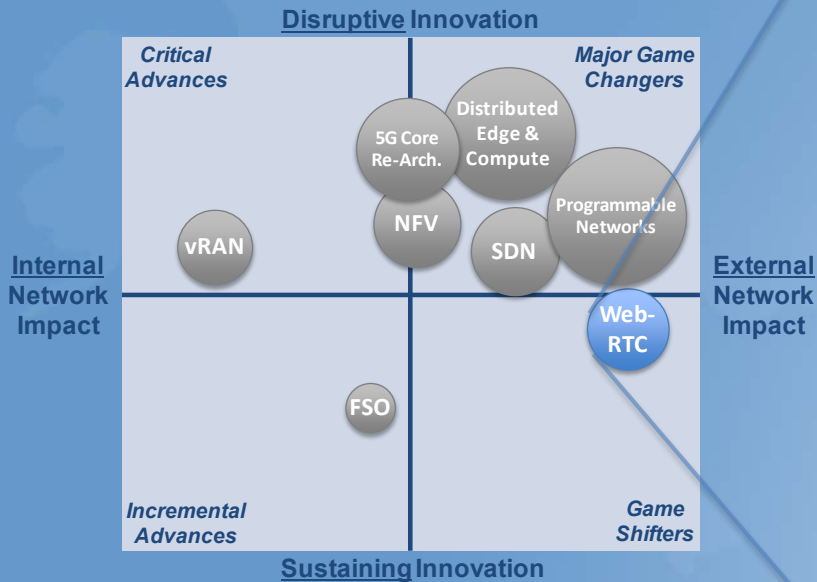


- 5G mobile core will be built on SDN/NFV foundation
 - independent scaling of control & data planes, disaggregating & virtualizing functions, leveraging converged IP data plane
 - flexible control over flows, and virtual slices of the network
- Optimization over wide range of devices and use cases
 - customized levels of mobility, QoS, network resources usage
- Intelligent use of hybrid access technologies/spectrum
 - coordinated multi-RAN/RAT (licensed/unlicensed/shared spectrum, 5G, 4G, WiFi, WiGig, etc.)

FCC impact: Many shades & hybrid combinations of wireless services to consider for spectrum planning
Timeframe: Widespread deployment expected 2020+, with lead early adopter deployments earlier

In 5G, the mobile core moves from specialized to converged elements, and wireless services move from “one-size-fits-all” to tailored.

WebRTC



- Open Source project that defines API's that enable browser and mobile applications with Real-Time Communications Capabilities.
- API's support Voice, Video Calling, Text, P2P
- Client/ plugins not required – simpler adoption
- Creates a contextual link between an activity and required communications

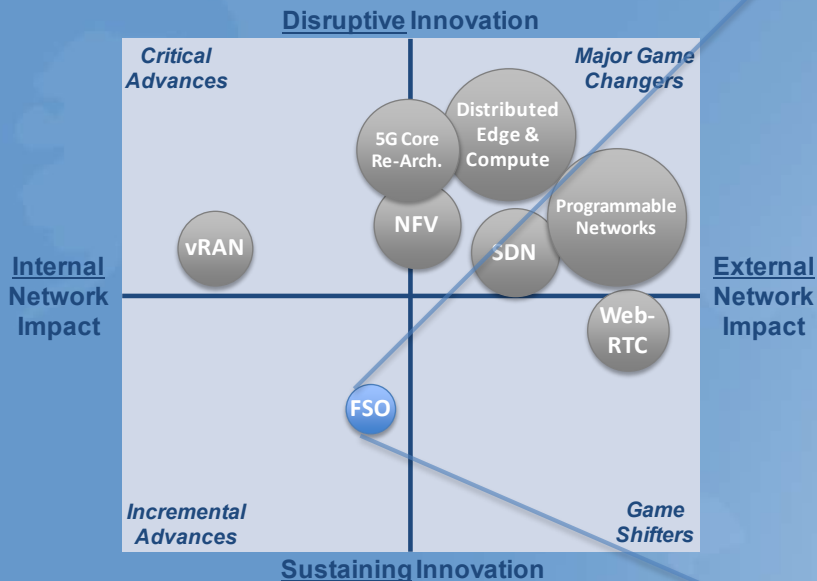
FCC impact: Technology may disintermediate service providers from communications delivery. Implications - TRS, VRS, CC, CALEA, e911

Timeframe: Available now with most desktop browsers. (IE has announced support, Safari has not). iOS by app, Android supports.

Disruptive communications enabler gaining rapid adoption momentum.



Free Space Optics



- FSO has traditionally been a niche technology for short reach line-of-sight connectivity
 - relatively expensive and subject to environmental degradations/blockages
- Now being used for satellite-ground and satellite-satellite communications – Space Mesh Networks
 - could supplement terrestrial optical networks
- Unlikely to compare to scalability and reliability of DWDM-based terrestrial/undersea networks but could serve a backup role during disruptions.

FCC impact: Potential regulatory role protecting against optical spectrum interference, safety concerns.

Timeframe: 2-7 Years

A potentially important supplementary technology with FCC implications.



Arch. FGCTs – Summary of Importance to the FCC

- Any transformation to the network that is as sweeping as these SDN/NFV-enabled game changers can have many implications (a few are highlighted, below)
 - Education on these emerging changes can better prepare the FCC
- Networks will have more degrees of flexibility than in the past
 - New forms of services, service controls, and optimizations for the FCC to consider
- Service providers and virtual network operators will have more options to construct service offerings without owning significant network infrastructure
 - Potentially more complex, dynamic ecosystem of service/content/application providers and network operators - virtual, physical, and mixed - for the FCC to engage with
 - Many new opportunities for emerging technology markets
- New models of roaming interconnection will be possible
 - Service chaining spanning operators for efficiency and/or consistent roaming experience
- New edge computing-enabled applications may require differentiated QoS



Future Game Changing Technologies

Capacity & Coverage SWG

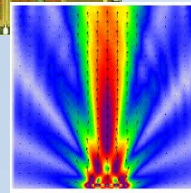
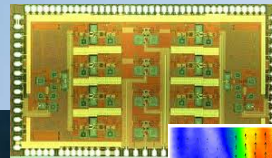
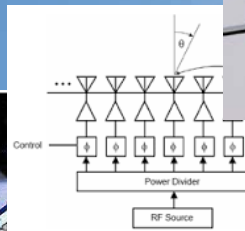
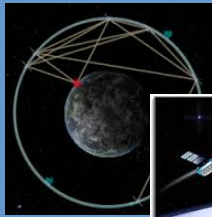
Jack Nasielski - Chair



FGCT Capacity Sub-Working Group

Capacity and Coverage Impacting Game Changing Technologies

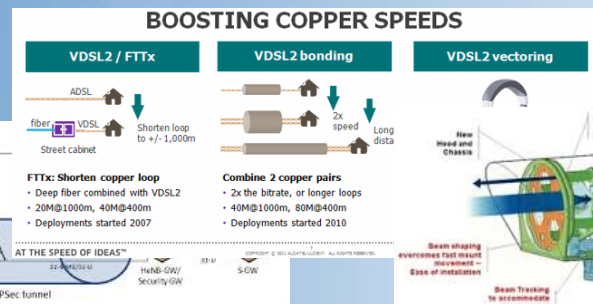
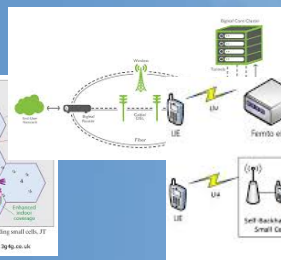
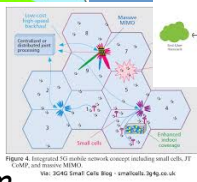
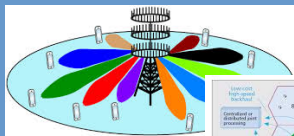
- Carrier aggregation
- Network efficiencies for IoT/M2M
- Drones and Airborne Transmitters
- High capacity Geo Sat MEO LEO
- Hybrid 4G/5G/Geo Sat
- RF Mirror Worlds
- National Public Safety Network
- Distributed intelligent network edge
- Micro antenna arrays
- ATSC 3.0 - NG Broadcast TV std
- Full Duplex radio



