virus BULLETIN

I AM THE CAVALRY

http://iamthecavalry.org

@iamthecavalry

SHOULDN'T YOU BE ALSO?

CLAUS CRAMON HOUMANN

Infosec Community Manager @ Peerlyst

(A start-up Infosec community/Social platform that wants to turn the tables on cyber security)

Infosec Consultant

The Analogies contributor

Twitter: @claushoumann 

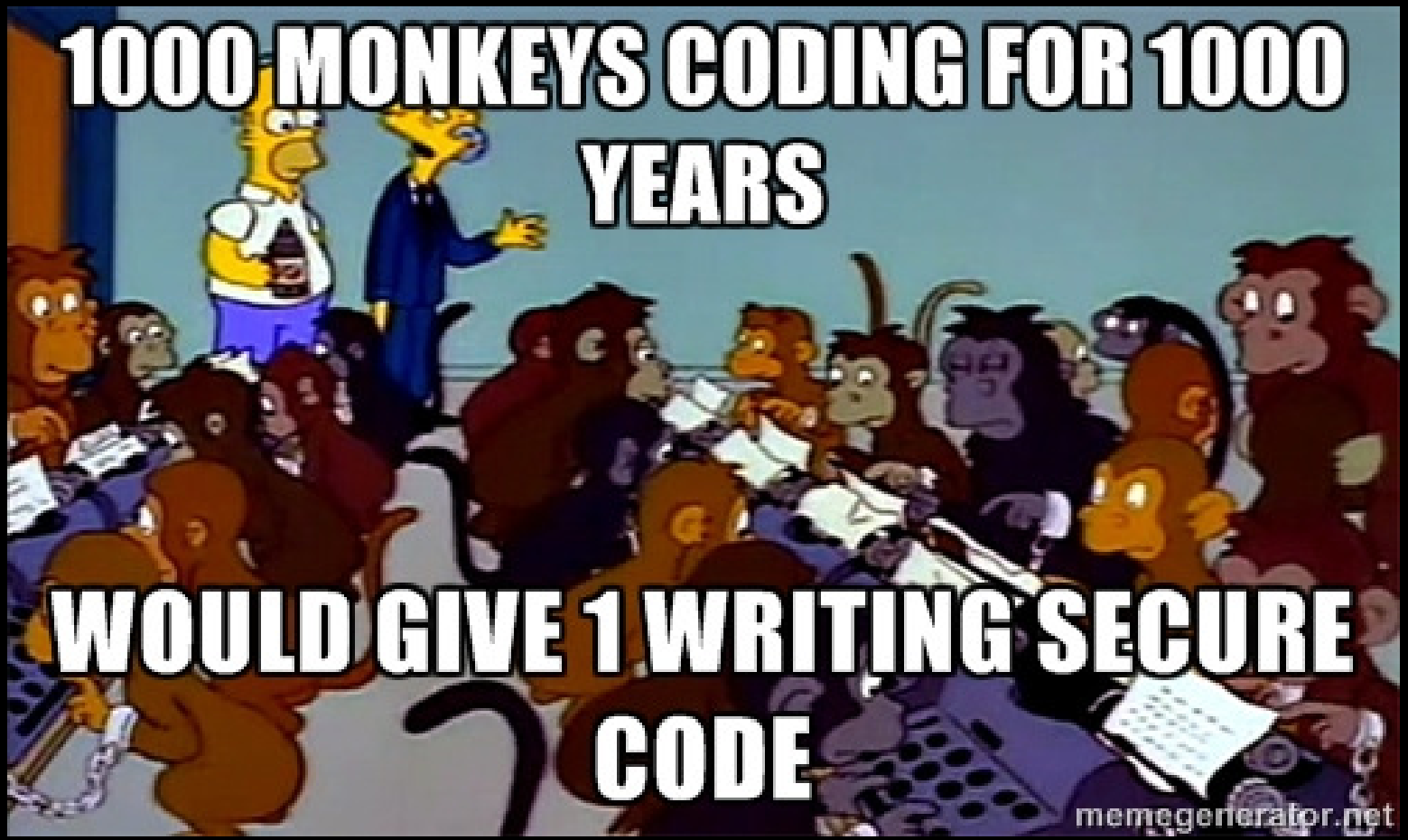
IDEA

"Our dependence on technology is growing faster than our ability to secure it"

IDEA

"Our society has evolved faster than our laws"

IDEA



But why wait.....

WHERE DO WE SEE CONNECTIVITY NOW?

In Our Bodies

In Our Homes

In Our Cars

In Our Infrastructure

HEARTBLEED + (UNPATCHABLE) INTERNET OF THINGS == ___ ?

In Our Bodies

In Our Homes

In Our Cars

In Our Infrastructure

SAY BABY MONITORS AGAIN?

