I AM THE Cavalry

Where Bits & Bytes Meet Flesh & Blood

2023 DevOps Enterprise Summit - Las Vegas *October 5, 2023*

Joshua Corman **@joshcorman** **@iamthecavalry**

www.iamthecavalry.org

Look Up...


STARK

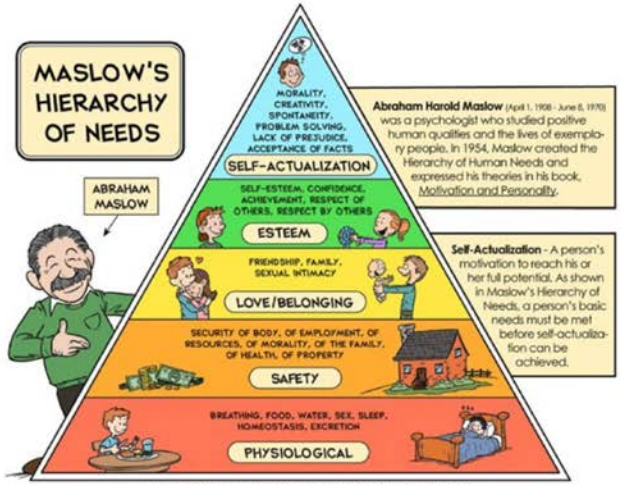
I AM THE Cavalry

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

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.**


MASLOW'S HIERARCHY OF NEEDS
ABRAHAM MASLOW
MORALITY, CREATIVITY, SPONTANEITY, PROBLEM SOLVING, LACK OF PREJUDICE, ACCEPTANCE OF FACTS
SELF-ACTUALIZATION
SELF-ESTEEM, CONFIDENCE, ACHIEVEMENT, RESPECT OF OTHERS, RESPECT BY OTHERS
ESTEEM
FRIENDSHIP, FAMILY, SEXUAL INTIMACY
LOVE/BELONGING
SECURITY OF BODY, OF EMPLOYMENT, OF RESOURCES, OF MORALITY, OF THE FAMILY, OF HEALTH, OF PROPERTY
SAFETY
BREATHING, FOOD, WATER, SEX, SLEEP, HOMEOSTASIS, EXCRETION
PHYSIOLOGICAL
Abraham Harold Maslow (April 1, 1908 - June 8, 1970) was a psychologist who studied positive human qualities and the lives of exemplary people. In 1954, Maslow created the Hierarchy of Human Needs and expressed his theories in his book, Motivation and Personality.
Self-Actualization - A person's motivation to reach his or her full potential. As shown in Maslow's Hierarchy of Needs, a person's basic needs must be met before self-actualization can be achieved.
www.timvandevall.com |Copyright © 2013 Dutch Renaissance Press LLC.

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

The Before Times...

iamthecavalry.org

I AM THE Cavalry

The NEW ENGLAND JOURNAL of MEDICINE

SPECIAL ARTICLE

CONCLUSIONS

Medicare beneficiaries who were admitted to marathon-affected hospitals with acute myocardial infarction or cardiac arrest on marathon dates had longer ambulance transport times before noon (4.4 minutes longer) and higher 30-day mortality than beneficiaries who were hospitalized on nonmarathon dates. (Funded by the National Institutes of Health.)

ABSTRACT

BACKGROUND

Large marathons frequently involve widespread road closures and infrastructure disruptions, which may create delays in emergency care for nonparticipants with acute medical conditions who live in proximity to marathon routes.

HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

June 2017

REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

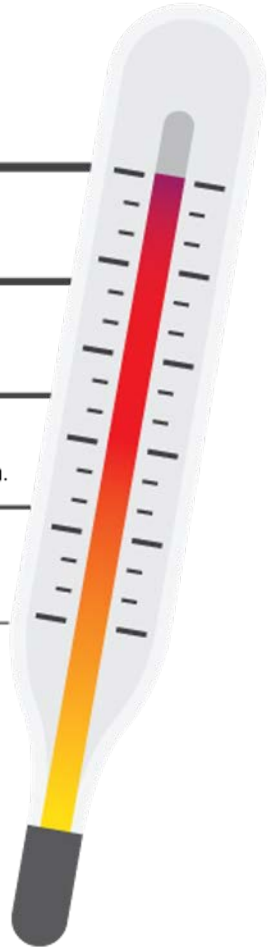
Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities



https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

If you can't afford to protect it...

You can't afford to connect it...

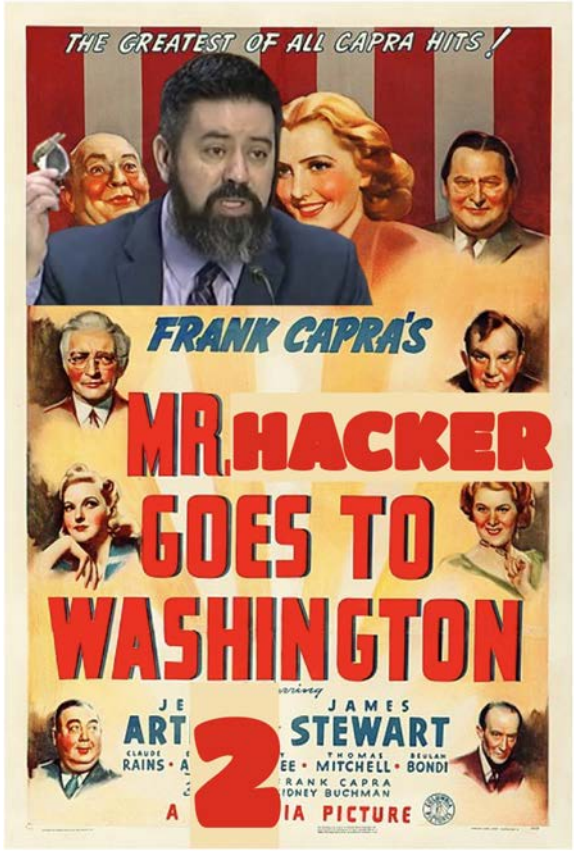
CyberMedSummit.org


B425 Sim Rm 5 Ceiling Camera
RØDE

Shattered Expectations...
[Pandemic]

