Perspectives on Cybersecurity

NASS
National Association of Secretaries of State

2019 Winter Conference
February 2, 2019

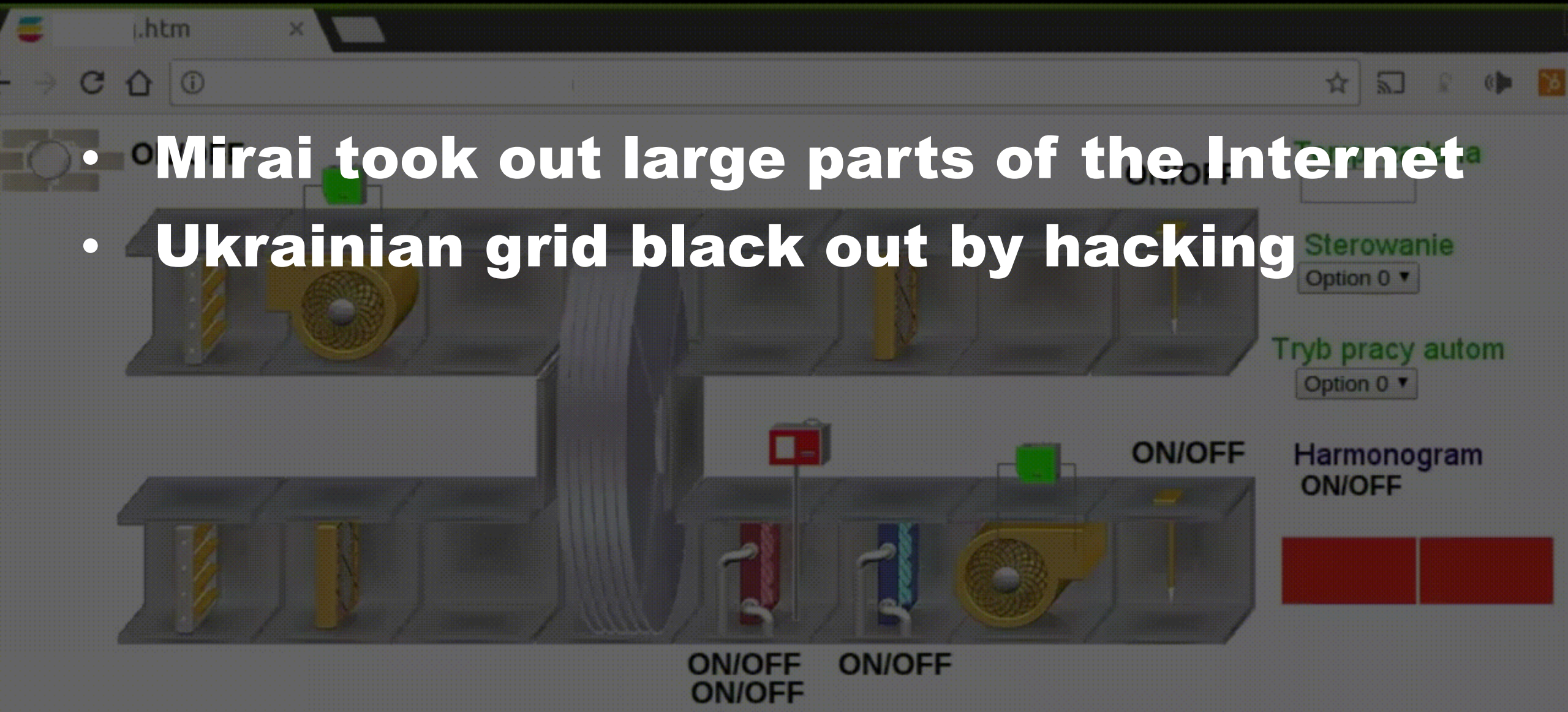
Beau Woods
Cyber Safety Innovation Fellow, Atlantic Council
Leader, I Am The Cavalry (.org)

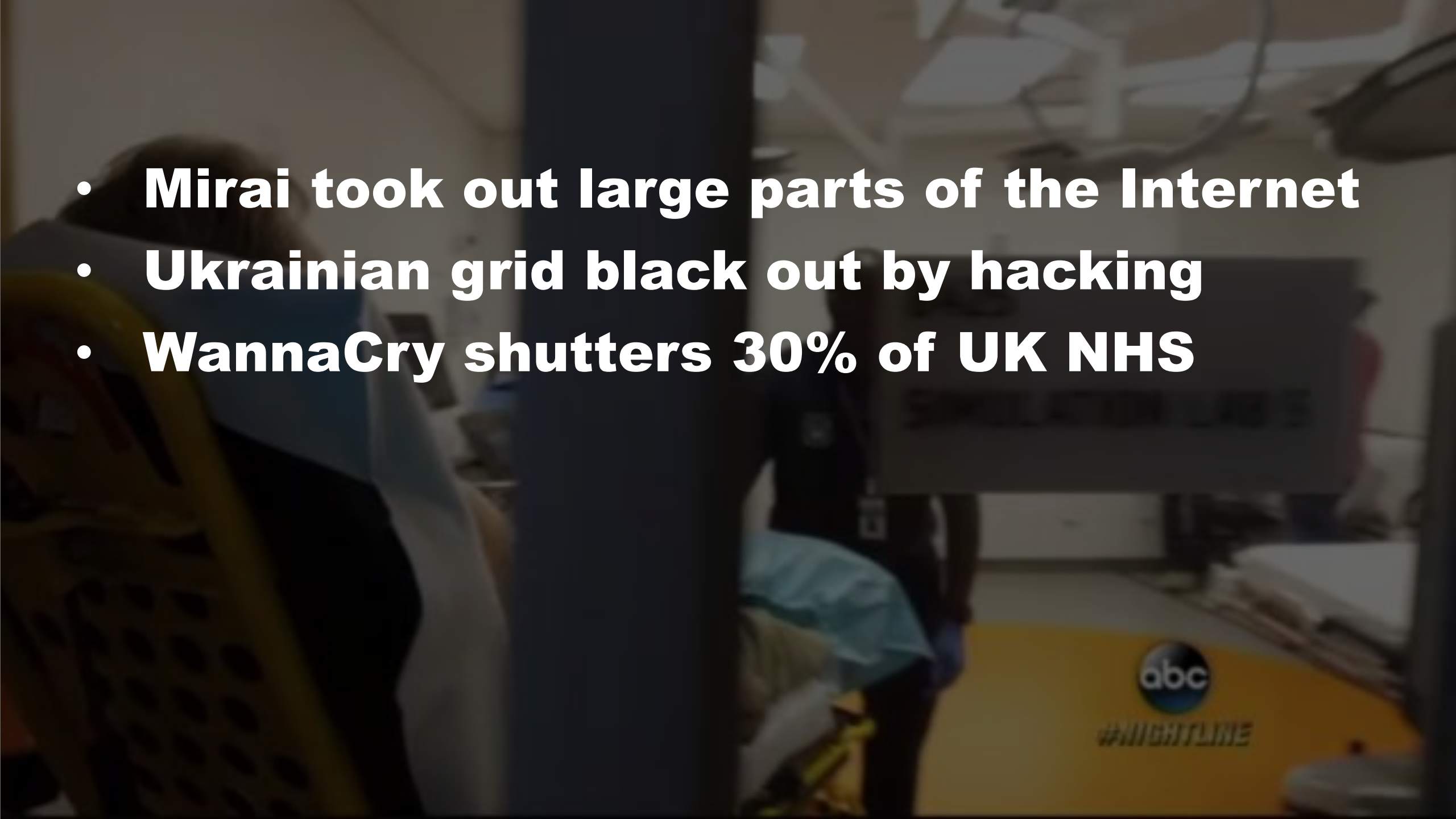
What’s at stake

- **Mirai took out large parts of the Internet**

https://intel.malwaretech.com/pewpew.html

- Mirai took out large parts of the Internet
- Ukrainian grid black out by hacking