CVE-2015-2886	Remote	R7-2015-11.1	Predictable Information Leak	iBaby M6
CVE-2015-2887	Local Net, Device	R7-2015-11.2	Backdoor Credentials	iBaby M3S
CVE-2015-2882	Local Net, Device	R7-2015-12.1	Backdoor Credentials	Philips In.Sight B120/37
CVE-2015-2883	Remote	R7-2015-12.2	Reflective, Stored XSS	Philips In.Sight B120/37
CVE-2015-2884	Remote	R7-2015-12.3	Direct Browsing	Philips In.Sight B120/37
CVE-2015-2888	Remote	R7-2015-13.1	Authentication Bypass	Summer Baby Zoom Wifi Monitor & Internet Viewing System
CVE-2015-2889	Remote	R7-2015-13.2	Privilege Escalation	Summer Baby Zoom Wifi Monitor & Internet Viewing System
CVE-2015-2885	Local Net, Device	R7-2015-14	Backdoor Credentials	Lens Peek-a-View
CVE-2015-2881	Local Net	R7-2015-15	Backdoor Credentials	Gynoii
CVE-2015-2880	Device	R7-2015-16	Backdoor Credentials	TRENDnet WiFi Baby Cam TV-IP743SIC

Table 2, Newly Identified Vulnerabilities

Source: Rapid7 research/Mark Stanislav: Baby monitors
https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-

THEN

BUT ALSO

Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication

Date Issued: July 31, 2015

Audience: Health care facilities using the Hospira Symbiq Infusion System

Device: Symbiq Infusion System, Version 3.13 and prior versions

The Hospira Symbiq Infusion System is a computerized pump designed for the continuous delivery of general infusion therapy for a broad patient population.

It is primarily used in hospitals, or other acute and non-acute health care facilities, such as nursing homes and outpatient care centers. This infusion system can communicate with a Hospital Information System (HIS) via a wired or wireless connection over facility network infrastructures.

Purpose:

The FDA is alerting users of the Hospira Symbiq Infusion System to cybersecurity vulnerabilities with this infusion pump. We strongly encourage that health care facilities transition to alternative infusion systems, and discontinue use of these pumps.

ALL SYSTEMS FAIL*

* Yes; all

Past versus Future

Bolt-On Vs Built-In

Ouch!