iamthecavalry.org

I AM THE Cavalry



CISA COVID Task Force

→ Secure Vaccine Supply Chains ←

Protect Hospitals and Healthcare Delivery

IMG SRC: Ben Mosier & Josh Corman 2022

7 vaccine candidates

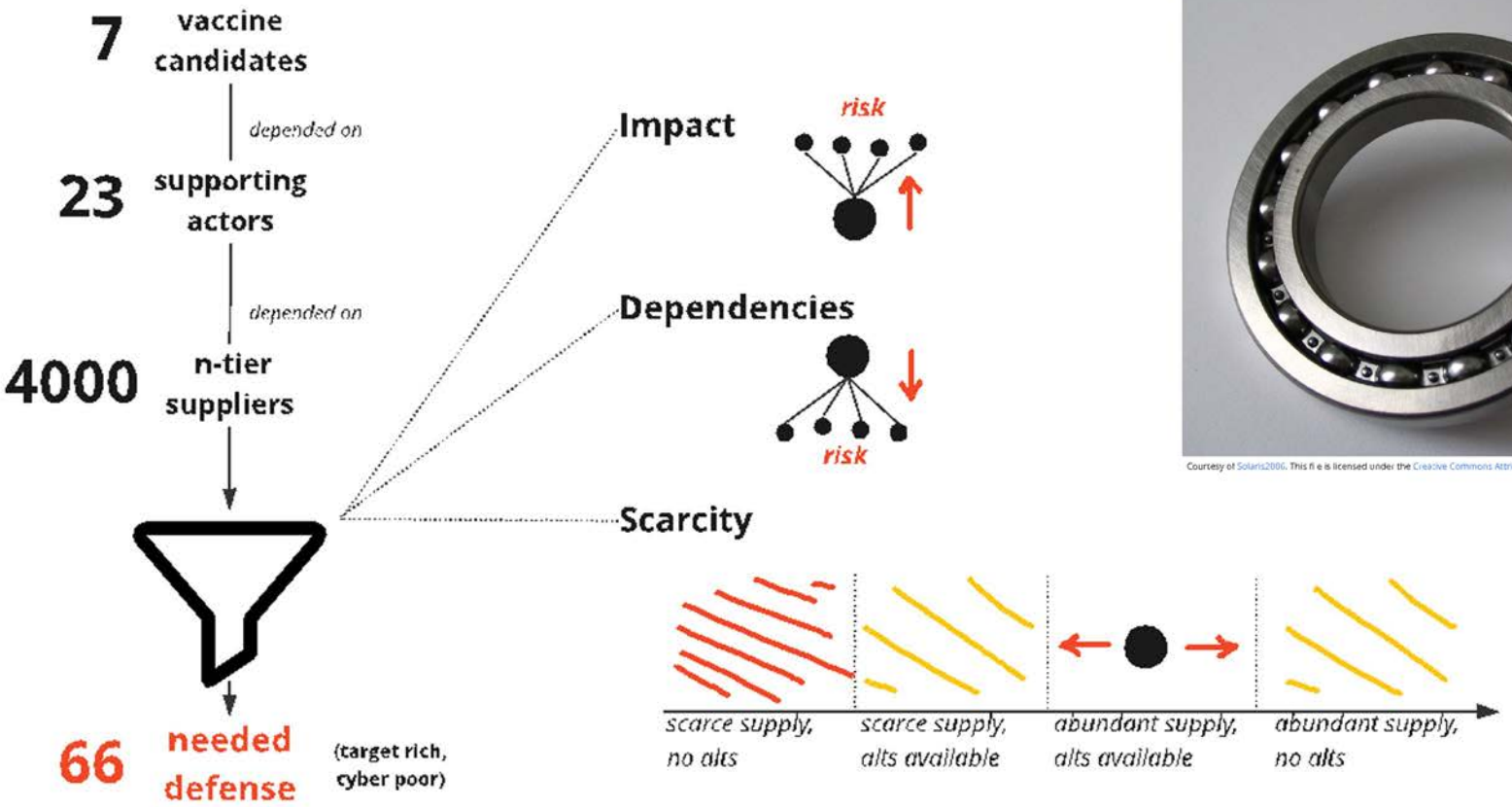
depended on

23 supporting actors

depended on

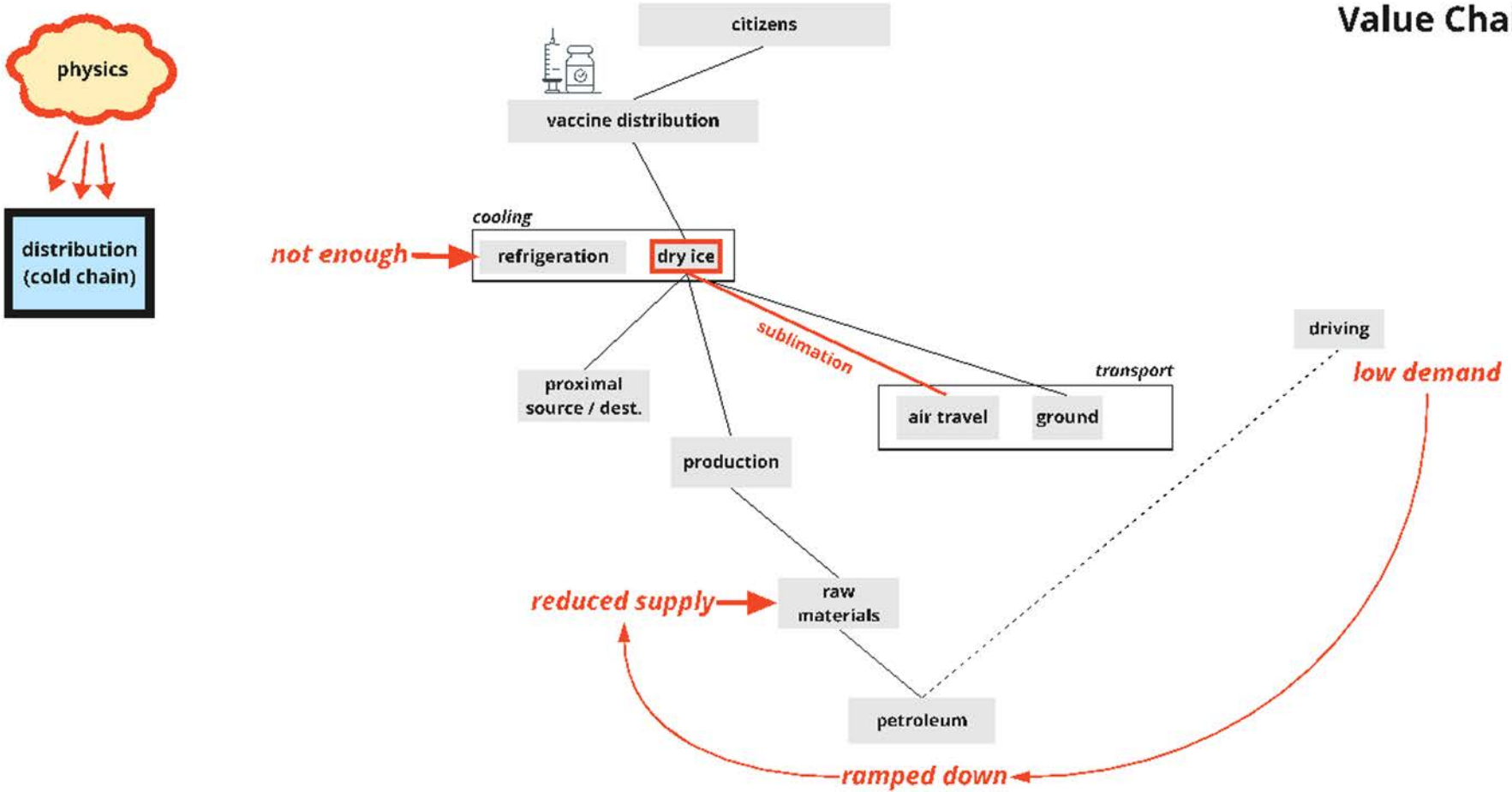
4000 n-tier suppliers

IMG SRC: Ben Mosier & Josh Corman 2022



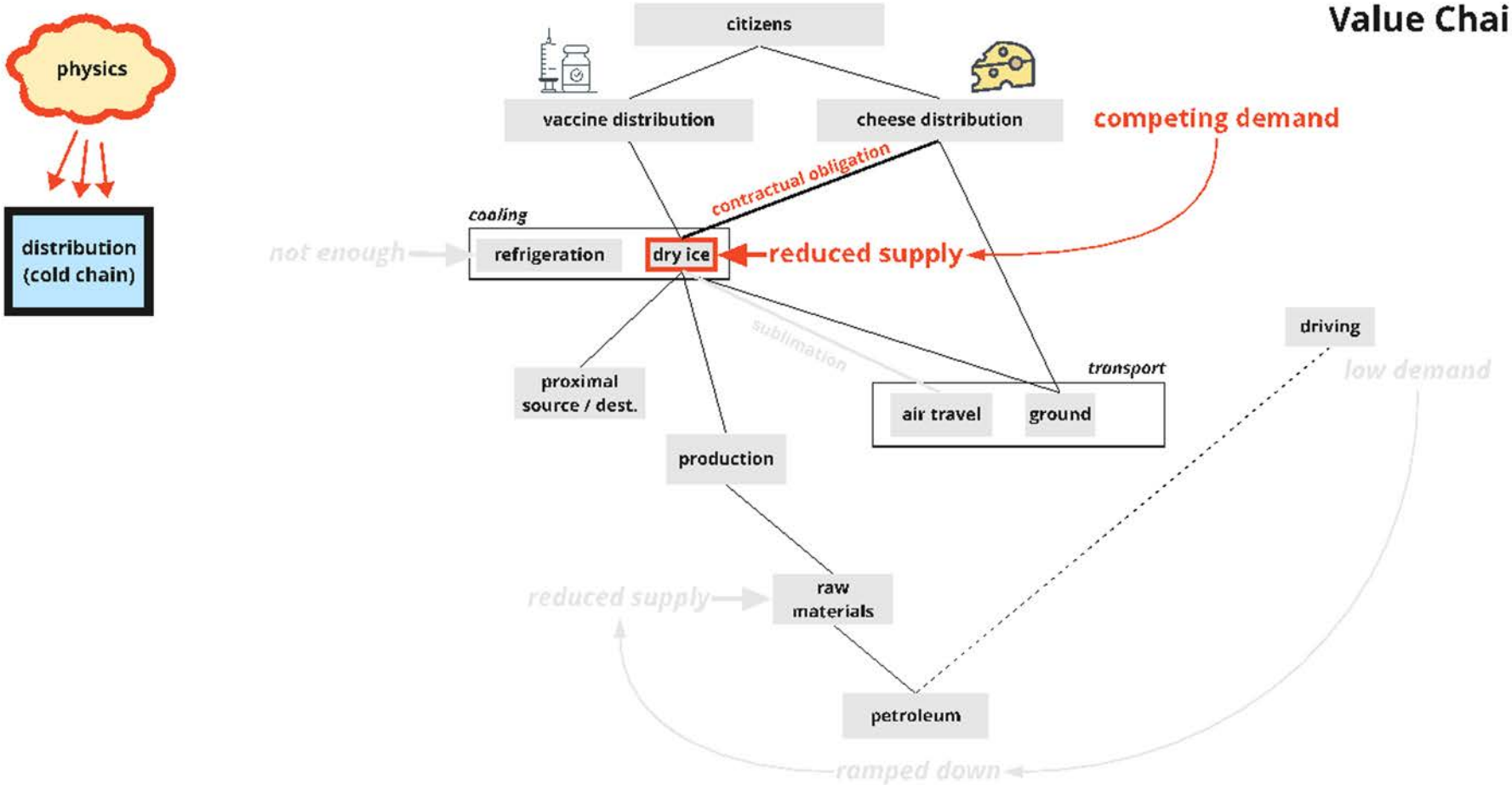
IMG SRC: Ben Mosier & Josh Corman 2022

Value Chain

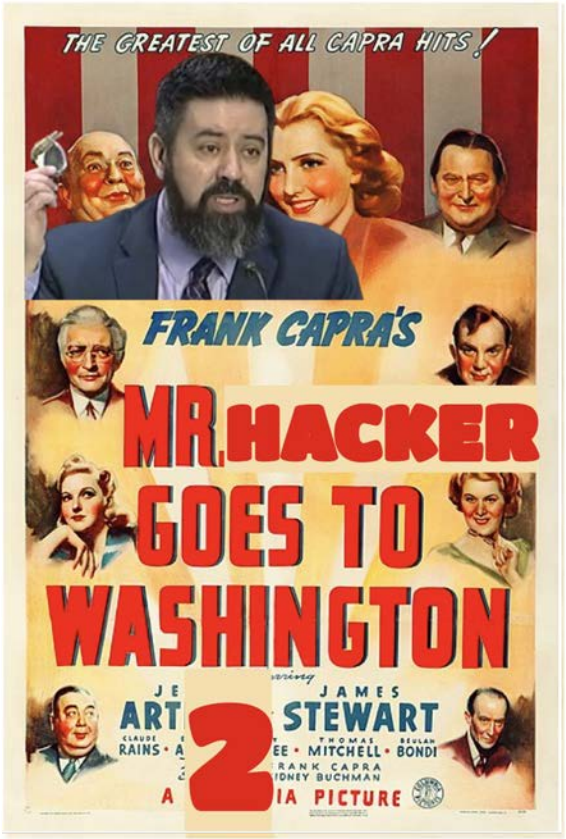


IMG SRC: Ben Mosier & Josh Corman 2022

Value Chain



