Bits & Bytes, Flesh & Blood, and Saving Real Lives via Clinical Simulations

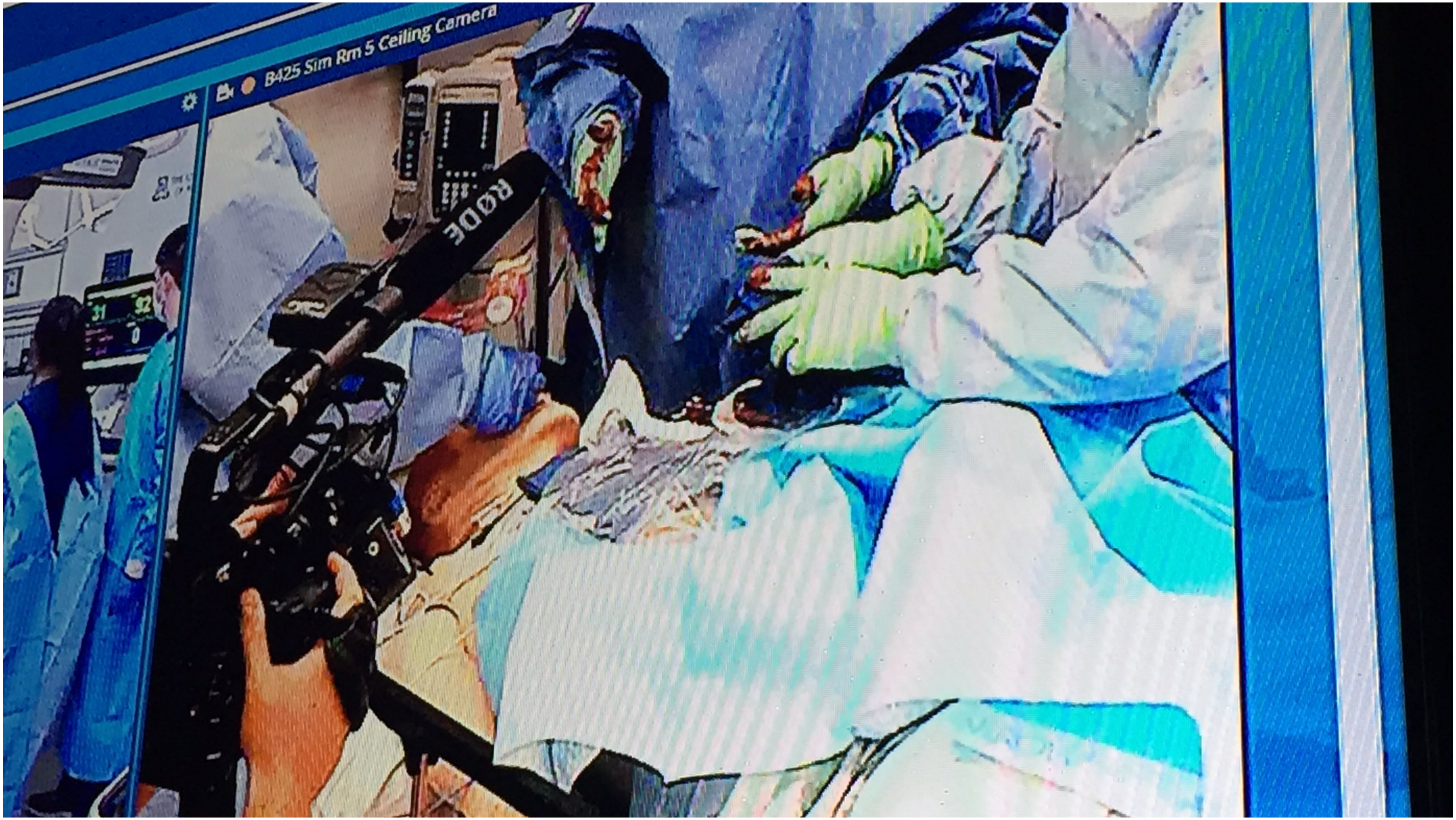
Joshua Corman
ENIGMA 2018

Safer | Sooner | Together

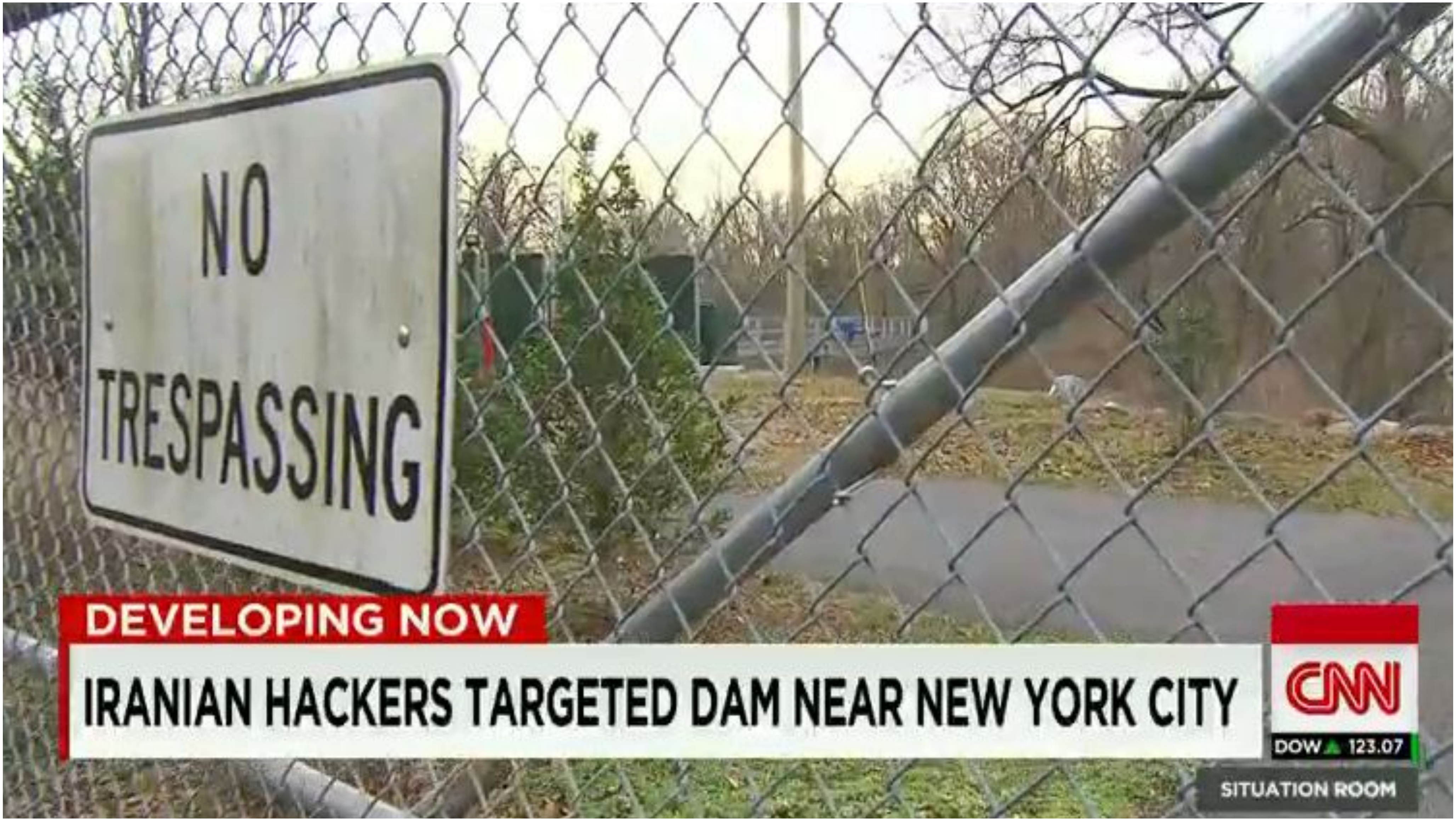
@joshcorman

@IamTheCavalry

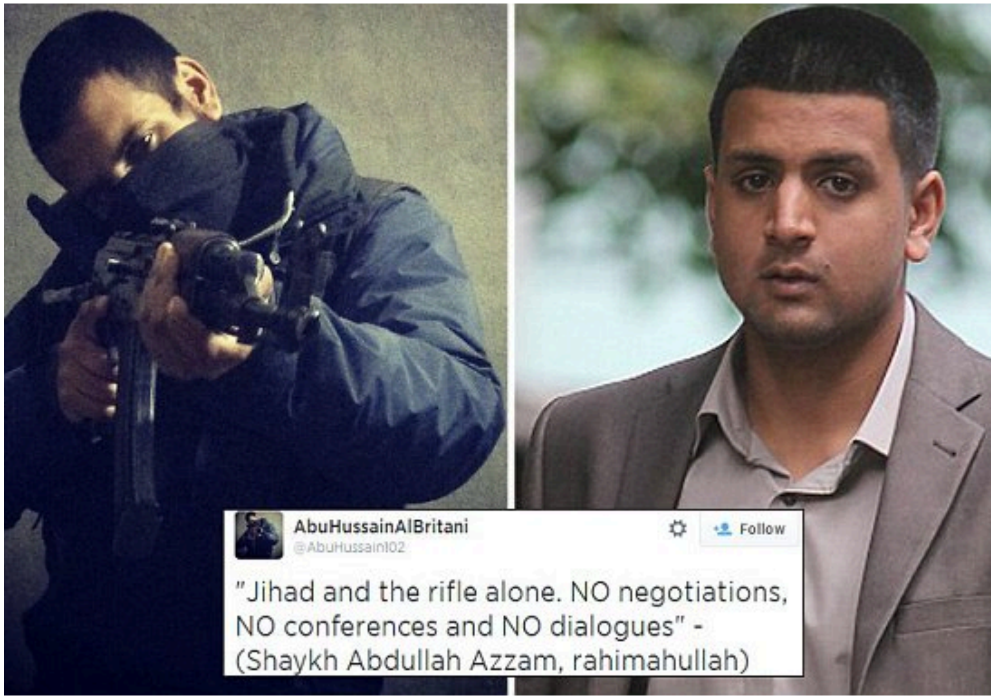
I am The Cavalry


B425 Sim Rm 5 Ceiling Camera
RØDE
31
92
0

BlackEnergy cybercrime tool


NO