FGCT Capacity Sub-Working Group

Capacity and Coverage Impacting Game Changing Technologies

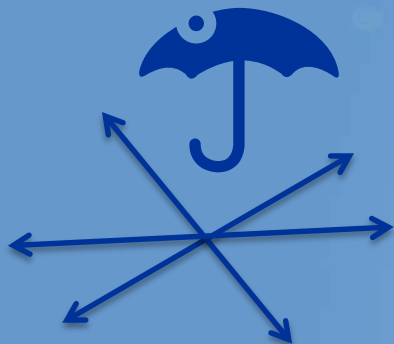
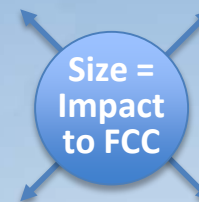
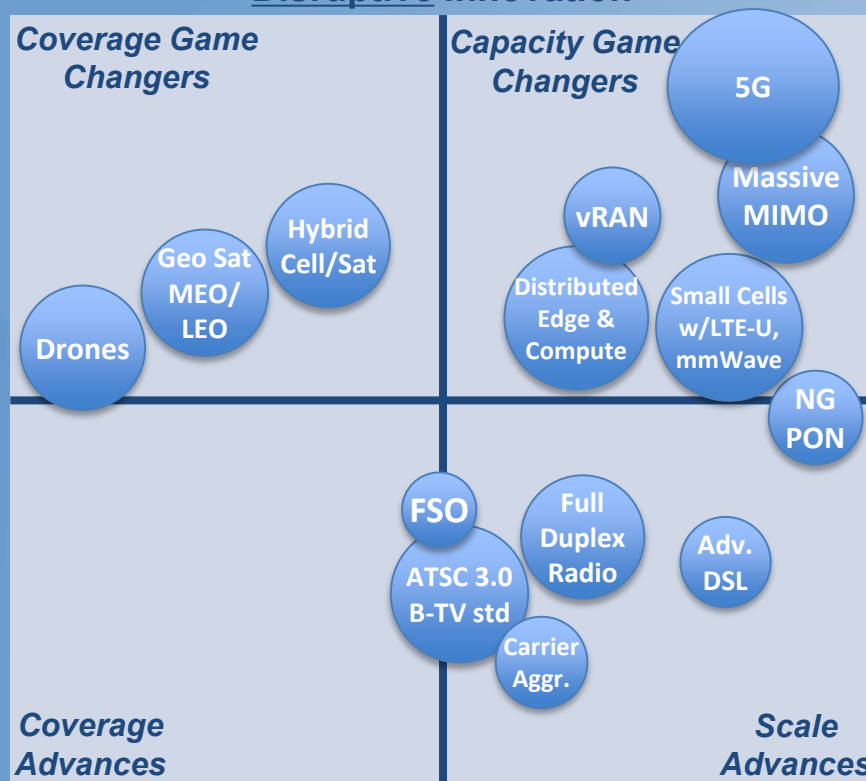
- Massive MIMO
- Virtual RAN/Cloud RAN
- UF-OFDM waveform
- Small cells w/LTE-U and w/mmWave
- Intelligent Multi-RAN/RAT Access
- Advanced DSL vectoring
- NG PON
- Free Space Optical Comms
- 5G (as a whole)
- Self-backhauling & Self-discoverable
- Defining new 3D channel models



Reference from
June TAC Readout

Capacity/Coverage SWG Analysis

Disruptive Innovation



Sustaining Innovation

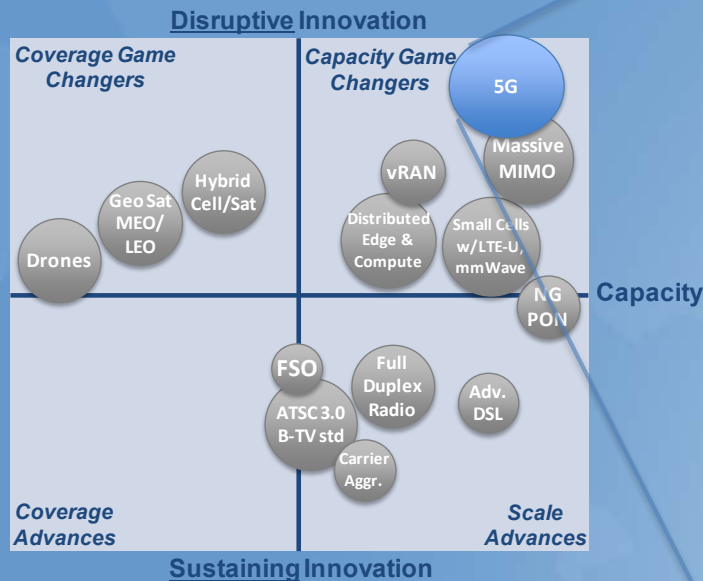


5G

- 5G standardization starting now, plan for deployments around 2020
- Wide range of services: mobile broadband, massive IoT, mission critical high reliability and low latency
- New technologies for mmWave bands, massive MIMO, and scalable flexible network virtualization
- Designs for licensed and unlicensed spectrum
- Multi-connectivity across bands and technologies.

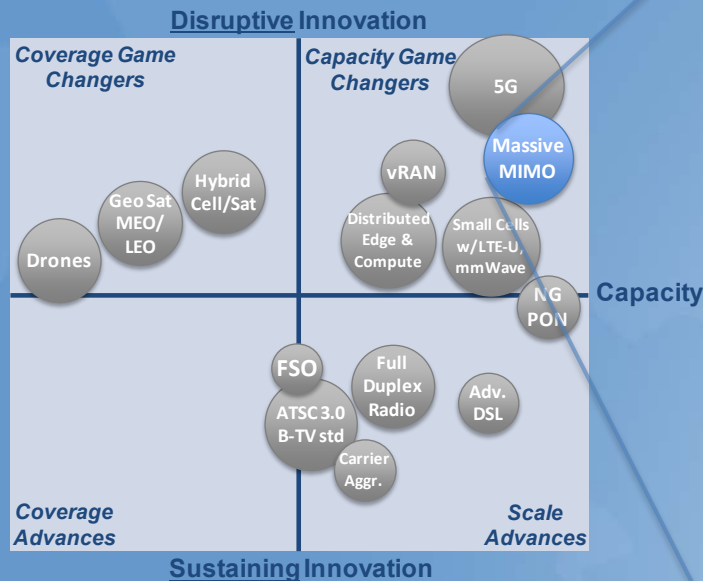
FCC impact: Spectrum policy from 600 MHz to 70 GHz, internet policy considerations

Timeframe: 3-5 Years



5G will provide significant improvements in capacity, latency, data rates, and flexibility.