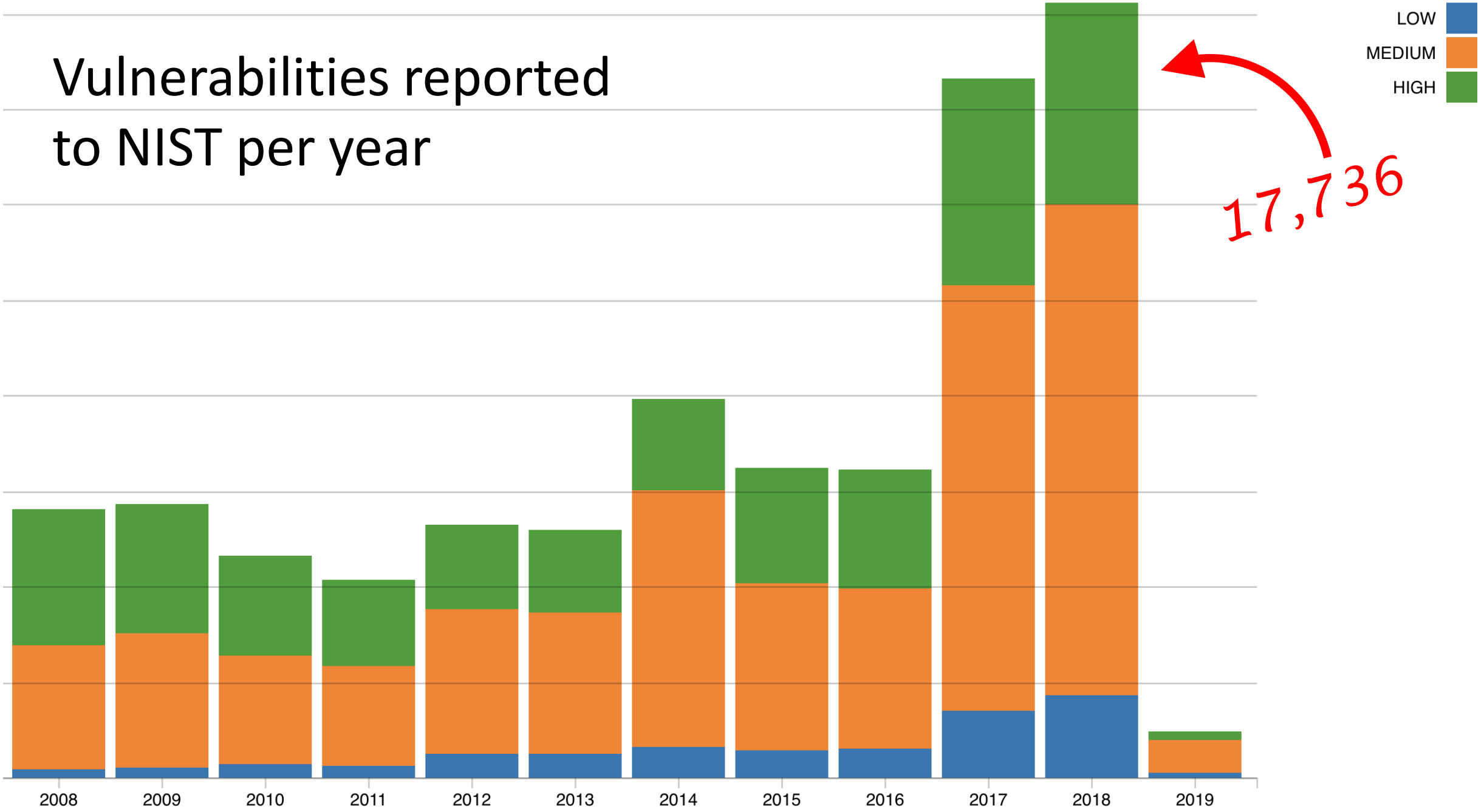


- Mirai took out large parts of the Internet
- Ukrainian grid black out by hacking
- WannaCry shutters 30% of UK NHS

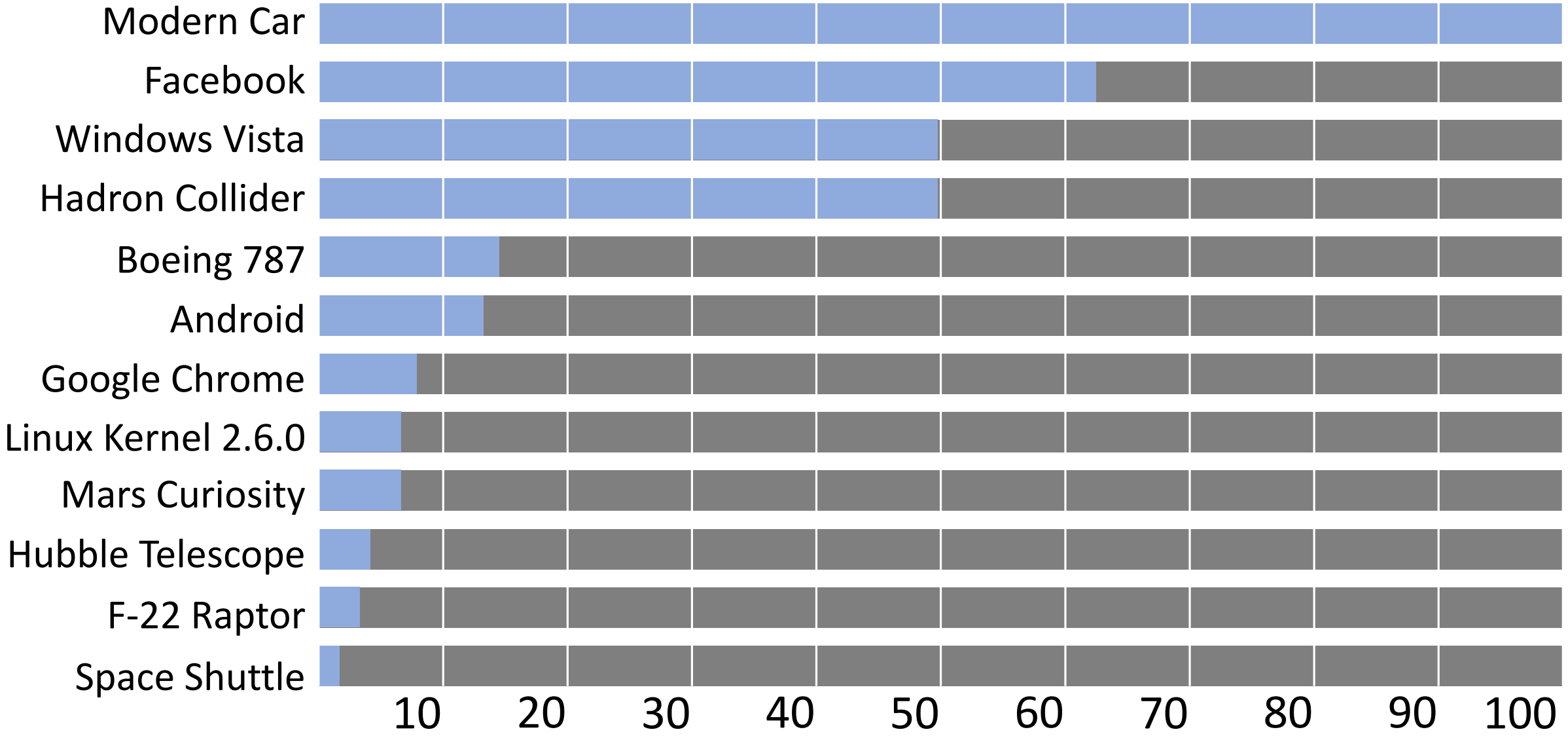
- Mirai took out large parts of the Internet
- Ukrainian grid black out by hacking
- WannaCry shutters 30% of UK NHS
- NotPetya disrupts global logistics & manufacturing, including vaccines

Are you vulnerable?