TRESPASSING
DEVELOPING NOW
IRANIAN HACKERS TARGETED DAM NEAR NEW YORK CITY
CNN
DOW ▲ 123.07
SITUATION ROOM

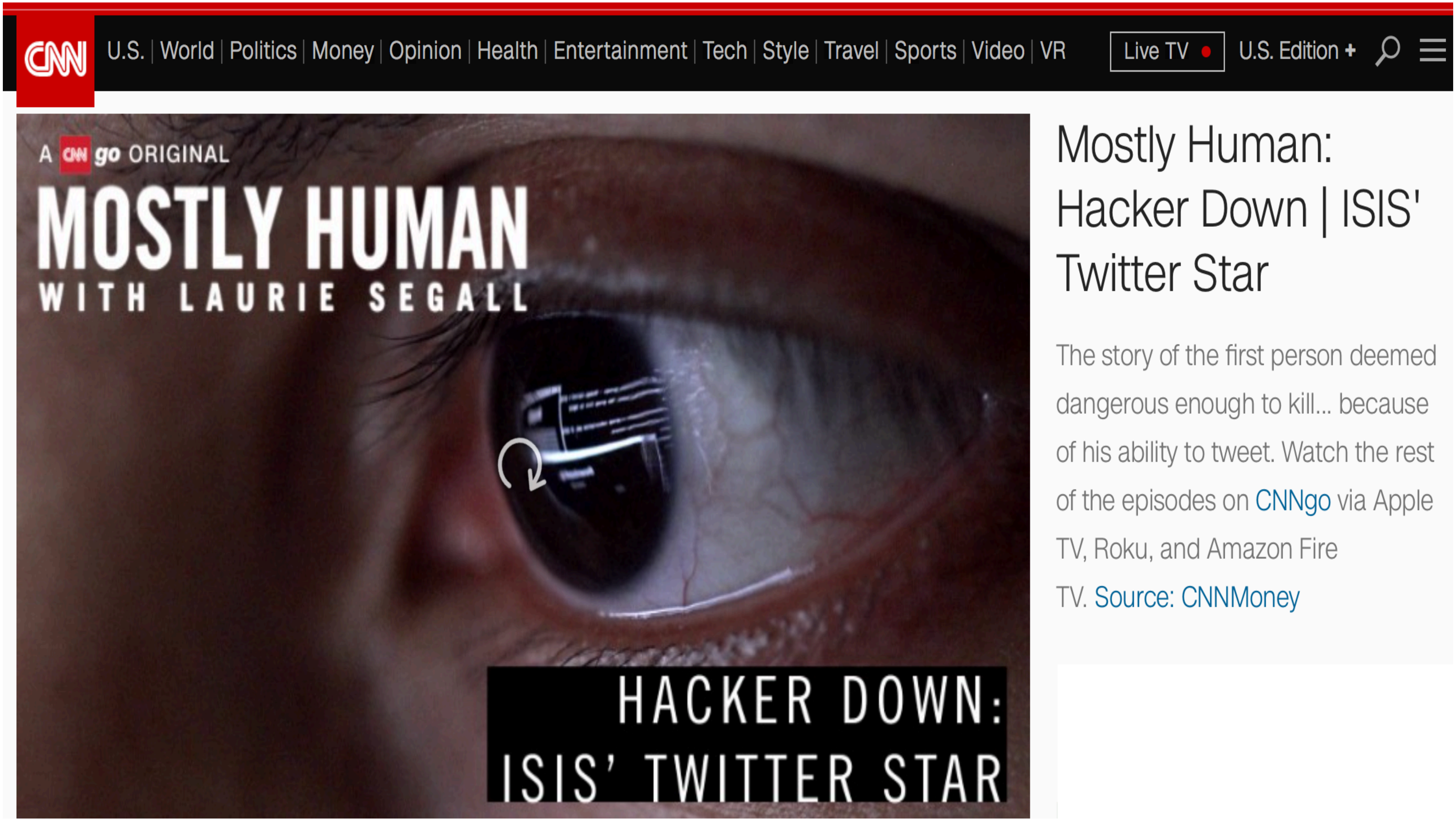
HOLLYWOOD
MEDICAL CENTER
E EMERGENCY
P Parking
H Hospital
D Doctor's Tower



AbuHussainAlBritani
@AbuHussain102

"Jihad and the rifle alone. NO negotiations, NO conferences and NO dialogues" - (Shaykh Abdullah Azzam, rahimahullah)

