



Lunch and Presentation: Security-by-Design

**Beau Woods, Cyber Safety
Innovation Fellow at Atlantic Council
& Co-Founder, I Am The Cavalry**

Cyber Safety

~~Security By Design~~

in

Smart Cities

Beau Woods

@beauwoods

I Am The Cavalry

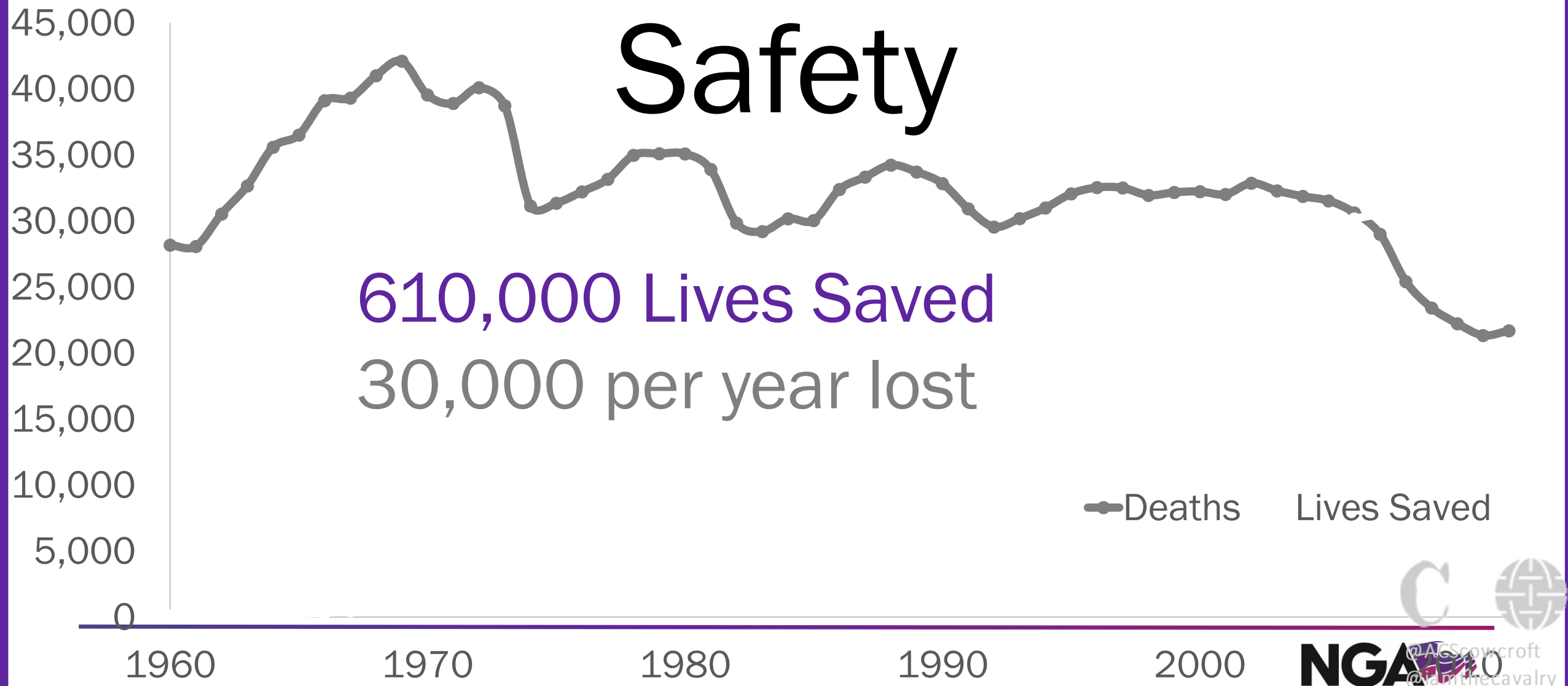


Atlantic Council





History of Auto Safety



Source: NHTSA Publication, "Lives Saved by Vehicle Safety Technologies and Associated Federal Motor Vehicle Safety Standards, 1960 to 2012"