Massive MIMO

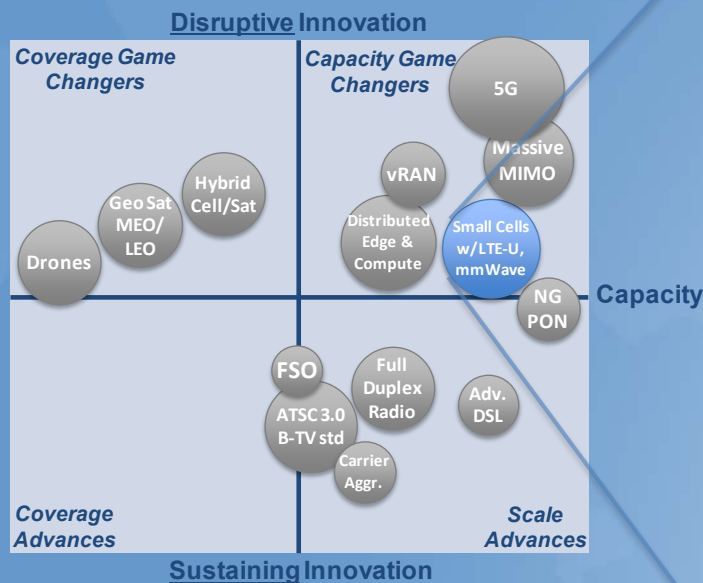


- New technology for achieving massive wireless scalability via aggressive spatial multiplexing
 - Large number (10s-100s) of small low power antennas
 - Utilizes *measured* (vs. estimated) channel characteristics
 - Enables beamforming gain that grow *linearly* with number of antennas (key to scalability)
 - High uniformity of service to users near/far from cell
 - Distributed array processing at cell site; no MIMO processing on mobiles (keeps devices simple)
- FCC impact:* Important advance for maximizing macro cellular spectral efficiency to be aware of/planning for
- Timeframe:* Expect Massive MIMO to be deployed first for 5G ~2020

Fundamental RAN capacity multiplier technology for addressing 5G capacity needs.



Small Cells w/LTE-U and mmWave

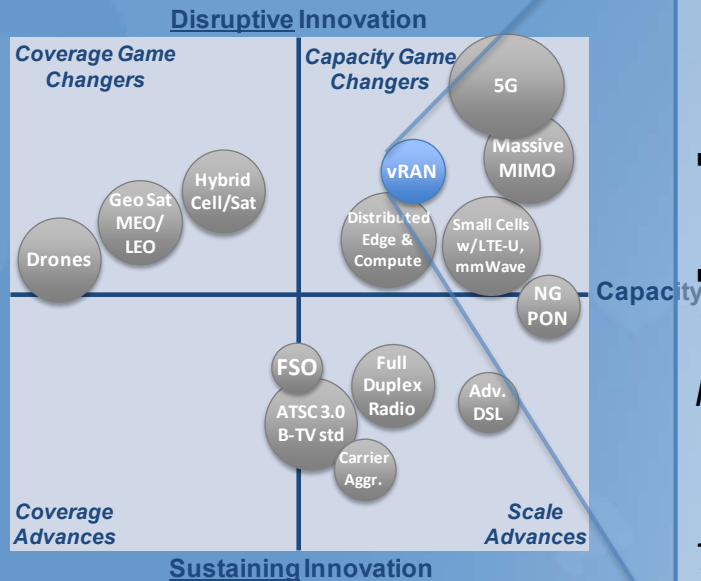


- Small cells are key to capacity scalability for dense areas through spatial reuse, supplementing macro cells
 - especially for low mobility/nomadic users
 - Adding alternative spectrum (not shared w/macros) greatly enhances the capacity gain
 - LTE-Unclicensed applies LTE quality to unlicensed or shared spectrum
 - mmWave can supply massive bandwidth over short distance
 - Efficient scaling via aggregation of licensed anchor spectrum with wide-but-variable unlicensed spectrum
- FCC impact:* Important scaling approach to factor into spectrum planning for capacity growth
- Timeframe:* Small cells now; LTE-U: 2016; mmWave: 5G

Another prime capacity multiplier, combining high spatial reuse and broad spectrum, to address demand in high density areas.

Cloud RAN/vRAN

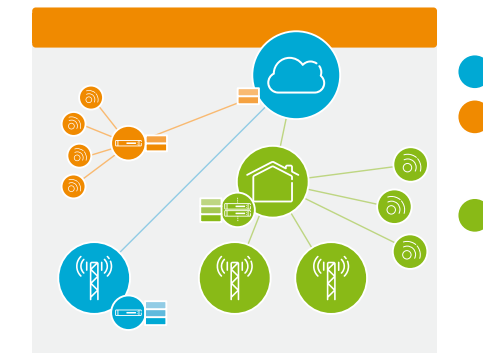
- Technology for simplifying field deployments and to move large parts of radio and access network functionality to pooled network components
 - Baseband pooling is an extreme case
 - Radio access network split towards general purpose processing
 - Useful for distributed antenna or radio head deployments
 - Large indoor networks for capacity, or urban capacity boosting
 - Benefits
 - Lower operational cost, and adoption of GPPs for parts of radio
- FCC impact:* vRAN can be a cost reducer for large operators who rely on high quality spectrum; needs good backhaul; highly market dependent in relevance.
- Timeframe:* Possible today but few years to cost effective solutions in all markets



Way to boost capacity in indoor and urban markets; high capacity provisioning with quality spectrum; a winning proposition for large operators in some scenarios

Cloud RAN/vRAN

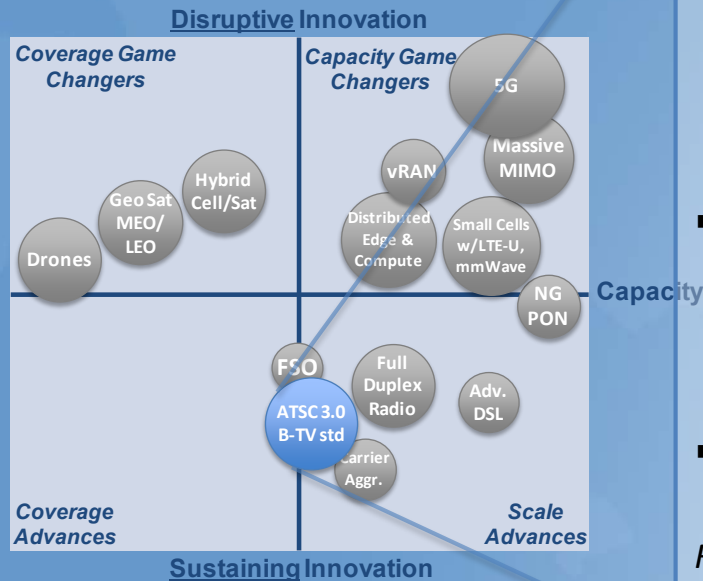
Cloud RAN/vRAN can take several different forms



n
nt and
tion with

*with different cost/
benefit tradeoffs.*

Next Generation Broadcast (ATSC 3.0)



Flexible Physical Layer

- Select operating points to match services
 - Robustness and data capacity
- Utilize multiple operating points simultaneously
- Different network topologies
 - On-channel repeaters, channel bonding etc.
- Ability to reach all device types
 - From large screen & rooftop antenna to handheld portable devices

Internet Protocol based Transport Layer

- Broadcast “bits” to a multitude of receivers simultaneously
- File based transmission capability
 - Down load content to receivers with storage
- Hybrid Broadband/Broadcast applications

UHDTV, immersive audio, improved accessibility, personalization and interactivity

FCC impact: Rules would need to be revised to allow use of ATSC 3.0

Timeframe: 2 -3 Years

A flexible and efficient IP-based technology to broaden the broadcast application space.



