NASEM HPH CIP Workshop

Session 3 Examining High Priority Vulnerabilities and Strategies for Resilience: Built Environment, Water and Wastewater, Energy

Monday, December 9, 2024

Joshua Corman - @joshcorman
IST - The Institute for Security and Technology
Undisruptable27.org

ABOUT IST: *The Critical Action Think Tank*

IST unites technology and policy leaders to create actionable solutions for emerging security threats.

Emerging technologies can disrupt the international balance of power. As governments compete, they shape innovation, supply chains, prosperity, and national and international security. IST shapes the incentives and alleviates the impediments to a more secure collective future.

Strategic Balancing Initiative

Dependence on digital technologies generates systemic security risks. IST works to identify incentives and mitigate digital security market failures by proposing ways to build trust, safety, and security into digital technologies from the ground up and sustain them for the future.

The Ransomware Task Force
Applied Trust & Safety
AI Foundation Model Access Initiative

Despite optimism about new technologies, some exacerbate or create existential threats to society. IST searches for solutions to the more severe risks introduced by technology, and strives to make technology itself a solution.

CATALINK
Nuclear Risk Reduction

I AM THE Cavalry

I Am The Cavalry is a grassroots organization focused on the intersection of digital security, public safety, and human life.

Safer. Sooner. Together.

iamthecavalry.org/about

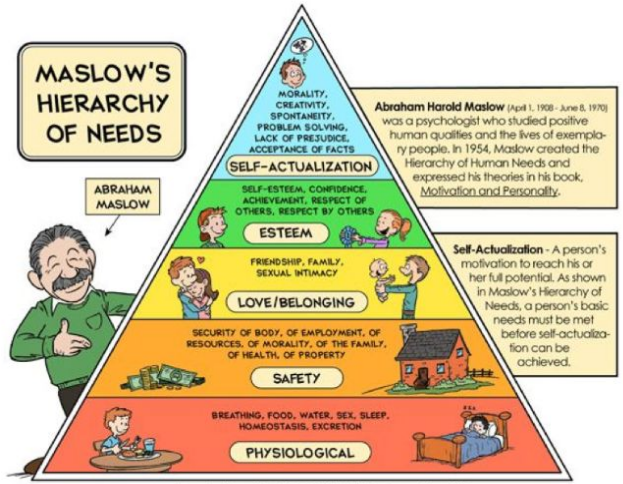
CyberMedSummit.org

UnDisruptable27.org

Through our **over dependence** on **undependable IT**, we have created the conditions such that the actions **any single outlier** can have a profound and asymmetric impact on **human life, economic, and national security**.

iamthecavalry.org

I AM THE Cavalry



The New York Times

Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack

A wave of damaging attacks on hospitals upended the lives of patients with cancer and other ailments. "I have no idea what to do," one said.

The University of Vermont Medical Center in Burlington, Vt., was the victim of a cyberattack in late October. Elizabeth Frantz for The New York Times


By Ellen Barry and Nicole Perlroth

Published Nov. 26, 2020 Updated Dec. 14, 2020

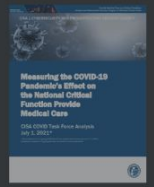

GNH
UAH
UAH
UAH


GNH
UAH
UAH
UAH
UAH


GNH


1


2


3


4

Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm

September 2021

CRITICAL INFRASTRUCTURE DECISION SUPPORT

By late September, at least four states have declared Crisis Standards of Care (CSC), and an additional eight have delayed elective surgeries and/or are at risk of enacting CSC. Patient diversions across state lines further punctuate the dynamic we outlined in the Cascading failures model (see page 7).

As the COVID-19 pandemic reaches another phase, with increased and protracted strains on the nation's critical infrastructure and related National Critical Functions such as *Provide Medical Care,* CISA is undertaking a renewed push for cyber preparedness and resilience, as well as decision support for stakeholders within critical infrastructure sectors. Over time, we find these original insights increasingly valuable, and in service of timely decision support, we offer them to you in their original form. As British statistician George E. P. Box noted, "All models are wrong, but some are useful." We hope that these models and insights are useful to you and stimulate additional discussion and exploration for mutual benefit.

This CISA Insight will speak to:

- Analysis and insights into strains on the nation's critical infrastructure, specifically through impacts to the National Critical Function *Provide Medical Care,*
- The compounding risks and harms that apply to all critical infrastructure sectors and the 55 National Critical Functions, through impact to essential critical infrastructure workers, and
- Our intention to share our preliminary analysis, enable decision support, and assist in risk reduction across multiple stakeholders and critical infrastructure sectors.

https://www.cdc.gov/mmwr/volumes/70/wr/mm7046a5.htm?s_cid=mm7046a5_w

Impact of Hospital Strain on Excess Deaths During the COVID-19 Pandemic — United States, July 2020–July 2021

Weekly / November 19, 2021 / 70(46);1613–1616

Geoffrey French, MA[1]; Mary Hulse, MPA[1]; Debbie Nguyen[2]; Katharine Sobotka[2]; Kaitlyn Webster, PhD[2]; Josh Corman[1]; Brago Aboagye-Nyame[2]; Marc Dion[2]; Moira Johnson[2]; Benjamin Zalinger, MA[2]; Maria Ewing[2] (View author affiliations)

View suggested citation

Summary

What is already known about this topic?

COVID-19 surges have stressed hospital systems and negatively affected health care and public health infrastructures and national critical functions.

What is added by this report?

The conditions of hospital strain during July 2020–July 2021, which included the presence of SARS-CoV-2 B.1.617.2 (Delta) variant, predicted that intensive care unit bed use at 75% capacity is associated with an estimated additional 12,000 excess deaths 2 weeks later. As hospitals exceed 100% ICU bed capacity, 80,000 excess deaths would be expected 2 weeks later.

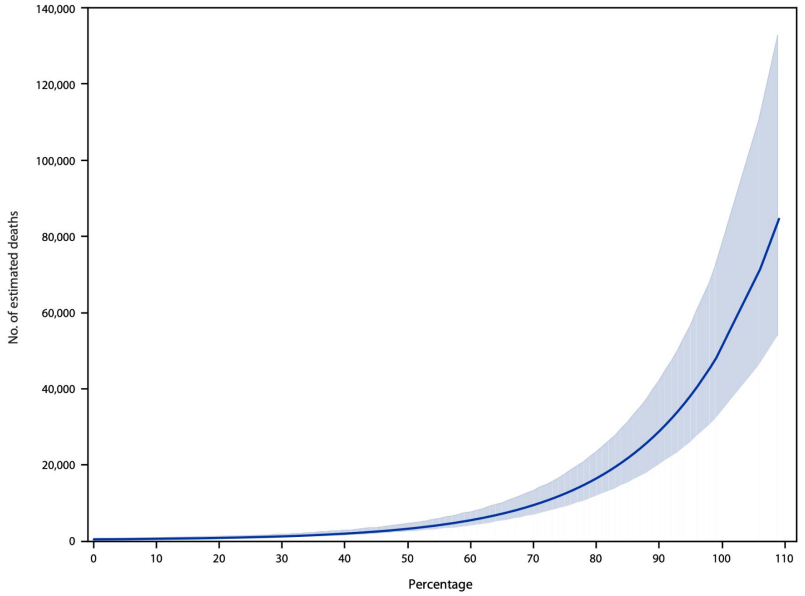
What are the implications for public health practice?

State, local, tribal, and territorial leaders could evaluate ways to reduce strain on public health and health care infrastructures, including implementing interventions to reduce overall disease prevalence such as vaccination and other prevention strategies, and ways to expand or enhance capacity during times of high disease prevalence.

Figure
References

Surges in COVID-19 cases have stressed hospital systems, negatively affected health care and public health infrastructures, and degraded national critical functions (*1*,*2*). Resource limitations, such as available hospital space, staffing, and supplies led some facilities to adopt crisis standards of care, the most extreme operating condition for hospitals, in which the focus of medical decision-making shifted from achieving the best outcomes for individual patients to addressing the immediate care needs of larger groups of patients (*3*). When hospitals deviated from conventional standards of care, many preventive and elective

FIGURE. Estimated number of excess deaths* 2 weeks after corresponding percentage of adult intensive care unit bed occupancy — United States, July 2020–July 2021



* Upper and lower boundaries of shaded area indicate 95% CIs.