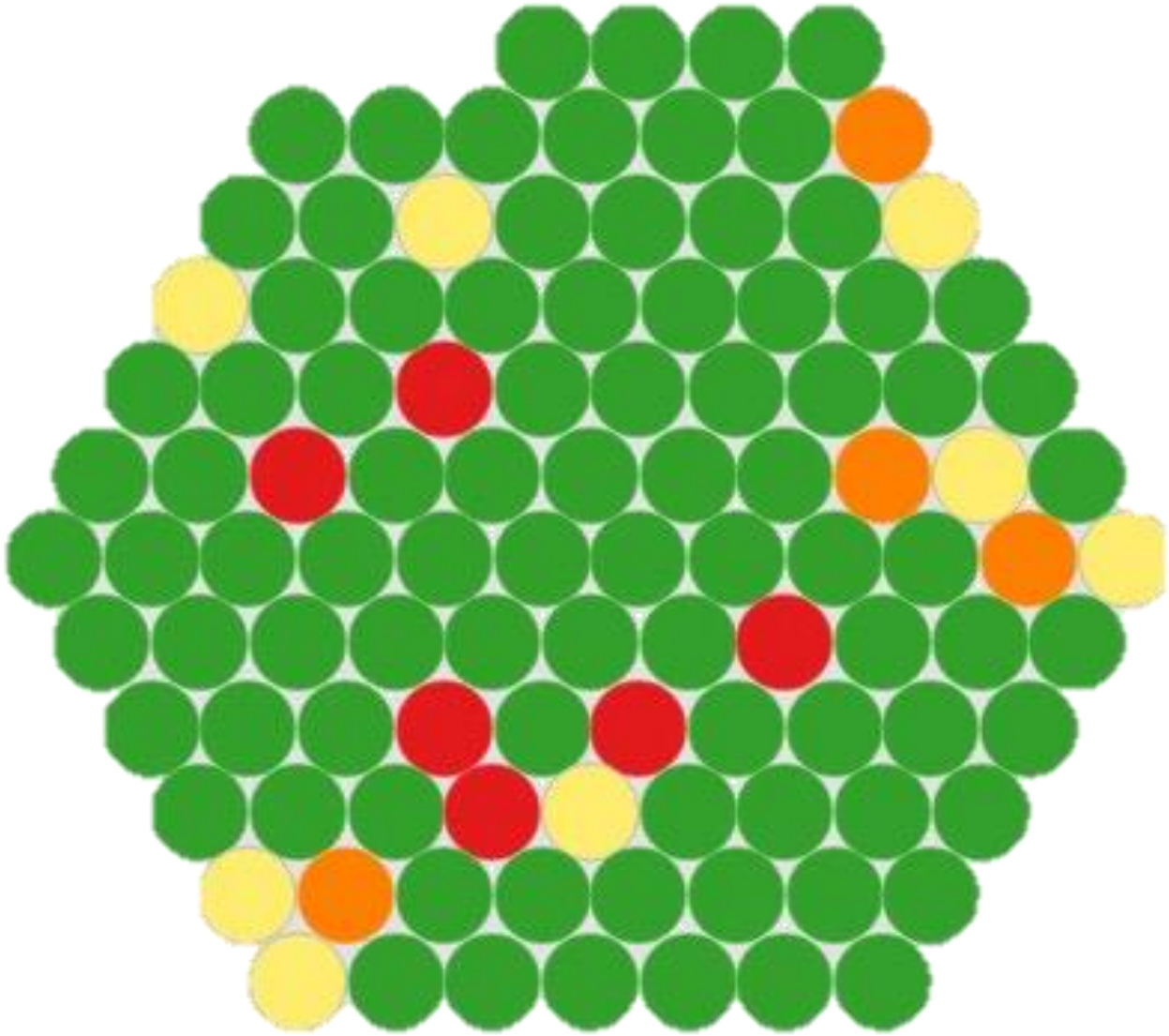
Vulnerabilities reported to NIST per year



Software Complexity

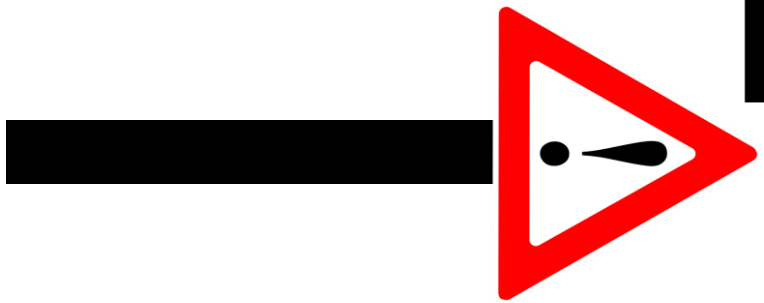


Supply Chain Vulnerabilities

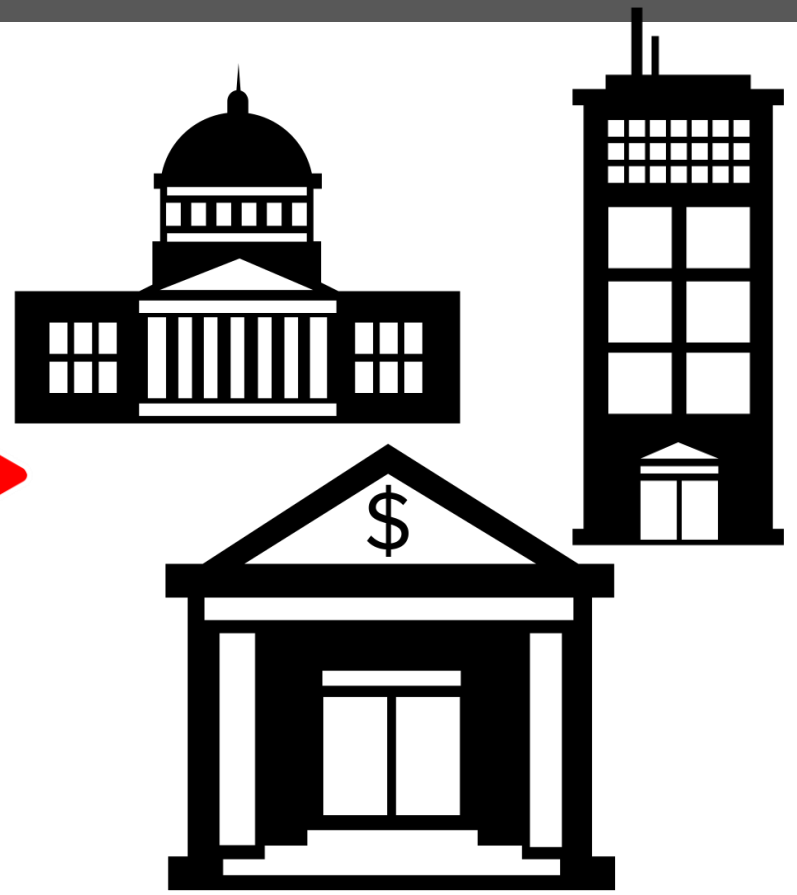


Is this how hacks work?

Highly Skilled Hacker



1337 0-Days



Best Defenses Known/Available

OPM	“Known but Unmitigated Vulnerabilities”
DNC	“Known but Unmitigated Vulnerabilities”
Mirai	“Known but Unmitigated Vulnerabilities”
WannaCry	“Known but Unmitigated Vulnerabilities”
NotPetya	“Known but Unmitigated Vulnerabilities”
Equifax	“Known but Unmitigated Vulnerabilities”


Forecasted Global Cybersecurity Spending, 2015-2019:
$1 Trillion
I Am The Cavalry
@iamthecavalry