IMG SRC: Ben Mosier & Josh Corman 2022

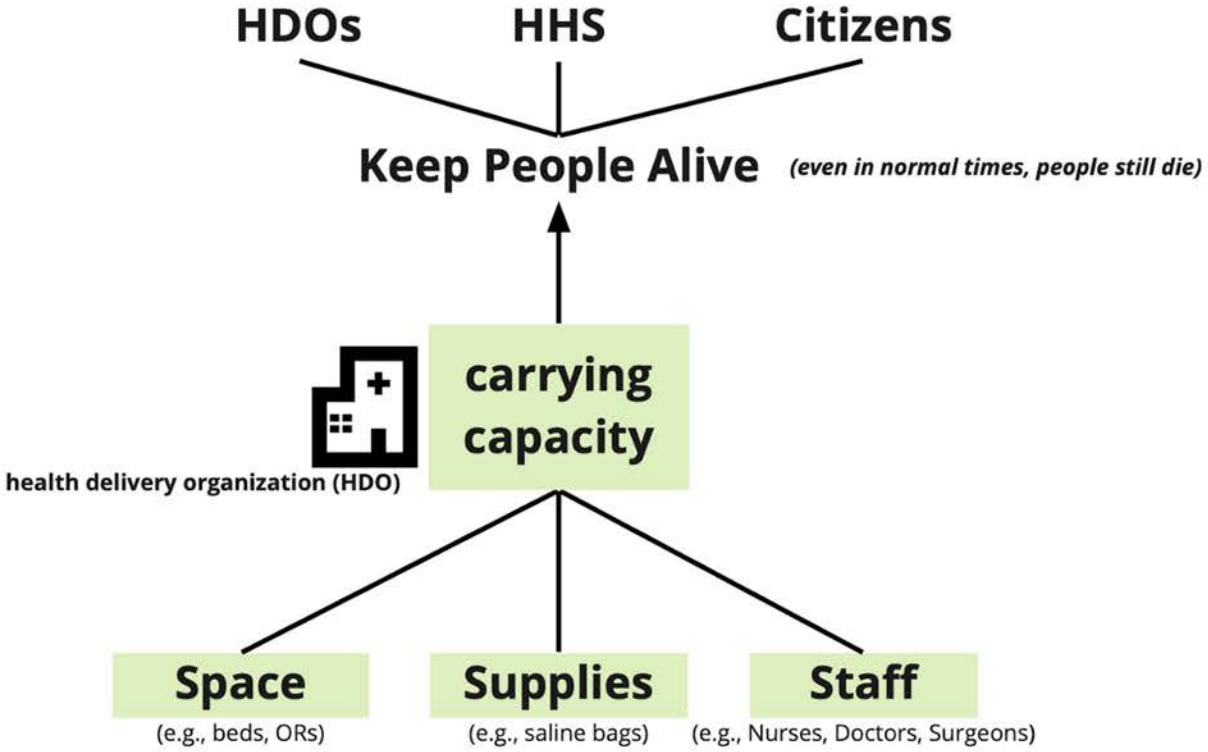


CISA COVID Task Force

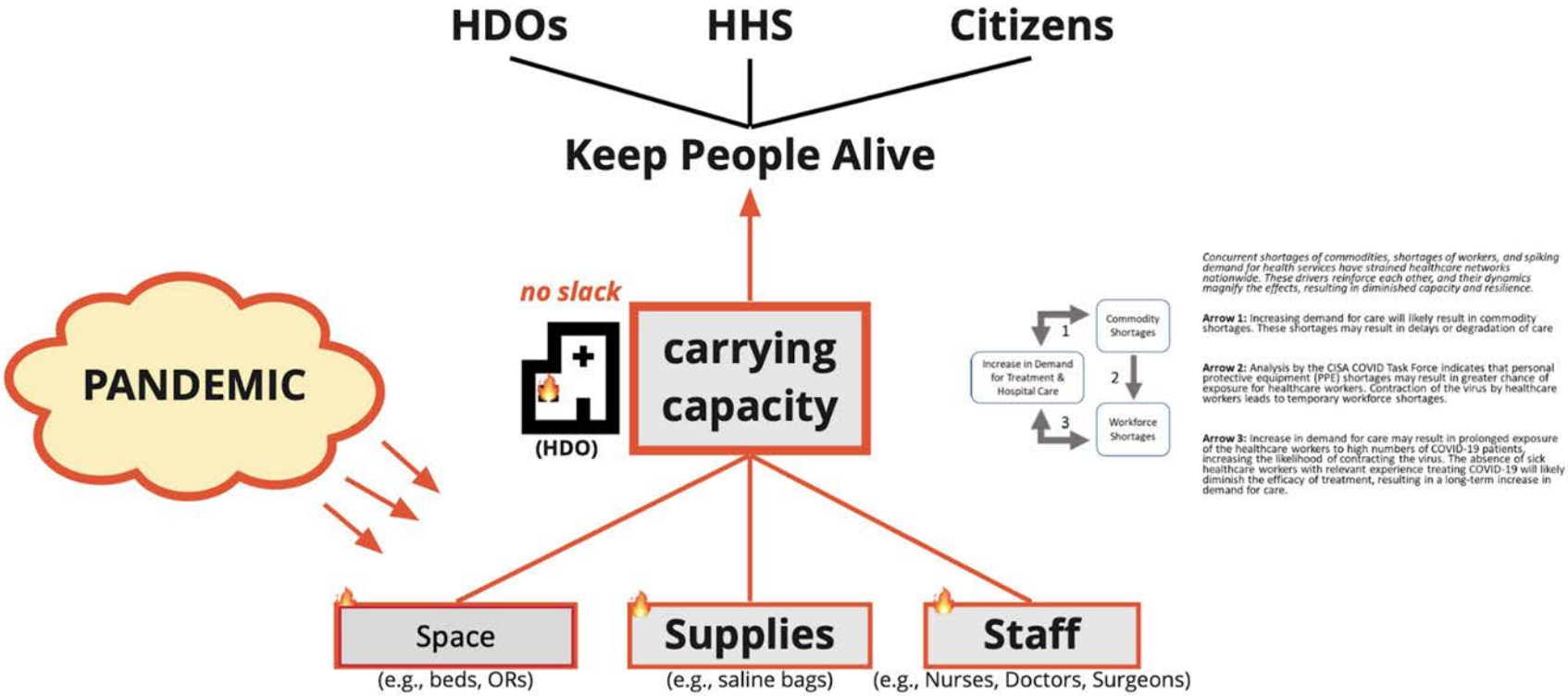
Secure Vaccine Supply Chains

→ Protect Hospitals and Healthcare Delivery ←

IMG SRC: Ben Mosier & Josh Corman 2022

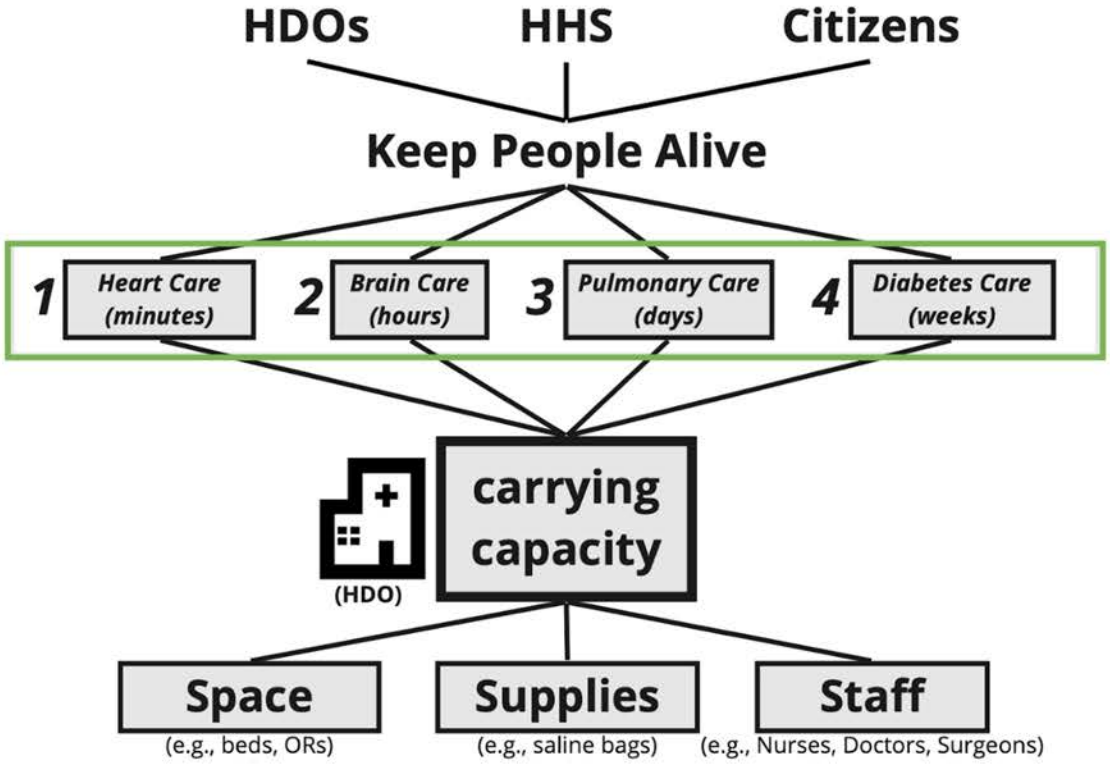


IMG SRC: Ben Mosier & Josh Corman 2022

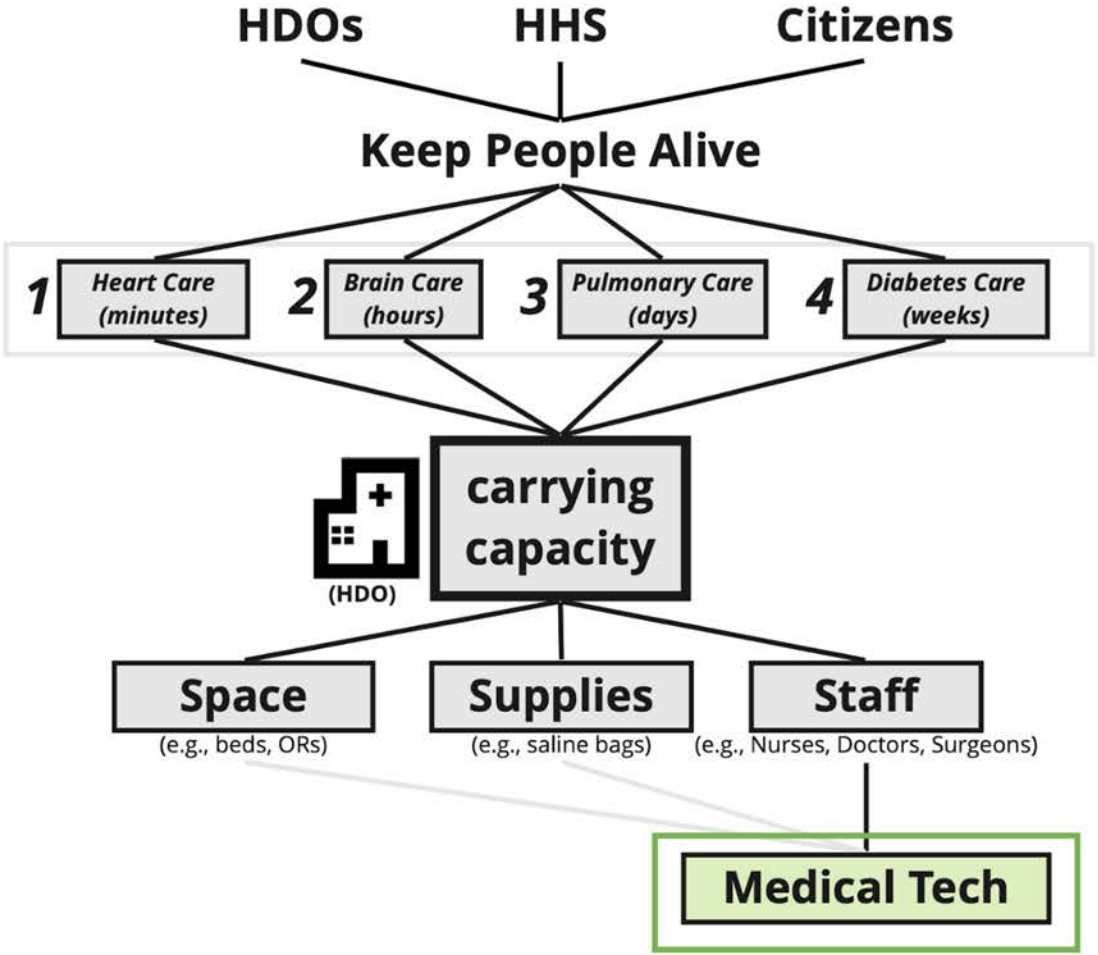


Cybersecurity & Infrastructure Security Agency. Provide Medical Care is in critical condition: analysis and stakeholder decision support to minimize further harm. Washington, DC: US Department of Homeland