C



@ACScowcroft

@iamthecavalry



IT Security Failures have become Mission Failures



@ACScowcroft
@iamthecavalry

Holding a Mirai to Our Neglect



@ACScowcroft

@iamthecavalry

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

Individual Human Lives



Atlantic Council



College of Medicine
Phoenix



#NIGHTLINE



@ACScowcroft
@iamthecavalry

Public Safety and Health



CYBERATTACK



@ACScowcroft
@iamthecavalry

Technology Supply Chain



Public Health Readiness



@ACScowcroft
@iamthecavalry

Global Shipping & Logistics

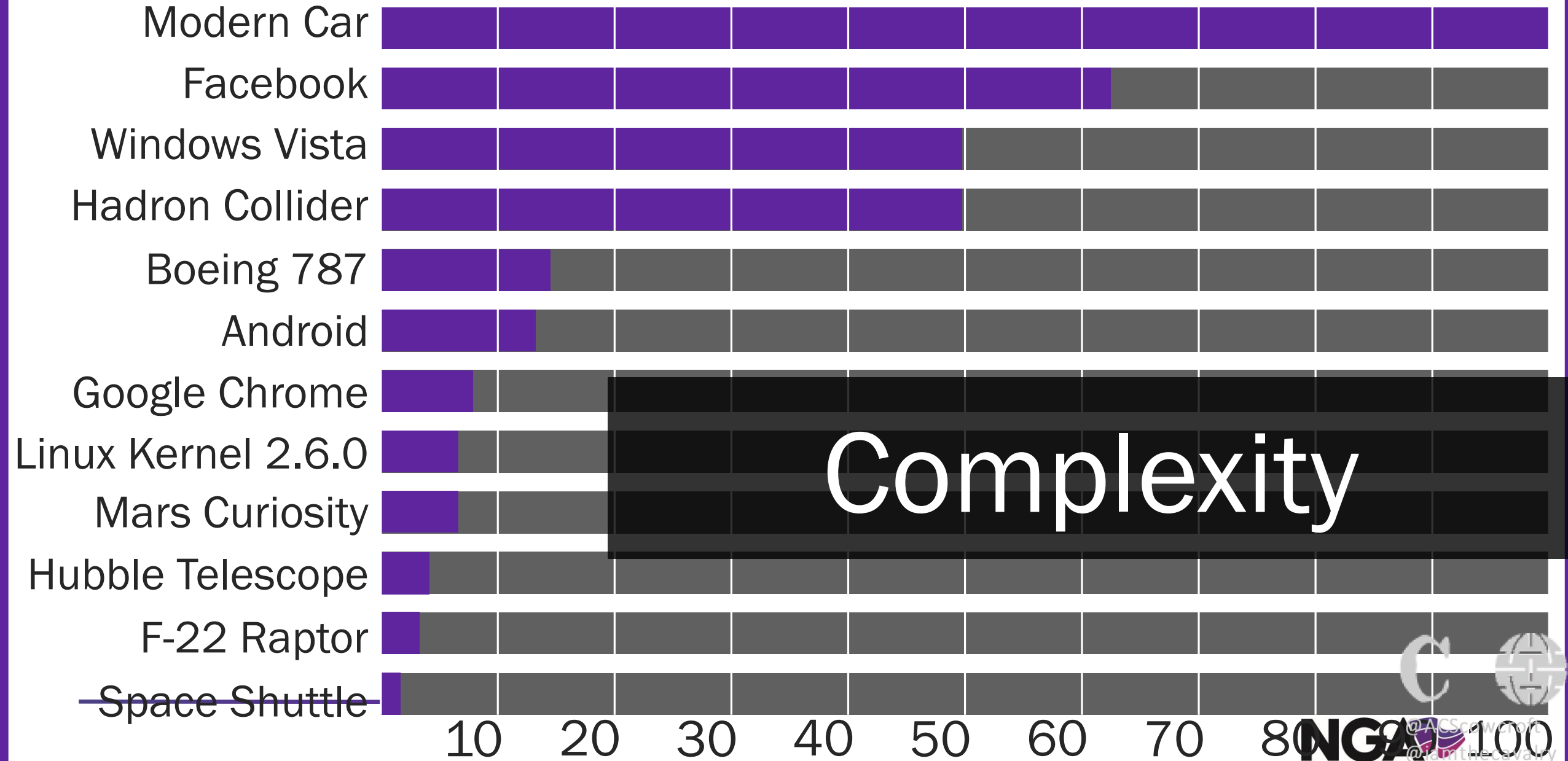


@ACScowcroft
@iamthecavalry

Dependence



Millions of Lines of Software Code



Vulnerability



C



@ACScowcroft
@Janthecavalry

Exposure

Range

Component

cm

Nearfield

Serial

meter

Wi-Fi

Bluetooth

km

3G/4G/5G/LTE

Global

Internet

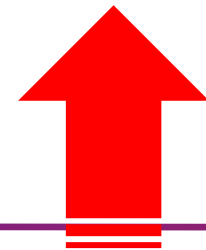
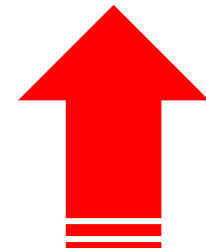
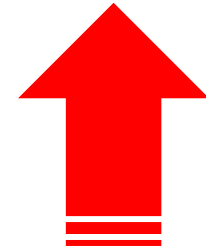
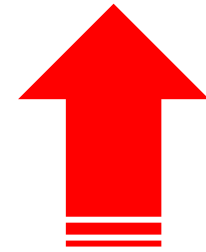


Dependence

Complexity

Vulnerability

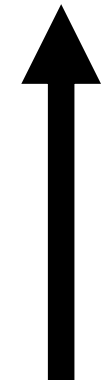