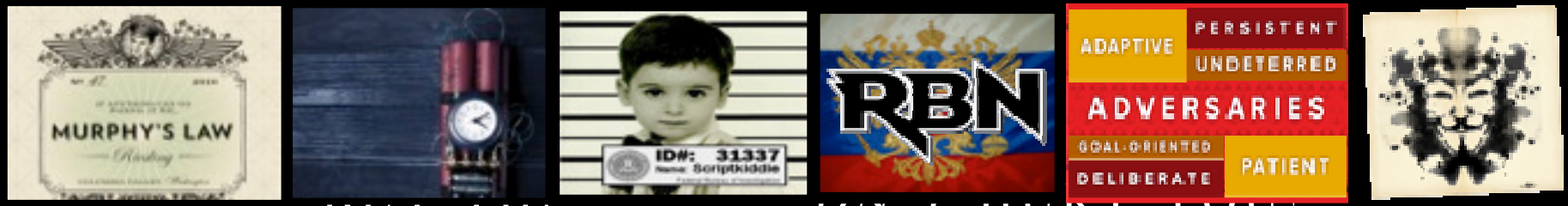
EVERYTHING CONNECTED IS VULNERABLE AND CAN/WILL BE HACKED

Cars have computers

Computers have security issues

Security issues in cars are safety issues

Safety issues can cost or imperil lives

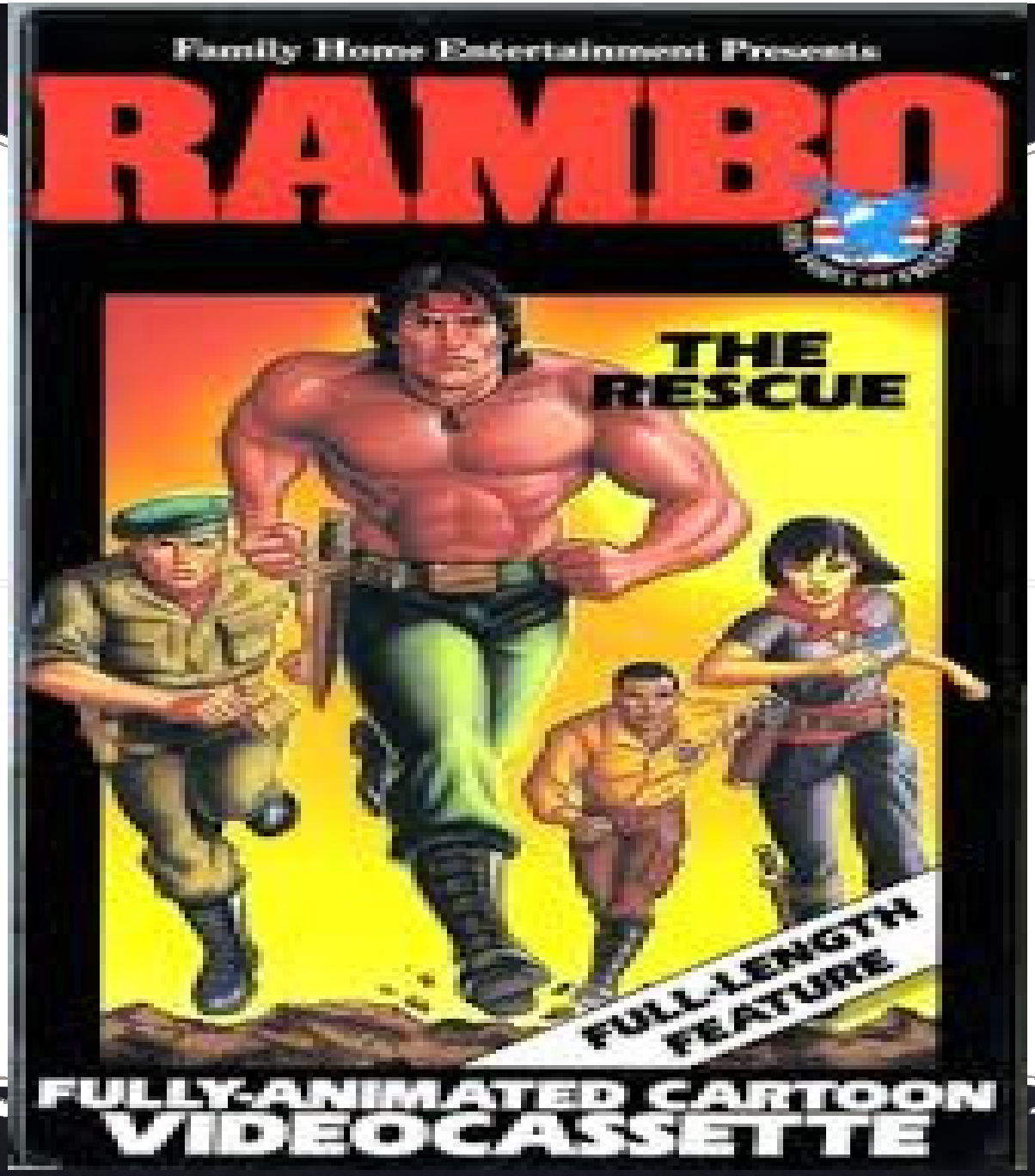


BUT THEY WOULDN'T HURT YOU?

"I'd prefer that they *couldn't* hurt me..."

Chapter 2

SOMEONE WILL FIX IT FOR US


Family Home Entertainment Presents
RAMBO
THE RESCUE
FULL-LENGTH FEATURE
FULLY ANIMATED CARTOON
VIDEOCASSETTE

Chapter 3

OR NOT.....