Future Game Changing Technologies

Demand SWG

Brian Markwalter - Chair

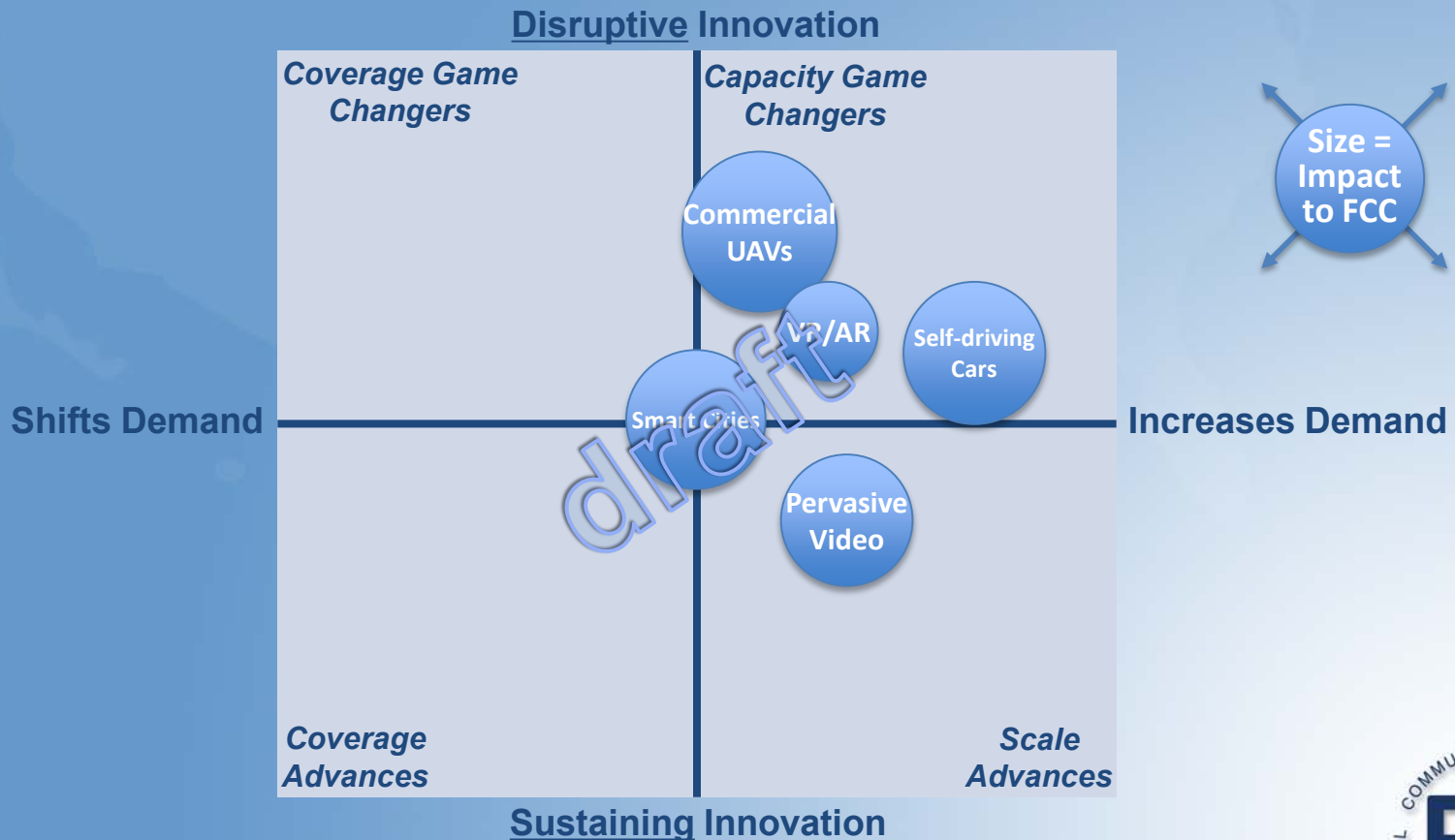


Demand SWG Topics

- Smart Cities Done
- Virtual/Augmented Reality Scheduled
- Self Driving Cars
- Personalized Medicine
- Commercial UAVs Done
- National Public Safety Network Scheduled
- Pervasive Video
- Device-device communications



Demand SWG Analysis



Preliminary Demand Analysis

- Smart Cities
 - Not analyzed as a demand category
 - Instead, a framework to think about future technologies and applications
- Commercial UASs
 - Large scale use of small UASs in commerce
 - Hundreds of thousands of flights per day
 - Factors: airborne radars, risk, spectrum allocation



Unmanned Aircraft Systems

- FAA proposed rules to allow small UAS
- Hundreds of thousands commercial flights per day once integrated into airspace
- Control and Non-Payload Communications, work in process by FAA
 - ISM (unlicensed), probably limited to low-risk flights
 - Commercial bands, impact of radios in the air
 - AM(R)S, WRC-12 grants 5030-5391 MHz, FCC proceeding 2015



Future Game Changing Technologies

In-Process Recommendations

FGCT WG In Process Recommendations

The pace of change of ICT technologies & networks is accelerating. How might the FCC commensurately evolve its awareness & expertise, in these areas?

- Devote resources to build internal technical capability and business analysis skills - notably to maintain its broad understanding and vision
- Continue to tap industry, academic, and government sources of expertise by creating venues and opportunities to systematically review emerging technologies and their impact
- Provide opportunities for Commission's personnel to further participate in standards, open source, and other activities important to the evolution of ICT eco-systems. This would include participation in international efforts – developments which increasingly have global impact on technology and business practices.
- Openly disseminate findings and analysis including an annual “hotlist” of emerging technologies.
- FCC should continue to monitor global efforts, focused on infrastructure and smart cities
 - Particularly as they relate to choosing metrics that reflect education, culture, sustainability, and well being
 - FCC Programs such as “Model Cities” should take advantage of existing investments in Smart Cities initiatives so that it may continue to provide leadership for development and deployment of advanced communication technologies, including experimentation with a broad range of business practices.



FGCT WG In Process Recommendations

- Both the consumption patterns for ICT services, as well as the way they are developed, operated, and maintained, have changed significantly. And, such change is likely to accelerate. This leads to new business models, practices and opportunities.
- In this setting it is valuable when the FCC can anticipate such changes to develop policies and regulation, that are technologically neutral, but which encourage innovation and investment
 - The FCC should frequently review existing rules and regulations to identify, eliminate or modify those that have been made obsolete by technological advances
 - The FCC should ensure that policies, rules and regulations do not hinder innovation, investment, and competition.
 - The FCC should continuously examine the national investments it spearheads with an eye to warrant those investments are informed by emerging practice and are technologically sound (USF and School and Libraries Programs)
 - The FCC should exploit these capabilities to anticipate needed changes that affect areas such as Public Safety and the ability to meet national societal goals.

FGCT WG In Process Recommendations

- Two critical patterns are emerging from the trends that we mark as important to the FCC:
 1. Increasing “digital virtualization” of Network functions and services using commonly available ICT Technologies.
 2. Investment by consumers in edge devices and capabilities that are economically important and that are changing the patterns of demand for media and consumption of ICT services, enabled and driven by the first trend.
- The FCC should encourage (and not hinder) better utilization of network resources by advocating practices that contain a greater degree of programmable consumption and optimization.
- The FCC should consciously and explicitly evaluate actions going forward with agile, programmable networks and dynamic service/network ecosystems in mind
- The FCC should maintain a technology neutral stance and allow changes in demand and availability of services to be met by market forces. Needs of disenfranchised parts of the market for essential services should be accomodated through appropriate incentives.