Cybersecurity & Infrastructure Security Agency, unpublished data, 2021). As hospitals exceed 100% ICU bed capacity, 80,000 (95% CI = 53,576–132,765) excess deaths would be

health care and public health sectors, with excess deaths emerging in the weeks after a surge in COVID-19 hospitalizations. The results of this study support a larger body of evidence

https://www.cisa.gov/publication/provide-medical-care-critical-condition-analysis-and-stakeholder-decision-support

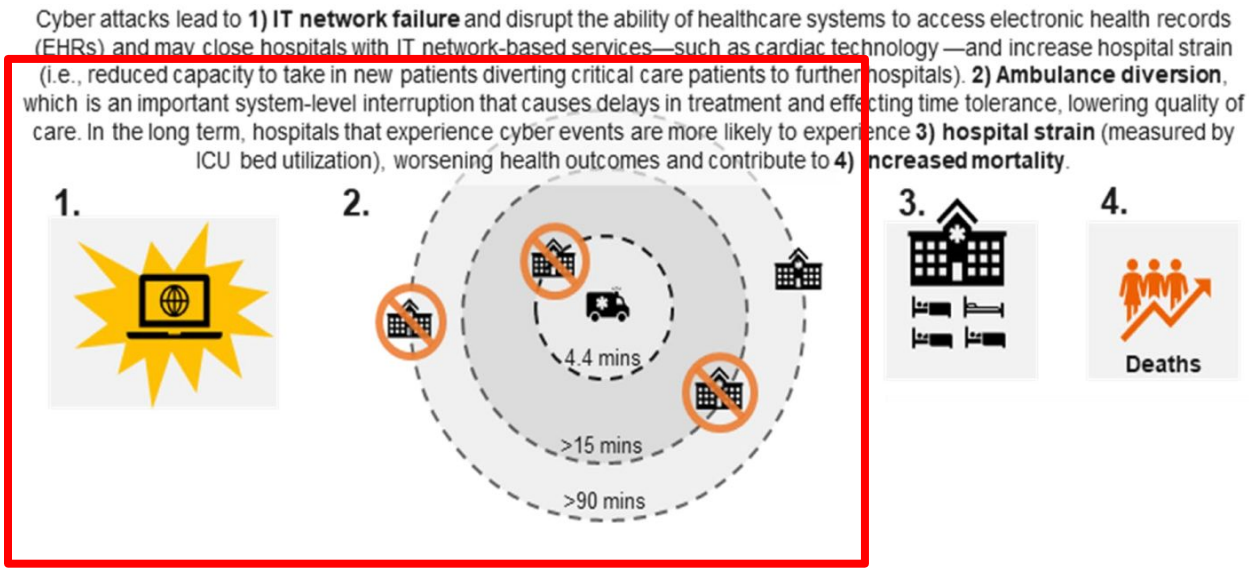
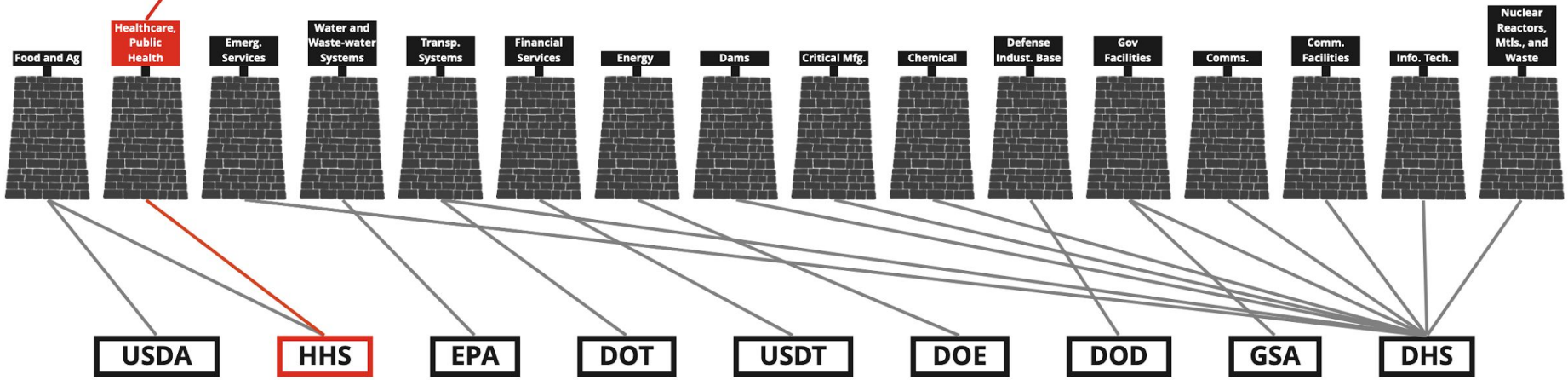


Figure 8 – Conceptual Model of Impact of Cyber Attack on Patient Outcomes

Operate Core Network	Distribute Electricity	Conduct Elections	Provide Medical Care	Provide Capital Markets and Investment Activities	Exploration and Extraction Of Fuels	Provide Housing	Provide Cable Access Network Services	Maintain Supply Chains	Educate and Train	Provide Public Safety	Provide Funding and Liquidity Services	Fuel Refining and Processing Fuels	Provide Information Technology Products and Services
Provide Internet Based Content, Information, and Communication Services	Transmit Electricity	Maintain Access to Medical Records	Store Fuel and Maintain Reserves	Provide Insurance Services	Generate Electricity	Provide Internet Routing, Access, and Connection Services	Transport Cargo and Passengers by Air	Manage Wastewater	Develop and Maintain Public Works and Services	Provide Payment, Clearing, and Settlement Services	Manufacture Equipment	Provide Materiel and Operational Support to Defense	Provide Positioning, Navigation, and Timing Services
Transport Cargo and Passengers by Rail	Perform Cyber Incident Management Capabilities	Enforce Law	Provide Wholesale Funding	Produce and Provide Agricultural Products and Services	R&D	Provide Radio Broadcast Access Network Services	Transport Cargo and Passengers by Road	Preserve Constitutional Rights	Manage Hazmat.	Support Community Health	Supply Water	Provide Satellite Access Network Services	Transport Cargo and Passengers by Vessel
Provide and Maintain Infrastructure	Operate Government	Produce and Provide Human and Animal Food Products and Services	Provide Wireless Access Network Services	Transport Materials by Pipeline	Provide Consumer and Commercial Banking Services	Prepare for and Manage Emergencies	Produce Chemicals	Provide Wireline Access Network Services	Transport Passengers by Mass Transit	Provide Identity Management and Associated Trust Support Services	Protect Sensitive Information	Provide Metals and Materials	



IMG SRC: Ben Mosier & Josh Corman 2022

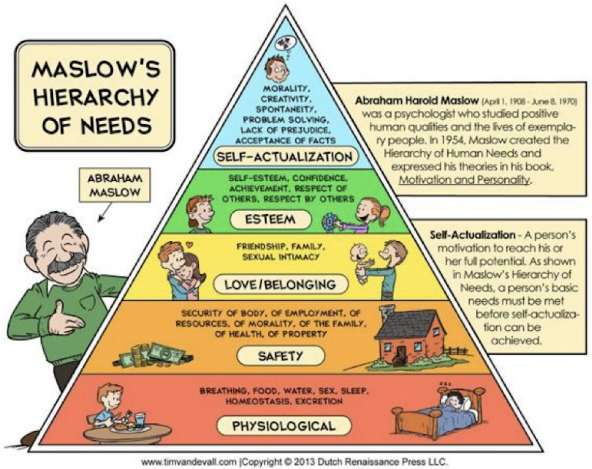
No critical infrastructure is an island.
Without multidisciplinary, multi-agency coordination, people die.