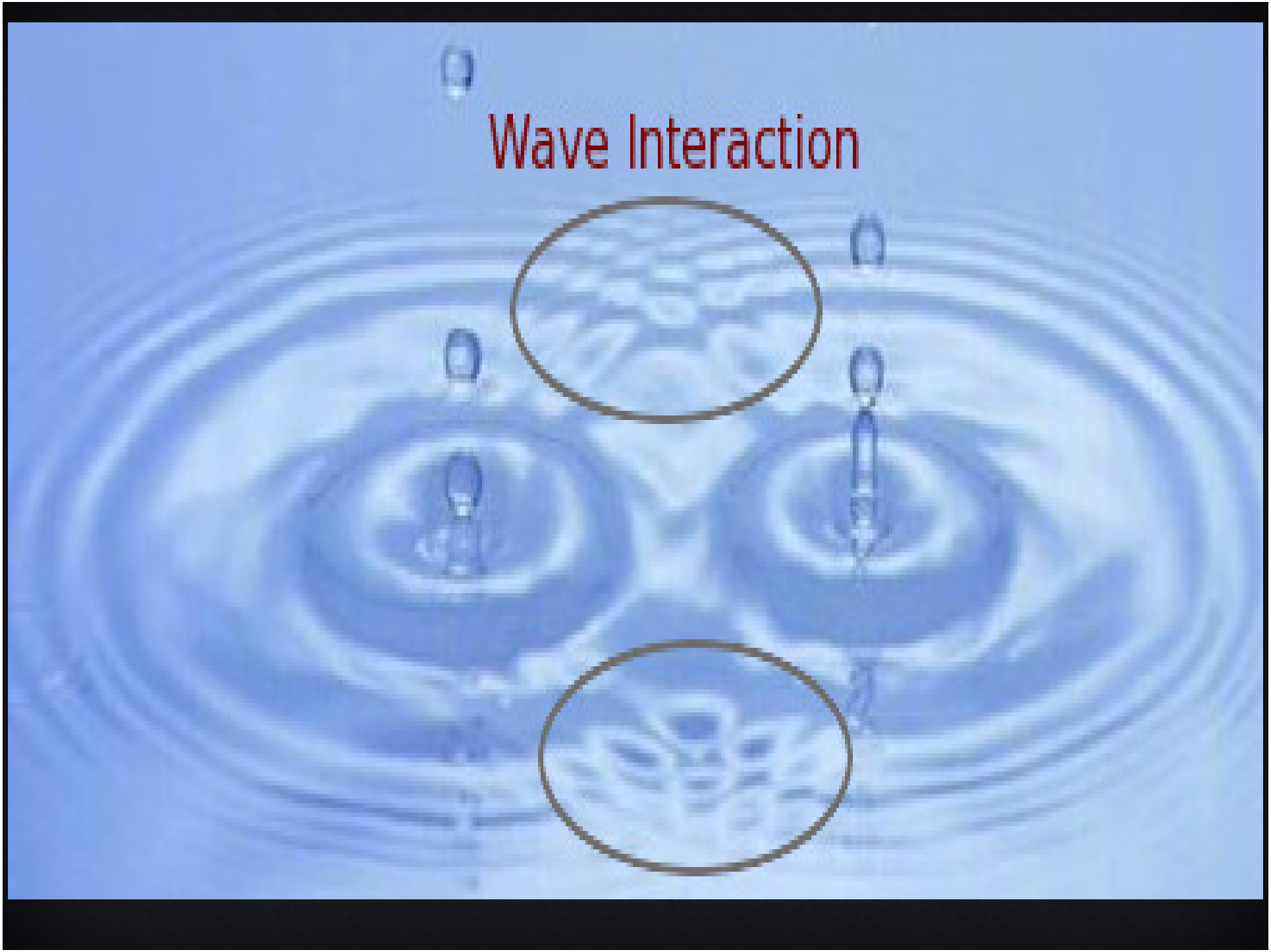
Let's create ripples

And by ripples I mean

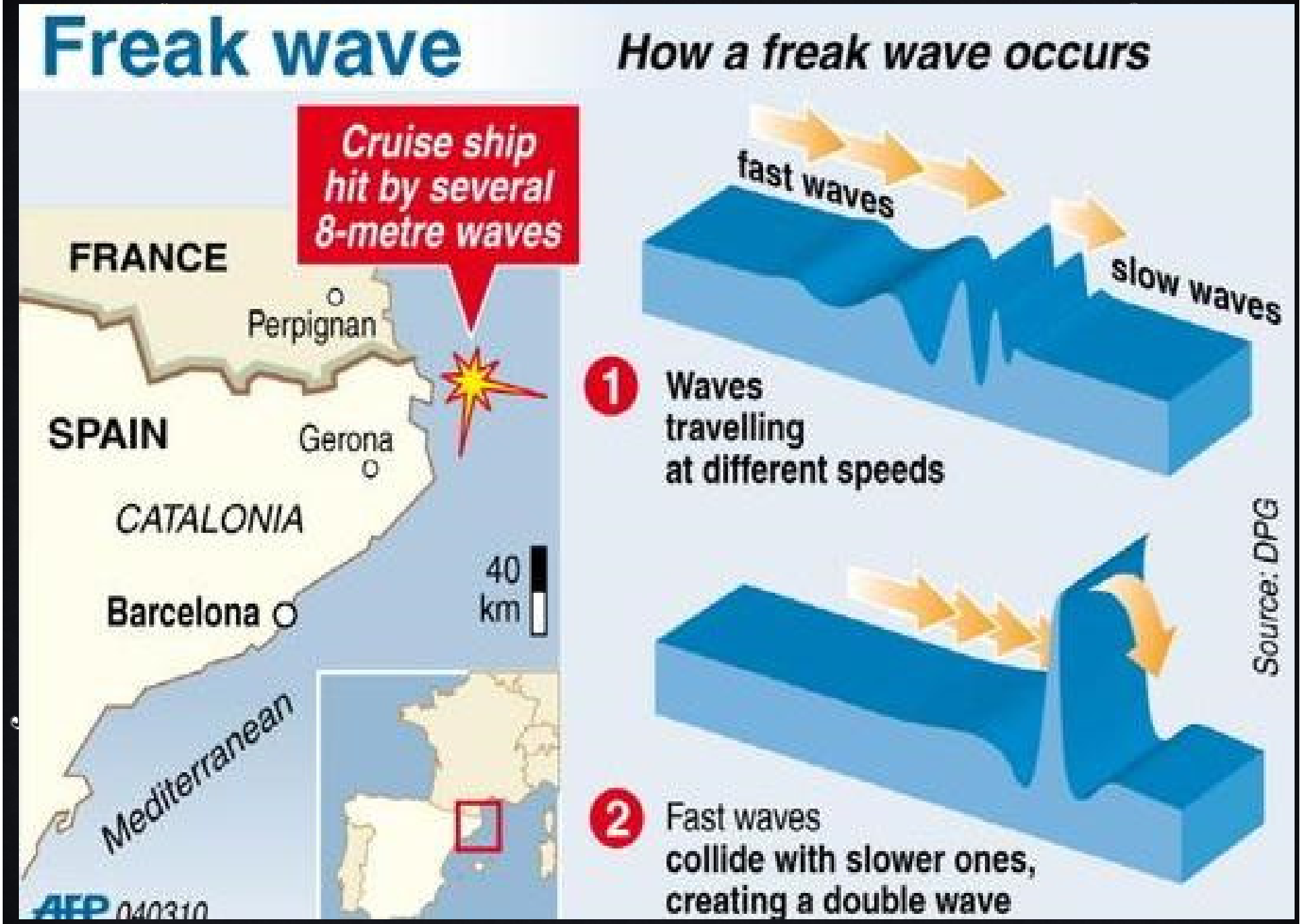
A DO-OCRACY OF DO'ERS.

