Reliability & survivability: Incentives, regulation and public policy

Henning Schulzrinne (Columbia University)

NSF workshop: *Towards Re-architecting Today's Internet for Survivability*

https://aqualab.cs.northwestern.edu/nsfworkshop23-internetsurvivability/

November 28-29, 2023

The views and opinions expressed in this presentation are those of the author and do not necessarily reflect the official policy or position of any agency of the U.S. government.

Airlines & networks

Equipment vendors & operators

commodity
(rarely loved, only hated less)

livery
advertising
pricing

BOEING AIRBUS

NOKIA ERICSSON HUAWEI

Boeing 737
designed 1967

INTERNET PROTOCOL

DARPA INTERNET PROGRAM

PROTOCOL SPECIFICATION

September 1981

UNITED 770-800

American Airlines

verizon

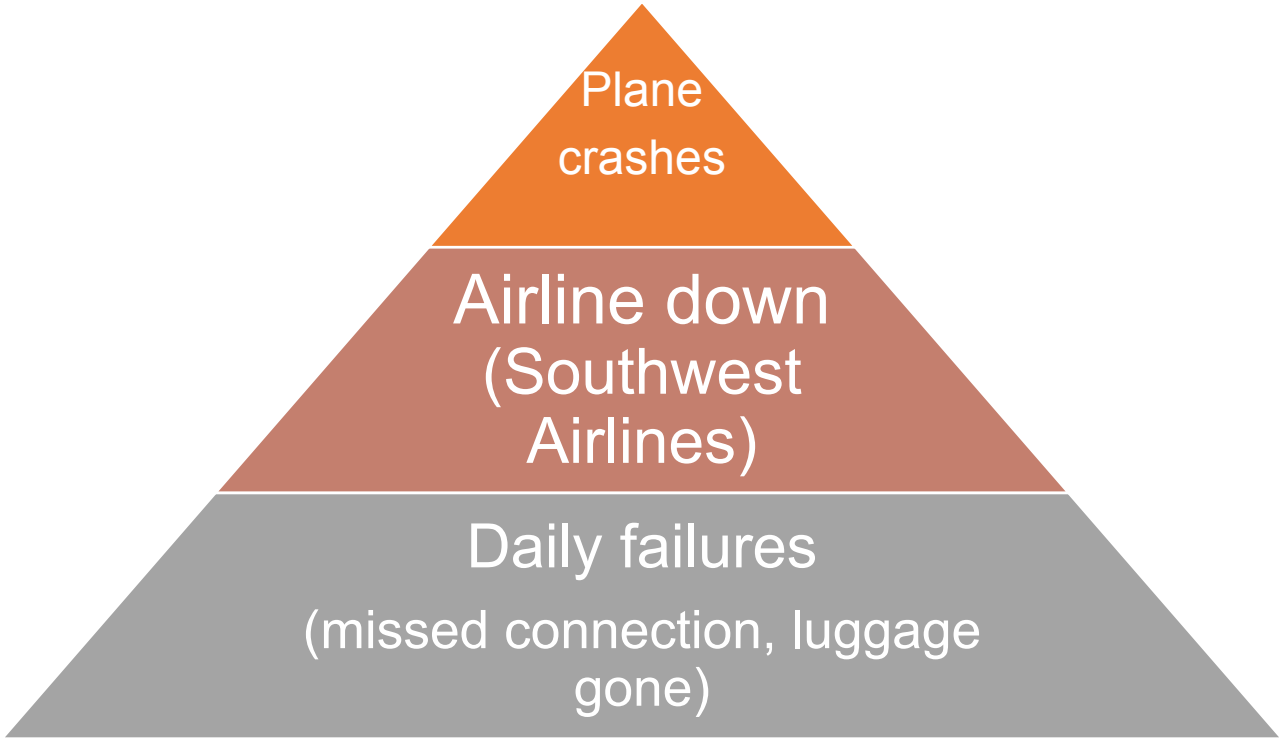
COMCAST

800 GSM operators

Airline reliability

RANK	CARRIER[1]	JANUARY - DECEMBER 2022		JANUARY - DECEMBER 2021	
		FLIGHT OPERATIONS SCHEDULED	PERCENT OF ON-TIME ARRIVALS	FLIGHT OPERATIONS SCHEDULED	PERCENT OF ON-TIME ARRIVALS
	TOTAL	6,729,125	76.61	5,995,397	81.19

Three layers of reliability



The internet as civil infrastructure

Civil infrastructure systems involves the design, analysis and management of *infrastructure that supports human activities*, such as electric power, oil and gas, water and wastewater, communications, transportation and the buildings that make up urban and rural communities. These networks deliver essential services, provide shelter and support social interactions and economic development. They are society's lifelines.

The Internet as core civil infrastructure

For Immediate Release — February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the

U.S. efforts shall address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency. This directive also identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors.

Ted Stevens (R-AK, 2006)

47 CFR Part 202: National Security and Emergency Preparedness Planning & Execution

§ 202.2 Criteria and guidance.

NS/EP planning in government and industry with respect to effective conservation and use of surviving telecommunications resources in a disaster, emergency or postattack period must provide for orderly and uninhibited restoration of services by the carriers and authoritative control of services allocation which will assure that priority will be afforded the most critical needs of government and the private sector with respect to these objectives.

(a) The preservation of the integrity of characteristics and capabilities of the Nation's telecommunications systems and networks during wartime or non-wartime emergencies is of the utmost importance. This can best be accomplished by centralized policy development, planning, and broad direction. Detailed operations management will remain decentralized in order to retain flexibility in the use of individual systems in responding to the needs of national security, survival and recovery. Each Federal agency responsible for telecommunications systems operations, and the carriers, are responsible for planning with respect to emergency operations. Guidance in this matter has been issued from a number of sources and contained in:

(1) Annex C-XI (Telecommunications), Federal Emergency Plan D (Classified).

(2) National Plan for Telecommunications Support in Non-wartime Emergencies.

(3) The National Communications System Management Plan for Annex C-XI (Telecommunications) Federal Emergency Plan D (Classified).

(b) The continuity of essential communications services will be maintained through the use of controls and operational procedures to assure that priority is given to vital services. NS/EP telecommunications services entail policies, procedures and responsibilities as described in parts 211 and 213 of this chapter.

Communications as linked critical infrastructure

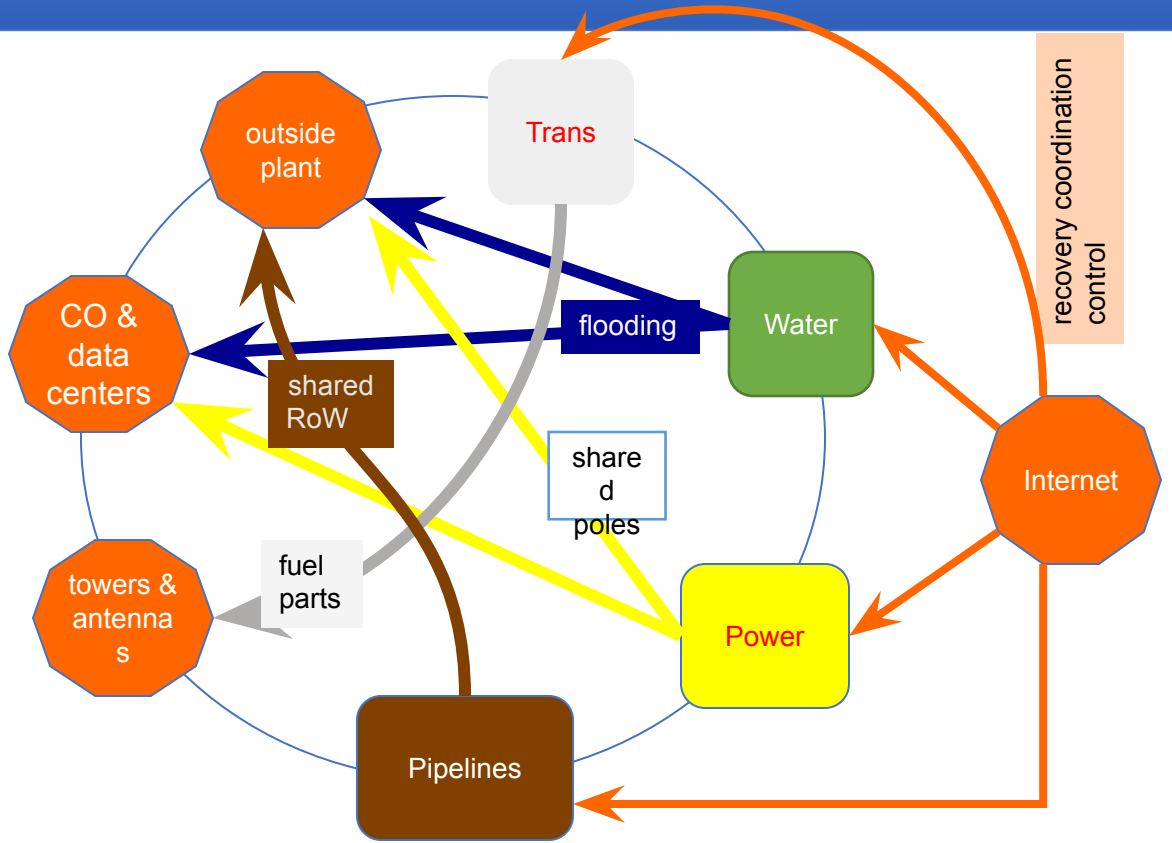
- ***Energy Sector***
  - *provides power to run cellular towers, central offices, and other critical communications facilities*
  - *relies on communications to aid in monitoring and controlling the delivery of electricity.*
- ***Information Technology Sector***
  - *provides critical control systems and services, physical architecture, and Internet infrastructure*
  - *relies on communications to deliver and distribute applications and services.*
- ***Financial Services Sector***
  - *for the transmission of transactions and operations of financial markets.*
- ***Emergency Services Sector***
  - *directing resources, coordinating response, operating public alert and warning systems, and receiving emergency 9-1-1 calls*
- ***Transportation Systems Sector***