Operate Core Network	**Distribute Electricity**	Conduct Elections	**Provide Medical Care**	Provide Capital Markets and Investment Activities	Exploration and Extraction Of Fuels	Provide Housing	Provide Cable Access Network Services	Maintain Supply Chains	Educate and Train	Provide Public Safety	Provide Funding and Liquidity Services	Fuel Refining and Processing Fuels	Provide Information Technology Products and Services
Provide Internet Based Content, Information, and Communication Services	**Transmit Electricity**	Maintain Access to Medical Records	Store Fuel and Maintain Reserves	Provide Insurance Services	**Generate Electricity**	Provide Internet Routing, Access, and Connection Services	Transport Cargo and Passengers by Air	Manage Wastewater	Develop and Maintain Public Works and Services	Provide Payment, Clearing, and Settlement Services	**Manufacture Equipment**	Provide Materiel and Operational Support to Defense	Provide Positioning, Navigation, and Timing Services
Transport Cargo and Passengers by Rail	Perform Cyber Incident Management Capabilities	Enforce Law	Provide Wholesale Funding	**Produce and Provide Agricultural Products & Svcs**	R&D	Provide Radio Broadcast Access Network Services	**Transport Cargo and Passengers by Road**	Preserve Constitutional Rights	Manage Hazmat	Support Community Health	**Supply Water**	Provide Satellite Access Network Services	Transport Cargo and Passengers by Vessel
Provide and Maintain Infrastructure	Operate Government	**Produce and Provide Human and Animal Food Products & Svcs**	Provide Wireless Access Network Services	Transport Materials by Pipeline	Provide Consumer and Commercial Banking Services	**Prepare for and Manage Emergencies**	**Produce Chemicals**	Provide Wireline Access Network Services	Transport Passengers by Mass Transit	Provide Identity Management and Associated Trust Support Services	Protect Sensitive Information	Provide Metals and Materials	

Food and Ag	Healthcare, Public Health	Emerg. Services	Water and Waste-water Systems	Transp. Systems	Financial Services	Energy	Dams	Critical Mfg.	Chemical	Defense Indust. Base	Gov Facilities	Comms.	Comm. Facilities	Info. Tech.	Nuclear Reactors, Mtls., and Waste
USDA	HHS	EPA	DOT	USDT	DOE	DOD	GSA	DHS							