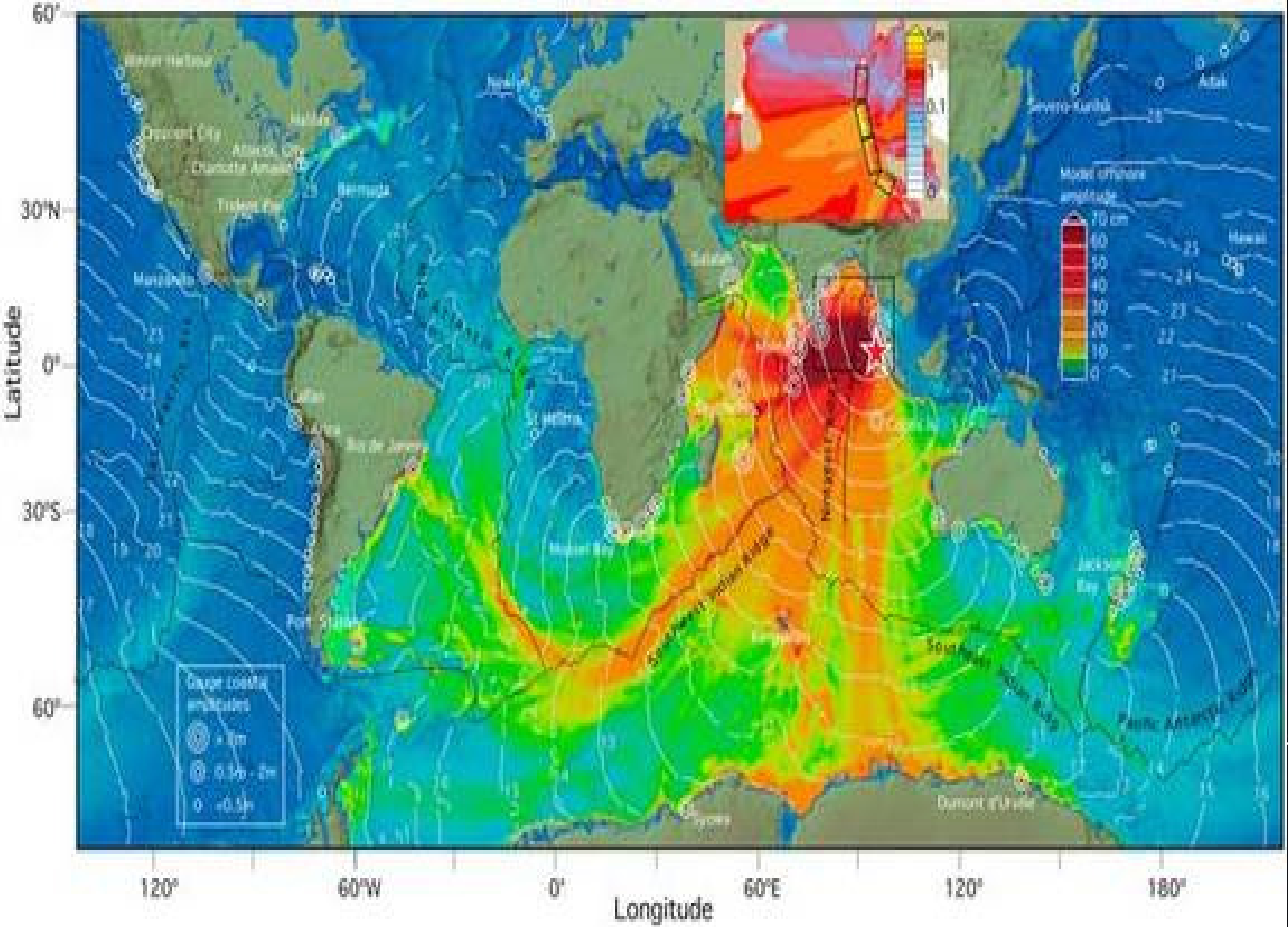
WHERE DOING STARTS WITH

EMPATHY


Wave Interaction

Freak wave


Cruise ship hit by several 8-metre waves
FRANCE
Perpignan
SPAIN
Gerona
CATALONIA
Barcelona
Mediterranean
40 km
AFP 040310
How a freak wave occurs
fast waves
slow waves
1 Waves travelling at different speeds
2 Fast waves collide with slower ones, creating a double wave
Source: DPG


Latitude
Longitude
60°
30°N
0°
30°S
60°
120°
60°W
0°
60°E
120°
180°
Model offshore amplitude
70 cm
60
50
40
30
20
10
0
Gauge coastal amplitudes
Crescent City
Bermuda
St Helena
Rio de Janeiro
Port Stanley
Southwest Indian Ridge
Pacific Antarctic Ridge
Dumont d'Urville
Hawaii
Adak
Severo-Kurilsk
Jackson Bay
Salalah
Manzanillo
Halifax
Atlantic City
Trident Pier

The Point?