Exposure



Examining the Adversaries



@ACSCowcroft
@iamthecavalry



Capabilities



Willingness



Nation State

- IR
- RU
- US
- UK
- FR
- IL
- NK
- SK
- CN
- AU

Capabilities

Willingness

Nation State

- IR
- RU
- US
- UK
- FR
- IL
- NK
- SK
- CN
- AU

Capabilities

Willingness

- Hacktivists
 - Terrorists
- Ideological

Nation State

- IR
- RU
- US
- UK
- FR
- IL
- NK
- SK
- CN
- AU

Professional

- Exploit Dev
- Coders
- Criminals
- DDoS
- Blackhat SEO
- Operators
- Social Bots
- Hosting
- Ransomware
- Botnets

- Hacktivists
- Terrorists

Ideological

Willingness

Nation State

- IR
- RU
- US
- UK
- FR
- IL
- NK
- SK
- CN
- AU

Professional

- Exploit Dev
- Coders
- Criminals
- DDoS
- Blackhat SEO
- Operators
- Social Bots
- Hosting
- Ransomware
- Botnets

- Hacktivists
- Terrorists

Ideological

5kr1p7 K1dd13

Willingness

Capabilities

Nation State

- IR
- RU
- US
- UK
- FR
- IL
- NK
- SK
- CN
- AU

Professional

- Exploit Dev
- Coders
- Criminals
- DDoS
- Blackhat SEO
- Operators
- Social Bots
- Hosting
- Ransomware
- Botnets