Security, Cybersecurity & Infrastructure Security Agency; 2020. https://www.cisa.gov/publication/provide-medical-care-critical-condition-analysis-and-stakeholder-decision-support

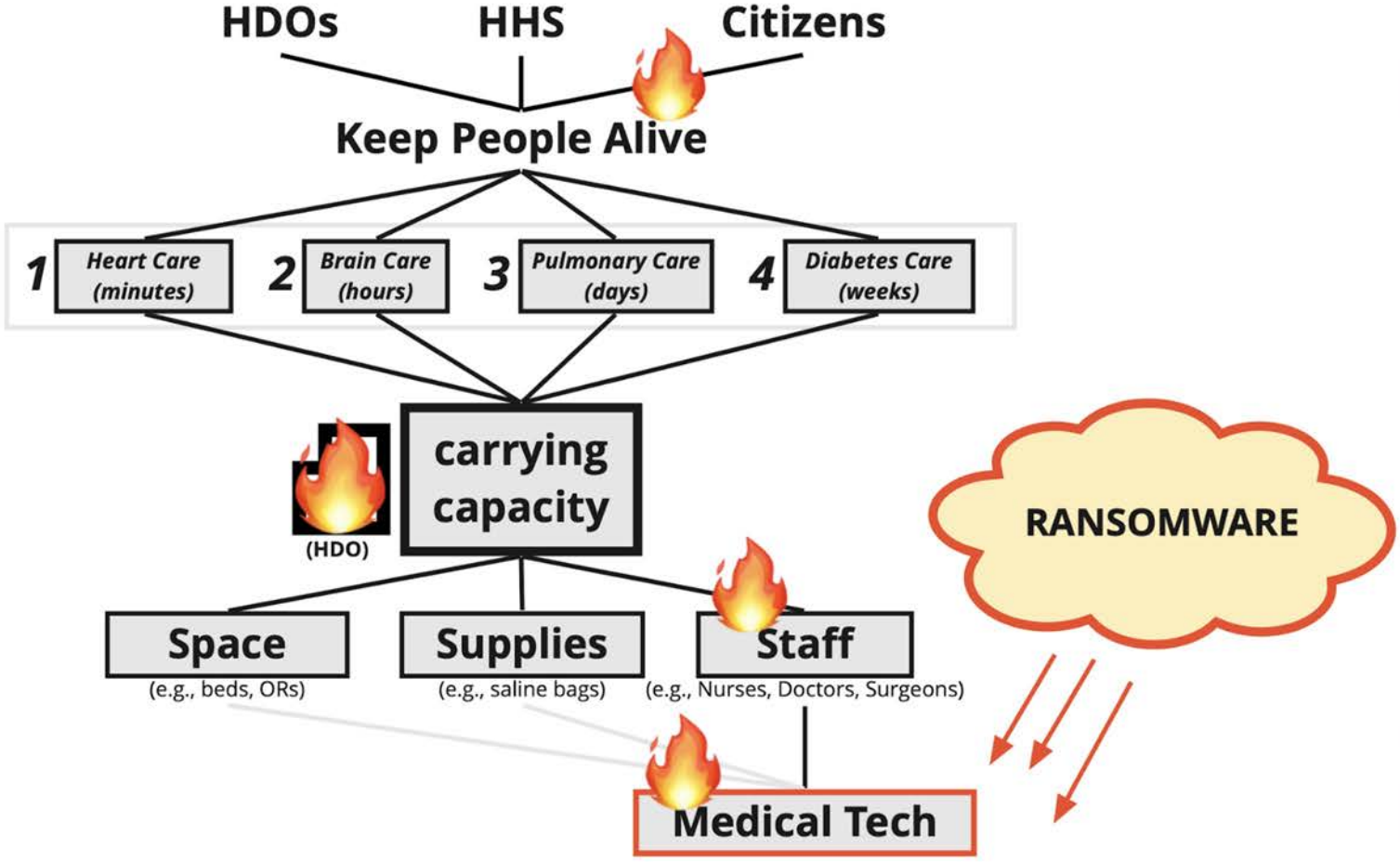
IMG SRC: Ben Mosier & Josh Corman 2022



IMG SRC: Ben Mosier & Josh Corman 2022



IMG SRC: Ben Mosier & Josh Corman 2022



IMG SRC: Ben Mosier & Josh Corman 2022


GNH
UAH
UAH
UAH


GNH
UAH
UAH
UAH


GNH
UAH
UAH
UAH


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.

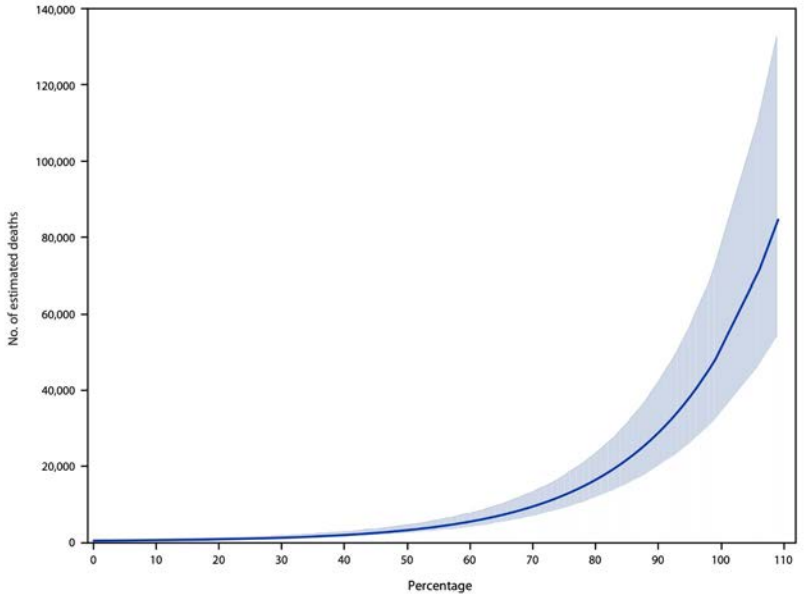
What are the implications for public health practice?