NEVER DOUBT THAT A SMALL GROUP OF THOUGHTFUL, COMMITTED CITIZENS CAN CHANGE THE WORLD; IT'S THE ONLY THING THAT EVER HAS.

- MARGARET MEAD
(AN AMERICAN CULTURAL ANTHROPOLOGIST)

I Am The Cavalry

The Cavalry isn't coming... It falls to us

Problem Statement

Our society is adopting connected technology *faster than we are able to secure it*.

Mission Statement

To ensure connected technologies with the potential to impact public safety and human life are *worthy of our trust*.

Medical

Automotive

Connected Home

Public Infrastructure

Why Trust, public safety, human life
How Education, outreach, research
Who Infosec research community
Who Global, grass roots initiative
What Long-term vision for cyber safety

Collecting existing research, researchers, and resources
Connecting researchers with each other, industry, media, policy, and legal
Collaborating across a broad range of backgrounds, interests, and skillsets
Catalyzing positive action sooner than it would have happened on its own

5-Star Framework

Addressing Automotive Cyber Systems

5-Star Capabilities

- ★ **Safety by Design** – Anticipate failure and plan mitigation
- ★ **Third-Party Collaboration** – Engage willing allies
- ★ **Evidence Capture** – Observe and learn from failure
- ★ **Security Updates** – Respond quickly to issues discovered
- ★ **Segmentation & Isolation** – Prevent cascading failure

Connections and Ongoing Collaborations

Security Researchers

Automotive Engineers

Policy Makers

Insurance Analysts

Accident Investigators

Standards Organizations

https://www.iamthecavalry.org/auto/5star/

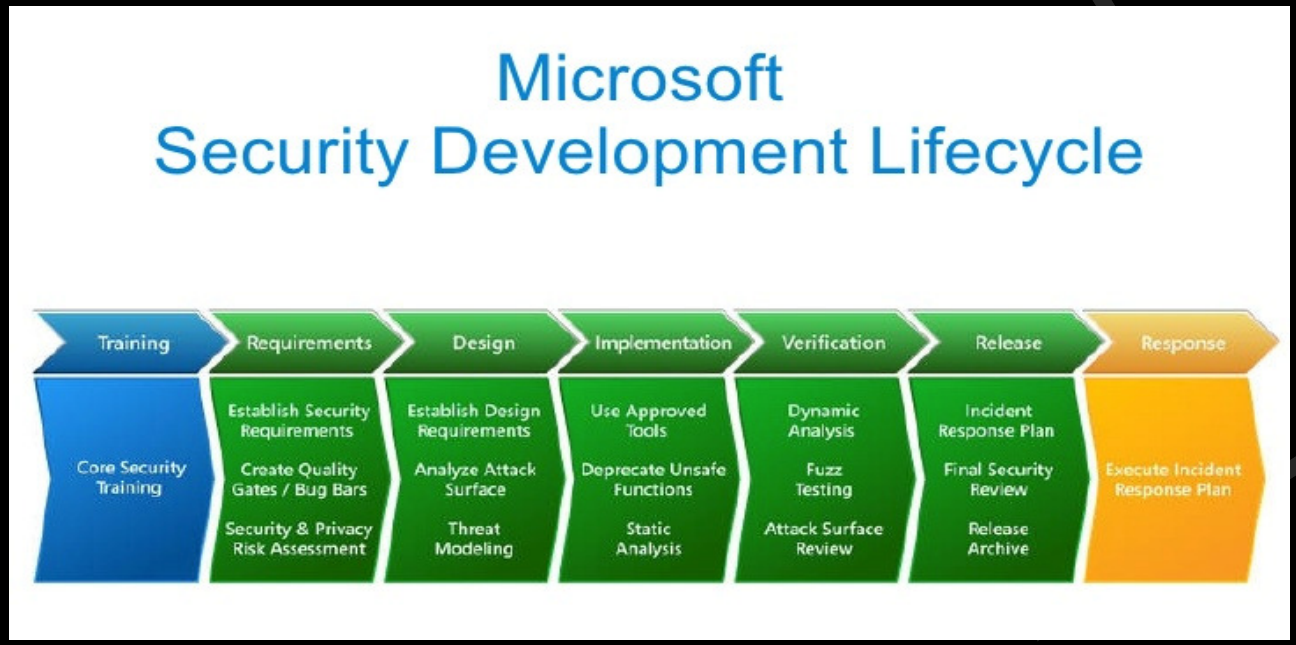
5-Star Cyber Safety

Formal Capacities	Plain Speak
1. **Safety By Design**	1. Avoid Failure
2. **Third Party Collaboration**	2. Engage Allies To Avoid Failure
3. **Evidence Capture**	3. Learn From Failure
4. **Security Updates**	4. Respond to Failure
5. **Segmentation and Isolation**	5. Isolate Failure

1) Safety By Design

Do you have a published attestation of your Secure Software Development Lifecycle, summarizing your design, development, and adversarial resilience testing programs for your products and your supply chain?