ONE HUNDRED PERCENT of

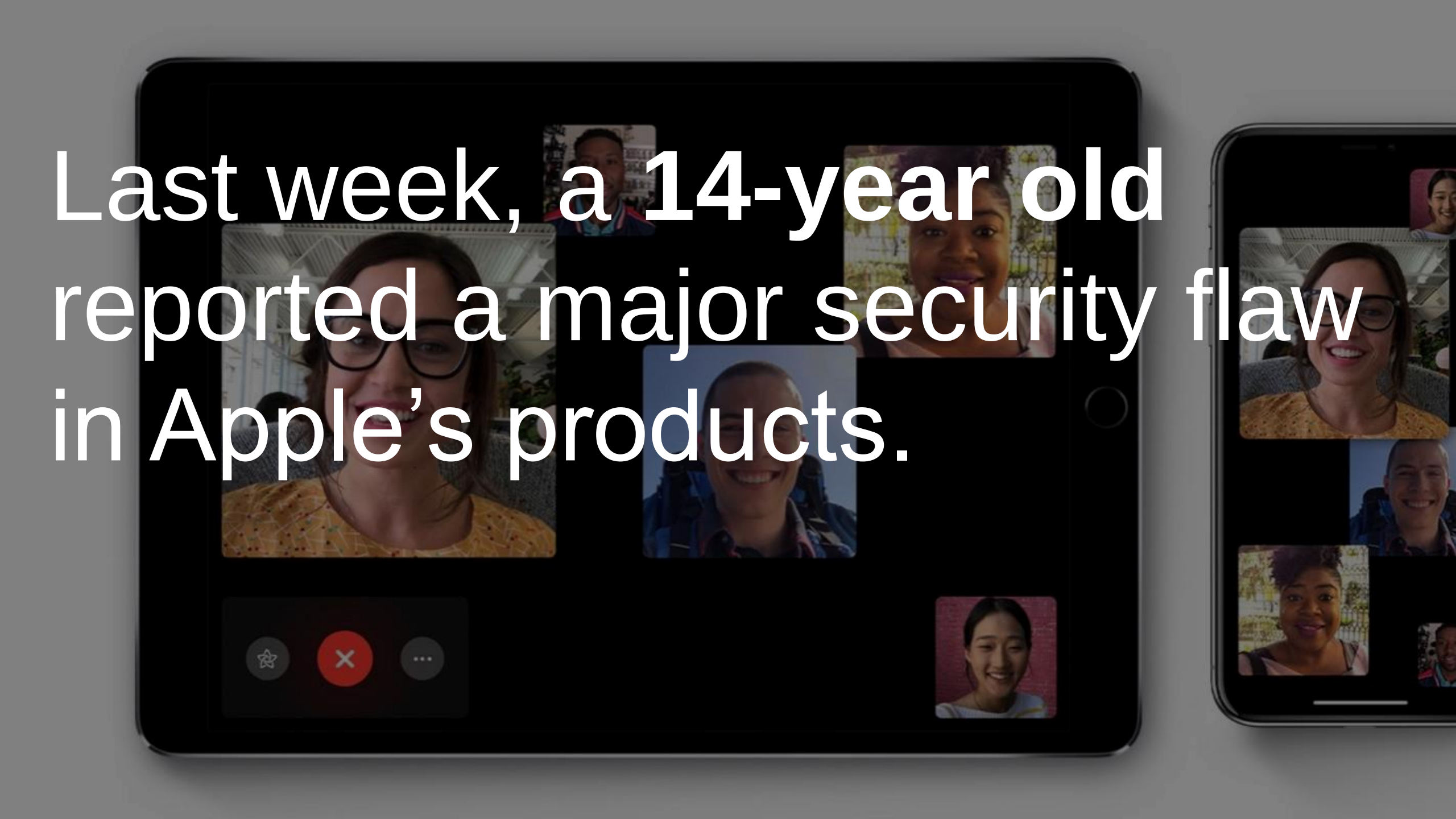
FORTUNE 500

companies will be hacked over the same time period

I Am The Cavalry
@iamthecavalry

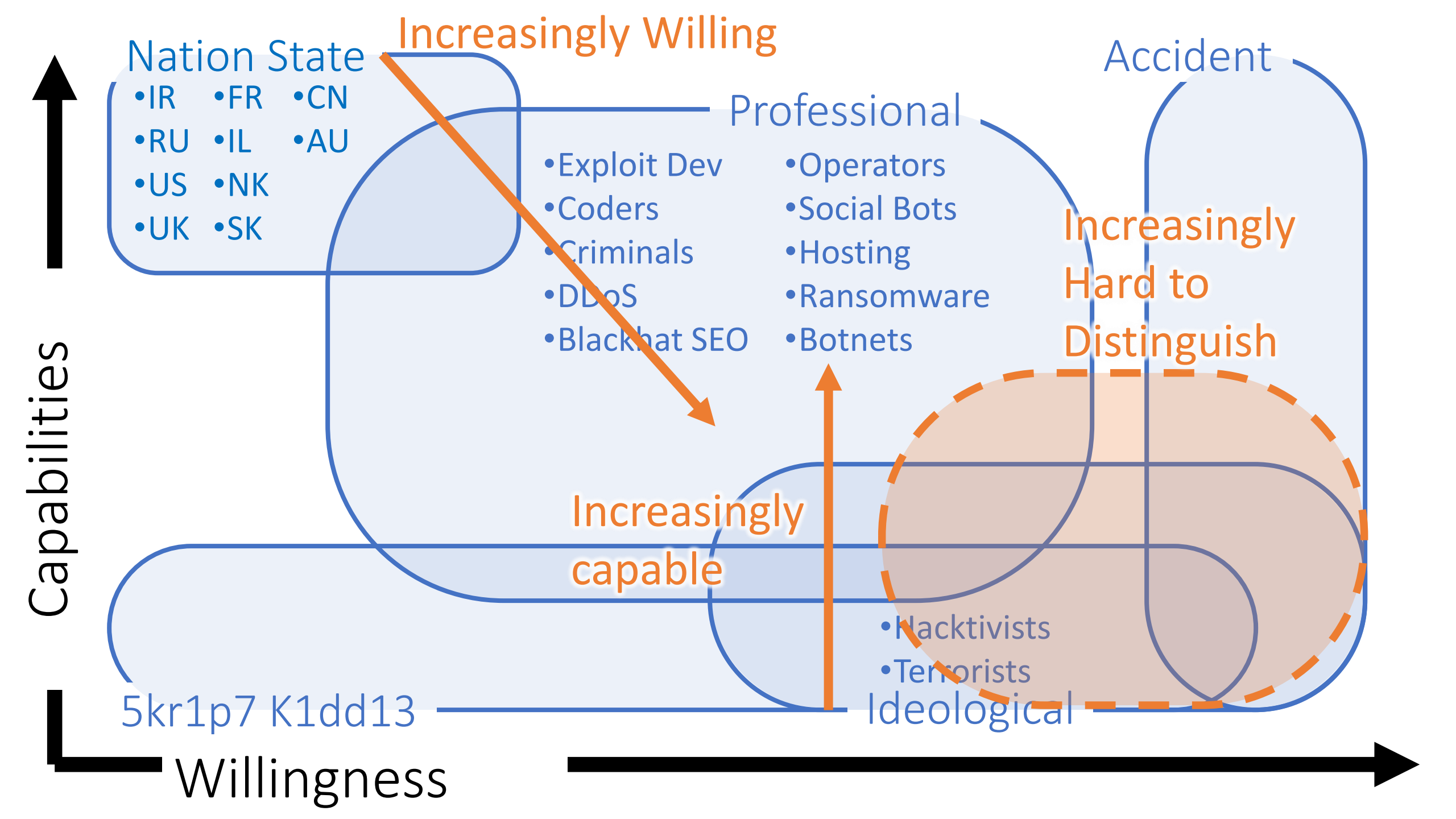
In 2018, Apple became the world's first **$1 Trillion** company.

In 2019, Apple will spend around **$1 Billion** on security.


Last week, a **14-year old** reported a major security flaw in Apple’s products.

Are you vulnerable?