Communications

https://www.fema.gov/sites/default/files/2020-07/fema_ESF_2_Communications.pdf

Interdep

Interdependencies with other lifelines



A web app is now “national infrastructure”

TECH

Ubiquitous South Korea App Goes Offline, Raising Fresh Concerns Over Tech Giants

Kakao’s widespread role in messaging, online banking and other services prompts officials to wonder if the ‘everything app’ has grown

The Kakao service breakdown drew quick attention from South Korean officials. On Monday, President Yoon Suk-yeol likened Kakao’s services to a national infrastructure and asked the country’s antitrust regulators to more deeply explore potential issues that come with a monopolized market. Lawmakers proposed adding companies like Kakao that operate critical online services and data centers to the national disaster-response system to ensure faster recovery and responses to potential service disruptions.

a book at the library to ordering food online. The Kakao messaging app tethers to an individual’s smartphone number, which must be connected to a person’s government-issued identification, making the app a convenient way to access many services, said Park Kyung-sin, director at Open Net Korea, a nonprofit advocating for digital rights.

“Kakao has become the go-to tool for identity verification,” said Mr. Park, who is also a law

Oct. 17, 2022 (WSJ)

Reliability & survivability

- Informal: reliability is the daily availability of ordinary capability
  - survivability is the ability to continue to function, possibly degraded, in face of extraordinary circumstances
    - such as natural or man-made disasters

Cost of outages vs. SLA

The average cost of downtime across all industries has historically been about $5,600 per minute, but recent studies have shown this cost has grown to about $9,000 per minute.

Of course, other factors play a role in this, such as:

- **The size of the business:** There's a significant difference in downtime costs between larger and
  $13
  $16,
- **Indu**
  com
  gove
  high

European airline compensation >> hourly wage

Amount in EUR	Distance
	00 km

8. Limitation of Liability and Indemnification. YOU ACKNOWLEDGE AND AGREE THAT COMCAST WILL NOT BE LIABLE FOR ANY SERVICE OUTAGE, INABILITY TO DIAL OR TEXT 911 USING THE SERVICE(S), AND/OR INABILITY TO ACCESS EMERGENCY SERVICE PERSONNEL. YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS COMCAST AND ITS AFFILIATES, SUPPLIERS OR AGENTS FROM ANY AND ALL CLAIMS, LOSSES, DAMAGES, FINES, PENALTIES, COSTS, AND EXPENSES (INCLUDING, BUT NOT LIMITED TO, REASONABLE ATTORNEYS' FEES) BY, OR ON BEHALF OF, YOU OR ANY THIRD PARTY OR USER OF THE SERVICE(S) RELATING TO THE FAILURE OR OUTAGE OF THE SERVICE(S), INCLUDING THOSE RELATED TO 911/E911.

cogent [redacted]

[redacted]

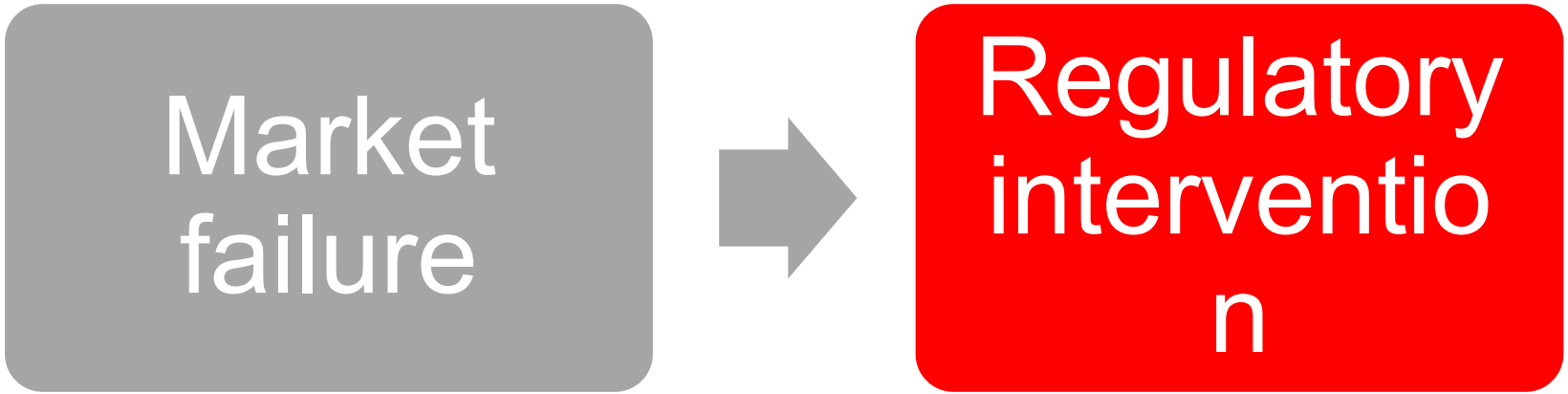
Asymmetric information & moral hazard

- *Asymmetric information* – one party to the bargain has relevant information unknown to the other party
  - regulated firm and regulatory agency, employee and employer
- *Moral hazard* – one party may undertake actions adverse to the other party that cannot be completely monitored
  - homeowner's private fire prevention efforts and insurance company
  - employee's intensity of effort and employer
  - health insurance

“Market for Lemons” (Akerlof, 1970)