IMG SRC: Ben Mosier & Josh Corman 2022

*positions illustrative, not definitive



Latency-*insensitive* — *months*

weeks

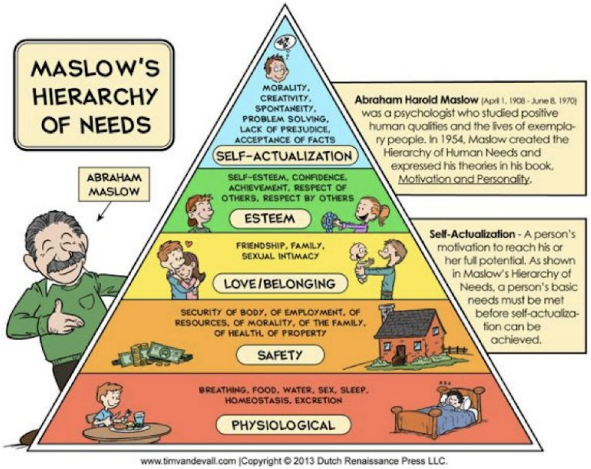
Latency-*sensitive* — *days*

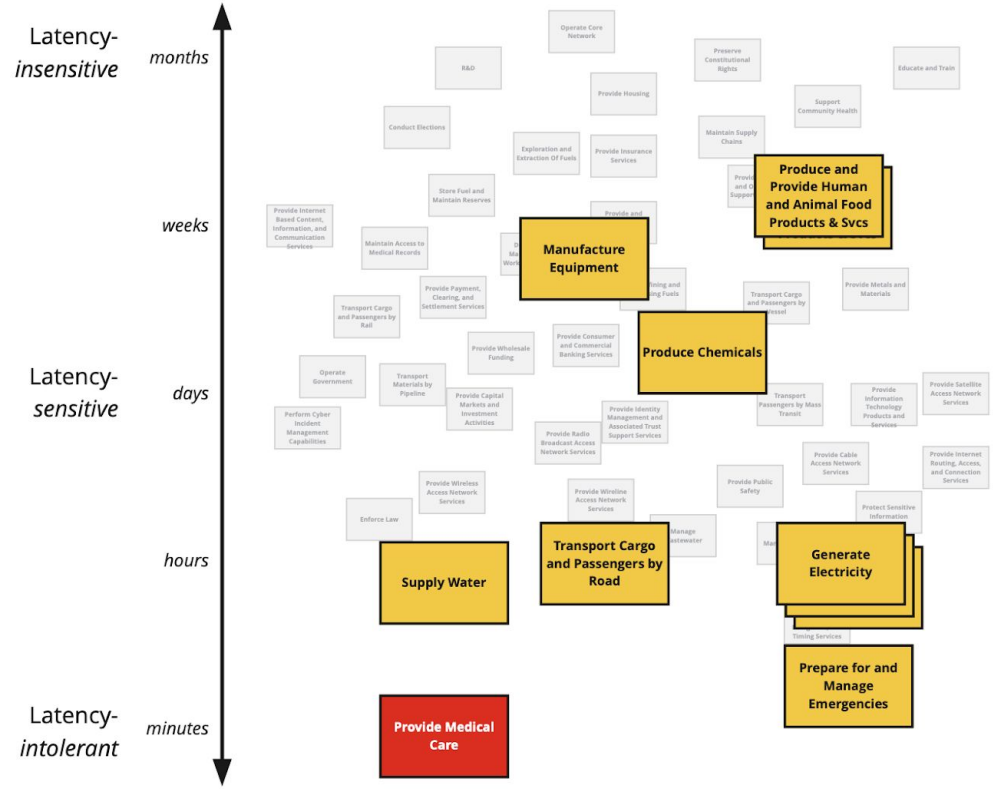
hours

Latency-*intolerant* — *minutes*

IMG SRC: Ben Mosier & Josh Corman 2022

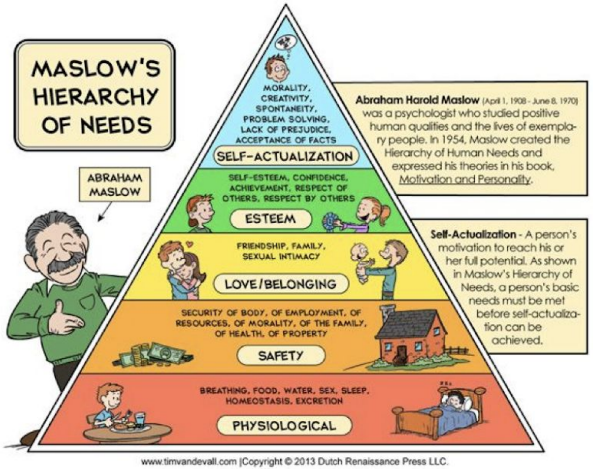
*positions illustrative, not definitive

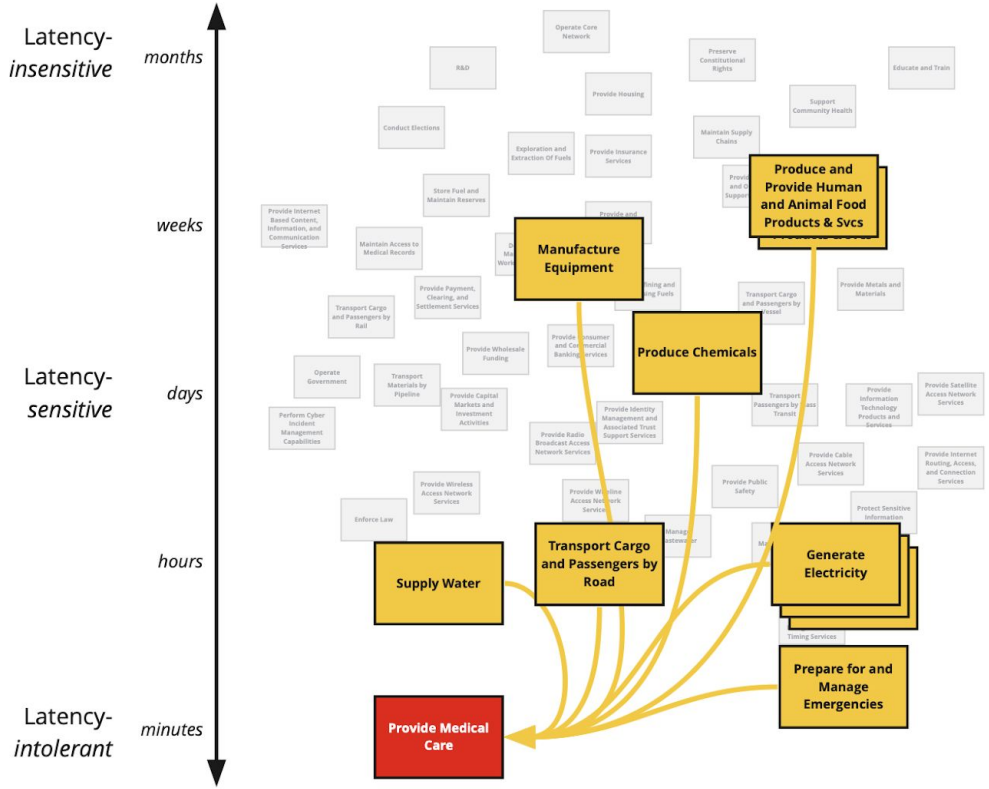




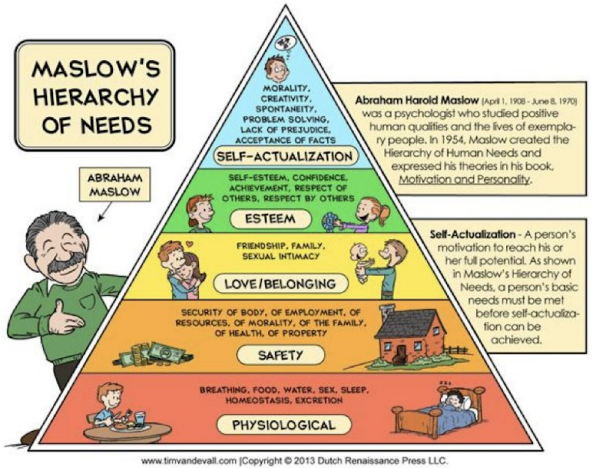
IMG SRC: Ben Mosier & Josh Corman 2022

*positions illustrative, not definitive





IMG SRC: Ben Mosier & Josh Corman 2022



*positions illustrative, not definitive

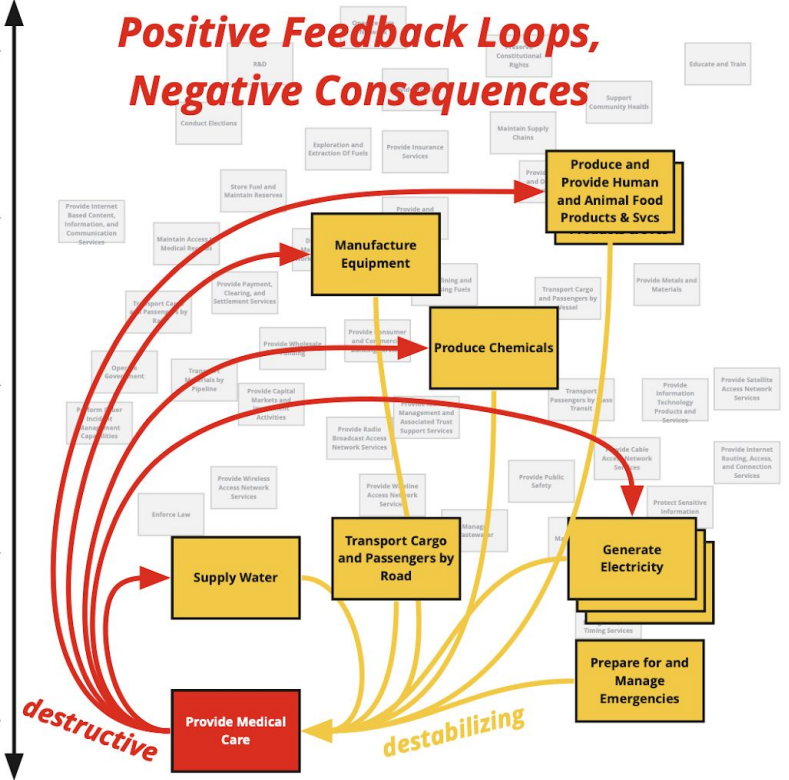
Latency-*insensitive* — *months*

Latency-*sensitive* — *days*

hours

Latency-*intolerant* — *minutes*

Positive Feedback Loops, Negative Consequences



IMG SRC: Ben Mosier & Josh Corman 2022

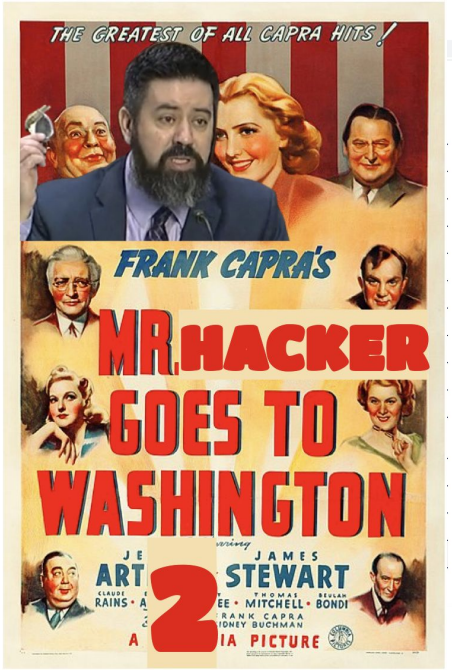
Target Rich; Cyber Poor

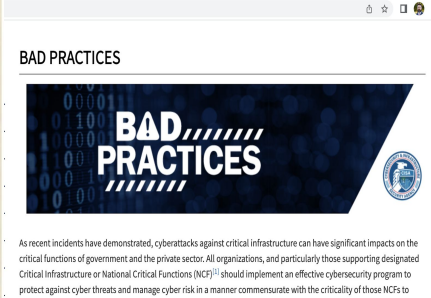
Information
Incentives
Resources

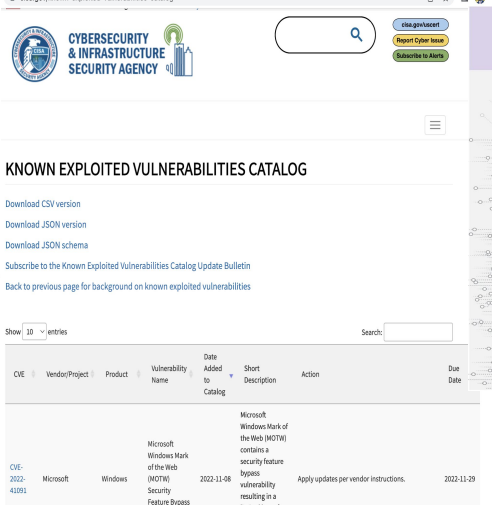
iamthecavalry.org

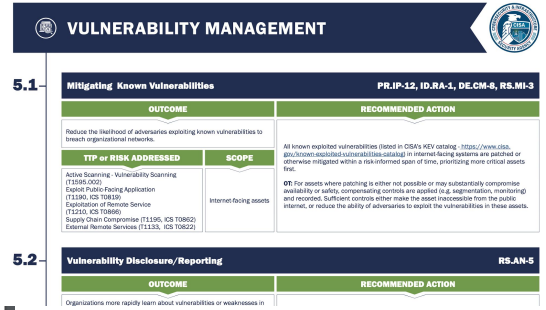