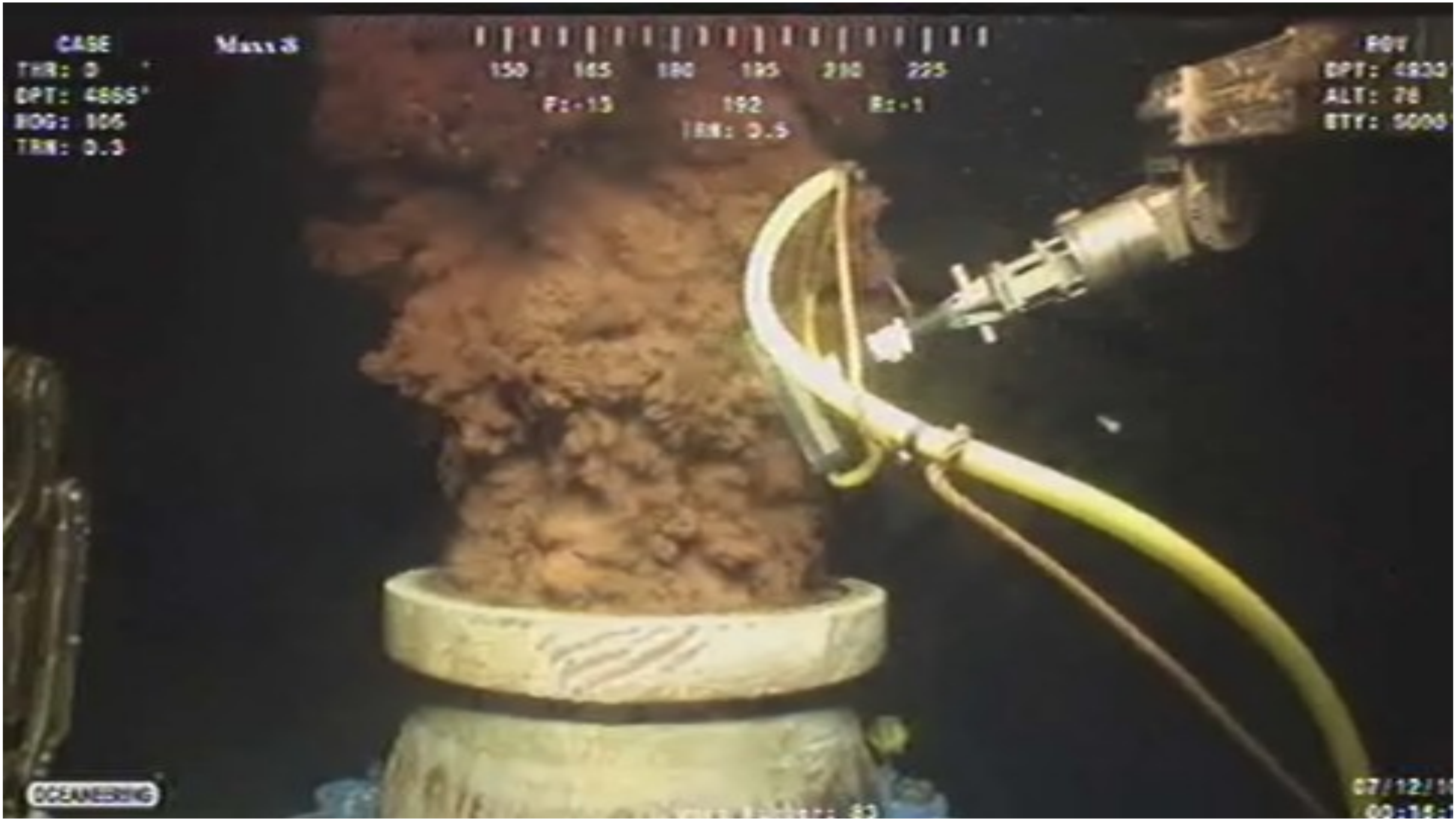
C


CNN
U.S. | World | Politics | Money | Opinion | Health | Entertainment | Tech | Style | Travel | Sports | Video | VR
Live TV ●
U.S. Edition +
A CNN go ORIGINAL
MOSTLY HUMAN
WITH LAURIE SEGALL
HACKER DOWN:
ISIS' TWITTER STAR

Mostly Human: Hacker Down | ISIS' Twitter Star

The story of the first person deemed dangerous enough to kill... because of his ability to tweet. Watch the rest of the episodes on CNNgo via Apple TV, Roku, and Amazon Fire TV. Source: CNNMoney

HOLLYWOOD
MEDICAL CENTER
E EMERGENCY
P Parking
H Hospital
D Doctor's Tower


CASE
Maxx 3
THR: 0
DPT: 4865'
HDG: 106
TRN: 0.3
150
165
180
195
210
225
P:-15
192
R:-1
TRN: 0.5
ROV
DPT: 4830'
ALT: 78
BTY: 5000'
OCEANEERING
07/12/10
00:15:1

Government has noticed in the last 18 months…

Presidential Commission Report

DOC/NTIA Guidance

FDA Guidance

DOJ Work Group

DOD Strategy

EU Guidance

DHS Guidance

FTC Guidelines

HHS Task Force

DOT Principles

NHTSA Guidance

Hippocratic Oath

Formal Capacities

1. Cyber Safety by Design
2. Third-Party Collaboration
3. Evidence Capture
4. Resilience and Containment
5. Cyber Safety Updates

Plain Speak

1. Avoid Failure
2. Engage Allies to Avoid Failure
3. Learn from Failure
4. Isolate Failure
5. Respond to Failure

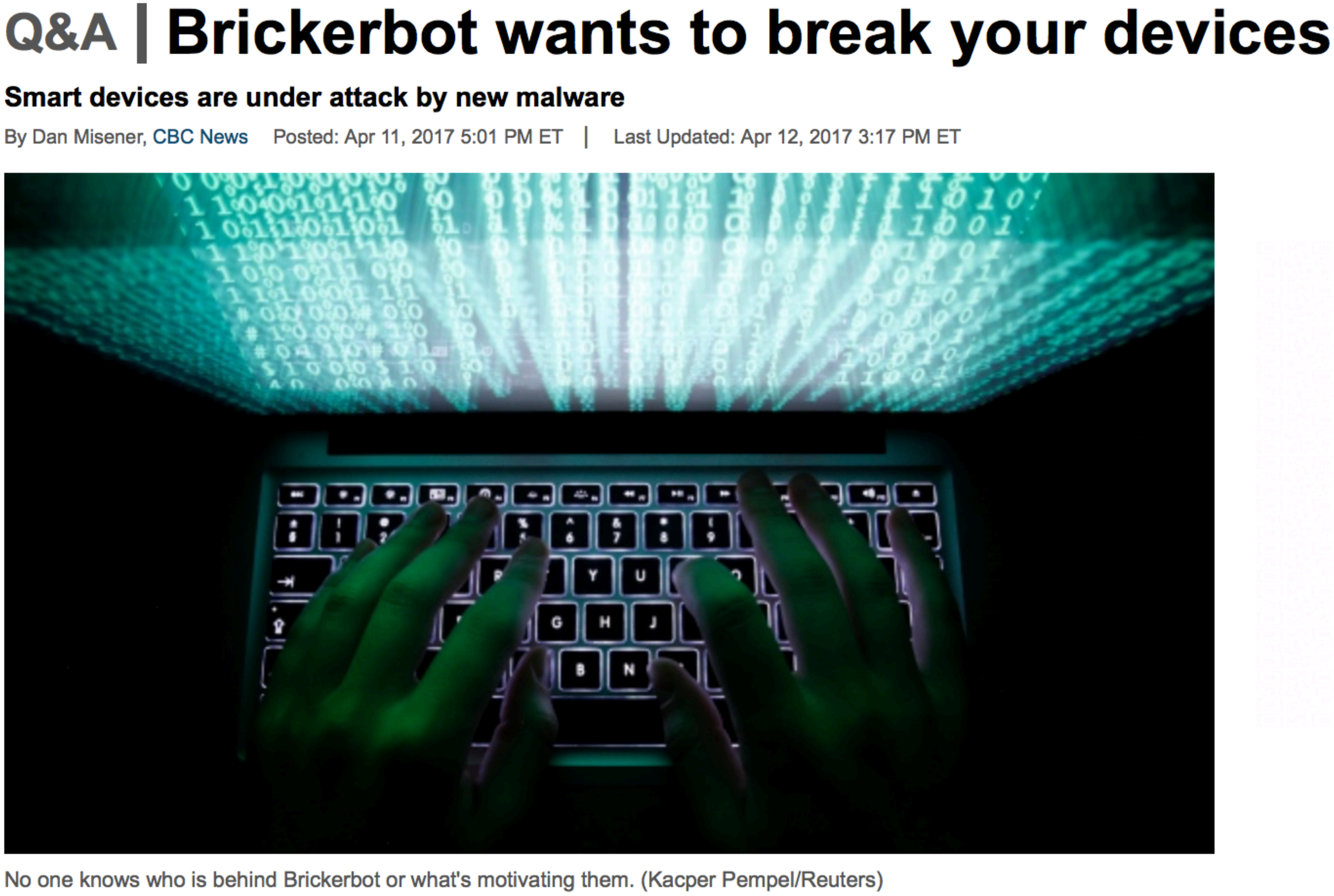
www.iamthecavalry.org
@iamthecavalry

New: How IoT is "different"