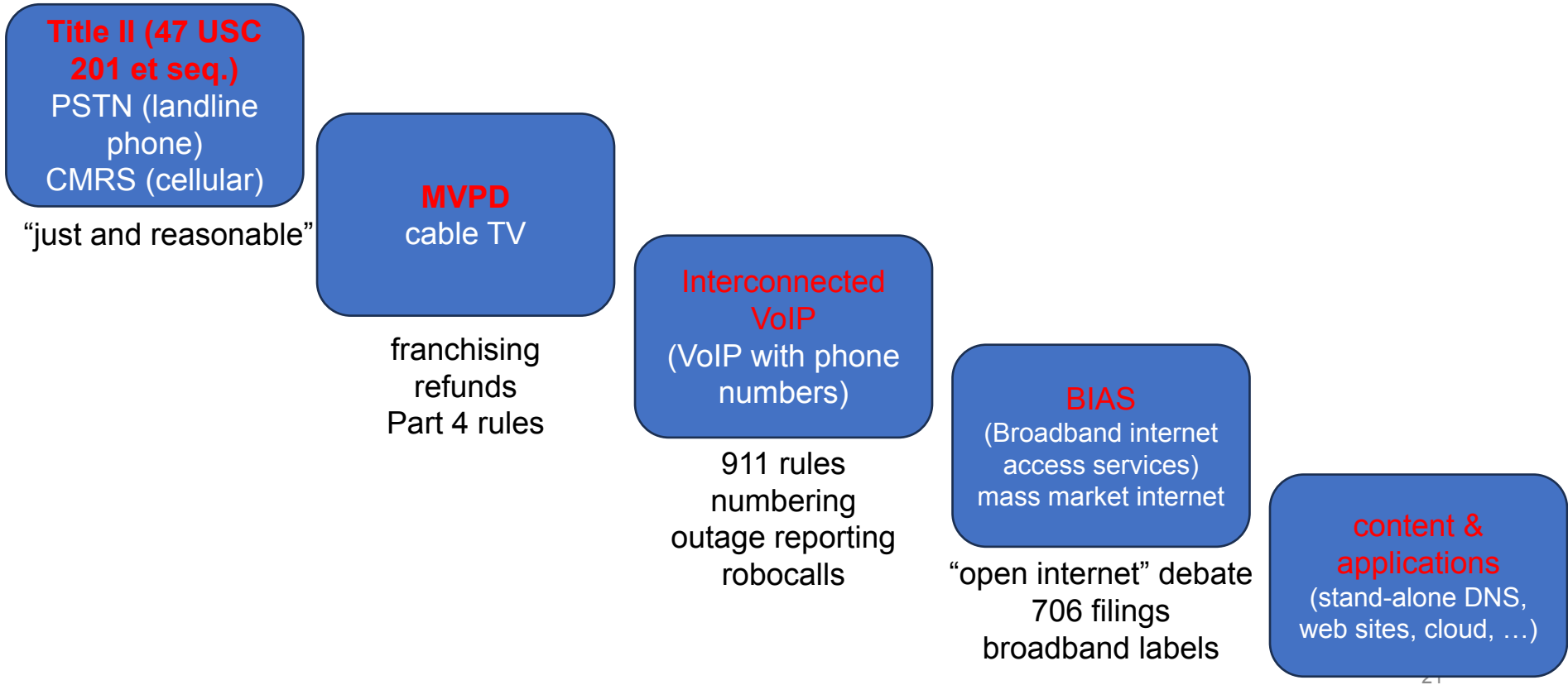
- Suppose buyers know that 50% of used cars are “lemons” worth $1000 and 50% are good cars worth $2000, but cannot distinguish between the good and bad cars.
- If neither buyers nor sellers can distinguish car types, the equilibrium price would be the expected value of $1500.
- If only sellers can distinguish, the equilibrium is to sell only bad cars at $1000.
- Asymmetric information combined with moral hazard creates adverse selection and eliminates the market for good used cars.

Econ 101



The US regulatory tool kit

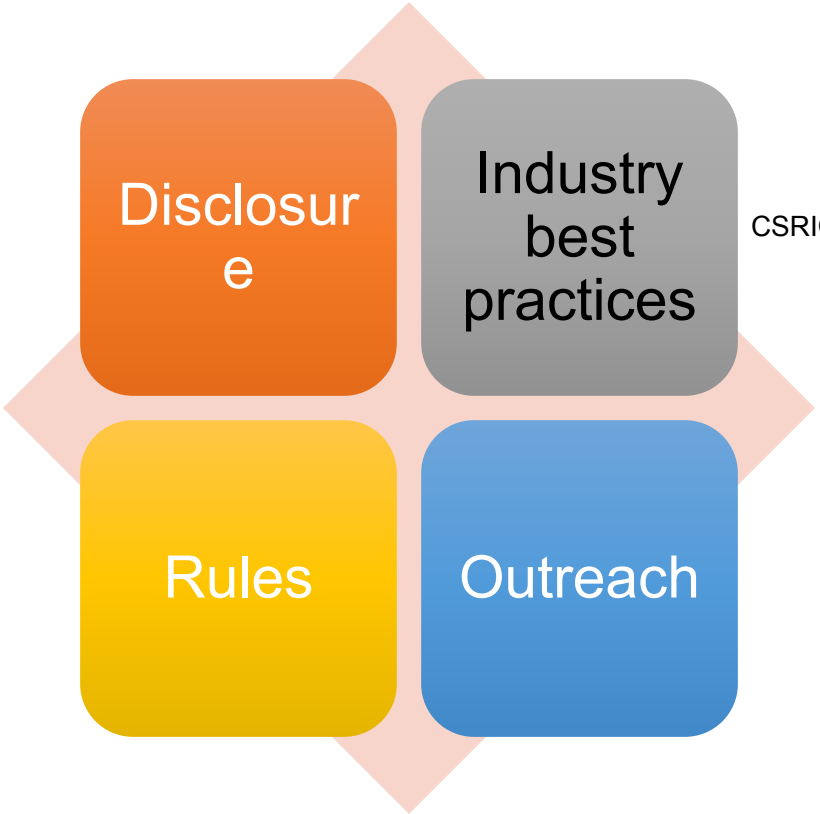
The US authority landscape



The FCC tool kit

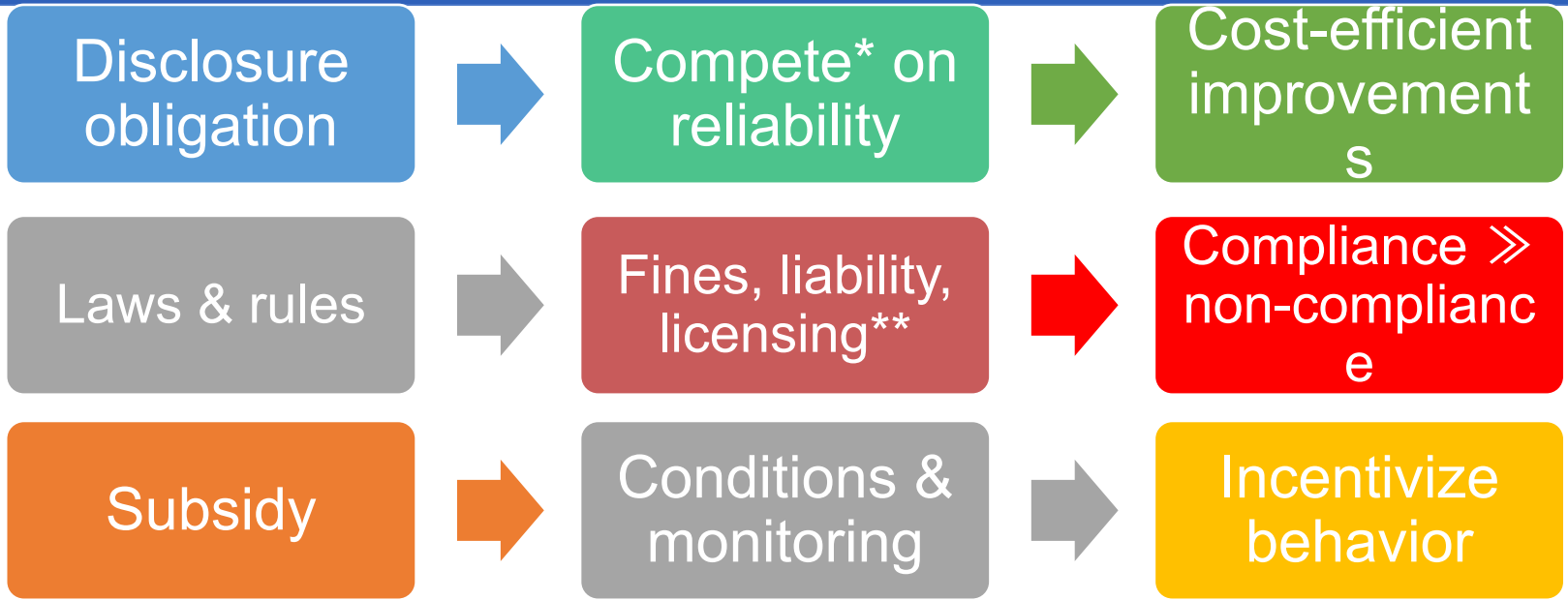
MBA
9-1-1 post-incident reports

47 CFR Part 4
communications
9-1-1



CSRIC

The regulatory tool kit – action model



but: relies on legal authority □ constrained actions & scope

- 1934 & 1996 Communications Act (47 USC)
- in the US, no clear legal authority for BIAS □ "Title II" ("open internet", "network neutrality")