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
Related Materials
PDF [319K]

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

Cyber attacks lead to **1) IT network failure** and disrupt the ability of healthcare systems to access electronic health records (EHRs) and may close hospitals with IT network-based services—such as cardiac technology—and increase hospital strain (i.e., reduced capacity to take in new patients diverting critical care patients to further hospitals). **2) Ambulance diversion**, which is an important system-level interruption that causes delays in treatment and effecting time tolerance, lowering quality of care. In the long term, hospitals that experience cyber events are more likely to experience **3) hospital strain** (measured by ICU bed utilization), worsening health outcomes and contribute to **4) increased mortality**.

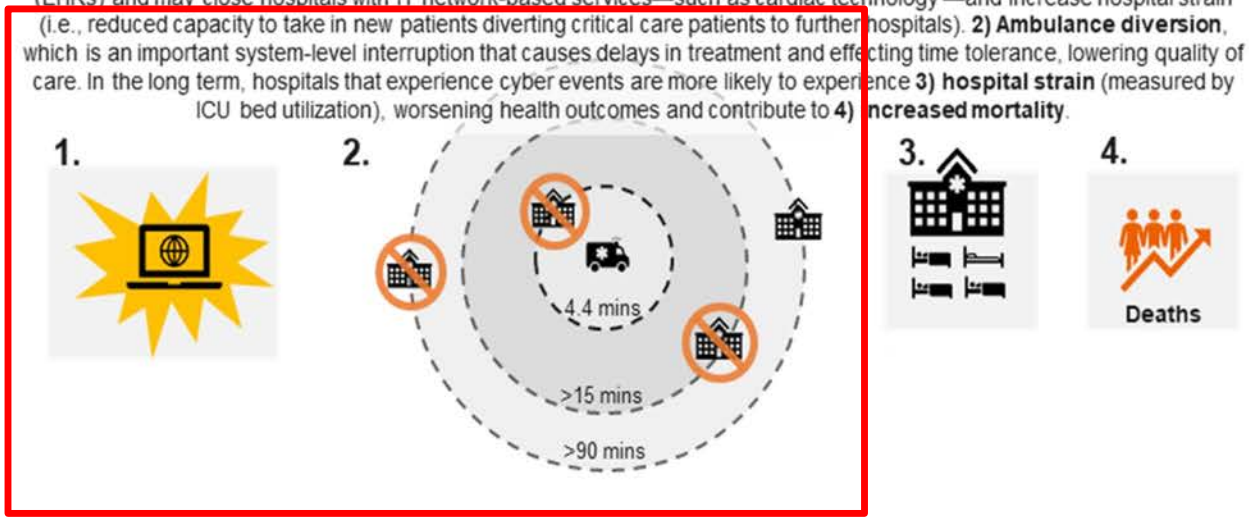
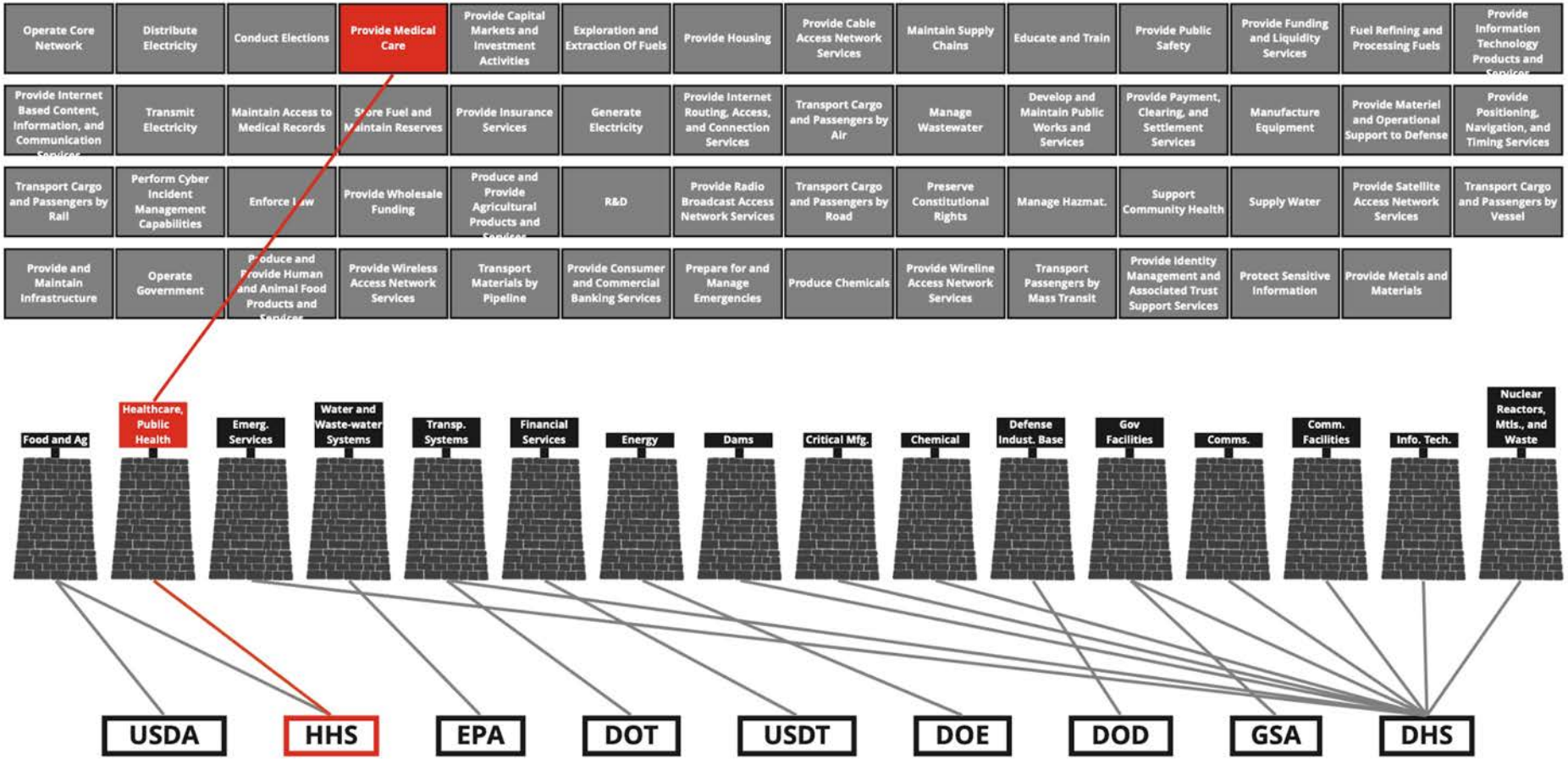


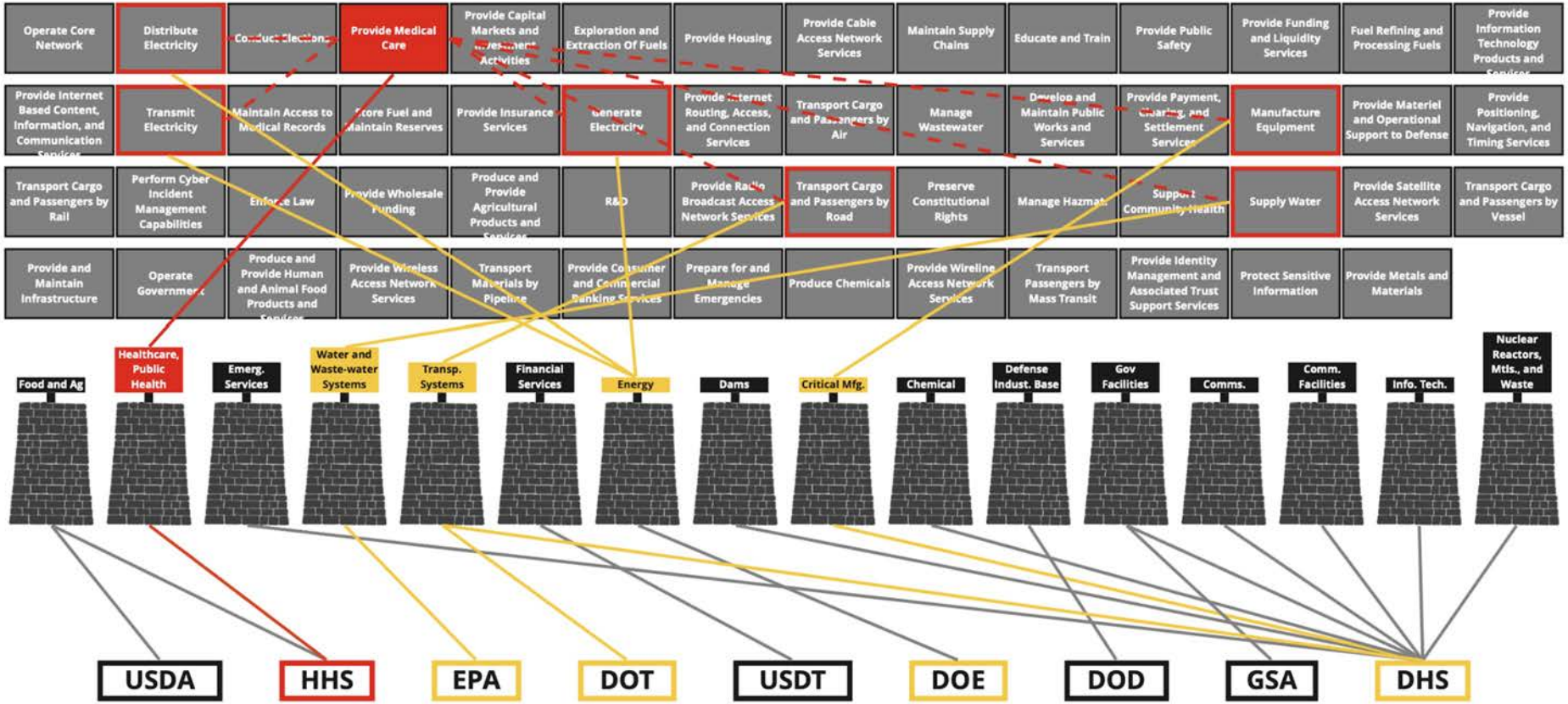
Figure 8 – Conceptual Model of Impact of Cyber Attack on Patient Outcomes