Aspect	Descriptions
Adversaries	Different adversaries with different motivations and capabilities
Consequences of Failures	Life & Limb, Physical Damage, Market Stability/Confidence, National Security
Context & Environment	Operational contexts can be quite different. Migratory, Perimeter-less, Inaccessible, Difficult to patch/replace
Composition of Goods	Differences in Hardware, Firmware, Software stacks
Economics	Margins, Buyers, Investors, Costs of Goods, etc
Time Scales	Time-to-Live (TTLs), R&D Cycles, Response Times

CC : From: http://www.flickr.com/photos/maiabee/2760312781/

C



Q&A | Brickerbot wants to break your devices

Smart devices are under attack by new malware

By Dan Misener, CBC News   Posted: Apr 11, 2017 5:01 PM ET | Last Updated: Apr 12, 2017 3:17 PM ET

No one knows who is behind Brickerbot or what's motivating them. (Kacper Pempel/Reuters)

HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

June 2017

REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

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.

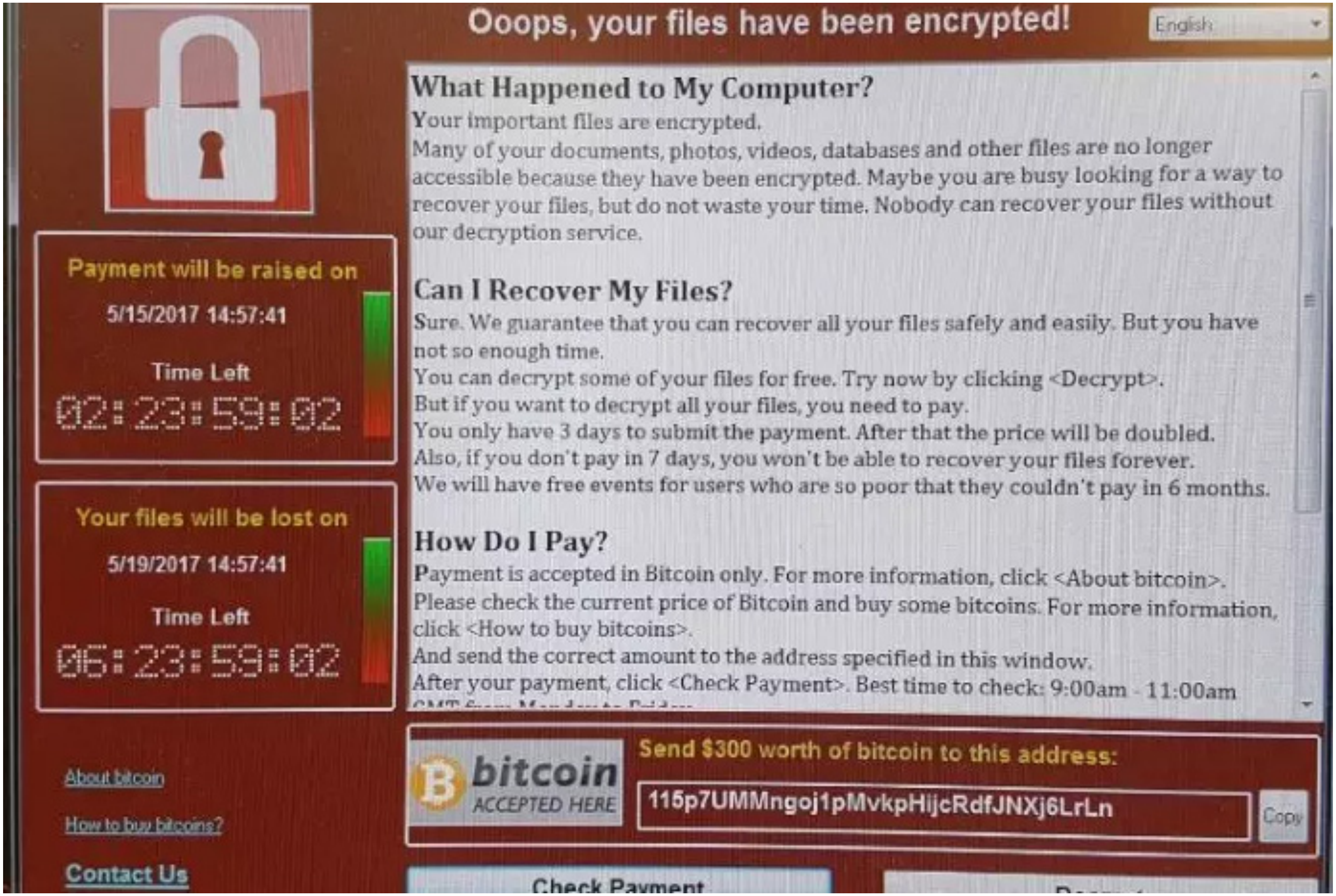
Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

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

If you can’t afford to ***protect*** *it*
then
you can’t afford to ***connect*** *it*

C

*With great **connectivity***
*comes great **responsibility***



Ooops, your files have been encrypted!

Payment will be raised on

5/15/2017 14:57:41

Time Left

02:23:59:02

Your files will be lost on

5/19/2017 14:57:41

Time Left

06:23:59:02

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

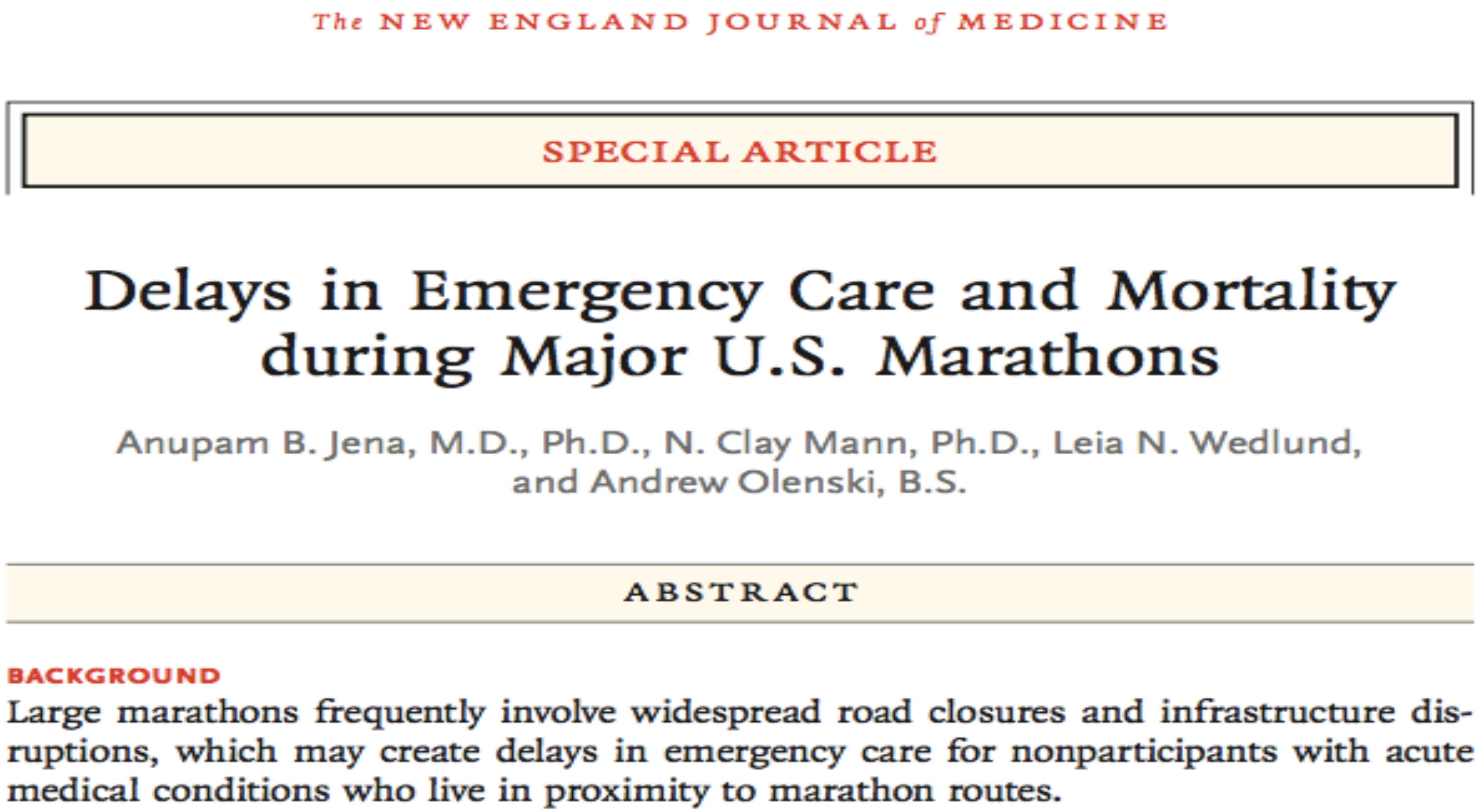
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