* assuming competition ** e.g., ETC

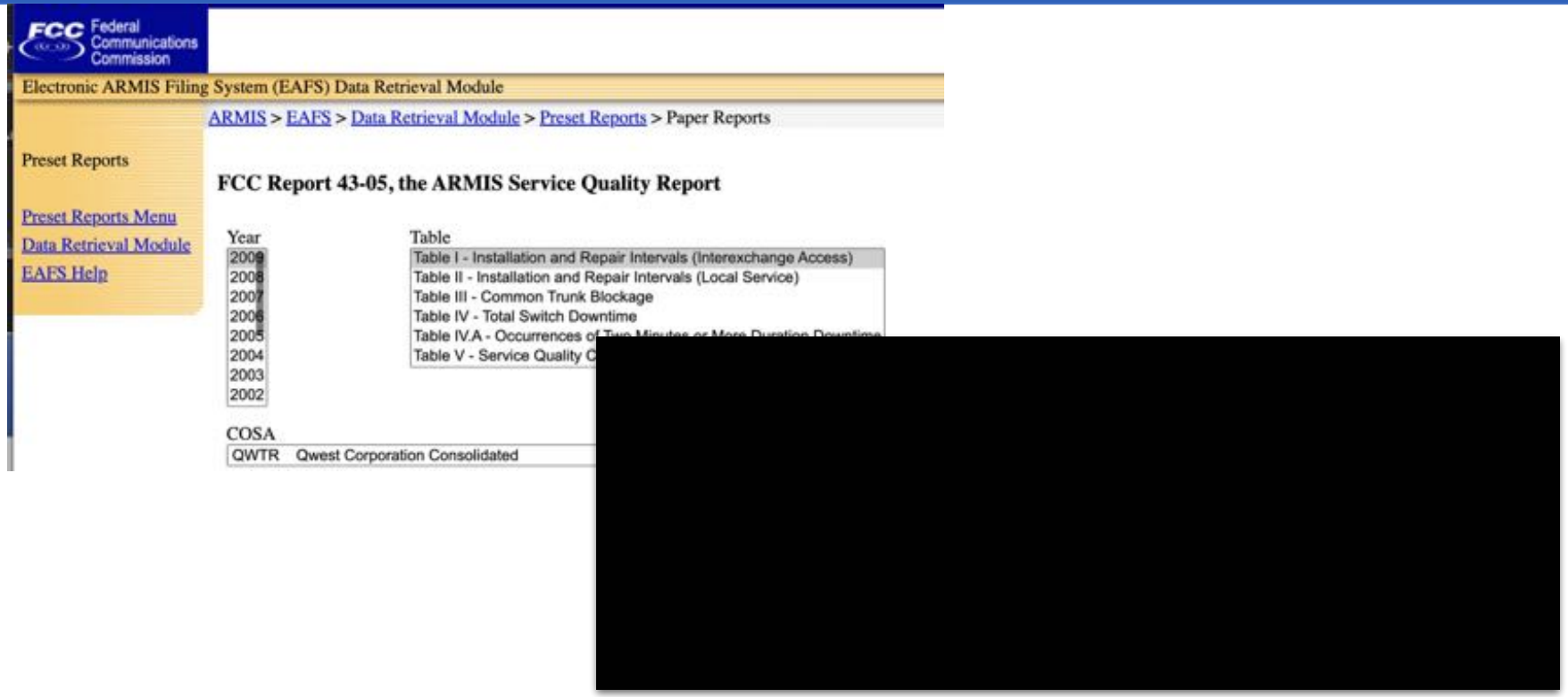
811 (Call-before-you-dig)

What is 811?

811 is the national call-before-you-dig phone number. Anyone who plans to dig should call 811 or go to their state 811 center's website before digging to request that the approximate location of buried utilities be marked with paint or flags so that you don't unintentionally dig into an underground utility line.

State regulators: classical service quality

FCC ARMIS service quality report

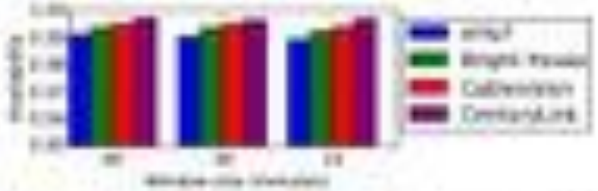


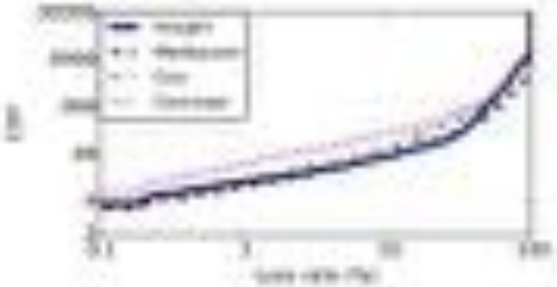
Performance measurement □ reliability measurement

- 2010-2023: *FCC Measuring Broadband America*
- roughly 2,800 hardware devices (2023) across ~10 large carriers

Metric	Primary Metric(s)
Download speed	Throughput in Megabits per second (Mbps) utilizing eight concurrent TCP connections
Upload speed	Throughput in Mbps utilizing eight concurrent TCP connections
Web browsing	Total page fetch time and all its embedded resources from a popular website
UDP latency	Average round trip time of a series of randomly transmitted UDP packets distributed over a long timeframe
UDP packet loss	Fraction of UDP packets lost from UDP latency test
Voice over IP	Upstream packet loss, downstream packet loss, upstream jitter, downstream jitter, round trip latency
DNS resolution	Time taken for the ISP's recursive DNS resolver to return an A record[21] for a popular website domain name
DNS failures	Percentage of DNS requests performed in the DNS resolution test that failed
ICMP latency	Round trip time of five evenly spaced ICMP packets
ICMP packet loss	Percentage of packets lost in the ICMP latency test
UDP Latency under load	Average round trip time for a series of evenly spaced UDP packets sent during downstream/upstream sustained tests

Reliability: "Characterizing and Improving the Reliability of Broadband Internet Access" (Bustamante et al., 2018)





ISP	Average availability			Average annual downtime (hours)		
	1%	5%	10%	1%	5%	10%
Fiber						
Frontier (Fiber)	98.58	99.47	99.77	124	46.8	20.3
Verizon (Fiber)	99.18	99.67	99.80	72	29.2	17.8
Cable						
Bright House	98.21	99.28	99.58	156	62.8	36.7
Cablevision	98.33	99.53	99.70	146	41.4	25.9
Charter	97.84	99.29	99.59	189	62.5	36.1
Comcast	98.48	99.45	99.66	134	48.0	29.7
Cox	96.35	98.82	99.33	320	103.0	58.4
Insight	96.38	98.31	98.94	318	148.0	93.0
Mediacom	95.48	98.34	99.03	396	146.0	85.3
TimeWarner	98.47	99.48	99.69	134	45.9	26.9
DSL						
AT&T	96.87	99.05	99.42	274	83.3	51.1
CenturyLink	96.33	98.96	99.39	322	90.9	53.7
Frontier (DSL)	93.69	98.18	98.87	553	160.0	98.7
Qwest	98.24	99.24	99.51	154	66.7	42.8
Verizon (DSL)	95.56	98.43	99.00	389	137.0	88.0
Windstream	94.35	98.72	99.42	495	112.0	50.6
Wireless						
Clearwire	88.95	96.96	98.13	968	266.0	164.0
Satellite						
Hughes	73.16	90.15	94.84	2350	863.0	453
Windblue/Viasat	72.27	84.20	96.37	2430	1380.0	318.0

Broadband is less reliable during busy hours (Bustamante, et al.)

ISP	A	% change in U	A	% change in U
	1%		10%	
Satellite				
Hughes	60.97	+45.4	91.38	+66.9
Wildblue/ViaSat	69.44	+10.2	94.14	+61.2
Wireless				
Clearwire	86.35	+23.6	97.57	+29.9
DSL				
Windstream	89.17	+91.8	99.13	+50.4
Frontier (DSL)	87.98	+90.4	98.42	+39.9
Verizon (DSL)	93.95	+36.2	98.90	+9.9
CenturyLink	94.19	+58.2	99.35	+6.9
AT&T	95.85	+32.4	99.38	+5.4
Qwest	97.92	+18.5	99.51	+1.2
Cable				
Cablevision	97.76	+34.2	99.64	+22.6
TimeWarner	98.03	+28.5	99.69	+1.3
Insight	95.31	+29.4	98.98	-3.9
Charter	97.75	+4.2	99.61	-6.4
Mediacom	94.52	+21.1	99.09	-7.0
Comcast	98.39	+5.3	99.70	-11.7
Brighthouse	98.15	+3.5	99.63	-11.8
Cox	96.30	+1.3	99.42	-13.3
Fiber				
Frontier (Fiber)	98.56	+1.4	99.78	-4.6
Verizon (Fiber)	99.11	+8.7	99.83	-14.7

Table 5: *Average availability (A) and percent change in unavailability (U) for subscribers of each ISP during peak hours. Some providers had significantly higher unavailability at the 10% threshold during peak hours, including Windstream and Cablevision, as well as satellite and wireless services. Cox and Verizon (fiber) had the largest improvement in availability during peak hours, as outages were concentrated during early morning or mid-day.*

Broadband label

by April 2024

Broadband Facts

Provider Name

Service Plan Name and/or Speed Tier

Fixed or Mobile Broadband Consumer Disclosure

Monthly Price [$]

This Monthly Price [is/is not] an introductory rate. [If introductory rate is applicable, identify length of introductory period and the rate that will apply after introductory period concludes]

This Monthly Price [does not] require[s] a [x year/x month] contract. [only required if applicable; if so, provide link to terms of contract]

Additional Charges & Terms

Provider Monthly Fees
[Itemize each fee or enter "None."] [$]

One-time Fees at the Time of Purchase
[Itemize each fee or enter "None."] [$]

Early Termination Fee [$]

Government Taxes [Varies by Location/Taxes Included]

Discounts & Bundles

Click Here for available billing discounts and pricing options for broadband service bundled with other services like video, phone, and wireless service, and use of your own equipment like modems and routers. [Any links to such discounts and pricing options on the provider's website must be provided in this section.]