FGCT WG Next Steps

- The WG and the SWGs will continue scheduling talks and presentations from SME's (Suggestions for speakers and sources of expertise welcome from the TAC)
- Each of the SWGs is completing the analysis to identify most promising technology areas and will provide on analysis of 2-3 technologies for the final product.
- Concentrate on deeper insights on potential impacts of interest to FCC and on accompanying actionable recommendations.
- Produce a final briefing for use by the FCC



Next Generation (NG) Internet Service Characteristics & Features Working Group

Chairs: Russ Gyurek, Cisco
John Barnhill, GENBAND

FCC Liaisons: Walter Johnston, Scott Jordan, Padma Krishnaswamy, Alec
MacDonell, Kristine Fargotstein

FCC On-Site Meeting, Washington DC
Sept 24, 2015



Working Group Team Members

- Mark Bayliss, Visualink
- Nomi Bergman, Bright House
- KC Claffy, CAIDA
- John Dobbins, Earthlink
- Adam Drobot, OpenTechWorks
- Andrew Dugan, Level3
- Lisa Guess, Juniper
- Stephen Hayes, Ericsson
- Theresa Hennesy, Comcast
- Farooq Kahn, Samsung
- Brian Markwalter, CE
- Kevin McElearney, Comcast
- Thyaga Nandagopal, NSF
- Tom McGarry, Neustar
- Milo Medin, Google
- Lynn Merrill, NTCA
- Jack Nasielski, Qualcomm
- Ramani Pandurangan, XO Comm
- Mark Richer, ATSC
- Marvin Sirbu, Carnegie Mellon
- Kevin Sparks, ALU
- Sanjay Udani, Verizon
- David Young, Verizon



WG Focus Areas - Updates

- CDN
- Encryption
- QoS Performance Metrics
- QoE
- End-to-end QoS



Content Delivery Networks - Current Status

- Small number of CDN providers deliver majority of Internet content
 - Effectiveness depends upon hit rate: success ratio of finding desired content in cache
 - Hit-rates may be declining (Democratization of content)
- Transparent caching by ISP networks
 - Dynamic caching of multi-services/general Internet content to minimize facilities issues and backbone/transit costs
 - Typically in smaller networks or wireless networks
 - Encryption will inhibit transparent caching
- CDN delivery efficiencies be evolving closer to consumer
 - Predictive pre-positioning of content ...all the way to consumer premises
- CDNs evolving to provide increased computation vs object delivery only



Summary: CDNs strongly impact content and Internet economics and performance

CDNs: Potential Concerns

- Relative role of CDN and ISP in QoE not well measured or understood
 - Emerging firms trying to measure QoE
- Weak coordination between CDNs and ISPs
 - CDN operator controls which server is used and SP ingress point
 - Lack of publisher planning for impact of major download events
 - e.g. major new software releases
 - Tendency for each party to self-optimize
 - Nash equilibrium << coordinated planning

CDNs: Potential Concerns – cont.

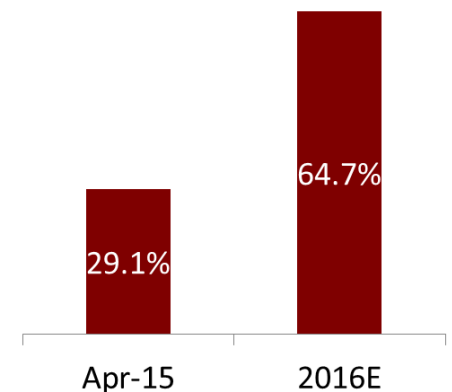
- Inadequate CDN coverage in rural environments
 - Emerging consortia arrangements
 - As CDN's become larger in size due to technology advances, economic qualifiers for smaller markets to obtain CDN's become less attractive
- CDNs have greatly reduced the cost of OTT (unicast packet delivery) video delivery, making it competitive with broadcast delivery for some use cases. Relative cost and pricing of OTT vs broadcast delivery models will continue to be contentious
 - E.g. zero rating, volume pricing

Encryption Summary

- Trend: Growth of encrypted data in the network
 - majority of traffic encrypted by end of 2016
 - Unstoppable trend driven by a variety of factors
 - Standards for trusted proxies not getting traction
 - Incorrect Implementation: EG. up to 15% invalid certs.
- Expected impacts
 - Transparent caching (wireless & wireline)
 - Value-Add Services (security, parental control, ..)
 - Network Management based on DPI/content awareness
- Aggregate subscriber service controls unaffected, but content-aware network management will be limited
- Network management (in presence of encryption) is not mature
- Conflicting industry interests make finding solutions difficult

Encrypted Traffic - % All Traffic
NA Fixed Access Service Providers

Source: Sandvine, Inc.



FCC Action: Assume encrypted data in all future policy decisions

Defining Quality of Experience (QoE) – Commission Interest

Quality of Service

- QoS describes technical network performance. A network centric concept
 - throughput, latency, jitter and packet loss
 - Easily measurable today in context of specified network endpoints and network conditions
- Users do not directly perceive these parameters



Quality of Experience

- User Perception = QoE: app performance degradation
- Experience based on usage model
 - applications consumed
 - BB speed/tier choice
- Limited methods & infrastructure to support QoE measurements
 - User surveys estimate QoE
- Collecting consistent, objective data will be challenging due to subjectivity of QoE concept

Performance - Defining Metrics/ Methodologies

- FCC MBA methodologies (combine User and ISP Sourced data)
- Goal: Common Metrics & Strategic Metrics
 - Determine what data to collect/monitor, and ability to collect such data
 - Define expected results. IE. Locate problem areas, Open Internet transparency
 - Define potential safe harbor(s)
- ISP Guidelines
 - *Consumer Advisory Committee* coordination: in process of creating consumer performance information
- Pair QoS with Applications:
 - Determine which services/applications to include, and not include
- Performance metrics will not be related to prioritization



Internet End-to-End QoS

- Will the *next generation Internet* require QoS, what is different?
- Hypothesis: E2E QoS is Technically feasible; business model uncertain
 - How would QoS be managed across multiple edges and govern in the core?
 - De Facto QoS standards at ISP and industry level.
 - Relative QoS vs guaranteed, SLA's
 - User controlled
 - Consider impact of factors such as CDN, Encryption, Encapsulation
- Is there a need to provide more granular service grades in the commodity Internet beyond the current practice
 - What data might substantiate going in this direction?
 - What would a greater granularity of service specifications look like



Questions & Comments



BACK UP MATERIAL



CDN MATERIAL



CDN History

- CDNs started in 1999 (Akamai) with a value proposition to offload and consolidate bulk web delivery from many customers through common distribution systems
- In the last decade, the majority of the Internet volume has consolidated to only a few CDN distributors all with similar delivery options
 - Content can use multiple CDNs (w/ SLAs) and dynamically switch between CDNs based on performance
 - Single purpose CDNs (.e.g. YouTube, Netflix) are mostly responsible for the QoE of their specific service
- CDNs determine much of the consumer experience for the services they support via the QoS choices they make around servers, storage, location and delivery network.
- Many CDNs have evolved to add advanced service features like security, web acceleration, transaction services, localized compute, etc
- Raw bit delivery CDNs (serving primarily OTT Video), have fewer feature requirements and most innovation incentives are designed around reducing Internet delivery costs. (e.g. better encoding, compression, deeper delivery, etc)
- CDN's now make up the vast majority of all Internet traffic with two over 50%

CDN Futures

- To improve the overall Internet ecosystem, CDNs need to continue to innovate and evolve towards greater end to end efficiency, and better consumer experience.
 - More efficient localization: Backbone -> Metro -> Access (what incentives exist?)
 - More efficient content delivery via compression, encoding, caching
- Use of multi-tenant Virtual Machine environments for CDN within ISPs
 - Rural ISP/Customer impact for CDNs that have less incentives to distribute into smaller locations/ISPs
- New DNS standards that will allow for better and more accurate CDN localization via data shared from ISP DNS servers to CDN servers.
- Home becomes part of the cloud – local storage to intelligently pre-position non-interactive content off-hours (patches, games, on-demand video)
 - Content rights barriers?
- Will “Compute” follow the path of CDN or are there more unique requirements?
- As much of the consumer Internet experience is determined by CDNs today, independent measurement, similar to MBA may be warranted to help isolate and address any end to end sources of performance problems that affect consumers.