C



The NEW ENGLAND JOURNAL of MEDICINE

SPECIAL ARTICLE

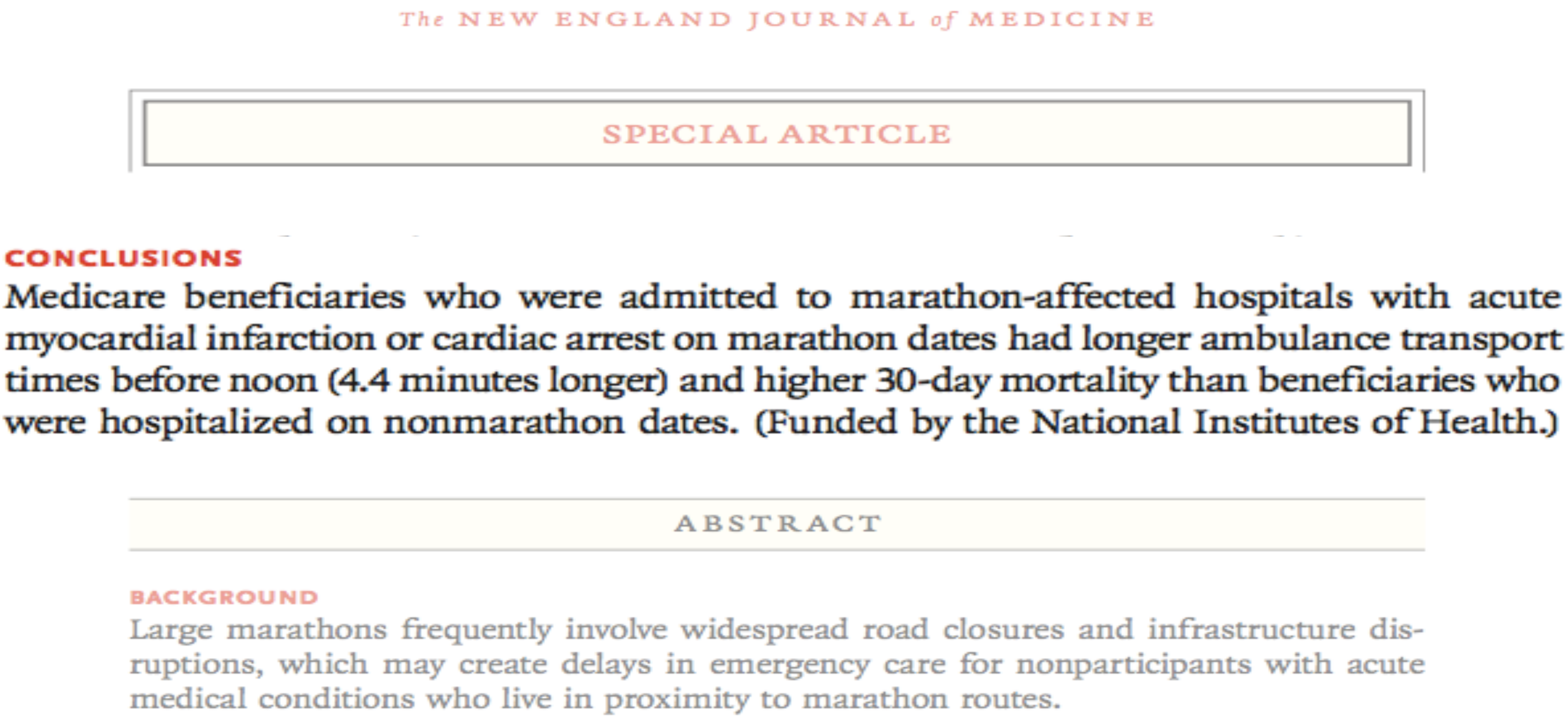
Delays in Emergency Care and Mortality during Major U.S. Marathons

Anupam B. Jena, M.D., Ph.D., N. Clay Mann, Ph.D., Leia N. Wedlund, and Andrew Olenski, B.S.

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.



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.