Affordable Connectivity Program (ACP)

The ACP is a government program to help lower the monthly cost of internet service. To learn more about the ACP, including to find out whether you qualify, visit GetInternet.gov.

Participates in the ACP [Yes/No]

Speeds Provided with Plan

Typical Download Speed [] Mbps
Typical Upload Speed [] Mbps
Typical Latency [] ms

Data Included with Monthly Price [] GB
Charges for Additional Data Usage [$/GB]

Network Management Read our Policy
Privacy Read our Policy

Customer Support

Contact Us: example.com/support / (555) 555-5555

Learn more about the terms used on this label by visiting the Federal Communications Commission's Consumer Resource Center.

fcc.gov/consumer

[Unique Plan Identifier Ex. F0000937974123ABC456EMC789]

Ofcom “Comparing customer service: mobile, landline and home broadband” (May 2023)

	Average	BT	EE	KCOM	NOW	plusnet	sky	TalkTalk	vodafone
Faults per 1000 customers per month: 2022	41↓	46↓	46↓	28↑	22↓	20↓	25↓	38↓	55↑	60↓
Average time to repair a total loss of service (days)	2	2	4↑	0	2	3↑	2	2	1	1

Reporting: Network Outage Reporting System (NORS)

- Established in 2004 (47 CFR Part 4)
- Confidential reporting
- Only for PSTN, mobile voice (CMRS), interconnected VoIP
  - i.e., not broadband
- ≥ 30 minutes duration
- ≥ 900,000 user minutes
- initial & final report

Disaster Recovery & Reporting

- Department of Homeland Secusity:
  - **Overall Coordination:** Coordinate the planning for and provision of national security and emergency preparedness communications for the Federal government during disasters and emergencies.
- Federal Communications Commission (FCC):
  - **Situation Awareness Data Collection:** Collect network status and restoration data. Develop charts, tables and maps summarizing the information.

Coordination: DIRS

Disaster Information Reporting System (DIRS)

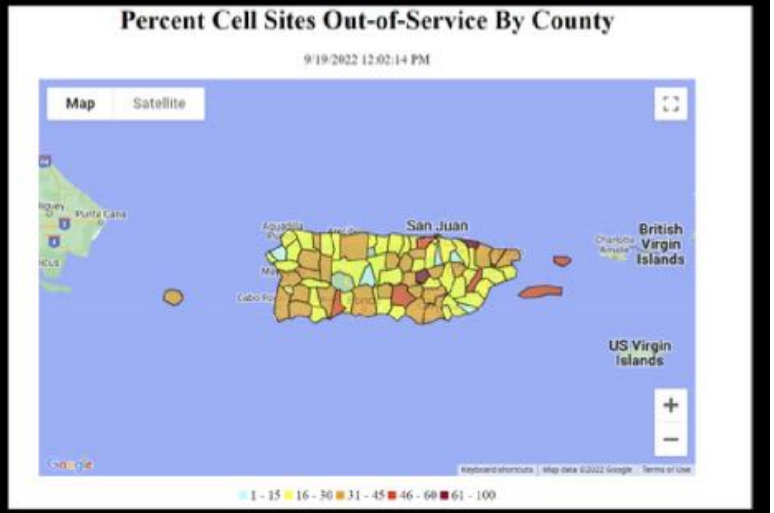
Operations and Emergency Management Division

- Emergency Communications/Preparedness
- Priority Services
- 24/7 Operations Center

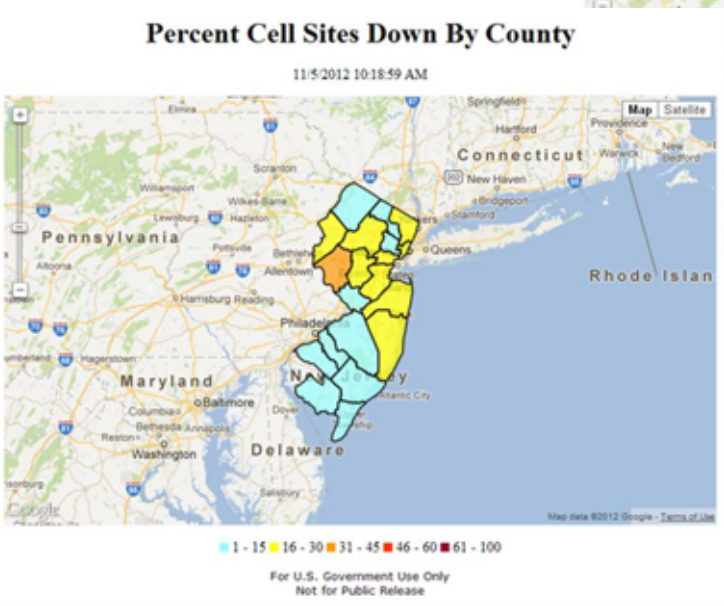
The FCC established the Disaster Information Reporting System (DIRS) on September 11, 2007, in response to the devastation caused by Hurricane Katrina.

DIRS is a voluntary, web-based system through which the Commission collects operational status and restoration information from communications providers during major disasters and subsequent recovery efforts. DIRS provides communications providers with a single, coordinated, consistent process to report their communications infrastructure status information during disasters. DIRS collects infrastructure status information from wireline, wireless, broadcast, cable, interconnected VoIP, and broadband service providers. DIRS reporting is mandatory for all Stage 2 recipients of the Uniendo a Puerto Rico Fund and the Connect USVI Fund.

Communications status reports



DIRS – Mapping Examples (Sandy)



FCC: Mandatory Disaster Response Initiative

FCC Improves Resiliency and Reliability of Mobile Wireless Networks

On July 6, 2022, the FCC released a Report and Order and Further Notice of Proposed Rulemaking to improve the resiliency and reliability of mobile wireless networks before, during, and after emergencies. In the Report and Order, the FCC adopts the Mandatory Disaster Response Initiative (MDRI) and requires all wireless providers to:

- Enter into reasonable arrangements for roaming during disasters;
- Establish arrangements for providing mutual aid during disasters;
- Take reasonable measures to enhance municipal preparedness and restoration;
- Take reasonable measures to increase consumer readiness and preparation; and
- Take reasonable measures to improve public awareness and stakeholder communications on service and restoration status.

https://www.fcc.gov/fcc-improves-resiliency-and-reliability-mobile-wireless-networks

Federally-subsidized networks: NTIA BEAD

The Broadband Equity, Access, and Deployment (BEAD) Program, provides $42.45 billion to expand high-speed internet access by funding planning, infrastructure deployment and adoption programs in all 50 states, Washington D.C., Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

[redacted]

https://broadbandusa.ntia.doc.gov/funding-programs/broadband-equity-access-and-deployment-bead-program

NTIA Middle Mile NOFO

[redacted]

[10] Relevant consider
infrastructure will in
broadband services,
infrastructure (*e.g.*, t
physical infrastructu

Applicant	Horizon Telcom Inc.	Blackfoot Telephone Cooperative, Inc.
Project Name	Appalachian Ohio Middle Mile Expansion	Sapphire Ring
Total Project Cost	$48,275,817.00	$16,795,000.00
Federal Funding Request	$27,540,553.83	$11,756,500.00
Primary State	Ohio	Montana
Secondary State(s)	N/A	N/A
Counties/Islands Impacted	Coshocton, Perry, Holmes, Muskingum, Athens, Knox, Tuscarawas, and Jefferson	Missoula, Granite, Deerlodge, Silverbow, Beaverhead, and Ravalli counties
	The Appalachian Ohio Middle Mile Expansion project focuses on key gaps in Appalachian Ohio's open middle mile infrastructure. Building upon NTIA's previous investments in the Ohio Middle Mile Consortium (OMMC), the applicant's design reaches two counties currently lacking any open middle mile, establishes new POPs in three counties, and densifies the existing network in six additional counties. The design closes multiple rings, increases reliability and resiliency for the entire service area, and creates additional interconnection points among the original OMMC members. The proposed	The project's purpose is to add 137 miles of new middle mile fiber in remote western Montana. Spread across six counties, covering more than 13,000 square miles, and impacting 42 communities, the project will enable affordable broadband to thousands of unserved and underserved locations. In addition, the project will create a fiber-ring totaling roughly 365 miles, delivering network reliability, resiliency, and positively impacting the broadband experience of thousands of Montanans.