CDN Team Notes

- CDN's must continue to become more efficient
- Problems is we don't view from larger network picture
- Business arguments will get in way of technical implementation
- For QoS/QoE, must all work together
- Potential impact on large content pushes to BIAS based on network capacity/saturation- Impact to BIAS and other parts of the network
- Eco-system approach for success: Best practices matter



ENCRYPTION MATERIAL



Encryption 9/3 Notes

- Lots of encoding/caching strategies that happen today, meant to be transparent
- Less transparency impacts mobile network
- Not encryption but, encapsulation (over UDP) problem-hiding protocol info
- What is impact to network management?
 - Potential transparent caching impact
- Encryption is broken
 - CDNs serving up to 15% invalid certs. Is this larger problem for mobile devices (not checking cert lists)?
- SPs & content providers collaborating to break trusted proxies?
 - IETF discussion (not supportive)



QOS, METRICS, QOE MATERIAL



QoE

- Defining QoE- clearly of interest, not OI. What direction is “I” going?
(Padma, KC, Russ, Alex)
 - Area that is nascent, different from QoS
 - Experience will depend on usage model: applications consumed and BB tier choice
 - Consumers do not typically understand technical variables and performance characteristics
 - Collecting consistent, objective data will be challenging
 - Consumer input will need to be combined with other data, metrics, and measurements
 - Positive: provide a baseline and trend data on network “experience” over time. Also, another point of reference outside of traditional network measurements
 - Negative: there are so many variables in an E2E application experience. One small problem could appear worse than reality- potential for misplaced blame



Notes 7.23.15

- Aspirations WP from KC and DC
- Do we know what to measure? More research needed.
- NSF workshop effort focused on measurement of QoE – Oct 23?
 - Focus on streaming: Video, gaming, real-time applications
 - BITAG is writing a report (August?)
 - Paper on history of differentiation (KC)
- Other talks on packet loss, KC will check on potential speaker
- User needs vary based on use (gaming vs streaming video...latency vs BB)
(Basket of Apps view)
- Interconnect (KC) – inter domain congestion, challenging, need a map of the internet, and exact locations, must pick sites based on hypothesis of what is congested (Paper available)



URL's

- http://www.caida.org/publications/papers/2014/challenges_inferring_interdomain_congestion/
- TPRC version:
http://www.caida.org/publications/papers/2014/measurement_analysis_internet_interconnection/
- Paper on Challenges in Inferring Internet Interdomain Congestion,
<http://conferences2.sigcomm.org/imc/2014/papers/p15.pdf>



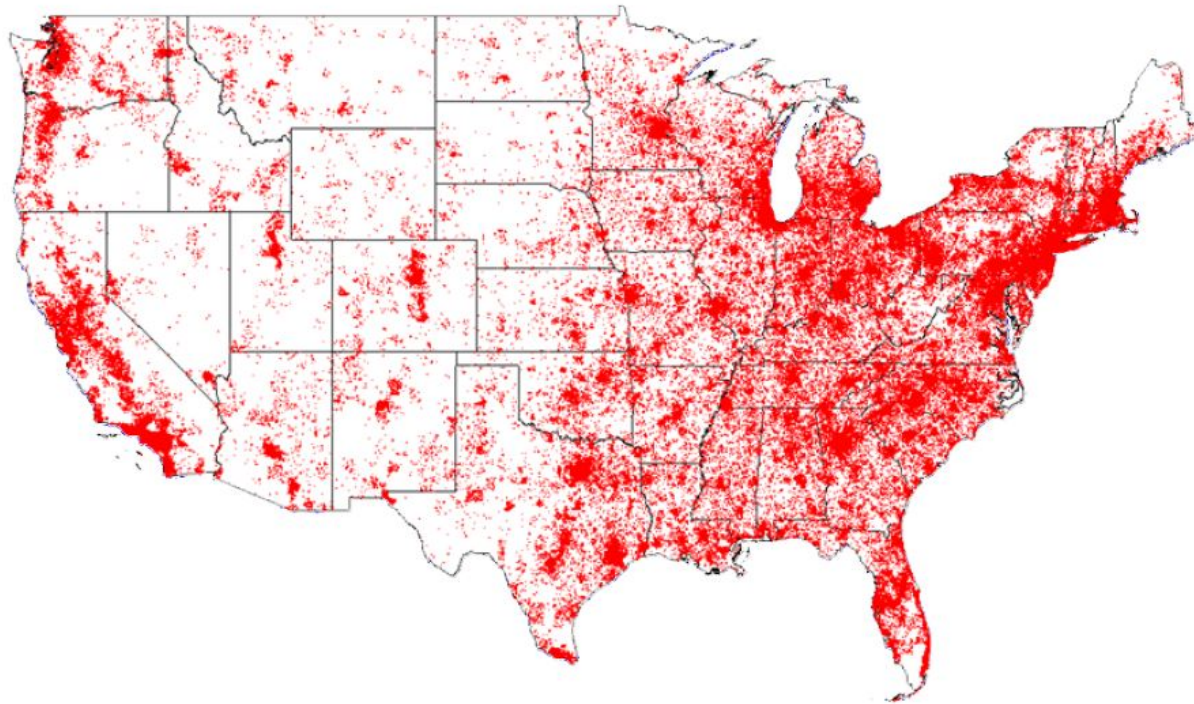
477 Testing

Steve Lanning
Chelsea Fallon (FCC liaison)
Ken Lynch (FCC liason)
Chris Feathers (Brighthouse)
Tom Wilson (Brighthouse)
Lynn Merrill (NTCA)
Megan Stull (Google)
John Barnhill (Genband)
Russ Gyurek (Cisco)



Customer Density Follows U.S. Population Density

ViaSat Customer Density



Available from google search:

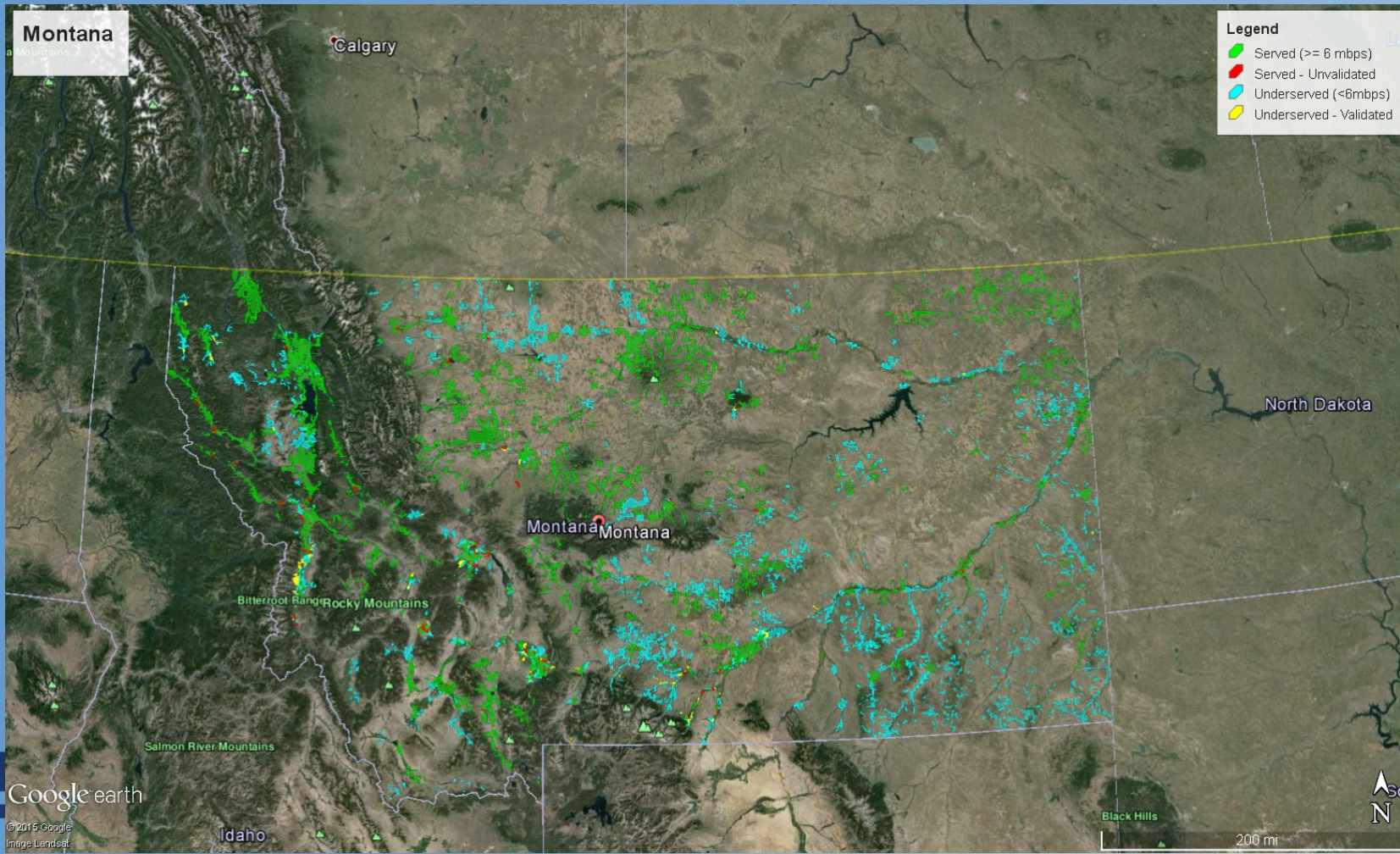
<https://prodnet.www.neca.org/publicationsdocs/wwpdf/92012viasat.pdf>

Investigate How Well Incidence Of Satellite Subscribers Follow Broadband Map

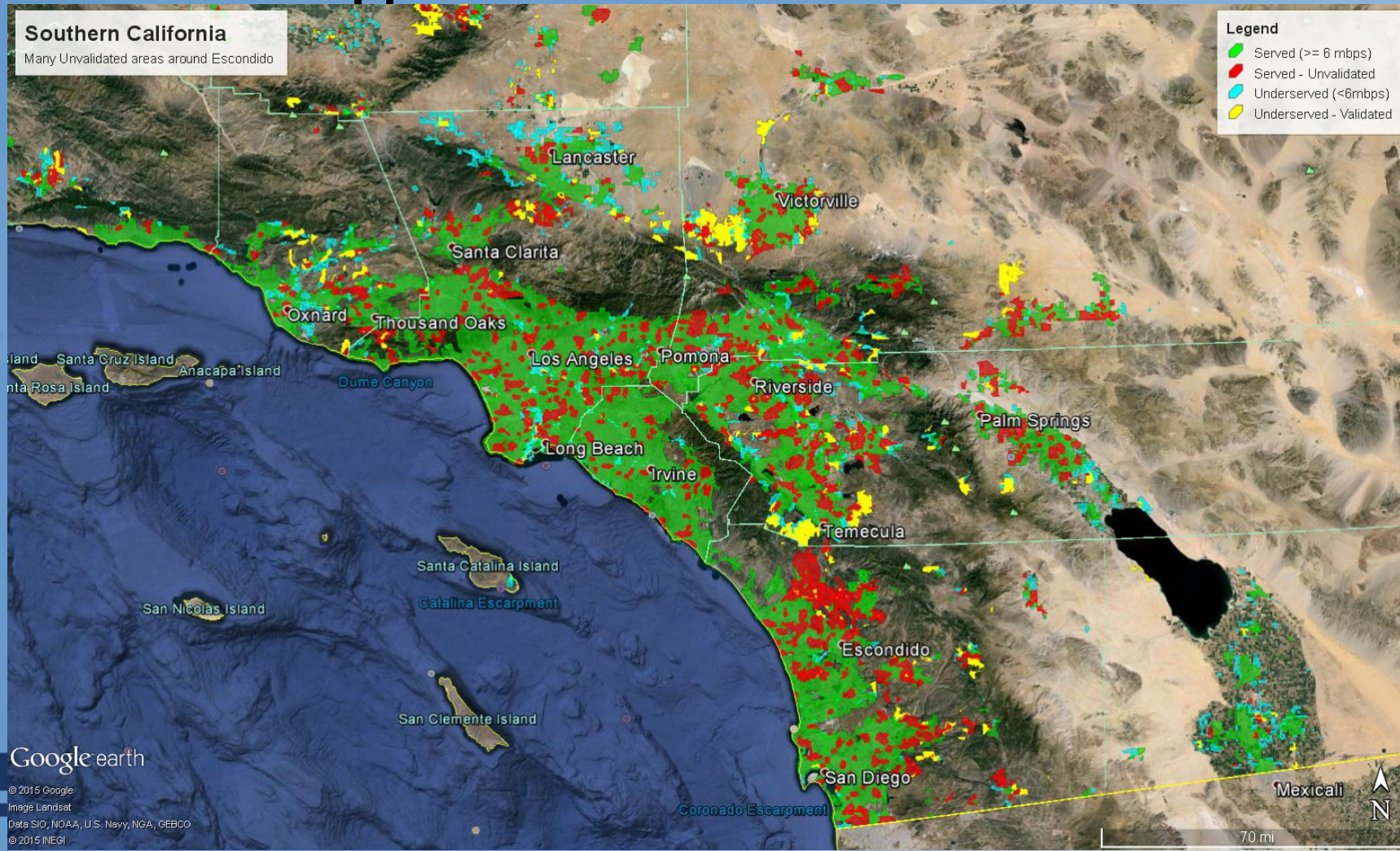
- 2014 June National Broadband map CBLOCK data
 - Code Served At 6 mbps or more - downstream
 - Underserved As 6 mbps or less - downstream
 - All end-user categories, except government
- If clusters of subscribers occur in served area, code as Unvalidated
 - Implies some homes in area is not served by comparable terrestrial or wireless alternative or satellite was preferred to available terrestrial alternatives
- If clusters of subscribers occur in under served areas code as Validated