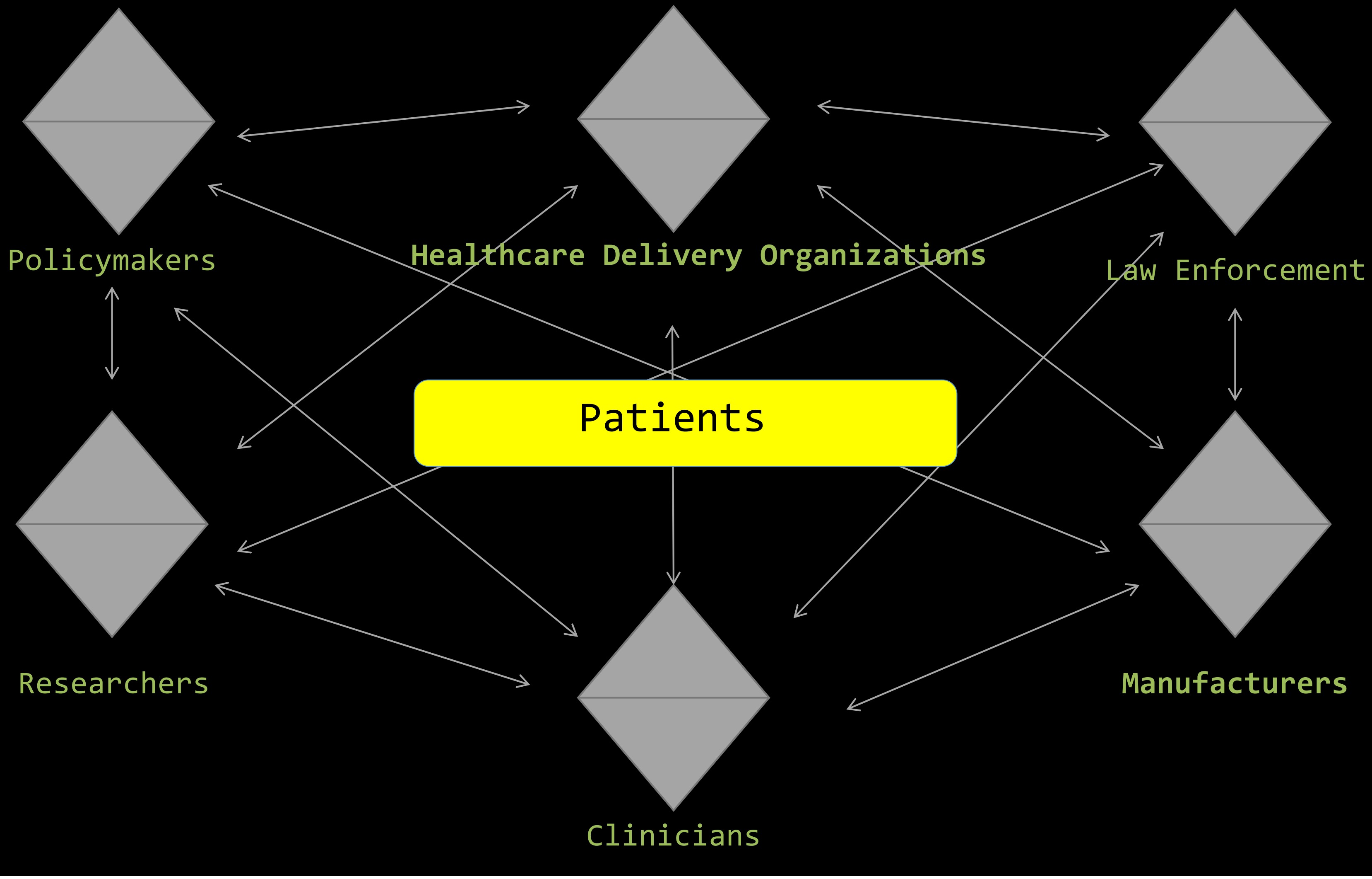
C

cybermedsummit.com

CYBERMED SUMMIT

Phoenix, 8-9 June 2017

Stakeholders



Policymakers

Healthcare Delivery Organizations

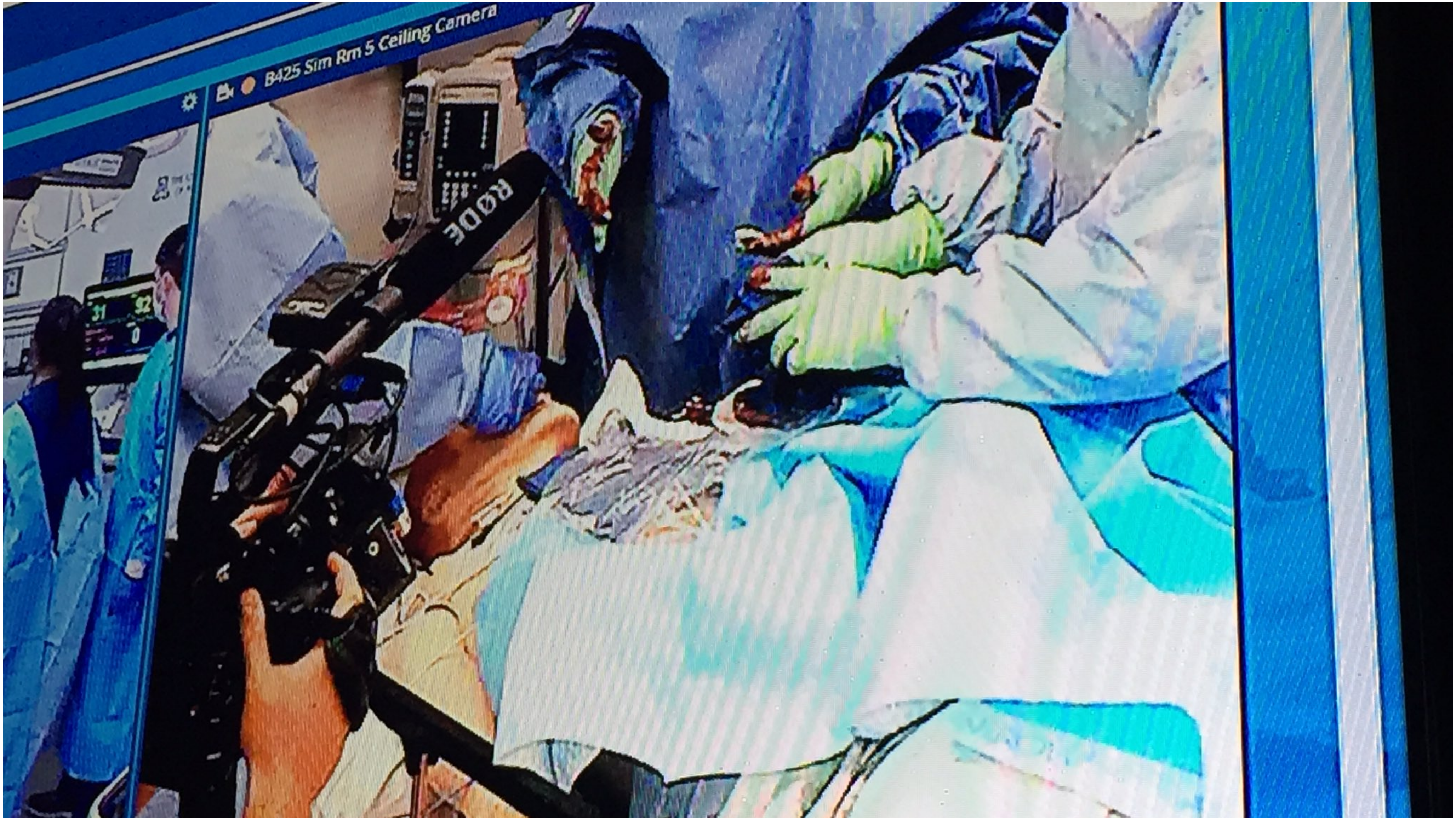
Law Enforcement

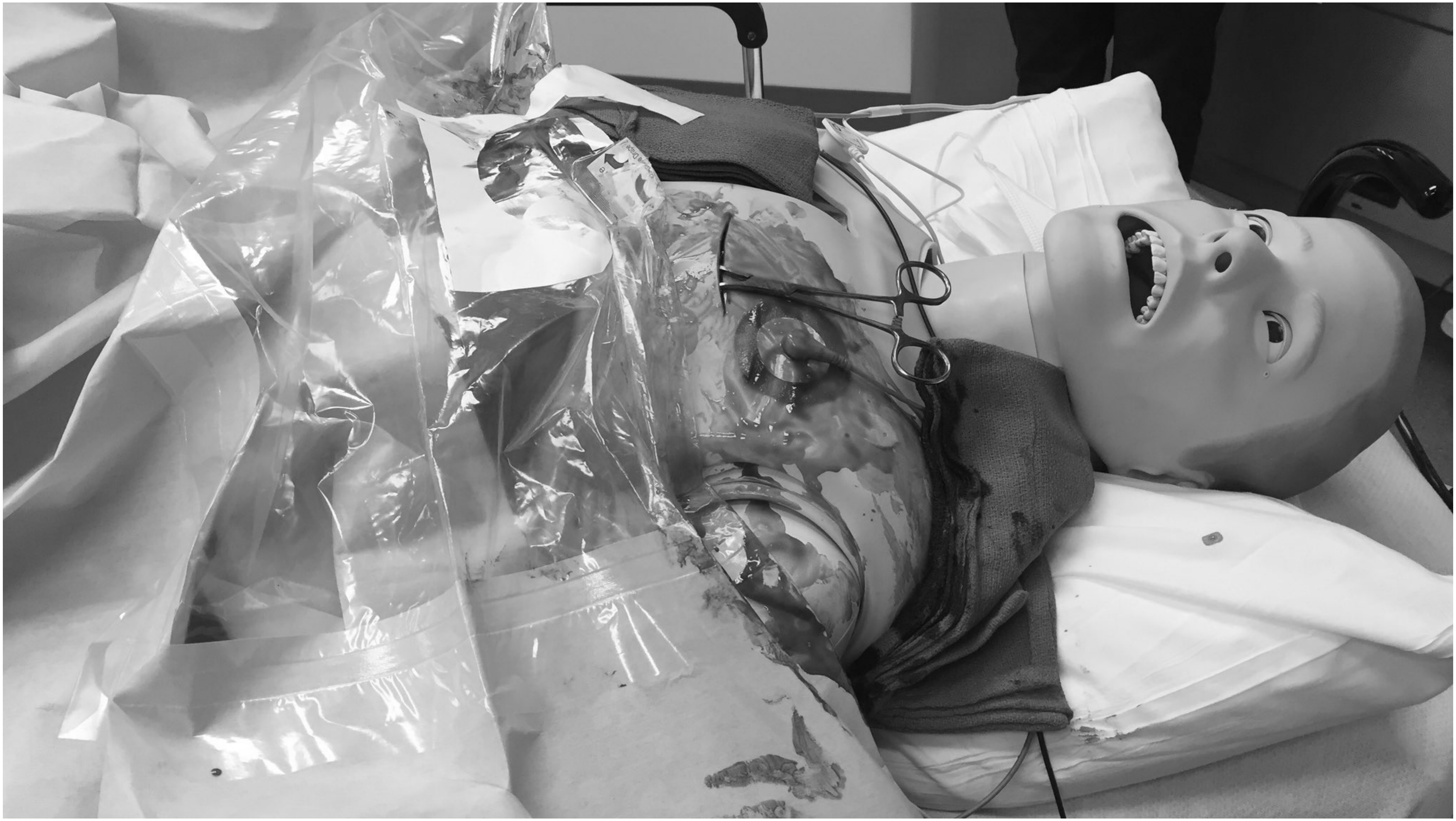
Patients

Researchers

Manufacturers

Clinicians


B425 Sim Rm 5 Ceiling Camera
RØDE
31
92
0



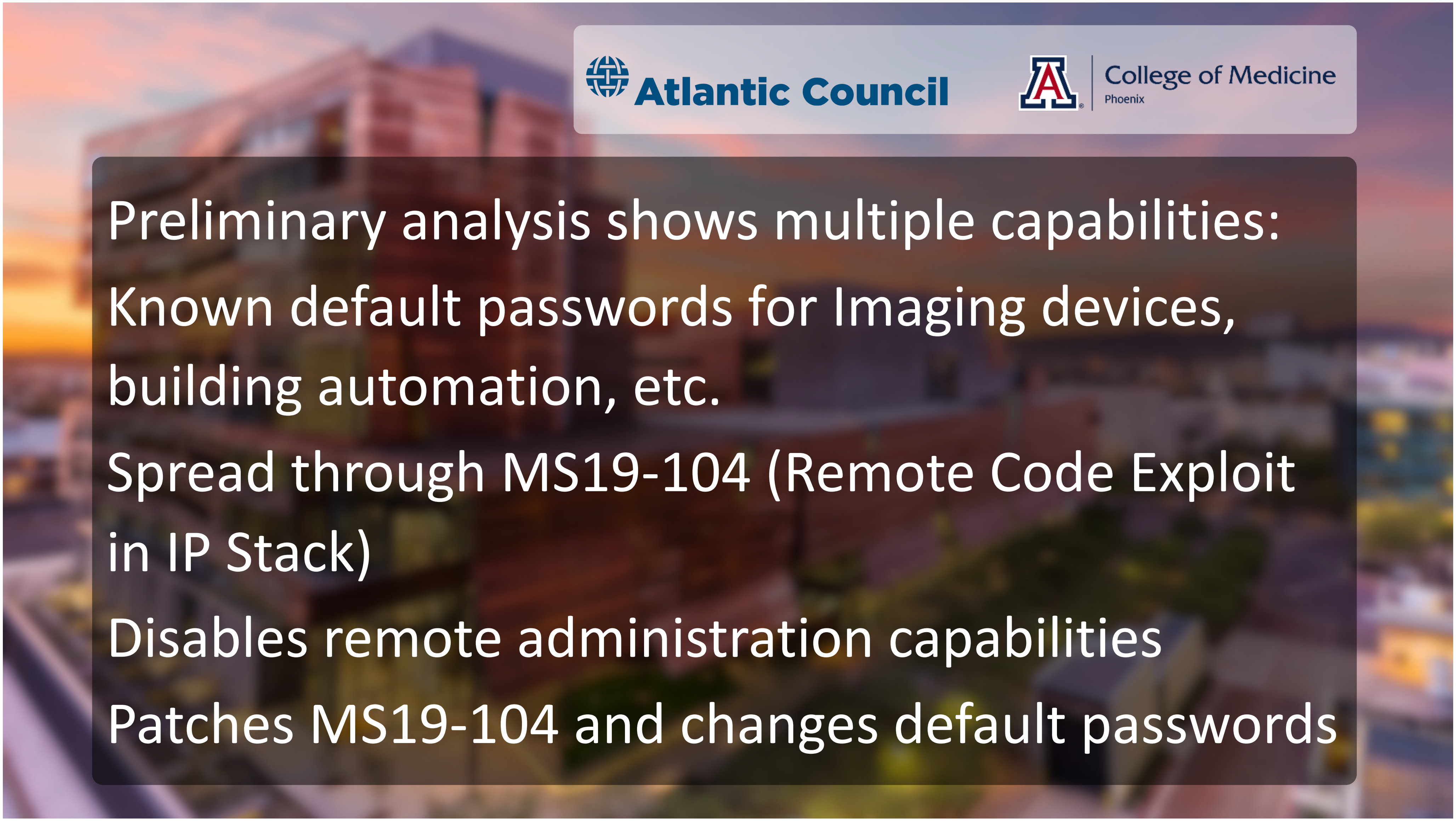
abc NIGHTLINE
A

Atlantic Council CYBER 9/12

Atlantic Council

College of Medicine
Phoenix

A cyber healthcare crisis is unfolding in Phoenix, with severe implications on patient care, industry, government, and citizens' trust extending far beyond any single hospital's borders. How do government entities, the private sector, and others respond to this escalating situation?