Example: 911 outages

Example: AT&T 9-1-1 outage on March 8, 2017

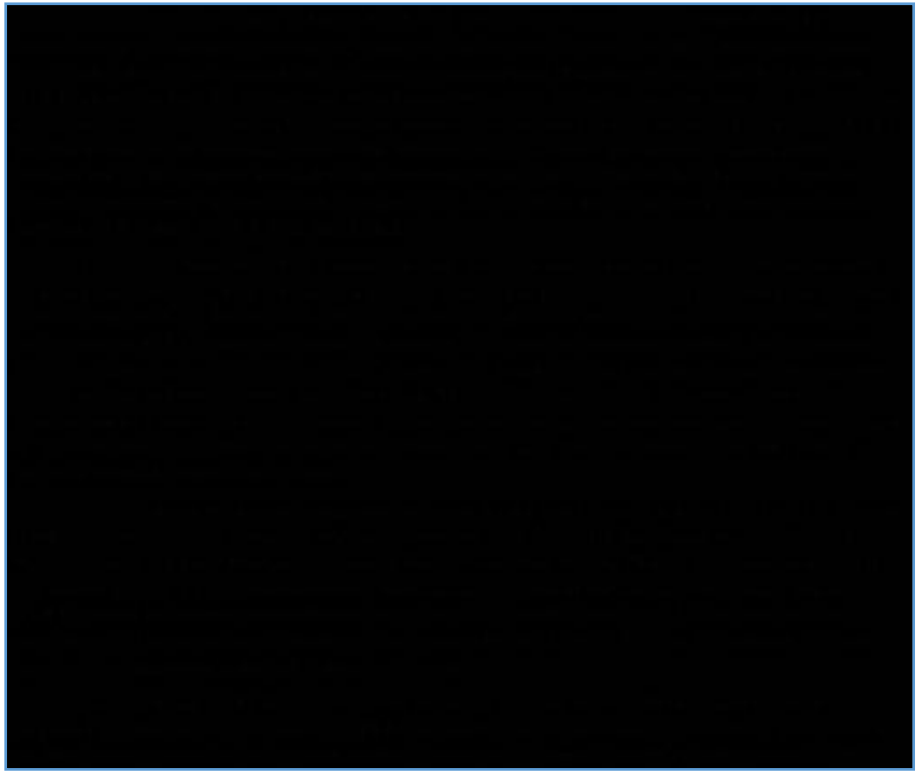
1. On the afternoon of March 8th, 2017, nearly all AT&T Mobility (AT&T)[1] Voice over LTE customers across the nation lost 911 service for five hours.[2] Federal Communications Commission

2. As described in greater detail below, the outage was caused by an error that likely could have been avoided had AT&T implemented additional checks (*e.g.*, followed certain network reliability best practices) with respect to their critical 911 network assets. Approximately 12,600 unique users attempted to call 911, but were unable to reach emergency services through the traditional 911 network. This was one of the largest 911 outages ever reported in NORS, as measured by the number of unique users affected.

3. Among the lessons learned from the March 8th outage is that when 911 service fails for any reason, Public Safety Answering Points (PSAPs) play a critical role in advising their jurisdictions of alternative ways to reach help. While AT&T and their subcontractors, Comtech and West, made efforts to notify thousands of PSAPs, the notifications were often unclear or missing important information, and generally took a few hours to occur. This outage also offers an illuminating case study that illustrates actions that stakeholders can take to promote network reliability and continued access to 911 service. For example, the March 8th outage emphasizes the importance of auditing all network assets critical to the provision of 911 service, and ensuring that such assets are safeguarded and designed to avoid single points of failure. The outage also demonstrates the need for closer coordination between industry and PSAPs, to improve overall situational awareness and ensure consumers understand how best to reach emergency services.

AT&T 2017: Security as the enemy of reliability – locking yourself out

- White list for security
- Maintain incorrect one in config
- Reboot to incorrect config



A sample of recent 911 failures

When	Carrier	impact	fine?	cause
April 2022	Shentel	WVa	$227k	Partial SBC upgrade lead to one-way audio
September 2020	CenturyLink Intrado	1h17m	$3.8M $1.75M	Blank configuration in call routers
September 2020	AT&T	3 hour NC	$460k	DWDM fan failure (+ same as above)
June 2020	T-Mobile	12 hours 21,000	$19.5M	The initial cause of the outage was the brief failure of a leased fiber transport link in the T-Mobile network. The outage revealed, and was compounded by, a temporary routing flaw in a single location and two previously undetected flaws in third-party software. Restoration was also impacted by a temporary failure of remote access to the affected transport link.
May 2020	Verizon	1h57m	$274k	SS7 network fails while backup is in maintenance

911 reliability (47 CFR 9.19)

- circuit audit
- eliminate single point of failure
- backup power for 24/72 hours

(c) ***Annual reliability certification.*** One year after the initial reliability certification described in paragraph (d)(1) of this section and every year thereafter, a certifying official of every covered 911 service provider shall submit a certification to the Commission as follows.

(1) ***Circuit auditing.***

(i) A covered 911 service provider shall certify whether it has, within the past year:

(A) Conducted diversity audits of critical 911 circuits or equivalent data paths to any PSAP served;

(B) Tagged such critical 911 circuits to reduce the probability of inadvertent loss of diversity in the period between audits; and

(C) Eliminated all single points of failure in critical 911 circuits or equivalent data paths serving each PSAP.

(ii) If a Covered 911 Service Provider does not conform with all of the elements in paragraph (c)(1)(i) of this section with respect to the 911 service provided to one or more PSAPs, it must certify with respect to each such PSAP:

(A) Whether it has taken alternative measures to mitigate the risk of critical 911 circuits that are not physically diverse or is taking steps to remediate any issues that it has identified with respect to 911 service to the PSAP, in which case it shall provide a brief explanation of such alternative measures or such remediation steps the date by which it anticipates such remediation will be completed, and why it believes those measures are reasonably sufficient to mitigate such risk; or

(B) Whether it believes that one or more of the requirements of this paragraph are not applicable to its network, in which case it shall provide a brief explanation of why it believes any such requirement does not apply.

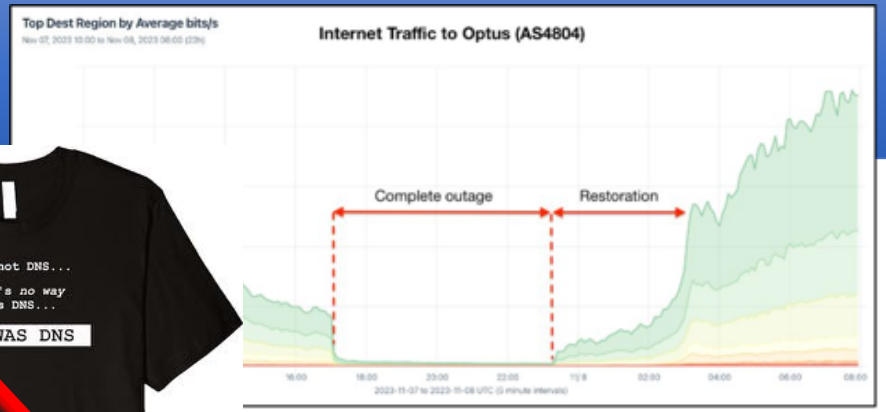
(2) ***Backup power.***

(i) With respect to any central office it operates that directly serves a PSAP, a covered 911 service provider shall certify whether it:

(A) Provisions backup power through fixed generators, portable generators, batteries, fuel cells, or a combination of these or other such sources to maintain full-service functionality, including network monitoring capabilities, for at least 24 hours at full office load or, if the central office hosts a selective router, at least 72 hours at full office load; provided, however, that any such portable generators shall be readily available within the time it takes the batteries to drain, notwithstanding potential demand for such generators elsewhere in the service provider's network.