Know your hackers


Increasingly Willing
Nation State
•IR •FR •CN
•RU •IL •AU
•US •NK
•UK •SK
Accident
Professional
•Exploit Dev
•Coders
•Criminals
•DDoS
•Blackhat SEO
•Operators
•Social Bots
•Hosting
•Ransomware
•Botnets
Increasingly Hard to Distinguish
Increasingly capable
•Hacktivists
•Terrorists
5kr1p7 K1dd13
Ideological
Capabilities
Willingness

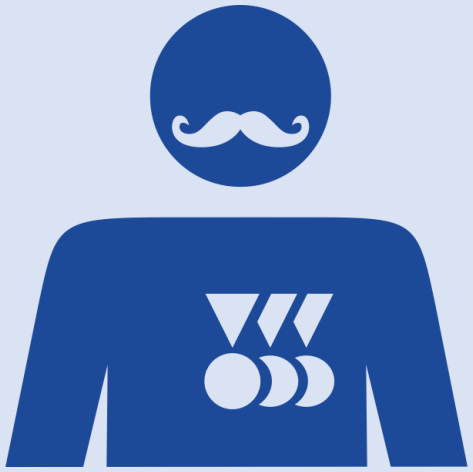
I Am The Cavalry

Five Motivations of Security Researchers

https://iamthecavalry.org/motivations

Protect

Puzzle



Pride/Prestige

Profit/Payment

Protest/Patriot

Jay Radcliffe

- Security researcher
- Diabetic patient
- Father of diabetic patient

Protect

Vulnerability Research, Disclosure, and Law

#WeHackers

Launched
January 29

DoD's Vulnerability Disclosure Policy Results

Total valid reports resolved **2,837**

Participating hackers **645+**

High or critical severity vulnerabilities **100+**

Hackers from **50** countries including: India, Great Britain, Pakistan, Philippines, Egypt, Russia, France, Australia and Canada

hackerone

DMCA Rules

- Intended to fight counterfeiting of DVDs
- Makes illegal circumvention of a technical protection mechanism (TPM) to access copyrighted works

- CFAA is the primary tool to prosecute cybercrimes

DMCA Exemptions

- “Solely for good-faith security research”
- “On a lawfully acquired device”
- “With the authorization of the owner”
- Conducted in an environment “designed to avoid any harm to individuals or the public”

- US DOJ in favor of exemptions:

“the DMCA was not created to protect [voting machines], and is ill-suited to do so.”

Supply Chain Risk

Supply Chain Risk Vectors

Supplier facilitated risk – Implementation, operation, and maintenance
Counterfeit – Unverified components
Malicious Taint – Subverted components or systems
Unintended Taint – Known software vulnerabilities

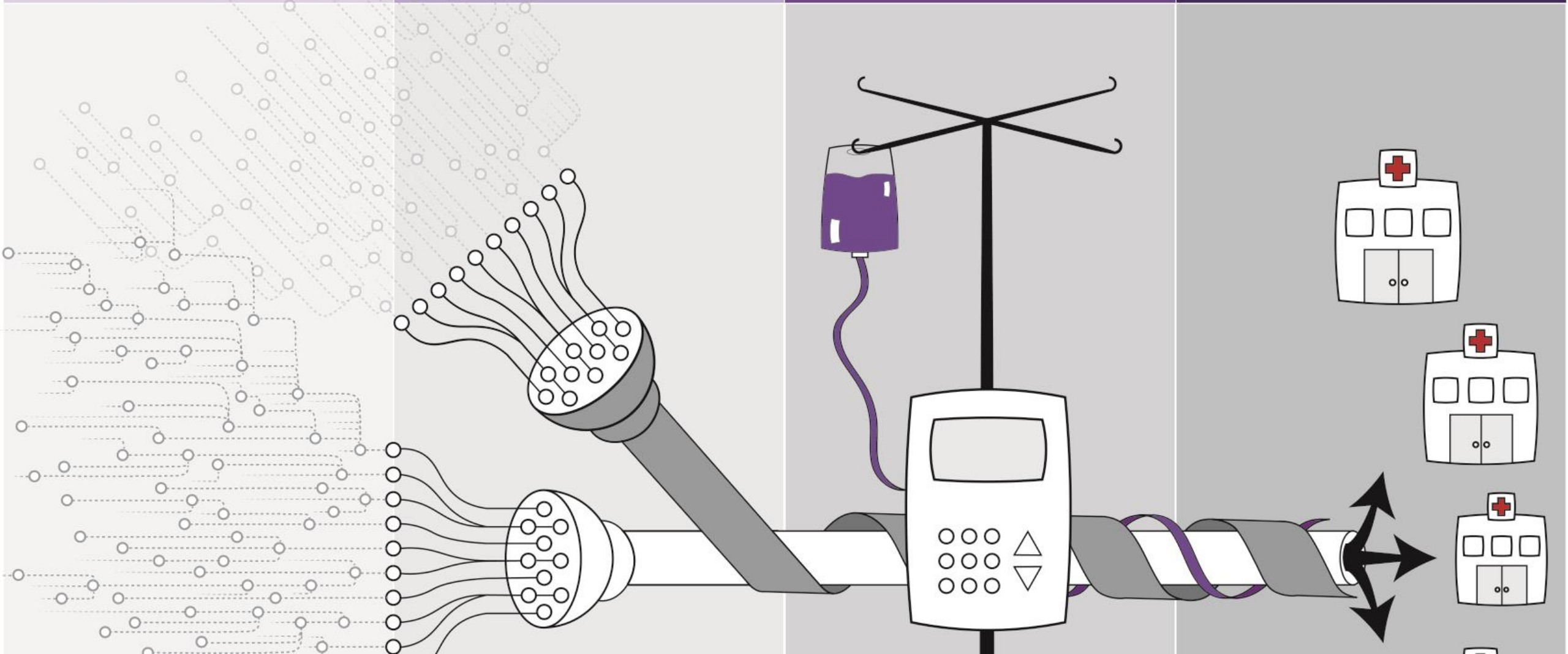

Touchscreen / Ion-X Glass
Display Module
Loudspeaker
Force Touch Sensor
Battery
Taptic Engine Module
Interconnect PCB B
Interconnect PCB A
Wireless Charging Coil
Optical Pulse Sensor PCB
Bluetooth / WLAN Antenna
Button PCB
Digital Crown / Home Button
Aluminum Housing
Watch Strap
Side Button