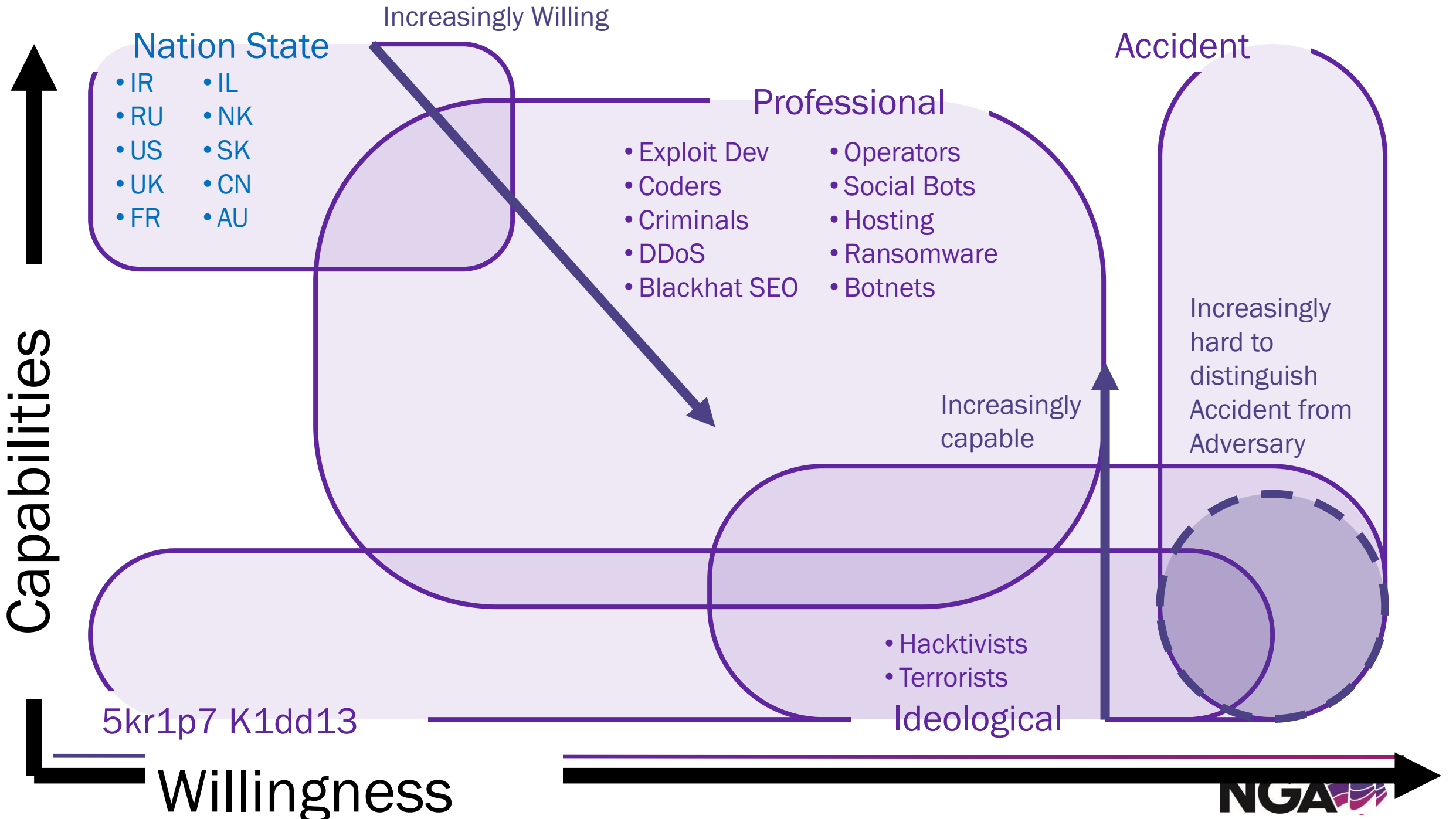
Accident

- Hacktivists
- Terrorists

Ideological

5kr1p7 K1dd13

Willingness



Nation State

- IR
- RU
- US
- UK
- FR
- IL
- NK
- SK
- CN
- AU

Professional

- Exploit Dev
- Coders
- Criminals
- DDoS
- Blackhat SEO
- Operators
- Social Bots
- Hosting
- Ransomware
- Botnets