I AM THE Cavalry

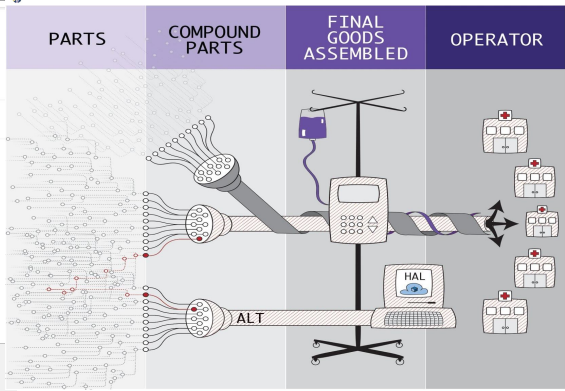
CISA COVID Task Force











SECURITY

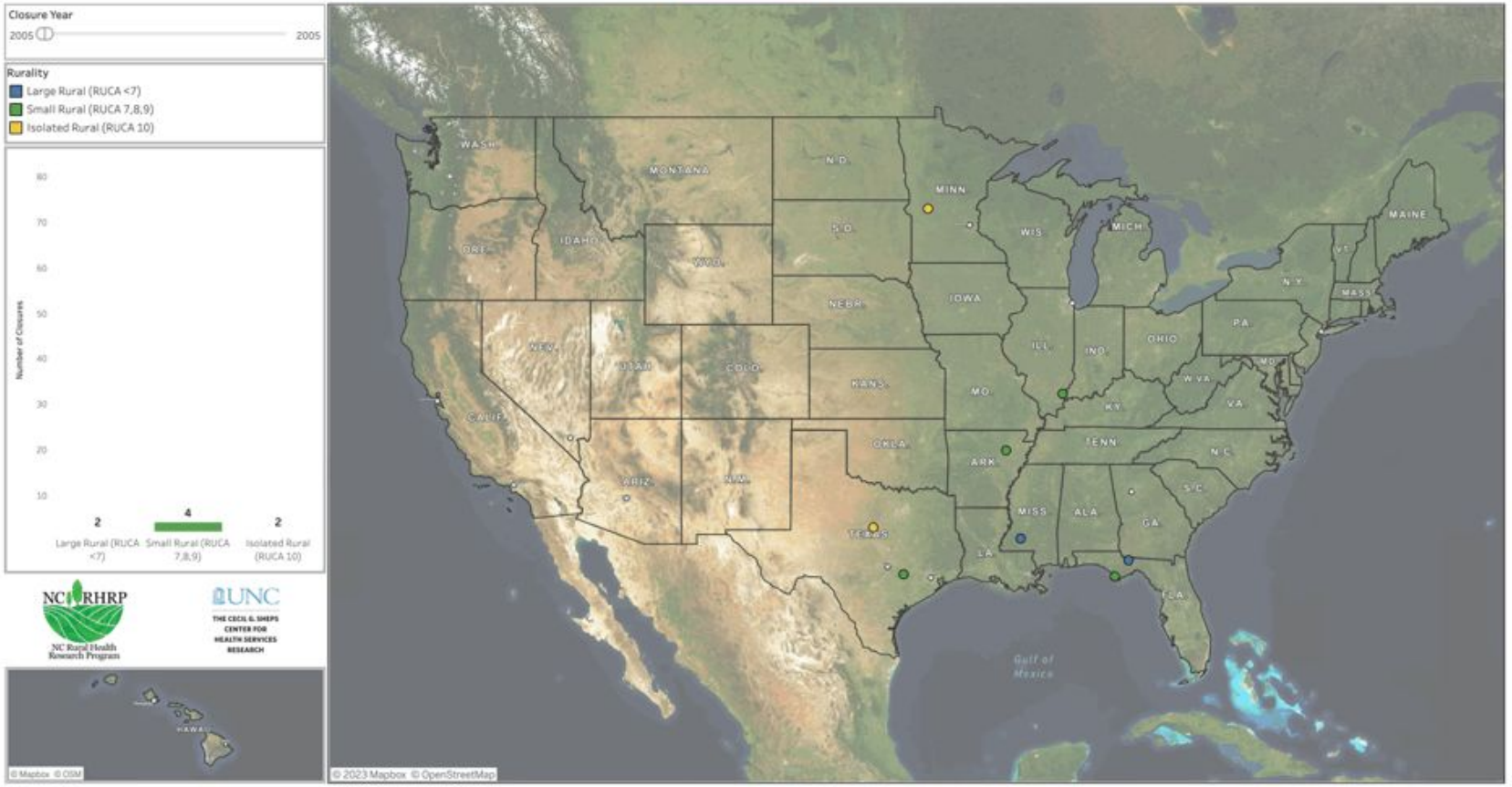
An Illinois hospital is the first health care facility to link its closing to a ransomware attack

A ransomware attack hit SMP Health in 2021 and halted the hospital's ability to submit claims to insurers, Medicare or Medicaid for months, sending it into a financial spiral.

St. Margaret's Health in Spring Valley, Ill. Google Maps

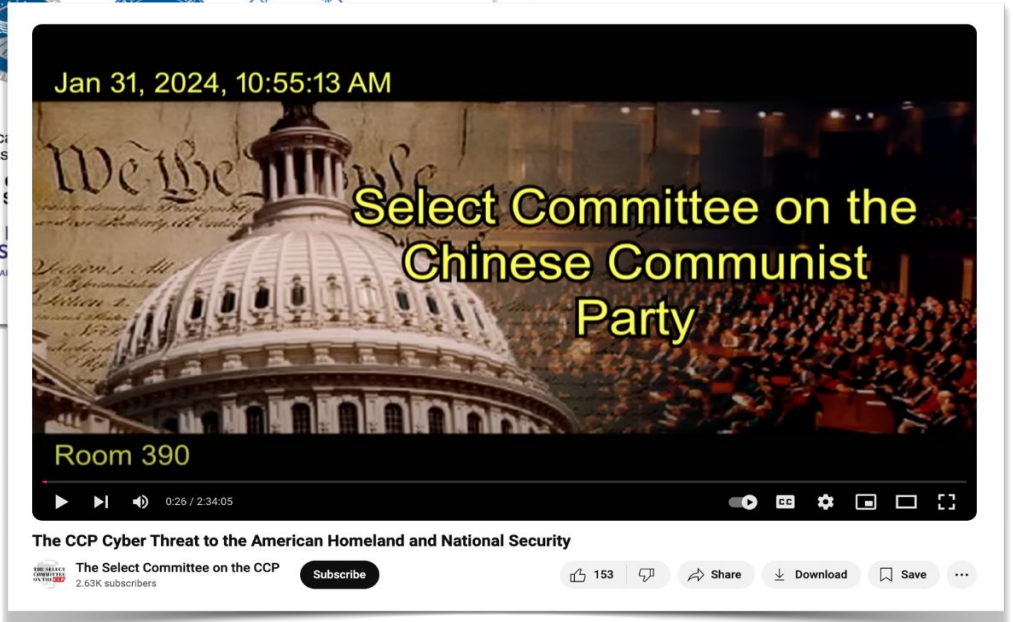
Rural Hospital Closures Maps, 2005 – Present

Closures by Era | Closures by Medicare Payment Classification | **Closures by Rurality** | Complete vs Converted Closures | Closures over time



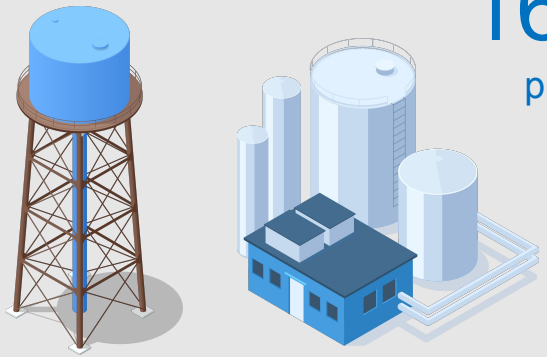
UnDisruptable27.org

Volt Typhoon 2027 (+/-) // China (Russia, Iran, DPRK)



US Water Systems Serving Population

151,000 public water systems serving 80% of the population



16,000 public wastewater systems serving 75% of the population

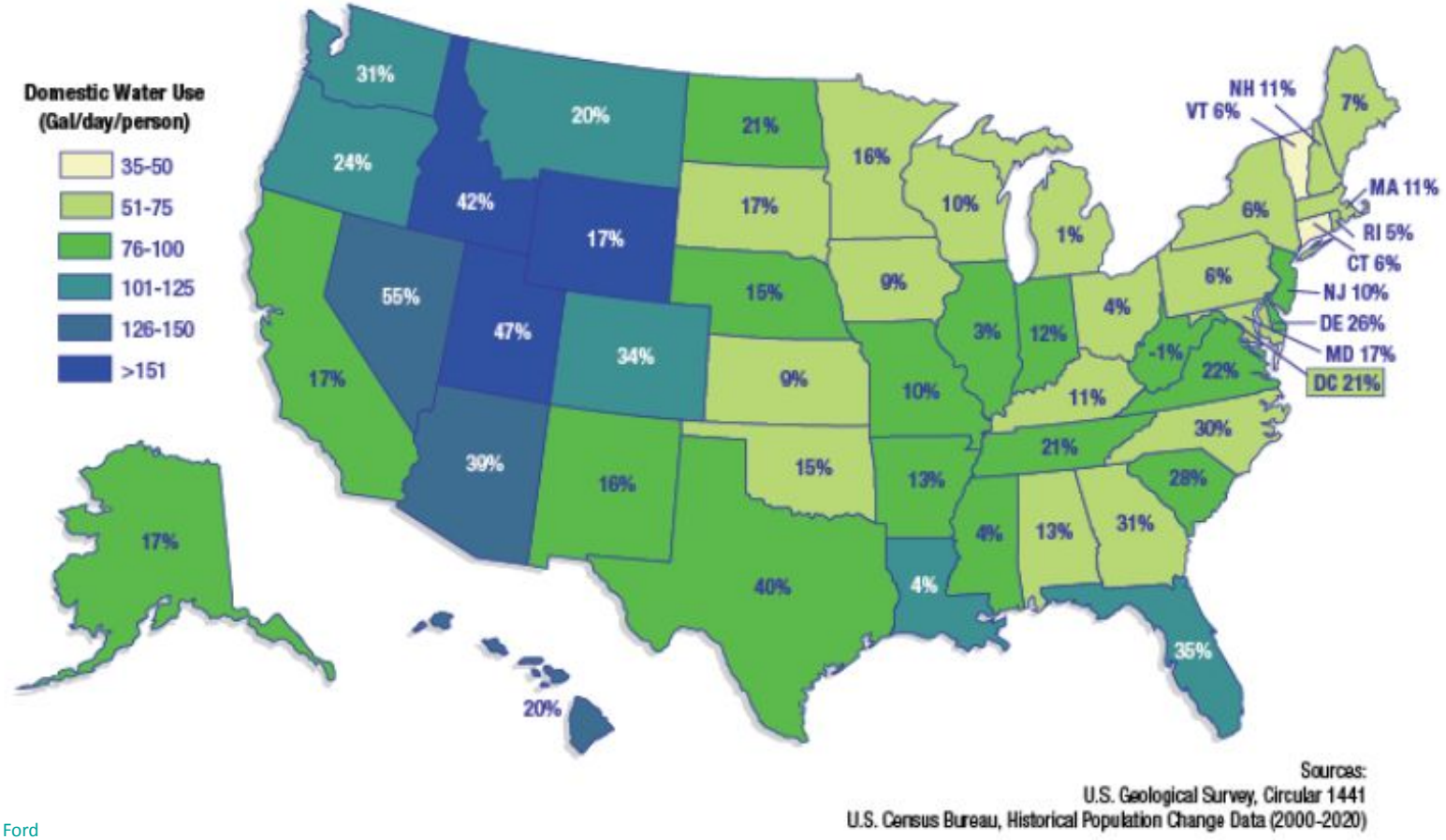
- Water systems are local. Nationwide grid does not exist.