PARTS

COMPOUND PARTS

FINAL GOODS ASSEMBLED

OPERATOR



Transparency & Awareness

Nutrition Facts

Serving Size 1 cup (228g)
Servings Per Container 2

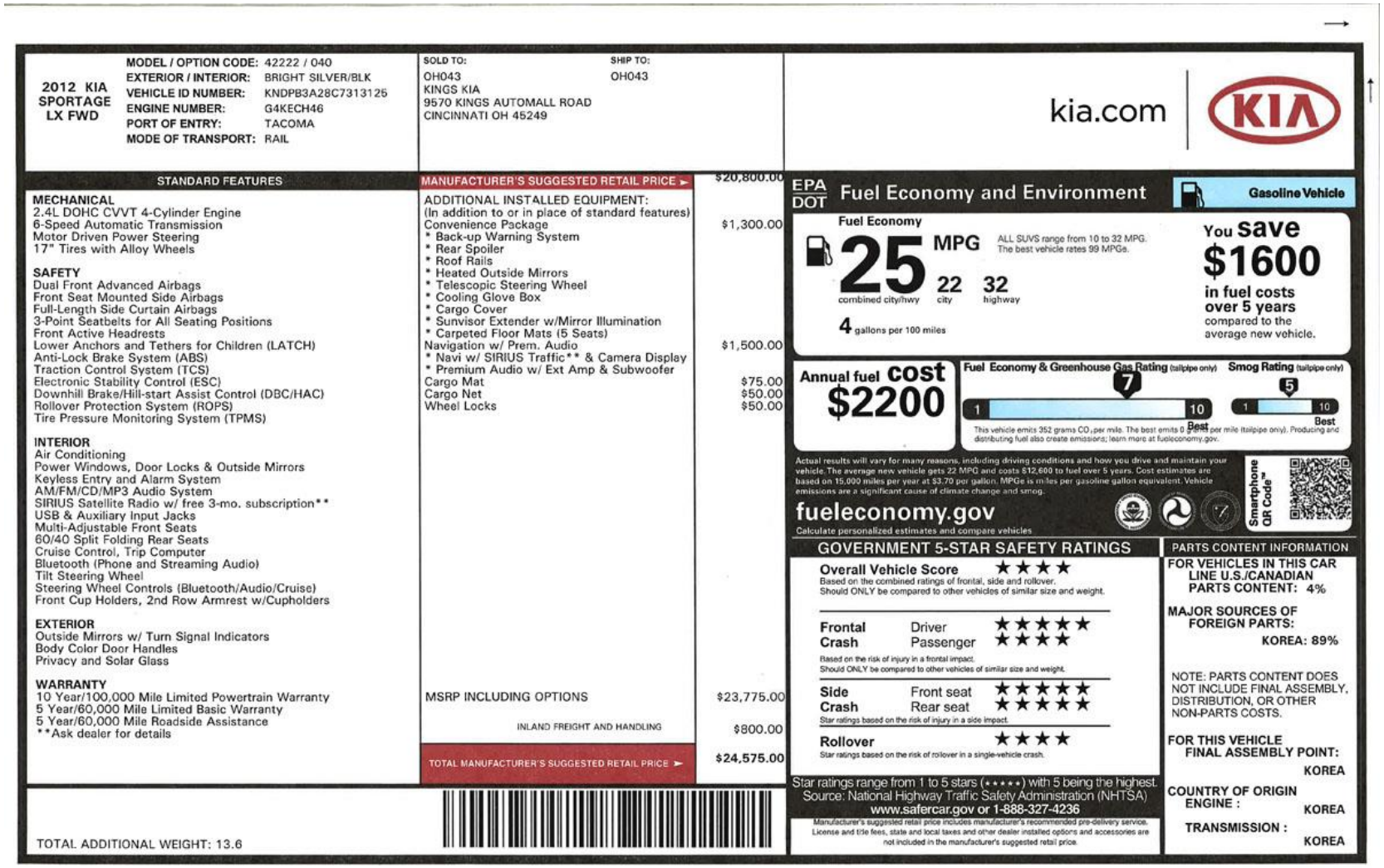
Amount Per Serving

Calories 250 Calories from Fat 110

	% Daily Value*
Total Fat 12g	18%
Saturated Fat 3g	15%
Trans Fat 3g	
Cholesterol 30mg	10%
Sodium 470mg	20%
Total Carbohydrate 31g	10%
Dietary Fiber 0g	0%
Sugars 5g	
Protein 5g	
Vitamin A	4%
Vitamin C	2%
Calcium	20%
Iron	4%

* Percent Daily Values are based on a 2,000 calorie diet. Your Daily Values may be higher or lower depending on your calorie needs.

	Calories	2,000	2,500
Total Fat	Less than	65g	80g
Sat Fat	Less than	20g	25g
Cholesterol	Less than	300mg	300mg
Sodium	Less than	2,400mg	2,400mg
Total Carbohydrate		300g	375g
Dietary Fiber		25g	30g



2012 KIA SPORTAGE LX FWD

MODEL / OPTION CODE: 42222 / 040
EXTERIOR / INTERIOR: BRIGHT SILVER/BLK
VEHICLE ID NUMBER: KNDPB3A28C7313125
ENGINE NUMBER: G4KECH46
PORT OF ENTRY: TACOMA
MODE OF TRANSPORT: RAIL

SOLD TO: OH043 KINGS KIA 9570 KINGS AUTOMALL ROAD CINCINNATI OH 45249

SHIP TO: OH043

kia.com

STANDARD FEATURES

MECHANICAL
2.4L DOHC CVVT 4-Cylinder Engine
6-Speed Automatic Transmission
Motor Driven Power Steering
17" Tires with Alloy Wheels

SAFETY
Dual Front Advanced Airbags
Front Seat Mounted Side Airbags
Full-Length Side Curtain Airbags
3-Point Seatbelts for All Seating Positions
Front Active Headrests
Lower Anchors and Tethers for Children (LATCH)
Anti-Lock Brake System (ABS)
Traction Control System (TCS)
Electronic Stability Control (ESC)
Downhill Brake/Hill-start Assist Control (DBC/HAC)
Rollover Protection System (ROPS)
Tire Pressure Monitoring System (TPMS)

INTERIOR
Air Conditioning
Power Windows, Door Locks & Outside Mirrors
Keyless Entry and Alarm System
AM/FM/CD/MP3 Audio System
SIRIUS Satellite Radio w/ free 3-mo. subscription**
USB & Auxiliary Input Jacks
Multi-Adjustable Front Seats
60/40 Split Folding Rear Seats
Cruise Control, Trip Computer
Bluetooth (Phone and Streaming Audio)
Tilt Steering Wheel
Steering Wheel Controls (Bluetooth/Audio/Cruise)
Front Cup Holders, 2nd Row Armrest w/Cupholders

EXTERIOR
Outside Mirrors w/ Turn Signal Indicators
Body Color Door Handles
Privacy and Solar Glass

WARRANTY
10 Year/100,000 Mile Limited Powertrain Warranty
5 Year/60,000 Mile Limited Basic Warranty
5 Year/60,000 Mile Roadside Assistance
**Ask dealer for details

MANUFACTURER'S SUGGESTED RETAIL PRICE ►	$20,800.00
ADDITIONAL INSTALLED EQUIPMENT: (In addition to or in place of standard features)	
Convenience Package	$1,300.00
* Back-up Warning System	
* Rear Spoiler	
* Roof Rails	
* Heated Outside Mirrors	
* Telescopic Steering Wheel	
* Cooling Glove Box	
* Cargo Cover	
* Sunvisor Extender w/Mirror Illumination	
* Carpeted Floor Mats (5 Seats)	
Navigation w/ Prem. Audio	$1,500.00
* Navi w/ SIRIUS Traffic** & Camera Display	
* Premium Audio w/ Ext Amp & Subwoofer	
Cargo Mat	$75.00
Cargo Net	$50.00
Wheel Locks	$50.00
MSRP INCLUDING OPTIONS	$23,775.00
INLAND FREIGHT AND HANDLING	$800.00
TOTAL MANUFACTURER'S SUGGESTED RETAIL PRICE ►	$24,575.00

TOTAL ADDITIONAL WEIGHT: 13.6

EPA DOT Fuel Economy and Environment — Gasoline Vehicle

Fuel Economy: 25 MPG combined city/hwy (22 city, 32 highway)
4 gallons per 100 miles
ALL SUVS range from 10 to 32 MPG. The best vehicle rates 99 MPGe.

You save $1600 in fuel costs over 5 years compared to the average new vehicle.

Annual fuel cost $2200

Fuel Economy & Greenhouse Gas Rating (tailpipe only): 7 (1 Worst, 10 Best)
Smog Rating (tailpipe only): 5 (1 Worst, 10 Best)

This vehicle emits 352 grams CO2 per mile. The best emits 0 grams per mile (tailpipe only). Producing and distributing fuel also create emissions; learn more at fueleconomy.gov.

Actual results will vary for many reasons, including driving conditions and how you drive and maintain your vehicle. The average new vehicle gets 22 MPG and costs $12,600 to fuel over 5 years. Cost estimates are based on 15,000 miles per year at $3.70 per gallon. MPGe is miles per gasoline gallon equivalent. Vehicle emissions are a significant cause of climate change and smog.

fueleconomy.gov
Calculate personalized estimates and compare vehicles

Smartphone QR Code™

GOVERNMENT 5-STAR SAFETY RATINGS

Overall Vehicle Score ★★★★
Based on the combined ratings of frontal, side and rollover. Should ONLY be compared to other vehicles of similar size and weight.

Frontal Crash — Driver ★★★★★ Passenger ★★★★
Based on the risk of injury in a frontal impact. Should ONLY be compared to other vehicles of similar size and weight.

Side Crash — Front seat ★★★★★ Rear seat ★★★★★
Star ratings based on the risk of injury in a side impact.

Rollover ★★★★
Star ratings based on the risk of rollover in a single-vehicle crash.

Star ratings range from 1 to 5 stars (★★★★★) with 5 being the highest.
Source: National Highway Traffic Safety Administration (NHTSA)
www.safercar.gov or 1-888-327-4236

Manufacturer's suggested retail price includes manufacturer's recommended pre-delivery service. License and title fees, state and local taxes and other dealer installed options and accessories are not included in the manufacturer's suggested retail price.

PARTS CONTENT INFORMATION

FOR VEHICLES IN THIS CAR LINE U.S./CANADIAN PARTS CONTENT: 4%

MAJOR SOURCES OF FOREIGN PARTS: KOREA: 89%

NOTE: PARTS CONTENT DOES NOT INCLUDE FINAL ASSEMBLY, DISTRIBUTION, OR OTHER NON-PARTS COSTS.