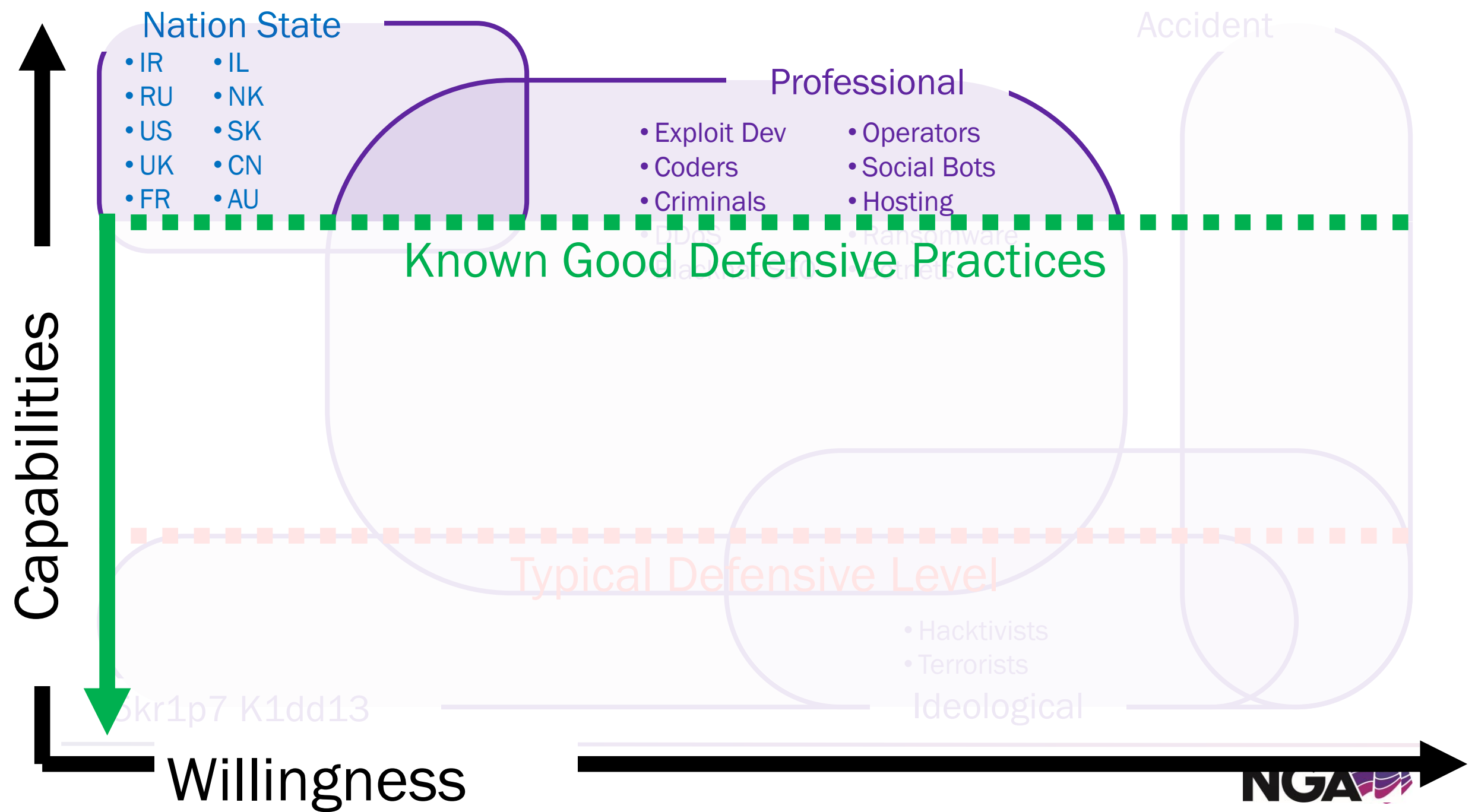
Accident

Typical Defensive Level

- Hacktivists
- Terrorists

Ideological

Willingness





IT Security Cost/Benefit



@ACSowcroft
@iamthecavalry



@ACScowcroft
@iamthecavalry

August 2, 2018

Apple became the world's 1st
\$1 Trillion company



@ACScowcroft
@iamthecavalry

August 17, 2018

Sixteen year old pled guilty to hacking Apple



@ACScowcroft
@iamthecavalry

Forecasted Global
Cybersecurity Spending,
2017-2021:

\$1 Trillion



@ACScowcroft
@iamthecavalry

ONE HUNDRED PERCENT of
FORTUNE
500
companies
will be hacked
over the same
time period

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

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

Needed for good health. Enjoy a variety every day.



@ACScowcroft
@iamthecavalry

ZOMBIE

Food Pyramid

Stomach Group
2-3 SERVINGS



Heart & Lungs Group
3-5 SERVINGS



Bones, Gristle
GNAW SPARINGLY



Intestines Group
2-3 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
- ...

Counter-
measures

Situational
Awareness

Operational
Excellence

Defensible
Infrastructure



Counter-
measures

\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$

Situational
Awareness

\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$

\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$

Operational
Excellence

\$ \$ \$ \$ \$ \$ \$

\$ \$ \$ \$ \$

\$ \$ \$

Defensible
Infrastructure

\$



ACScowcroft
@thecavalry

Secure by Design



@ACSCowcroft
@iamthecavalry

Automotive 5-Star Cyber Safety Framework



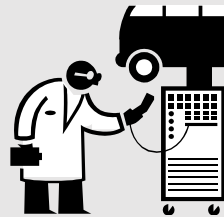
All systems fail. What is your ready posture toward failure?

- ★ **Safety by Design** – Anticipate and avoid failure
- ★ **3rd Party Collaboration** – Engage willing allies to avoid failure
- ★ **Evidence Capture** – Observe and learn from failure
- ★ **Security Updates** – Correct failure conditions once known
- ★ **Segmentation & Isolation** – Prevent cascading failure