Some states appear to be accurate



Other states appear to include Unvalidated areas

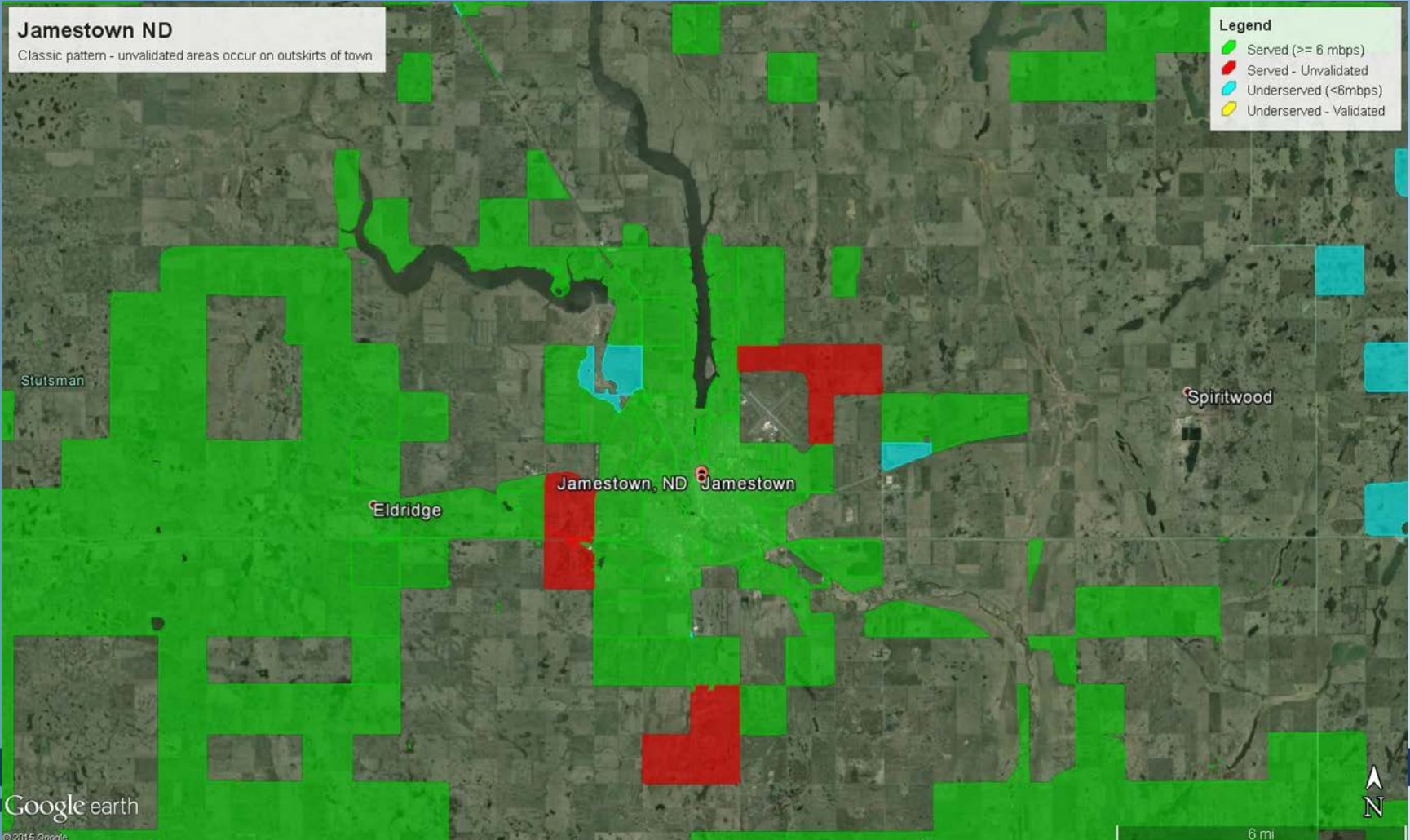


Google earth

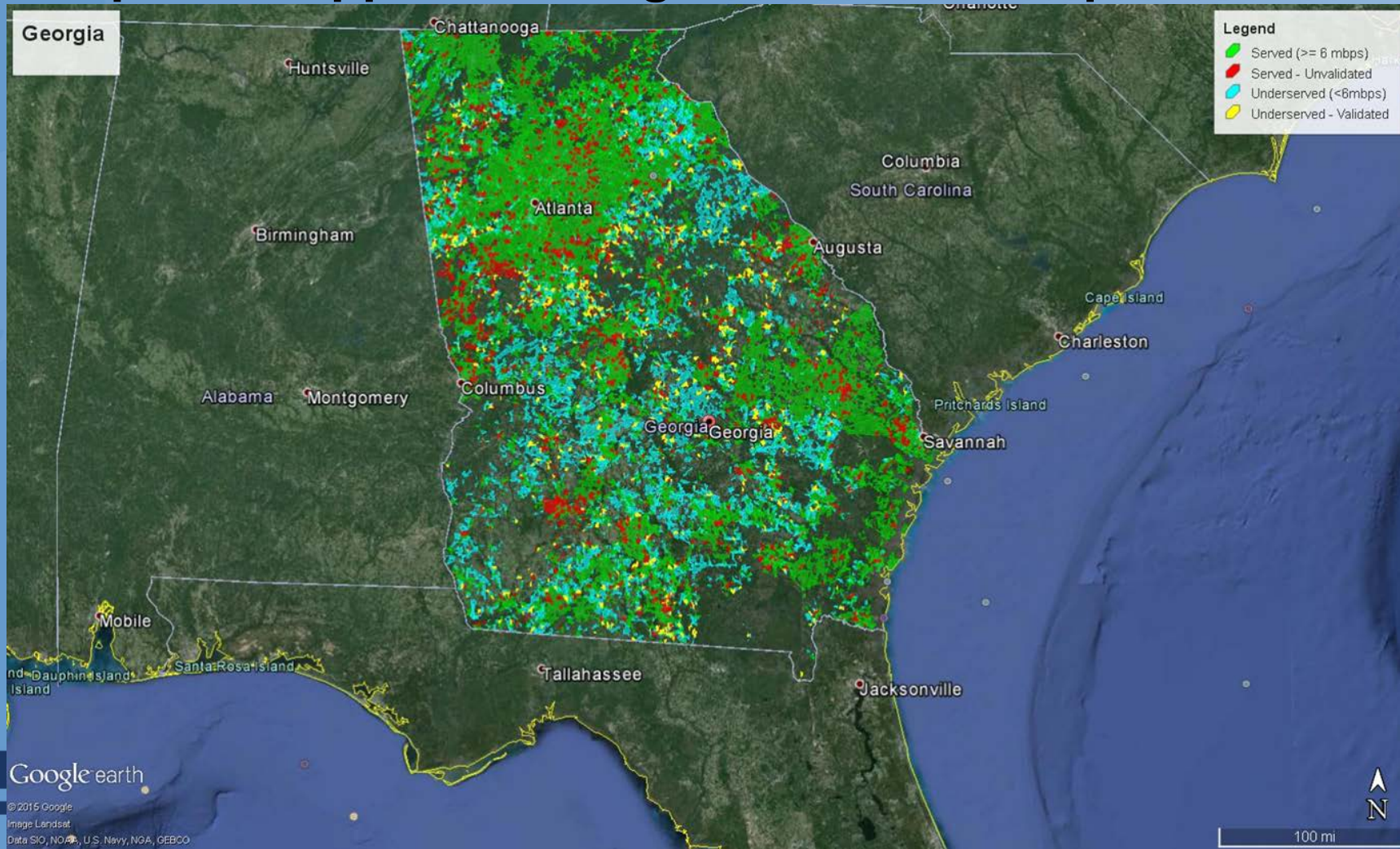
© 2015 Google
Image Landsat
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2015 INEGI



Classic Example: coverage at center of town and Unvalidated areas on outskirts



The pattern appears in larger context, example: Atlanta GA



Summary

FCC already aware of some differences

Satellite Evidence	Served	Underserved	Grand Total
Unvalidated	11%		11%
Validated		27%	1%
No Validation	89%	73%	89%
Grand Total	120,635,903	2,893,014	123,528,917



Recommendations

- Resume work on 477 data collection improvements for accuracy, consistency in reporting and streamlined workflow
- Apply improved 477 data to improve National Broadband Map
- Make collection of data from consumers not able to get broadband service at their address through FCC website as addition to 477 reporting easier to use



Q4 Work Program

- Support FCC liaisons in assessment of improved data collection processes and requirements
- Follow up with TAC members who did not participate in Q3 work
- October call to capture input from September filers