- Failures can lead to specific and contained local collapse

- We must treat the waste side for sanitary and pollution reasons.

Slide via Dean Ford

Domestic Water Use in Gallons per Day per Person and Percent Population Growth from 2000 to 2020



Slide via Dean Ford

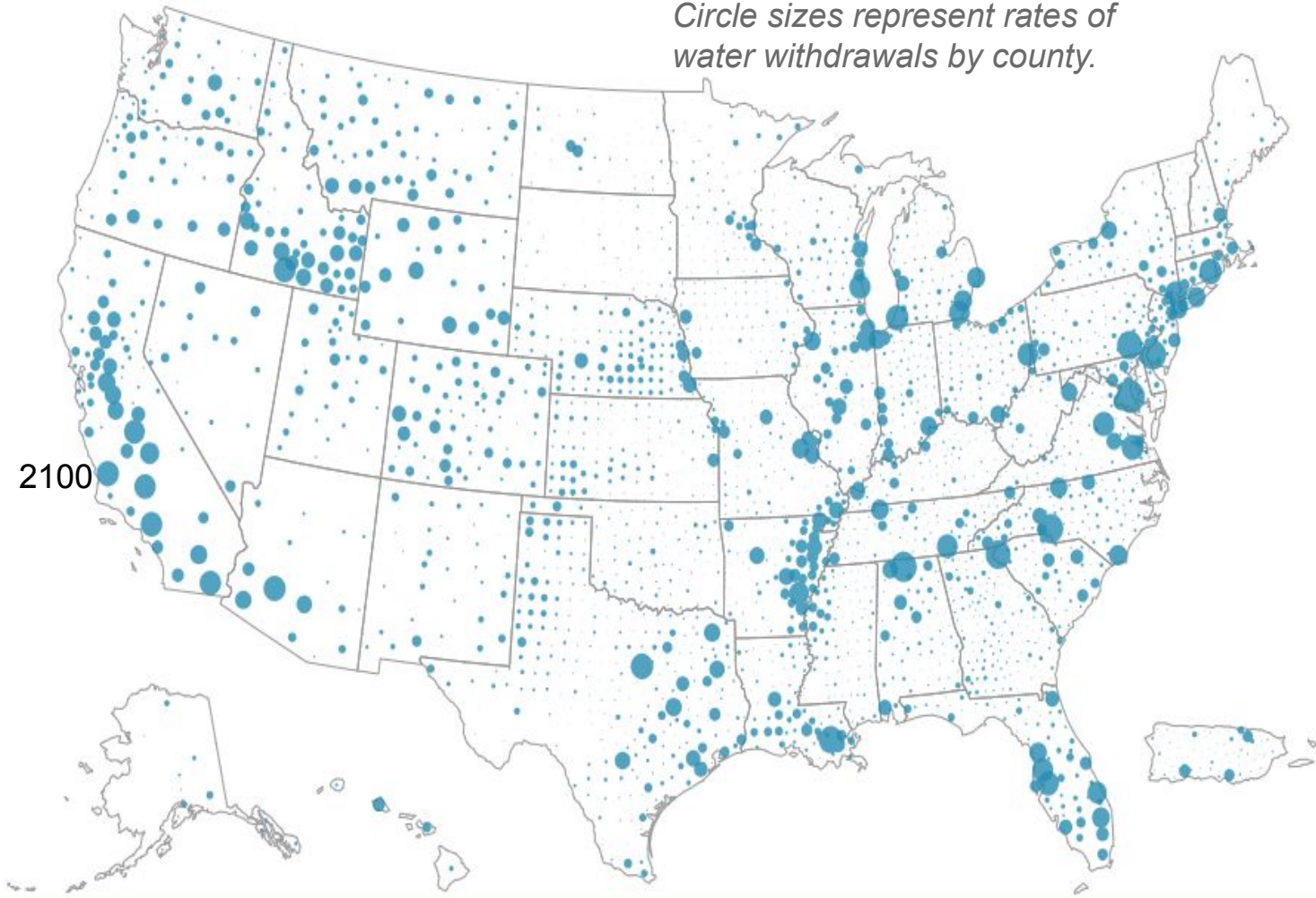
Circle sizes represent rates of water withdrawals by county.

U.S. Water Withdrawals

(million gallons per day)