Atlantic Council

College of Medicine
Phoenix

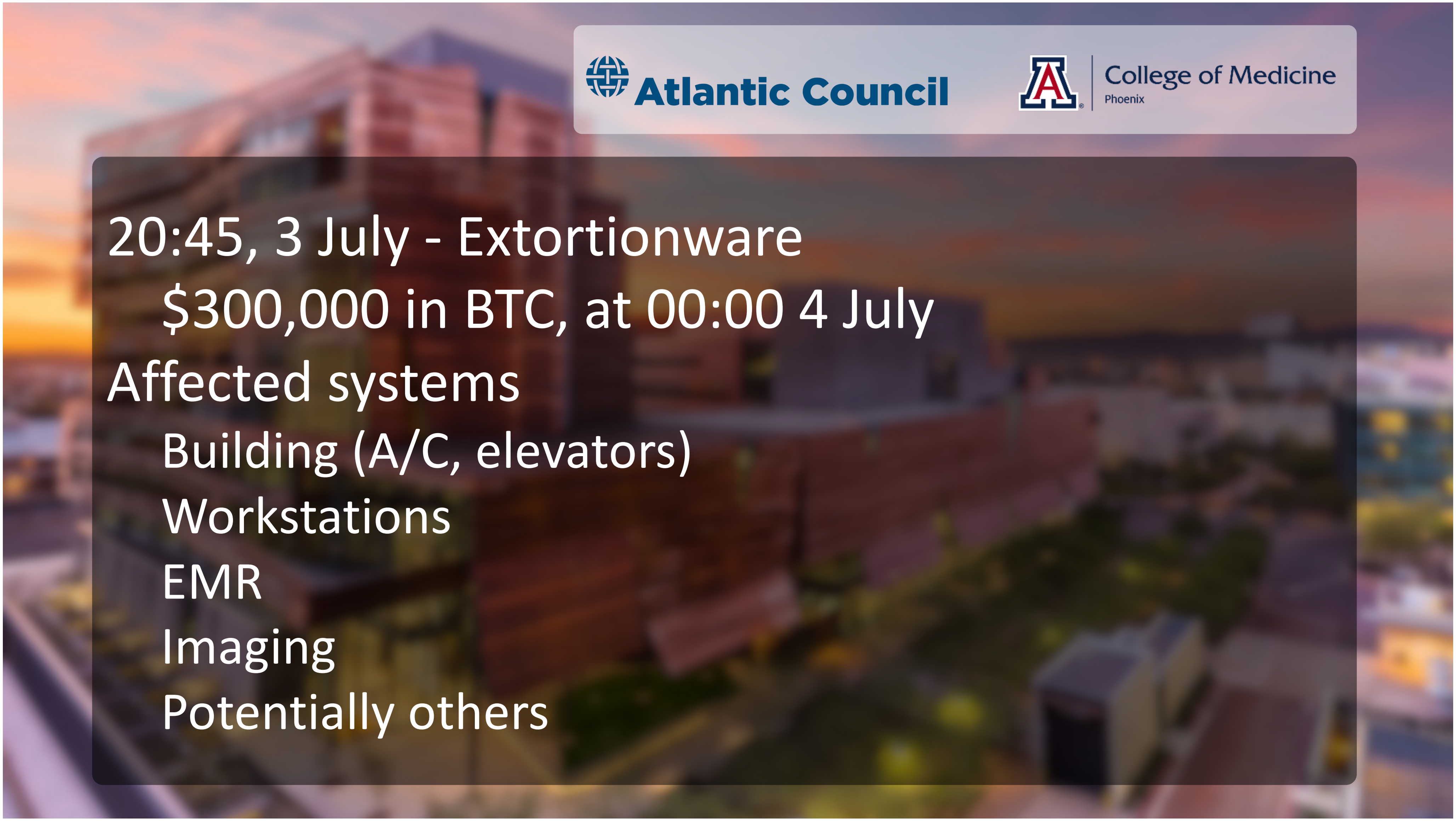
Preliminary analysis shows multiple capabilities:

Known default passwords for Imaging devices, building automation, etc.

Spread through MS19-104 (Remote Code Exploit in IP Stack)

Disables remote administration capabilities

Patches MS19-104 and changes default passwords

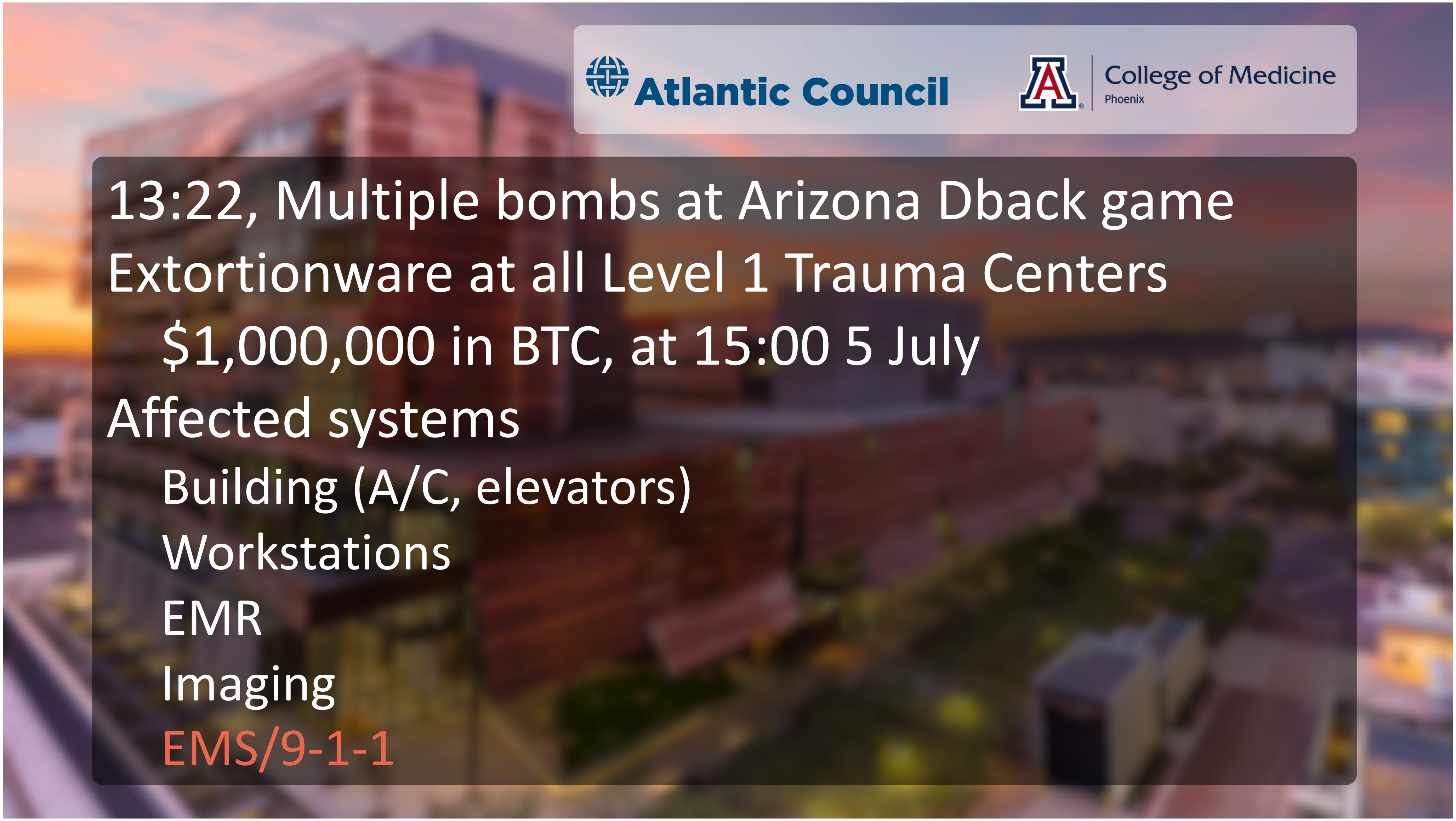


Atlantic Council

College of Medicine
Phoenix

20:45, 3 July - Extortionware
- $300,000 in BTC, at 00:00 4 July

Affected systems
- Building (A/C, elevators)
- Workstations
- EMR
- Imaging
- Potentially others



13:22, Multiple bombs at Arizona Dback game

Extortionware at all Level 1 Trauma Centers

- $1,000,000 in BTC, at 15:00 5 July

Affected systems

- Building (A/C, elevators)
- Workstations
- EMR
- Imaging
- EMS/9-1-1

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

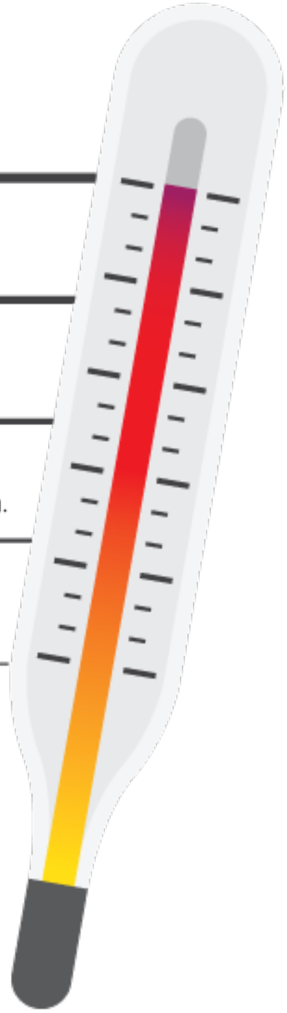
Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

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



*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**.*

Uncomfortable Truths Require Uncomfortable Response

Safer | Sooner | Together

@joshcorman

@IamTheCavalry

I am The Cavalry