1) Safety By Design



2) Third Party Collaboration

Do you have a published Coordinated Disclosure policy inviting the assistance of third-party researchers acting in good faith?

2) Third Party Collaboration

Vs

3) Evidence Capture

Do your vehicle systems provide tamper evident, forensically-sound logging and evidence capture to facilitate safety investigations?

3) Evidence Capture

4) Security Updates

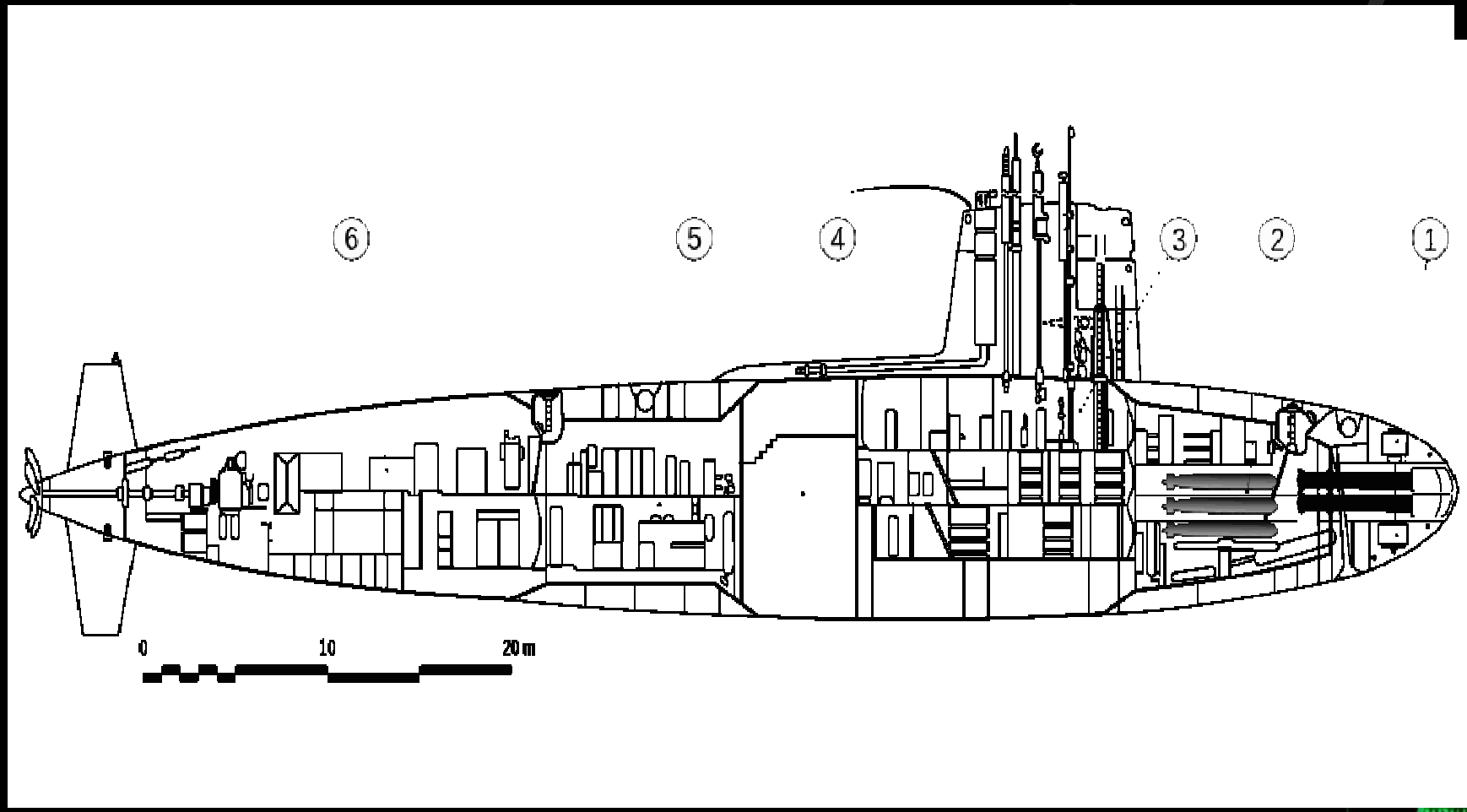
Can your vehicles be securely updated in a prompt and agile manner?

4) Security Updates

5) Segmentation and Isolation

Do you have a published attestation of the physical and logical isolation measures you have implemented to separate critical systems from non-critical systems?