Large-scale outages & lessons

Optus outage – iBGP?



In the early hours of 8 November 2023, a widespread servic
disruption left Optus subscribers, Australia's second-larges
provider, without Internet connectivity. This extensive outa
affected the fixed broadband and mobile communications
million individuals and 400,000 businesses and services, inc
emergency services, hospitals, banks, and public transport

Another possibility is that Optus did use MA
old on its exterior
perimeter than on the interior — allowing a
der routers but taking
down sessions internally. When MAXPREF is r
red to automatically re-
establish the session after a retry interval or go down forever, requiring manual intervention. *Be aware that Cisco's default behavior is to go down forever.*

The unnamed "international peering network" that Optus said had contributed to its 16-hour-long network meltdown last week is run by its Singaporean parent company Singtel, it can be revealed.

Optus outage

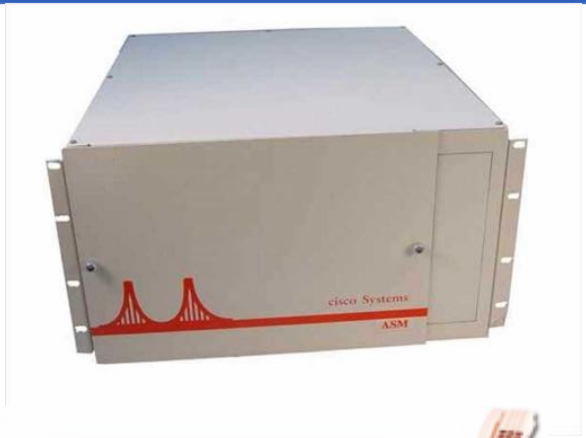
The key piece of equipment that might have brought down Optus

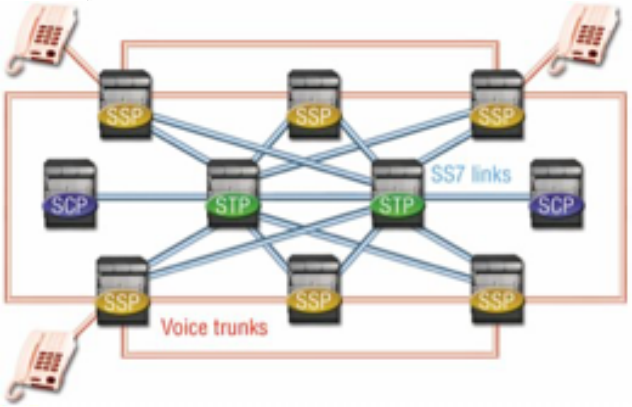
As well as bringing down Optus' landline, mobile phone and internet services, the outage also appears to have brought down the internal network used by Optus to manage its network, forcing technicians to travel to affected locations and attempt to fix problems in person.

Industry insiders said it was "unusual" for a telecommunications company not to keep that management network "out of band", or completely separate from its main backbone, so devices can still be managed remotely when the main network is down.

One insider who asked not to be named said that running the management network "in-band" – on the same backbone it is meant to manage – was "not a choice I would make".

The classic out-of-band mechanism





Security ∈ Reliability

- Many security problems manifest themselves as reliability problems
- □ system does not perform to specification
- including confidentiality and (data) integrity
- e.g., ransomware impacts are largely business disruption impacts

BUT

- many large-scale outages are caused or exacerbated by access control

Single points of failure

Residents hit by rural Alaska fiber network outage turn to satellite internet, analog operations

By Alena Naiden
Updated: June 15, 2023

On Sunday, heavy ice movement 34 miles offshore from Utqiagvik cut the subsea fiber network operated by broadband provider Quintillion. Fixing the fiber cut might take between six and eight weeks, depending on when the ice breaks up and how challenging the repairs will be, Quintillion President Mac McHale said.

Since the breakage, Utqiagvik, Wainwright, Point Hope, Kotzebue, Nome and Atqasuk have experienced service interruptions, which varied widely among the telecommunication providers using Quintillion's fiber system, McHale said.

Many city government services were down in Utqiagvik and Kotzebue. Several residents in affected communities couldn't use their phones to communicate with friends and family, and some businesses struggled to conduct financial transactions without having an internet connection.

Weeks-long outage shows need for better broadband

'Internet is now as essentia

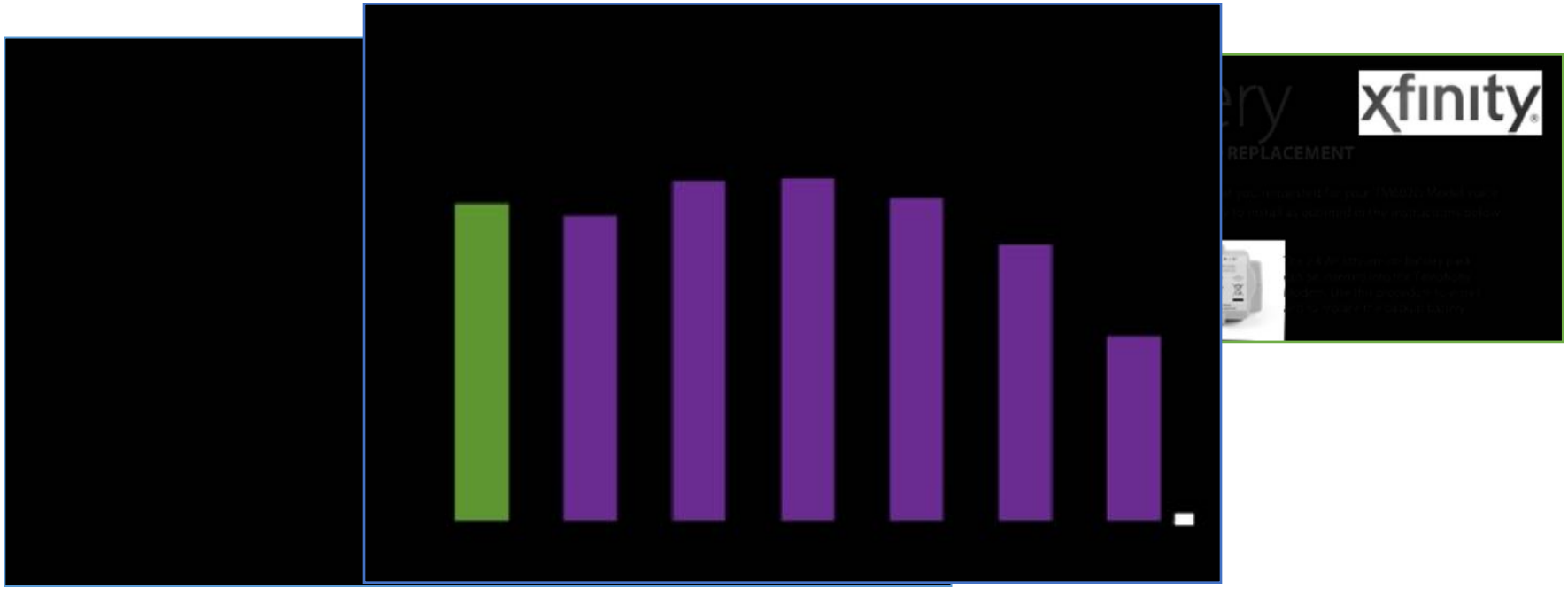
The neighborhood where
in a rural part of the coun
Liberty, and runs along th
U.S. 421 to the east. Neigh
Brightspeed — formerly k
serves just under half of C
according to the FCC's na

The first outage was a result of strong winds from Hurricane Ian, which knocked out broadband and electricity. The second one, just a month later, came out of the blue when a tractor trailer snagged allegedly low-hanging power lines.

Since cell service is also limited in the neighborhood, residents could not rely on 5G to access the internet during the extensive outages.

Siler City, NC

Replace old resiliency (CO power) with new



Sunset date. The requirements of this section shall no longer be in effect as of September 1, 2025.

Xfinity storm-ready Wi-Fi

STORM-READY WIFI FEATURES

- Tri-Band WiFi 6 extender compatible with Xfinity Gateways XB7 or XB8.
- 4G LTE connection with automatic switching during a network or power outage.
- External battery provides up to four hours of backup during a power outage when fully charged.