IMG SRC: Ben Mosier & Josh Corman 2022

exponential excess deaths

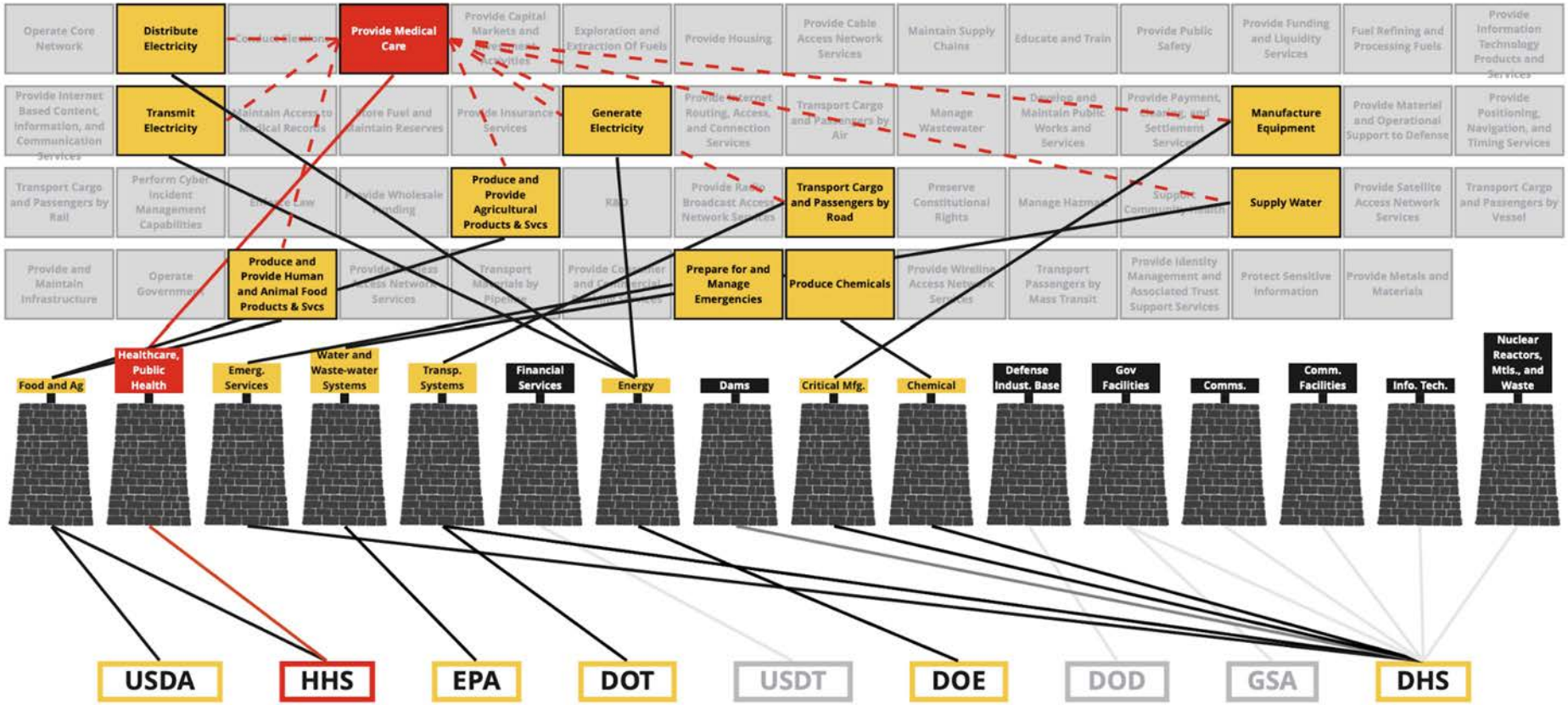
No critical infrastructure is an island.
Without multidisciplinary, multi-agency coordination, people die.