Total	321,672.0
Thermoelectric	
Irrigation	
Public Supply	
Industrial	

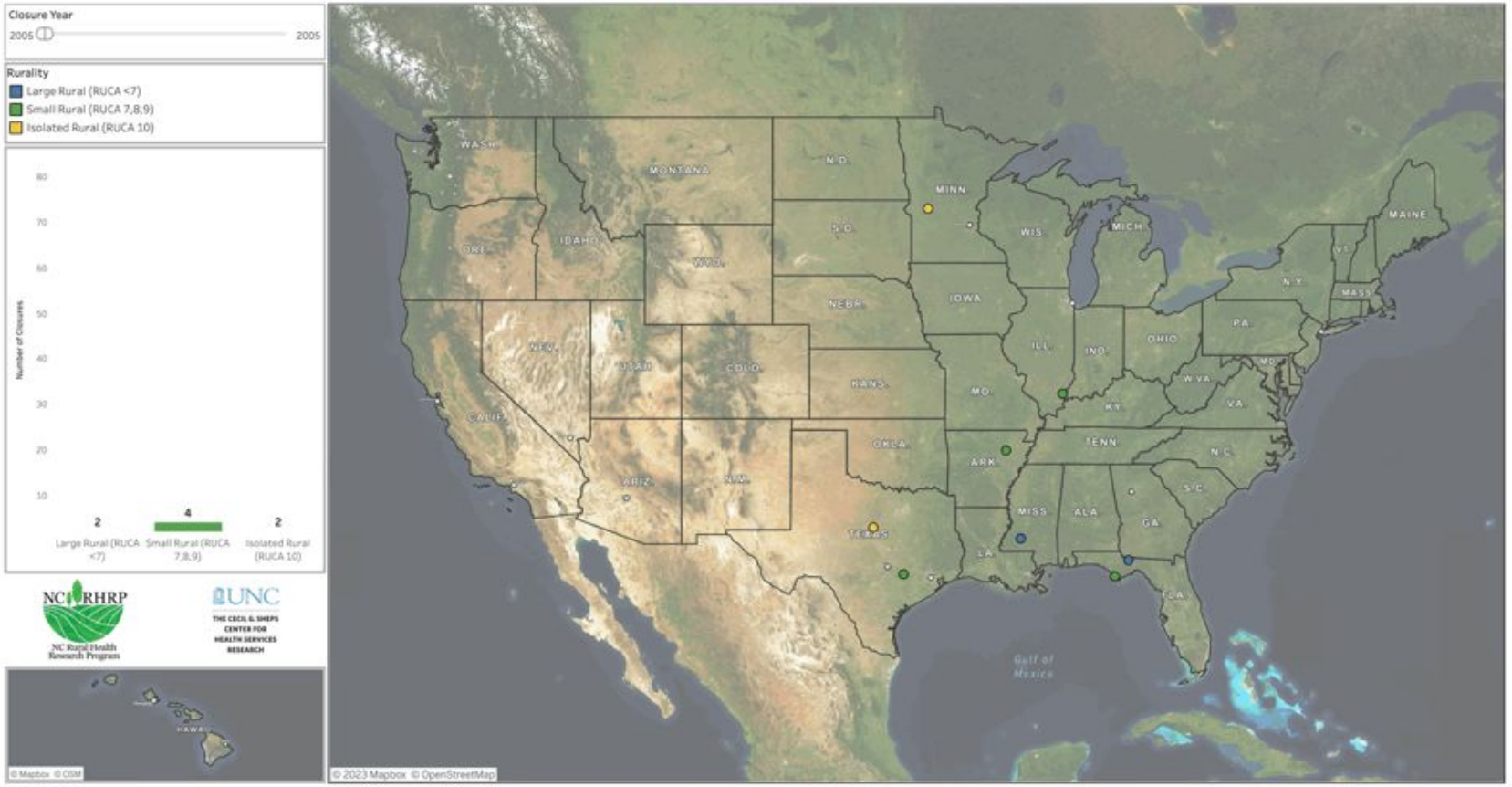
2100



Slide via Dean Ford

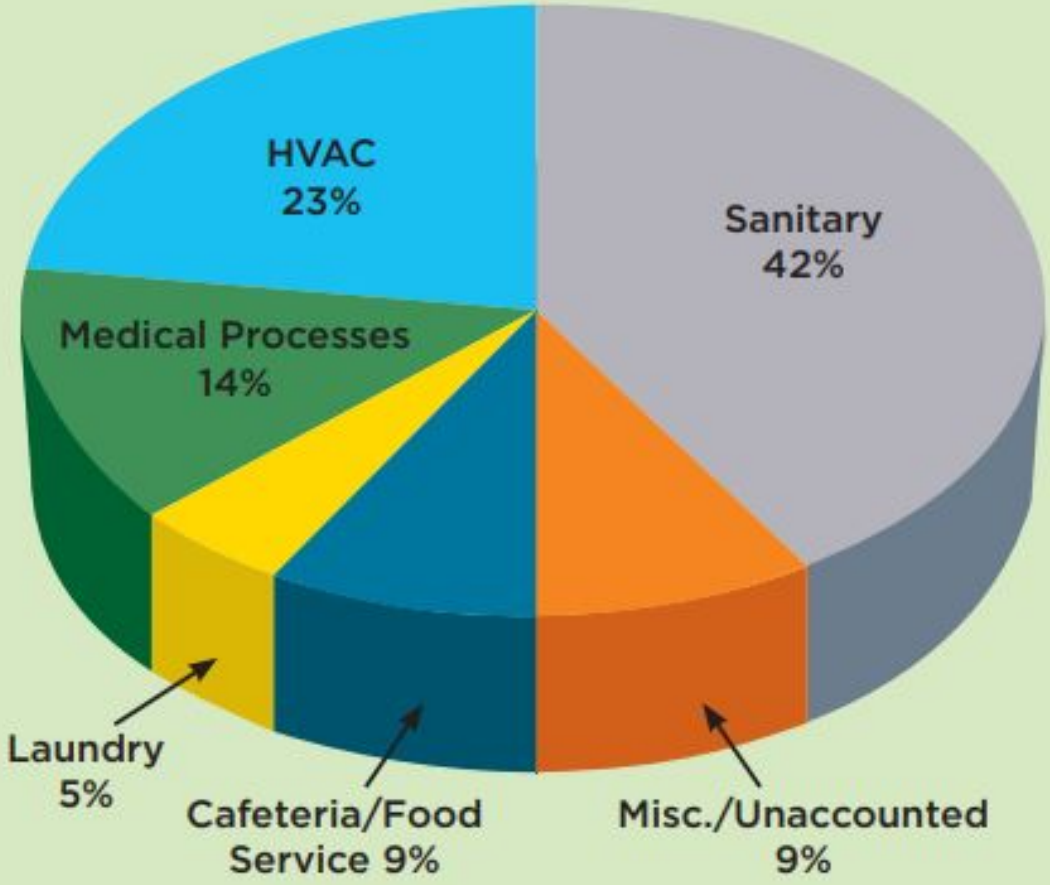
Rural Hospital Closures Maps, 2005 – Present

Closures by Era | Closures by Medicare Payment Classification | **Closures by Rurality** | Complete vs Converted Closures | Closures over time