FOR THIS VEHICLE FINAL ASSEMBLY POINT: KOREA

COUNTRY OF ORIGIN ENGINE : KOREA
TRANSMISSION : KOREA

MAYO CLINIC

Procurement Guidance

4. System information: • List of 3rd Party Software • List of Accounts • List of Network Ports • List of firewall rules (if applicable) • Documentation of Security Capabilities/Configurations for System Hardening • Scanning Requirements	Provides more granular information as to how the system is setup and managed within the Mayo Clinic environment.	Provide vendor documentation (i.e. Bill of Materials) for the bulleted items. Template provided.	 Deliverable 4 - System Information T
5. Vulnerability Assessment, including: • Testing Results • Remediation Tracking	Provides an in-depth vulnerability assessment, outstanding vulnerabilities and appropriate remediation plans and timelines to resolve the issues. This provides Mayo Clinic with appropriate information on risks that may be introduced into the patient care environment and allows for collaborative mitigation strategies to be detailed.	Complete a vulnerability assessment as detailed in the Vendor Assessment Book (pdf). Once testing is completed, complete the VA Statement of Methodology and document findings and remediation plans in a report. Example VA Statement of Methodology (pdf) and Vulnerability Assessment Template report provided.	 Vulnerability Assessment Book.pdf  VA Statement of Methodology - mocku  VA Statement of Methodology.docx  Vulnerability Assessment Template
6. Mayo Clinic Information Security Schedule	**Provides advanced copy** of Mayo Clinic's Information Security Schedule that Supply Chain Management will negotiate as part of the purchase contract or vendor agreements.	1. Ensure appropriate vendor internal staff receives Mayo's Information Security Schedule for review. 2. Perform review and prepare any proposed redline items. 3. Provide a vendor contact to the Mayo proponent for the redlined ISS negotiation.	 Deliverable 6 - Information Security S

https://www.mayoclinic.org/documents/medical-device-vendor-instructions/doc-20389647

Perspectives on Cybersecurity

NASS
National Association of Secretaries of State

2019 Winter Conference
February 2, 2019

Beau Woods
Cyber Safety Innovation Fellow, Atlantic Council
Leader, I Am The Cavalry (.org)

Appendix

Coordinated Vulnerability Disclosure

US Department of Commerce, NTIA Template

https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf

ISO/IEC 29147 Standard for Vulnerability Disclosure

https://www.iso.org/standard/45170.html

ISO/IEC 30111 Standard for Vulnerability Handling Processes

https://www.iso.org/standard/53231.html

National Governor's Association

https://ci.nga.org/files/live/sites/NGA/files/pdf/2018/HSPS/Crowdsourcing%20Cybersecurity%20101.pdf

US Department of Justice

https://www.justice.gov/criminal-ccips/page/file/983996/download

It Takes a Village Comic (Atlantic Council and HackerOne)

http://publications.atlanticcouncil.org/hacktivity/

BSides Events Tracker

http://www.securitybsides.com/w/page/12194156/FrontPage

Hackers: the Internet's immune system (TED Talk, Keren Elazari

https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system

Can hackers break my heart (TEDx Talk, Marie Moe)

https://www.youtube.com/watch?v=W1YWpVMpPi8

The **Food Pyramid**

For adults, teenagers and children aged five and over

Not needed for good health.

Foods and drinks high in fat, sugar and salt

NOT every day

! Maximum once or twice a week

Needed for good health. Enjoy a variety every day.