IMG SRC: Ben Mosier & Josh Corman 2022

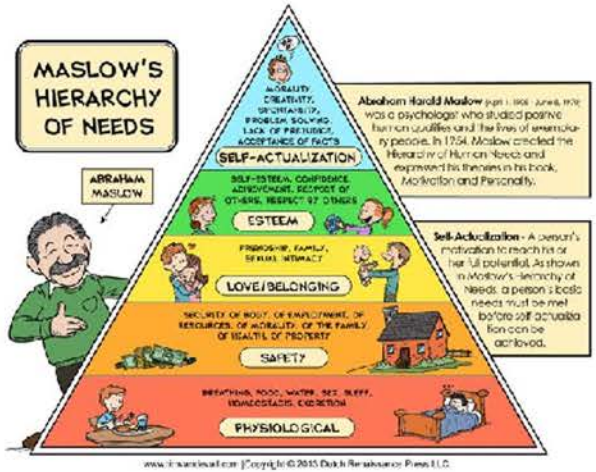
exponential excess deaths

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



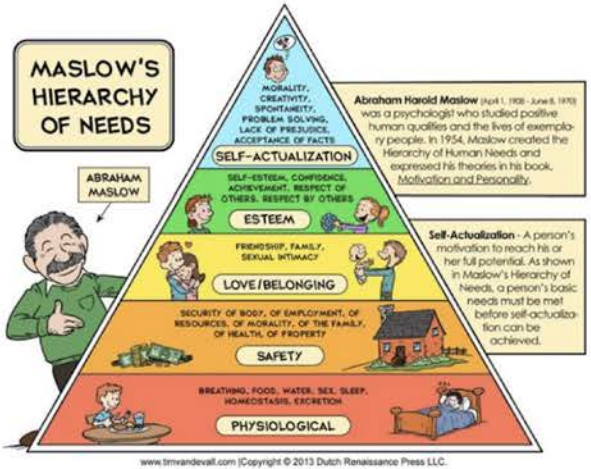
IMG SRC: Ben Mosier & Josh Corman 2022

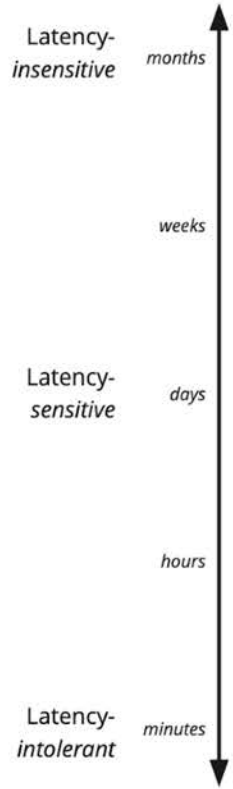
*positions illustrative, not definitive



IMG SRC: Ben Mosier & Josh Corman 2022

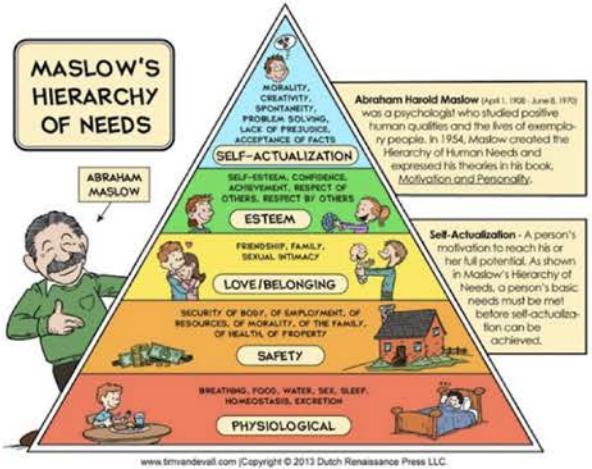
*positions illustrative, not definitive

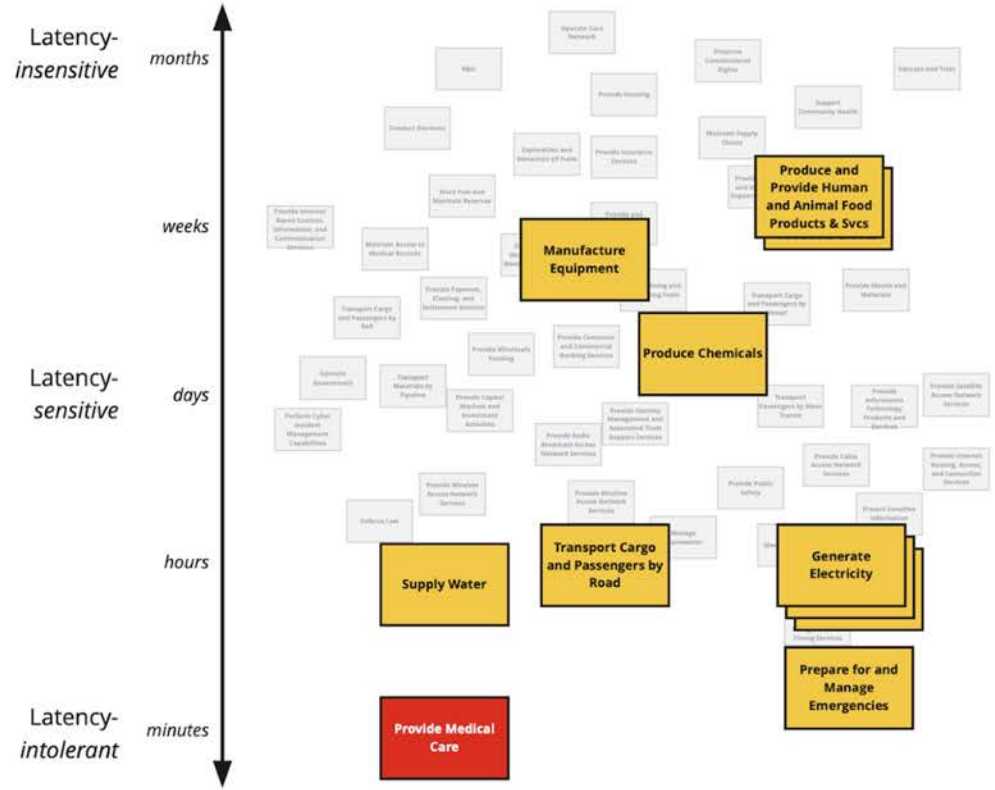




IMG SRC: Ben Mosier & Josh Corman 2022

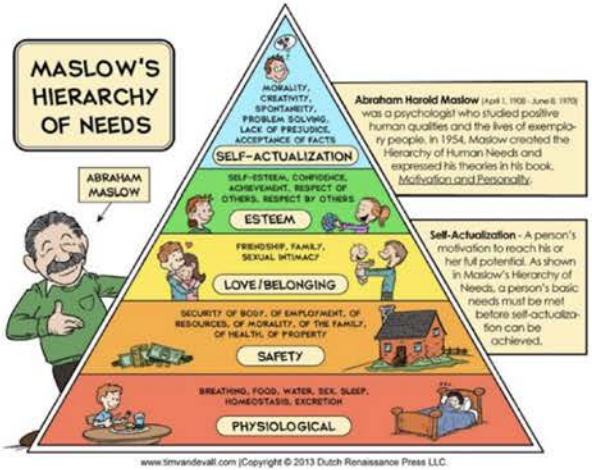
*positions illustrative, not definitive

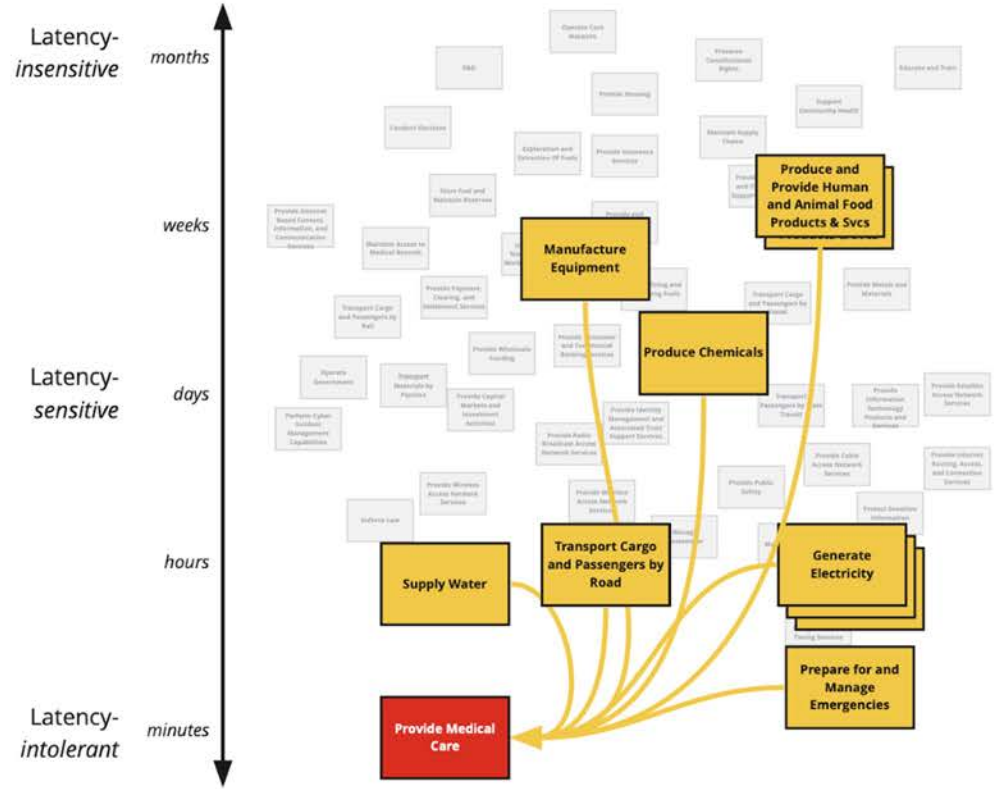




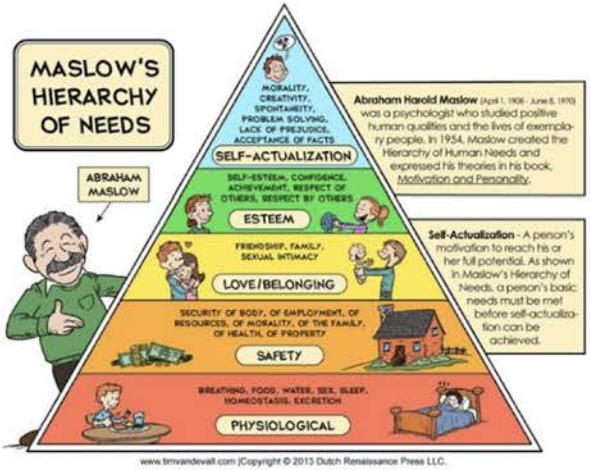
IMG SRC: Ben Mosier & Josh Corman 2022

*positions illustrative, not definitive





IMG SRC: Ben Mosier & Josh Corman 2022



*positions illustrative, not definitive

Latency-*insensitive* — *months*

Latency-*sensitive* — *weeks* / *days* / *hours*

Latency-*intolerant* — *minutes*

Positive Feedback Loops, Negative Consequences

- Produce and Provide Human and Animal Food Products & Svcs
- Manufacture Equipment
- Produce Chemicals
- Supply Water
- Transport Cargo and Passengers by Road
- Generate Electricity
- Prepare for and Manage Emergencies
- Provide Medical Care