Connections and Ongoing Collaborations



Security
Researchers



Automotive
Engineers



Policy
Makers



Insurance
Analysts



Accident
Investigators



Standards
Organizations

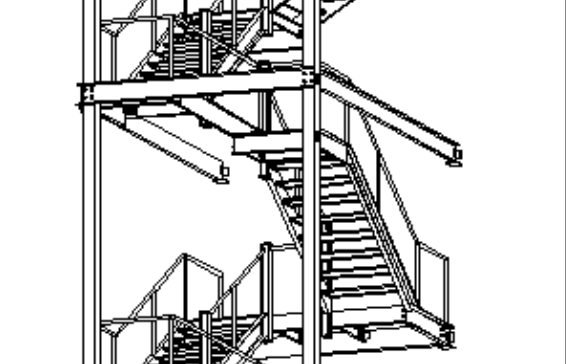
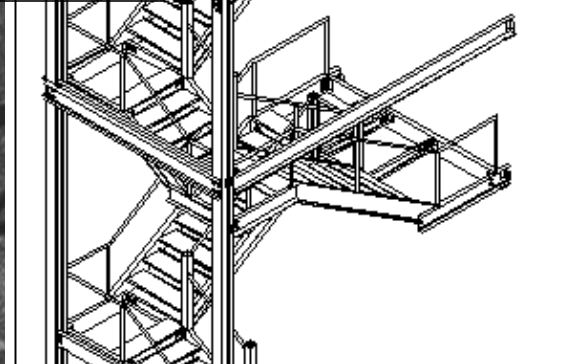
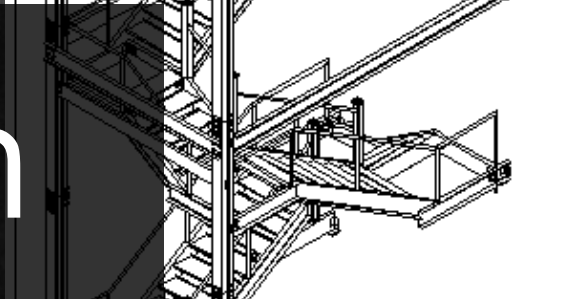
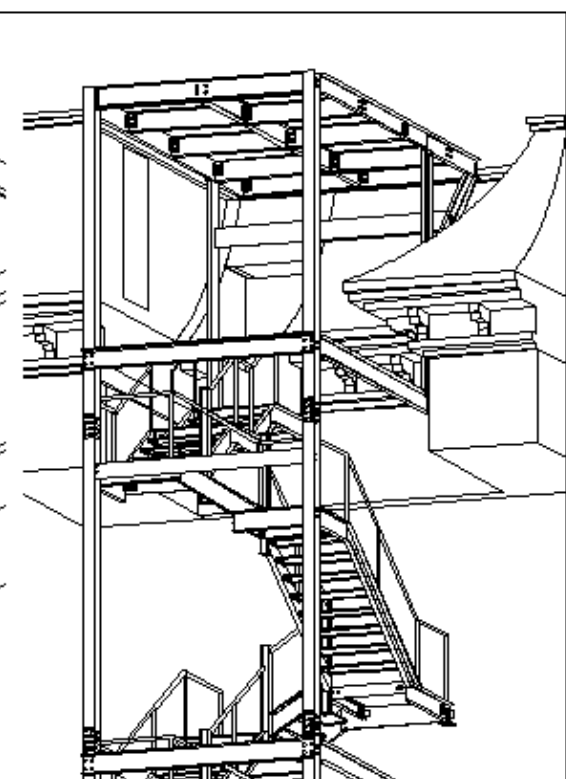
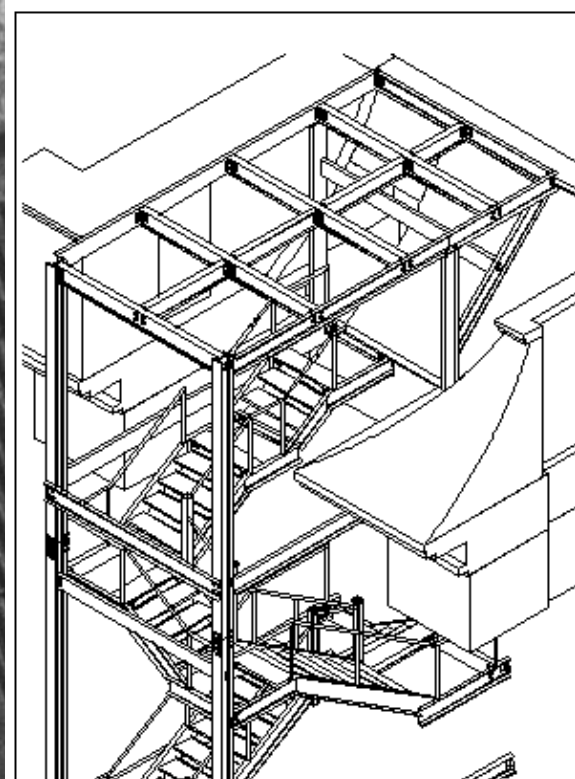