30/7 Mbps

But: industry may push back

- Katrina report (2007): 8-hour cell site backup requirements
- 2008: CTIA appeals
  - CTIA- The Wireless Association v. FCC (D.C. Cir. 2008)
- 2011: deleted
  - 2011. Redundancy of Communications Systems: Backup Power, Order, 26 FCC Rcd 15453

DARPA RADICS: an internet alternative for blackstart recovery

DARPA RADICS Program

"RADICS program delivers novel technologies, custom testbed, and evaluation exercises to enable utilities and first responders to quickly restore critical infrastructure amidst a cyberattack"

- 2016 - 2020
- Develop tools for:
  - cybersecurity personnel
  - grid operators and utilities
  - first responders
- Enable blackstart recovery during a cyberattack
- Without relying on external resources (including power and communication)

Field exercise at Plum Island, NY

Source: https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems

DARPA RADICS Program (continued)

- Joint government, academia, and industry effort led by DARPA
- Custom testbed to replicate real-world conditions
  - designed around commonly deployed systems in North America
  - multi-utility grid infrastructure
  - miniaturized substations (substation-in-a-box), RTO/ISO, power lines, data networks
- Field exercises on Plum Island, NY every six month (7 in total)
  - volunteers from the energy sector recruited by the U.S. DOE
  - learn to respond to simulated attacks
- Grid restoration technology (tools for the energy sector & first responders)

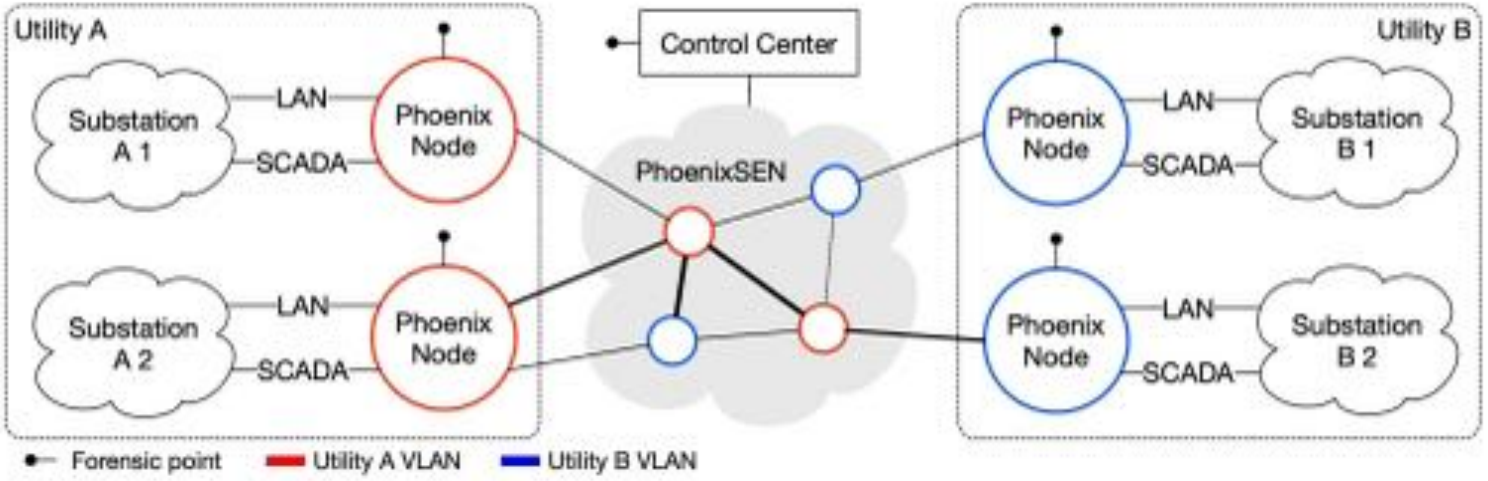
Source: https://www.darpa.mil/news-events/2021-02-23

RADICS Field Exercises on Plum Island, NY

Phoenix Secure Emergency Network (PhoenixSEN)

- Uniform node architecture
- Deployable after blackout
- Built-in services for the grid

- Ad hoc backup network for blackstart
- hybrid, isolated (virtualized), self-forming
- drop-in replacement for ISP networks



PhoenixSEN Prototype

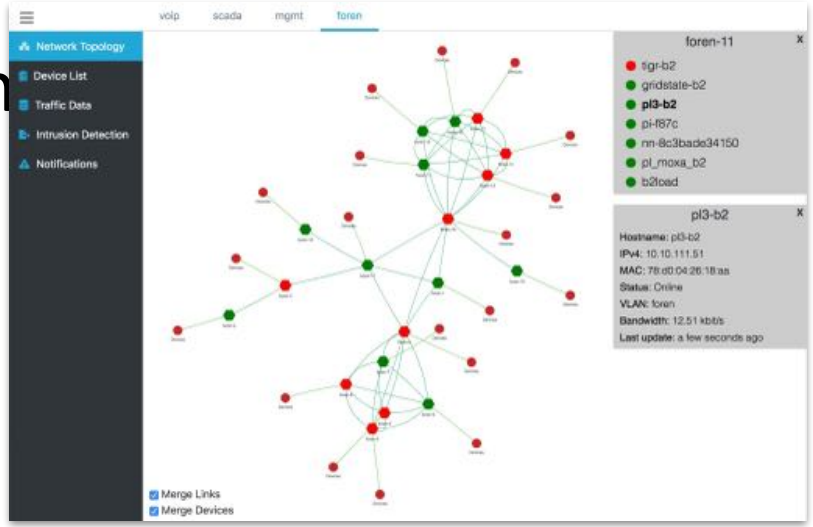
Prototype evaluated during live field exercises

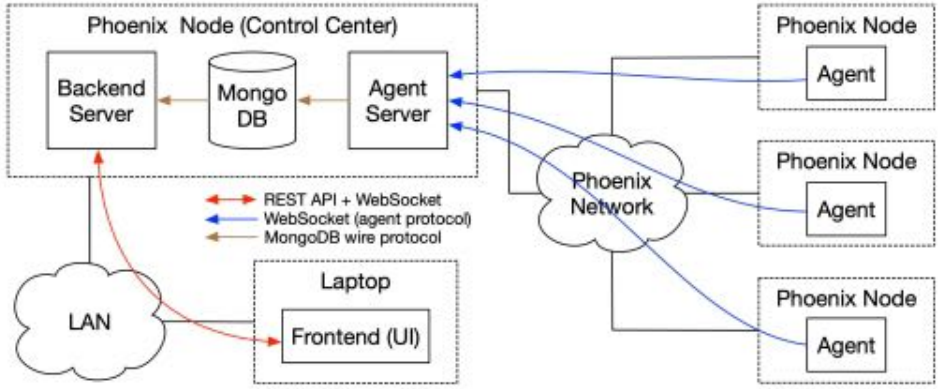
PhoenixSEN node detail

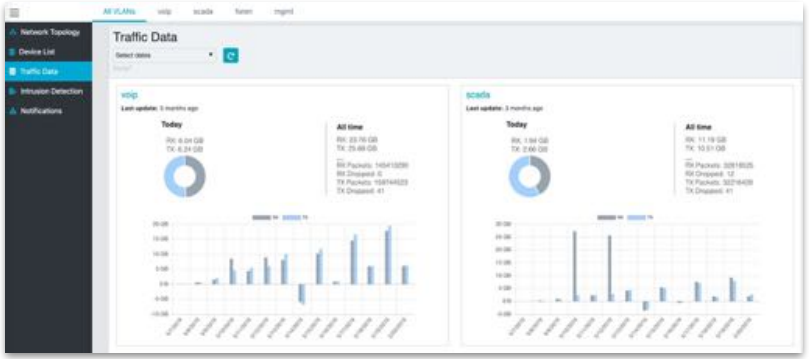
Photo credit: Hema Retty (BAE Systems)

PhoenixSEN Network Monitorin

- Situation awareness via in-situ monitoring
- SCADA device discovery via active probing
- Time-traveling debugging for post-mortem analysis
- https://github.com/irtlab/netmon







Lessons

- Policy can better align infrastructure decisions with societal objectives
  - laws, rules, disclosure, subsidies
- Private actors may be reluctant to share incident analysis
- Currently, no systematic body of knowledge
  - e.g., similar to NTSB or FAA reporting for safety
  - may well be harder than relatively uniform flight operations
- Increasing emphasis on inter-system redundancy
  - operator diversity
  - out-of-band more resiliency, more security risks if separate company
    - return to SS7 model?