destructive

destabilizing

IMG SRC: Ben Mosier & Josh Corman 2022

Target Rich; Cyber Poor

Information
Incentives
Resources

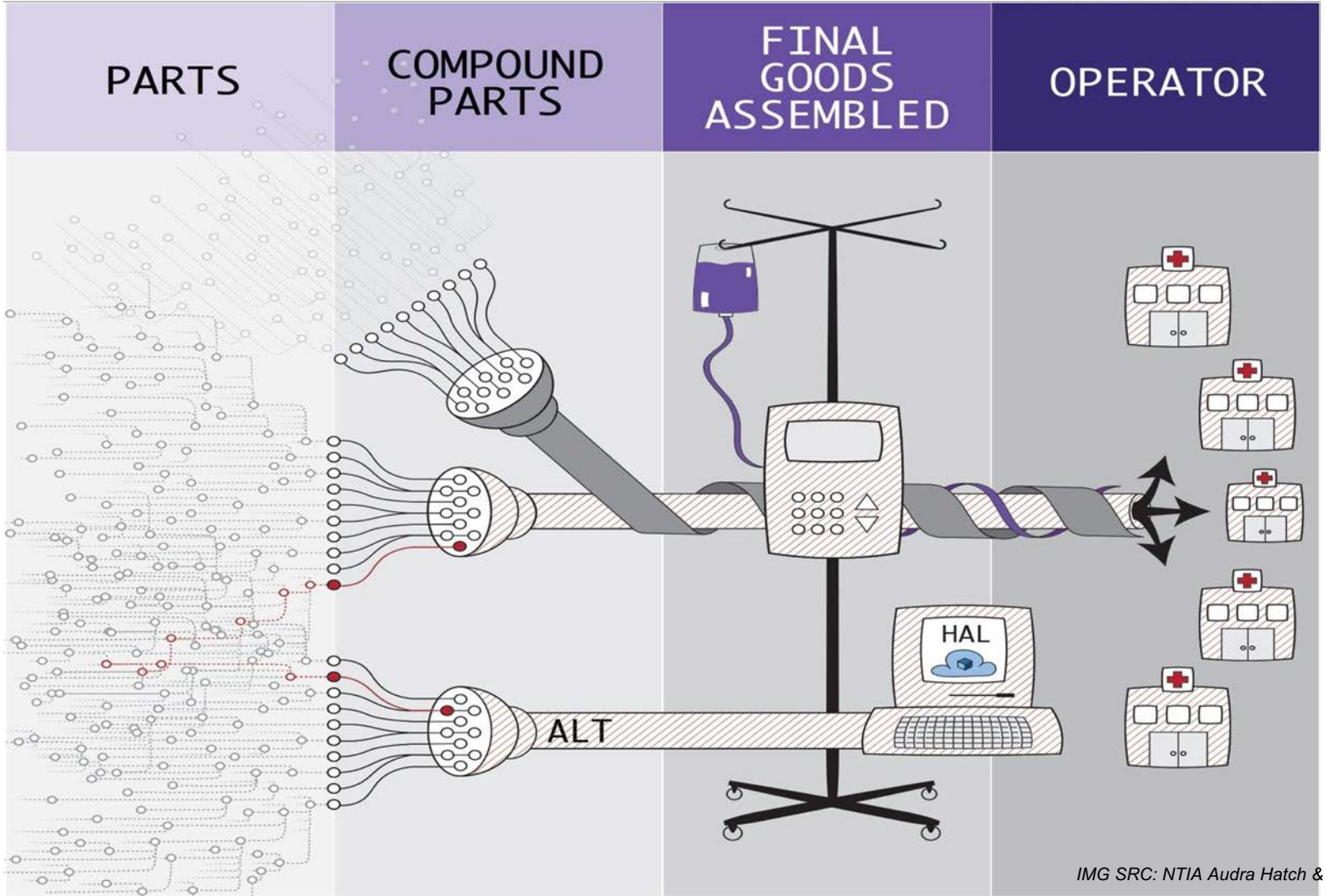
iamthecavalry.org

I AM THE Cavalry

Do NOT F*** with Maslow

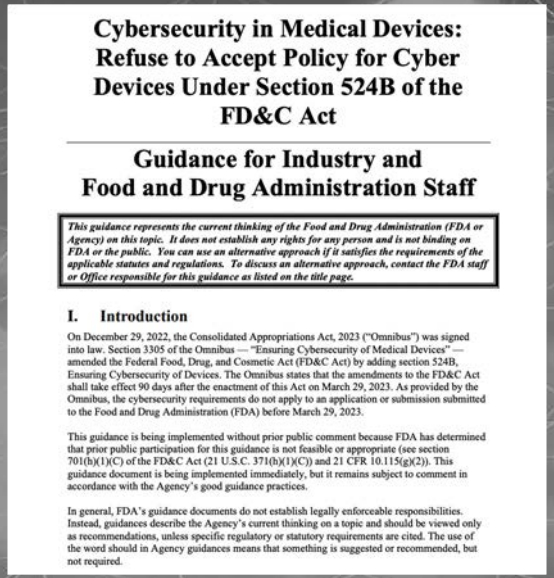
iamthecavalry.org

I AM THE Cavalry



IMG SRC: NTIA Audra Hatch & Josh Corman

PATCH Act… ++
Law of the Land



Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices Under Section 524B of the FD&C Act

Guidance for Industry and Food and Drug Administration Staff

This guidance represents the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.

I. Introduction

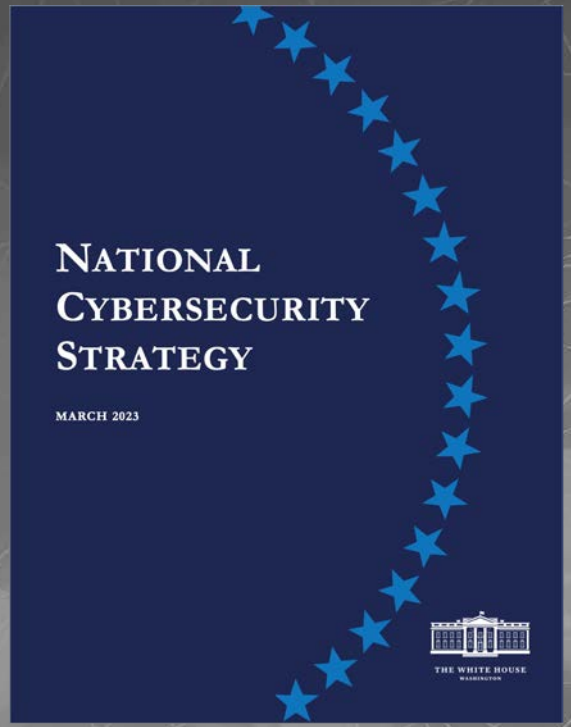
On December 29, 2022, the Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law. Section 3305 of the Omnibus — "Ensuring Cybersecurity of Medical Devices" — amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices. The Omnibus states that the amendments to the FD&C Act shall take effect 90 days after the enactment of this Act on March 29, 2023. As provided by the Omnibus, the cybersecurity requirements do not apply to an application or submission submitted to the Food and Drug Administration (FDA) before March 29, 2023.

This guidance is being implemented without prior public comment because FDA has determined that prior public participation for this guidance is not feasible or appropriate (see section 701(h)(1)(C) of the FD&C Act (21 U.S.C. 371(h)(1)(C)) and 21 CFR 10.115(g)(2)). This guidance document is being implemented immediately, but it remains subject to comment in accordance with the Agency's good guidance practices.

In general, FDA's guidance documents do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word should in Agency guidances means that something is suggested or recommended, but not required.

I AM THE Cavalry

White House National Cybersecurity Strategy



The strategy is organized across five pillars:

1. Defending our critical infrastructure
2. Disrupting threat actors
3. Shaping market forces
4. Investing in our future
5. Forging international partnerships

OFFICE OF SEN. MARK R. WARNER

Cybersecurity is Patient Safety

POLICY OPTIONS IN THE HEALTH CARE SECTOR

Mark R. Warner
US Senator from the Commonwealth of Virginia

NOVEMBER 2022

Close Your Eyes...

SECURITY

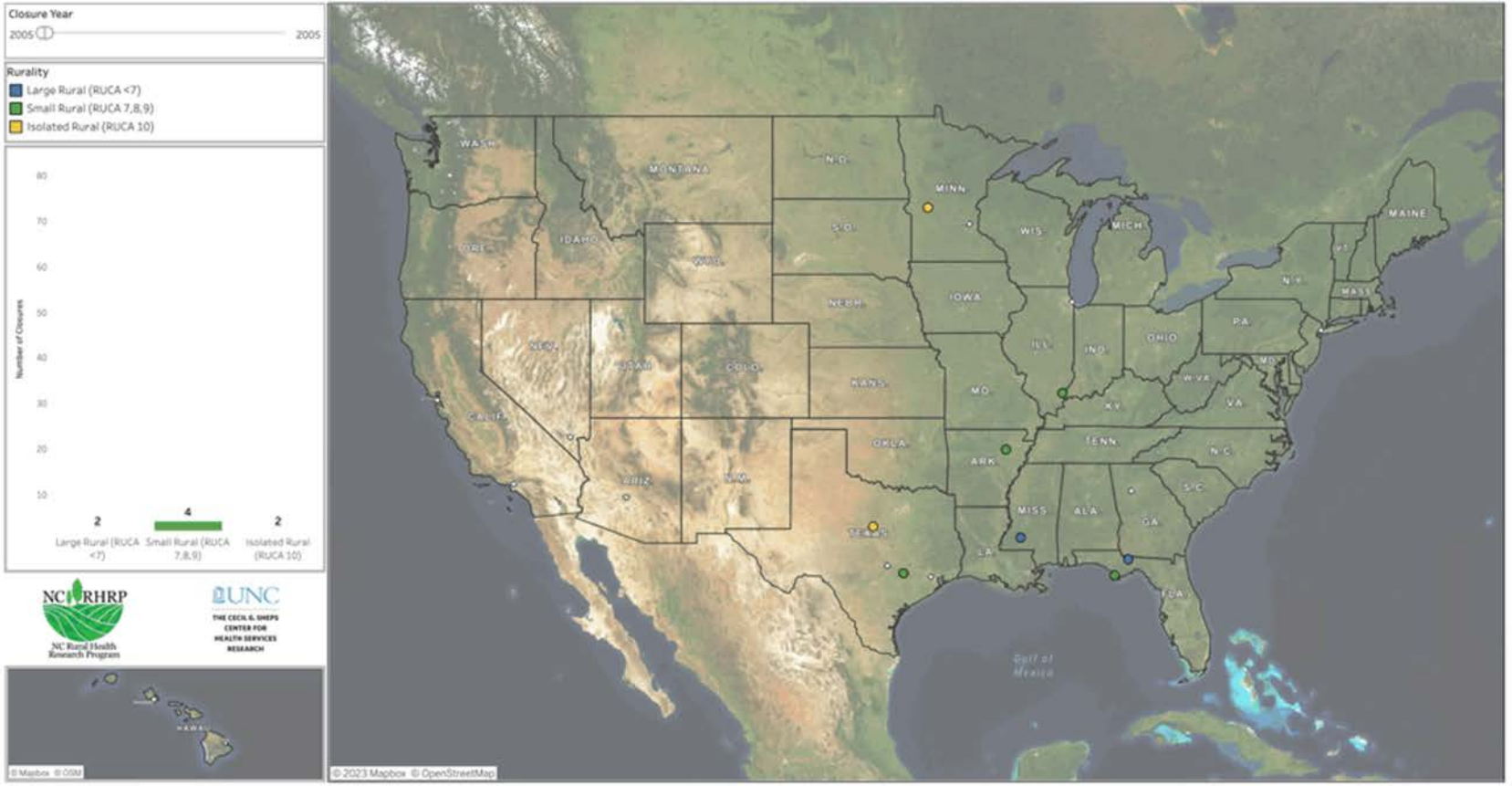
An Illinois hospital is the first health care facility to link its closing to a ransomware attack

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



What are our constraints?


STARK

Humble Seekers
System Thinkers
Boundary Spanners

iamthecavalry.org

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

THANK YOU!

@joshcorman

@iamthecavalry

I AM THE Cavalry

www.iamthecavalry.org