5) Segmentation and Isolation



Highlights from the past year

With FDA as a key partner

- **Atlantic Council workshop and paper[1]**
- **FDA Pre-Market Guidance and Workshop[2]**
- **IEEE Workshop**
- Embraced by healthcare community conferences
- **Atlantic Council Cyber Wednesday[3]**
- Vulnerability Disclosure Policies
- **Vulnerability Disclosure Brainstorming and Education with FDA**
- **Safety Communications BEFORE evidence of harm**

[1]http://www.atlanticcouncil.org/publications/reports/the-healthcare-internet-of-things-rewards-and-risks
[2]http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm
[3]http://www.atlanticcouncil.org/events/webcasts/cyber-risk-wednesday-the-healthcare-internet-of-things-rewards-and-risks

And!

- Dräger on board with I am the Cavalry as first medical device producer working directly in sync with us
- Their Product Security Manager is even directly involved now

5 STARS

5 star ICS

5 star IoT

5 star medical devices

AND MORE IN OTHER AREAS COMING

We try to connect researchers to

1. Lawmakers to inform of meaningful changes to laws to enforce secure by default

2. Vendors/producers to inform of secure ways to build securely by design and of identified vulnerabilities

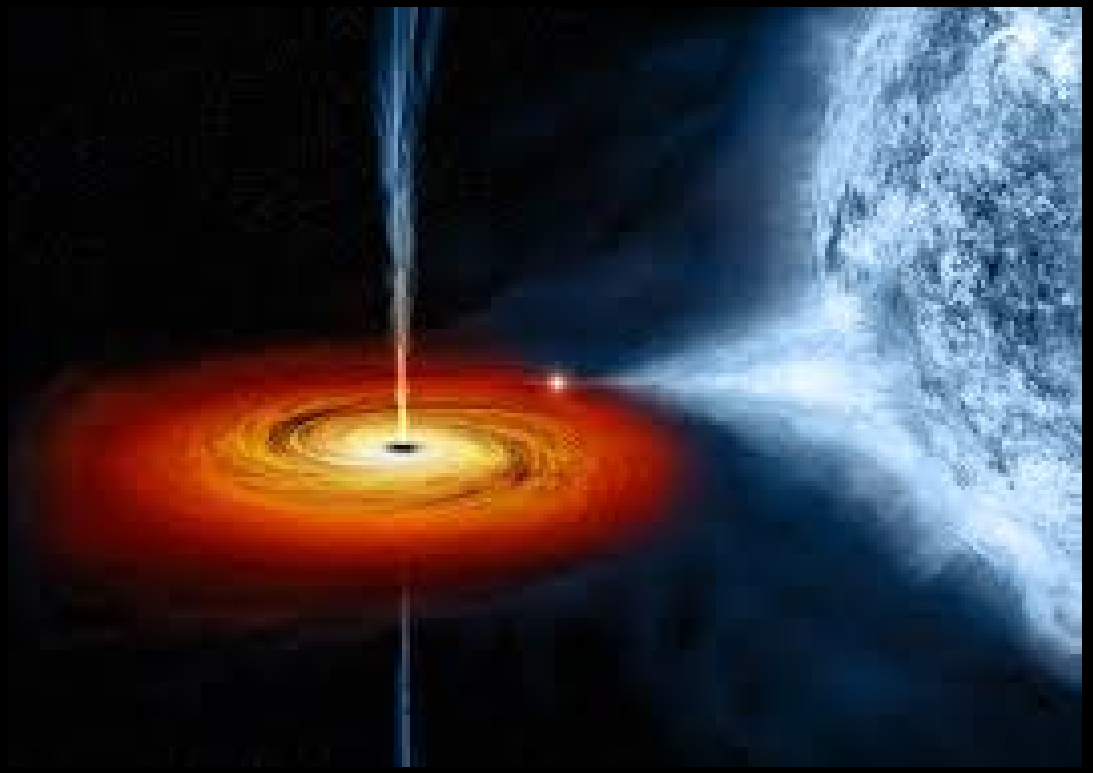
3. Purchasers of devices (example: Pacemakers, car distributors) to explain to them why they need to contractually demand security – if there is demand vendors will supply

AND YES I DID SAY LAWMAKERS

It is WEIRD for you to have to listen to. I agree, but

AND YES I DID SAY LAWMAKERS

It is WEIRD for you to have to listen to. I agree, but



KEY SIGNING CEREMONIES

Secure remote updates – but the backend can be your enemy -> disable whole fleets?

Chapter 5

WHAT YOU CAN DO

CONNECTIONS/CONNECTORS WANTED

Breakers and Builders

Legal and Policy

Citizens, Connectors

Parents/Guardians

Community Leaders/Bloggers/Podcasters/etc.

MOUNT UP AND BE THE CAVALRY

YOU DON'T ACTUALY NEED A HORSE

I am The Cavalry

SAFER.
SOONER.
TOGETHER

http://iamthecavalry.org

@iamthecavalry