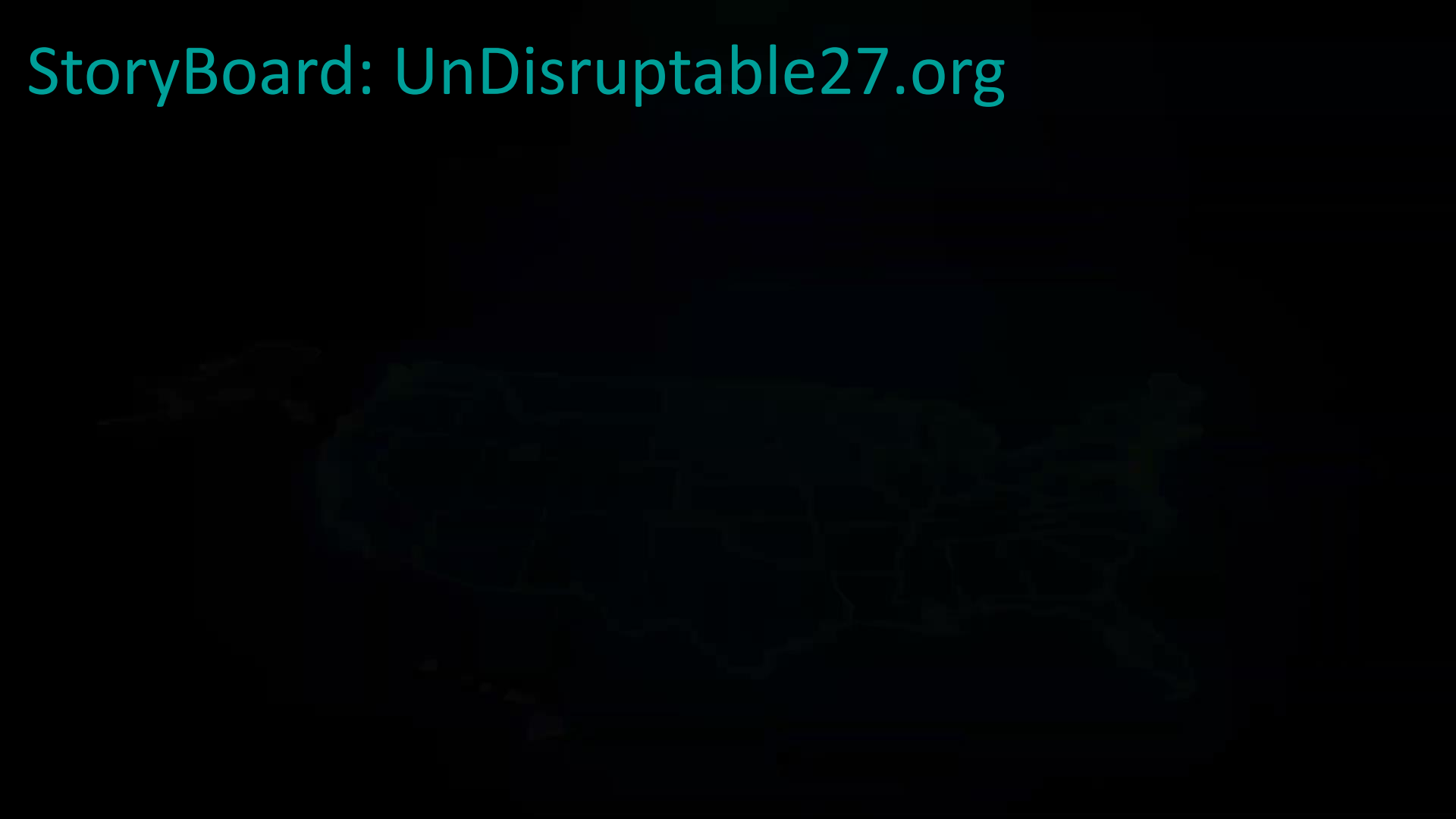
Hospital Water Usage—Example Study

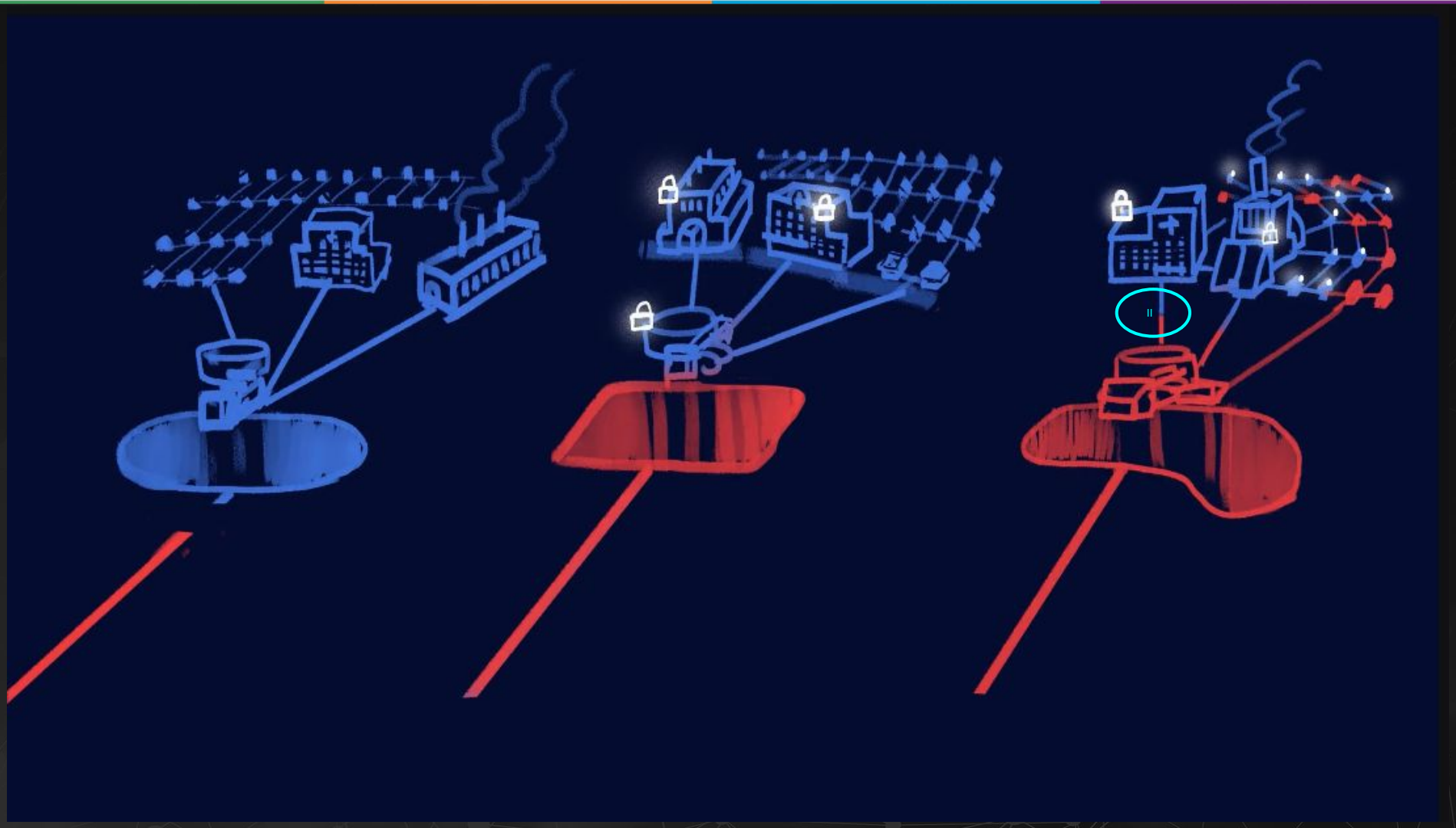
Source: Massachusetts Water Resources Authority

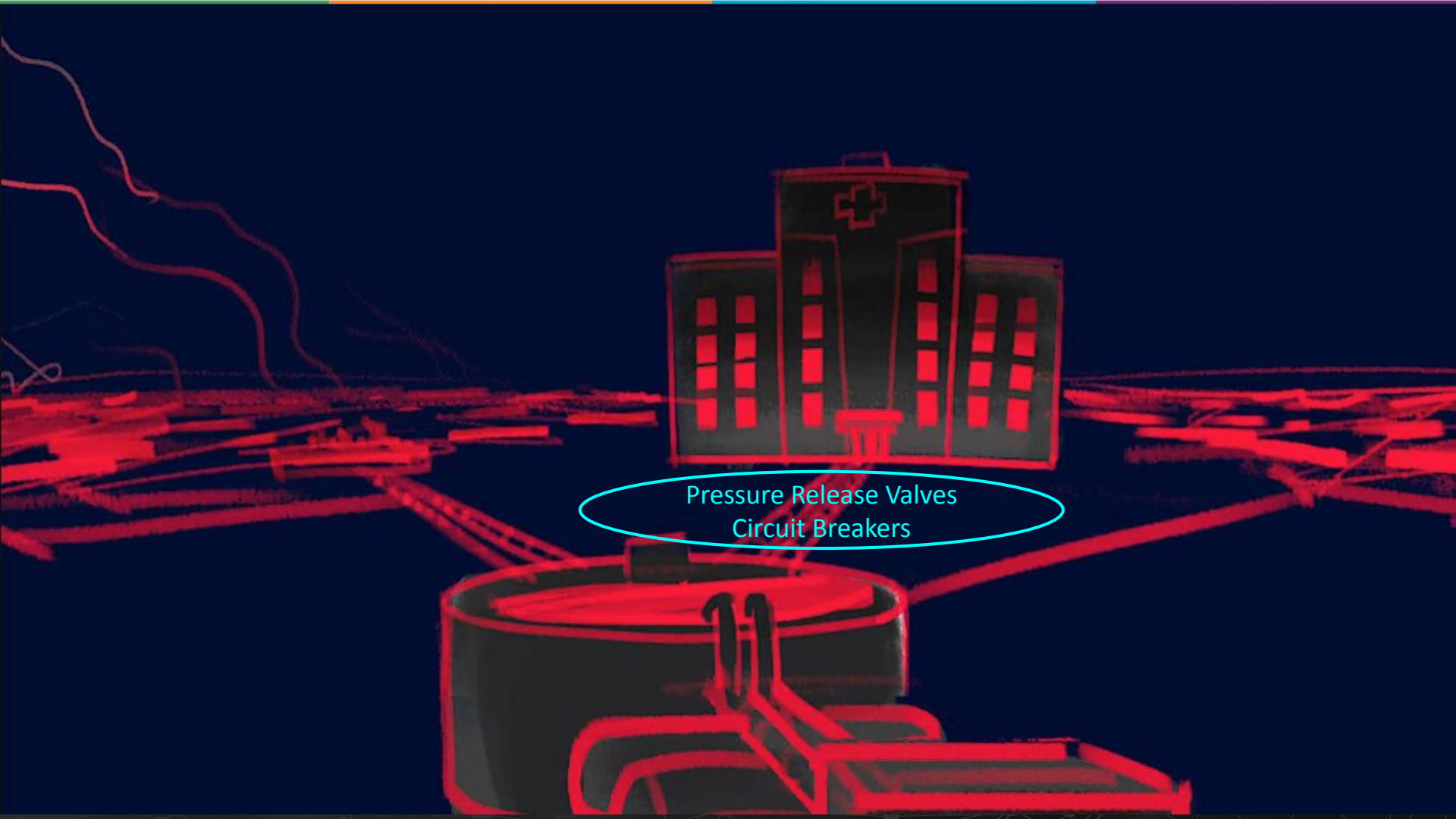


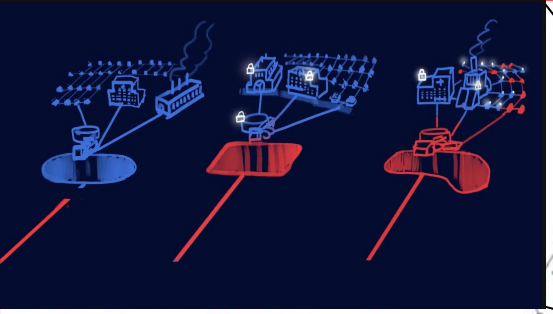
Slide via Dean Ford

StoryBoard: UnDisruptable27.org






Pressure Release Valves
Circuit Breakers



U.S. Water Withdrawals

(million gallons per day)

Total	321,672.0
Thermoelectric	
Irrigation	
Public Supply	
Industrial	

2100

Circle sizes represent rates of water withdrawals by county.

Mutual Assistance?

Everything? Everywhere?

All at Once?

Focus on Trauma Centers?

Slide via Dean Ford

I Am The Cavalry is a grassroots organization focused on the intersection of digital security, public safety, and human life.

Safer. Sooner. Together.

iamthecavalry.org


©fossilguy.com/travel

THANK YOU!

@joshcorman

@iamthecavalry

I AM THE Cavalry

www.iamthecavalry.org

NASEM HPH CIP Workshop

Thank You

Monday, December 9, 2024

Joshua Corman - @joshcorman

IST - The Institute for Security and Technology
Undisruptable27.org