Fats, spreads and oils

In very small amounts

Meat, poultry, fish, eggs, beans and nuts

2 Servings a day

Milk, yogurt and cheese

3 Servings a day

5 for children age 9–12 and teenagers age 13–18

Wholemeal cereals and breads, potatoes, pasta and rice

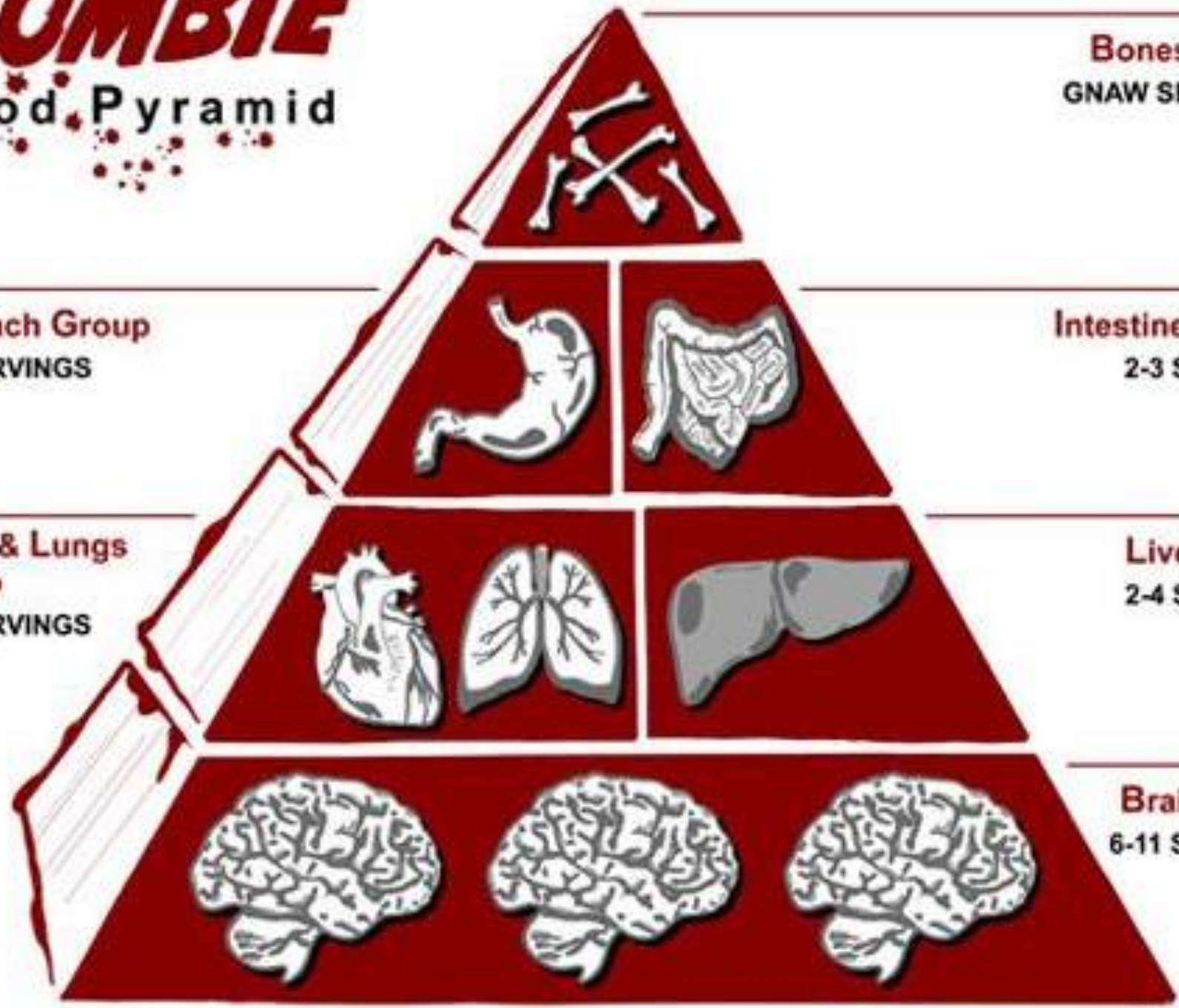
3-5* Servings a day

Up to 7* for teenage boys and men age 19–50

Vegetables, salad and fruit

5-7 Servings a day

ZOMBIE
Food Pyramid



Bones, Gristle
GNAW SPARINGLY

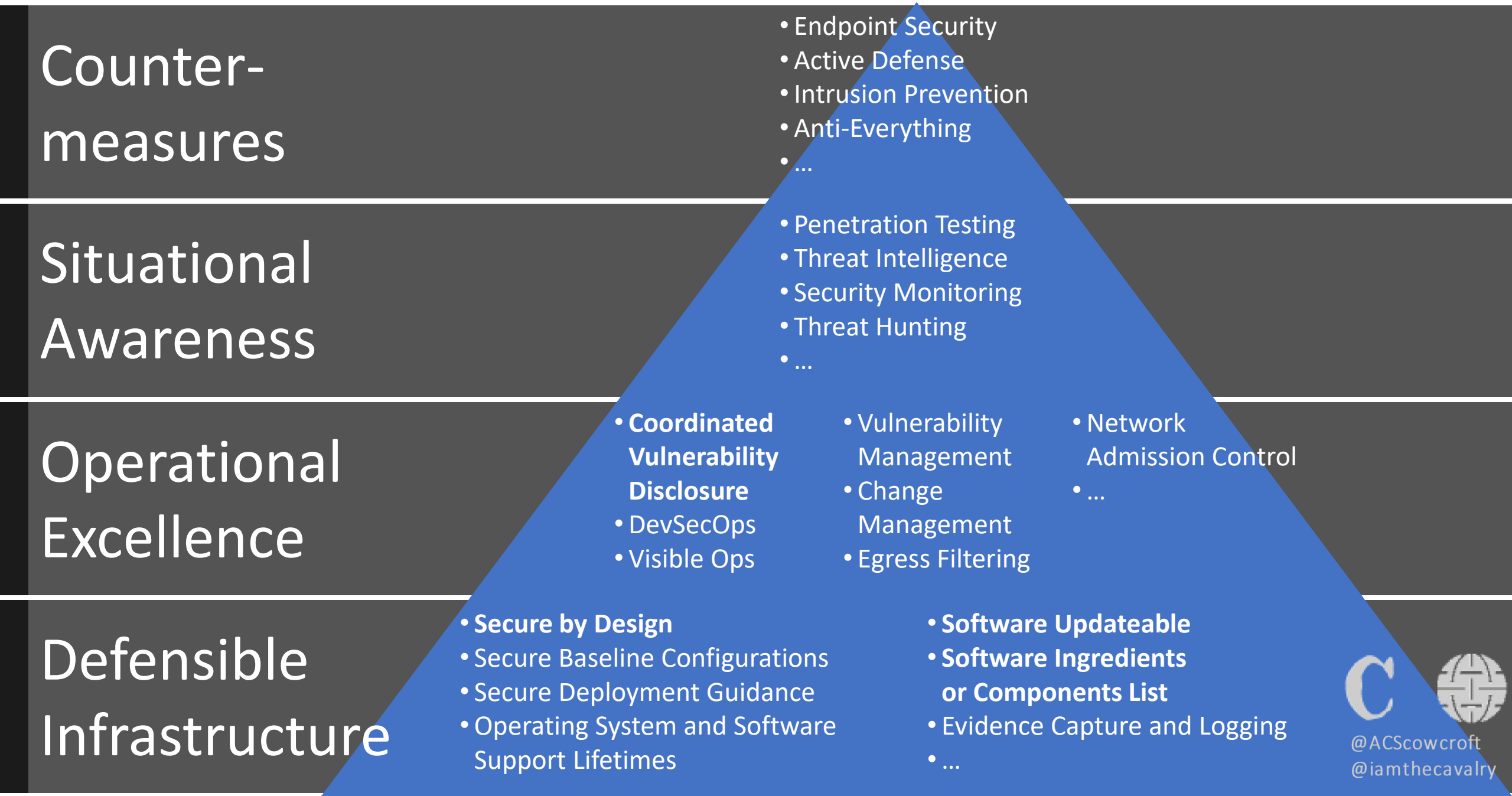
Stomach Group
2-3 SERVINGS

Intestines Group
2-3 SERVINGS

Heart & Lungs Group
3-5 SERVINGS

Liver Group
2-4 SERVINGS

Brain Group
6-11 SERVINGS


Counter-measures
• Endpoint Security
• Active Defense
• Intrusion Prevention
• Anti-Everything
• …
Situational Awareness
• Penetration Testing
• Threat Intelligence
• Security Monitoring
• Threat Hunting
• …
Operational Excellence
• Coordinated Vulnerability Disclosure
• DevSecOps
• Visible Ops
• Vulnerability Management
• Change Management
• Egress Filtering
• Network Admission Control
• …
Defensible Infrastructure
• Secure by Design
• Secure Baseline Configurations
• Secure Deployment Guidance
• Operating System and Software Support Lifetimes
• Software Updateable
• Software Ingredients or Components List
• Evidence Capture and Logging
• …
@ACScowcroft
@iamthecavalry

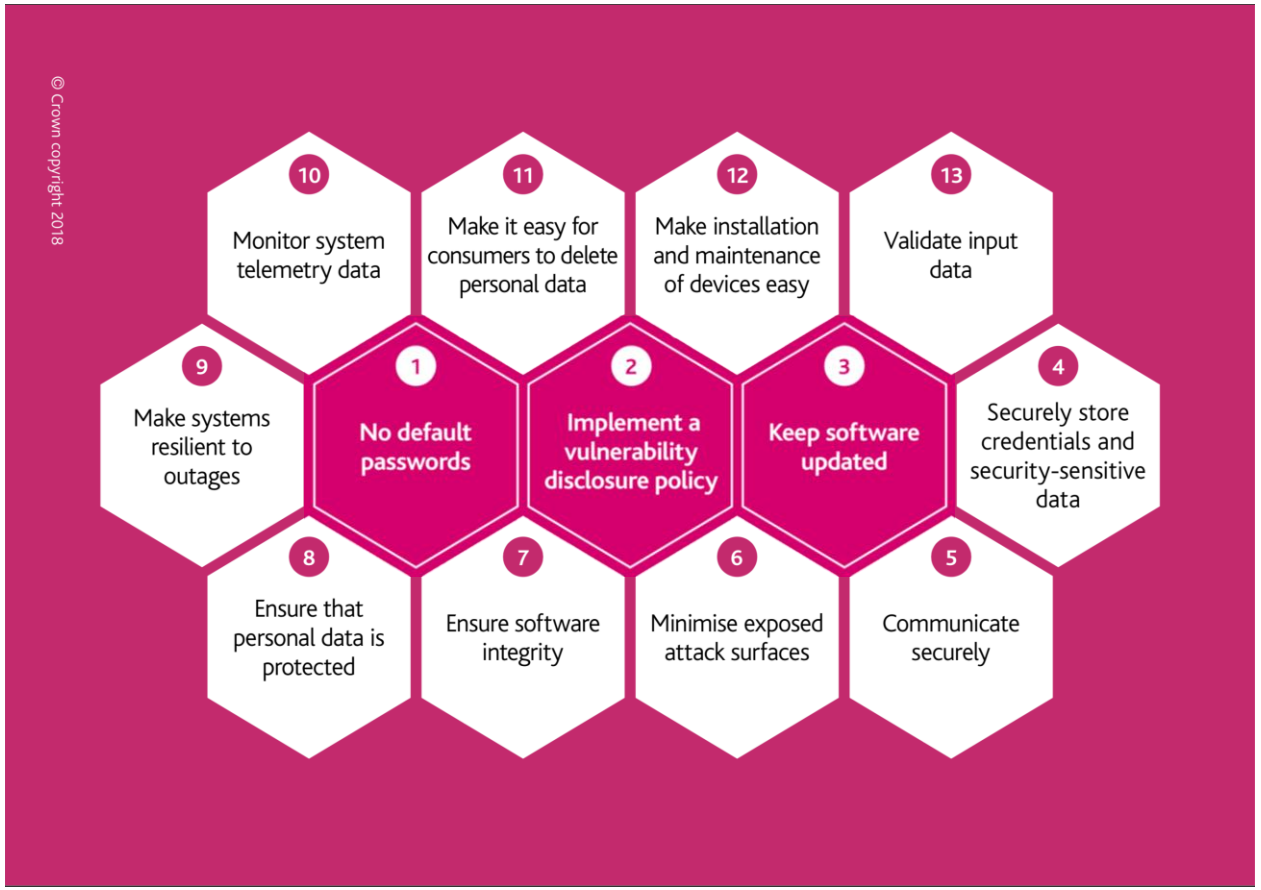

Counter-
measures
Situational
Awareness
Operational
Excellence
Defensible
Infrastructure
@ACScowcroft
@iamthecavalry


Counter-measures
Situational Awareness
Operational Excellence
Defensible Infrastructure
$ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $
$ $ $ $ $ $
$ $ $ $ $
$ $ $
$
C
ACScowcroft
@
thecavalry

Department for Culture Media & Sport

GOV.UK

Code of Practice for IoT Security



https://www.gov.uk/government/publications/secure-by-design