Government
Agencies

Great Fire

October 8-10, 1871





Built In vs Bolt On

Traceability & Transparency

① **Start Here** →

② **Check Calories**

③ **Limit these Nutrients**

④ **Get Enough of these Nutrients**

⑤ **Footnote**

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

⑥ **Quick Guide to % DV**

- 5% or less is Low
- 20% or more is High



@ACScowcroft

@iamthecavalry

Collaboration with Security Researchers



I Am The Cavalry

Five Motivations of Security Researchers

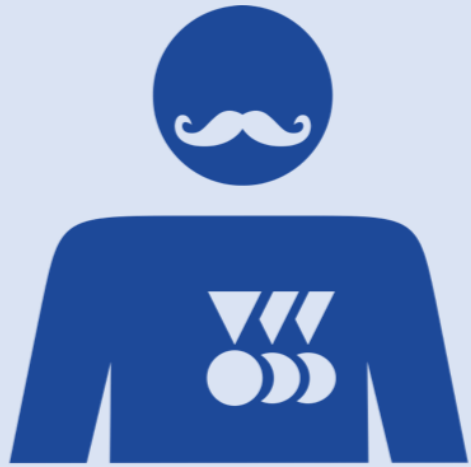
<https://iamthecavalry.org/motivations>



Protect



Puzzle



Pride/Prestige



Profit/Payment



Protest/Patriot



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 



@ACSCowcroft
@iamthecavalry

Software Security Updatability

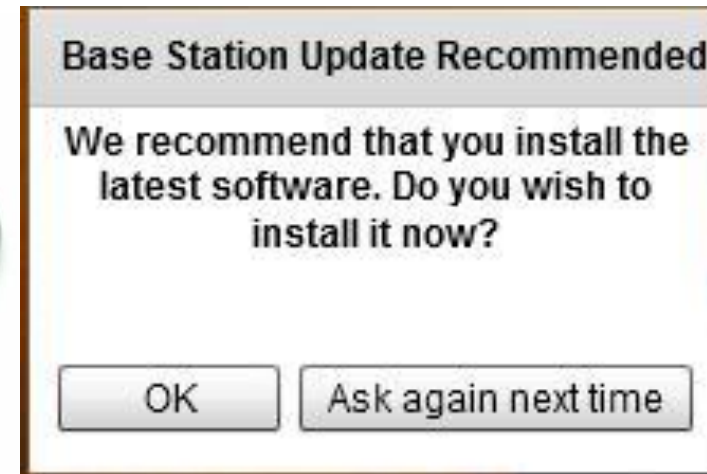
Increasing Agility & Decreasing Cost



Hardware
Replacement



Connected
Updates



Remote
Updates



Automatic
Updates

Cyber Safety

~~Security By Design~~

in

Smart Cities

Beau Woods

@beauwoods

I Am The Cavalry

Atlantic Council



Resources



@ACSCowcroft
@iamthecavalry

5-Star Framework

Addressing Automotive Cyber Systems

5-Star Capabilities



All systems fail. What is your ready posture toward failure?

- ★ **Safety by Design** – Anticipate and avoid failure
- ★ **3rd Party Collaboration** – Engage willing allies to avoid failure
- ★ **Evidence Capture** – Observe and learn from failure
- ★ **Security Updates** – Correct failure conditions once known
- ★ **Segmentation & Isolation** – Prevent cascading failure

<https://iamthecavalry.org/oath>

<https://iamthecavalry.org/5star>

Hippocratic Oath

For Connected Medical Devices

Cyber Safety Capabilities What is your ready posture toward failure?



- ⌘ **Cyber Safety by Design** – Anticipate and avoid failure
- ⌘ **Third-Party Collaboration** – Engage willing allies to avoid failure
- ⌘ **Evidence Capture** – Observe and learn from failure
- ⌘ **Resilience and Containment** – Prevent cascading failure
- ⌘ **Cyber Safety Updates** – Correct failure conditions once known

H.R.5793 - Cyber Supply Chain Management and Transparency Act of 2014

113th Congress (2013-2014)

BILL

Hide Overview ✕

Anything sold to the US Government must:

- A. Provide a software component list
Software Bill of Materials or Food Label
- B. Disclose known vulnerabilities
- C. Be software updateable

S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017

115th Congress (2017-2018) | [Get alerts](#)

BILL

Hide Overview ✕

Anything sold to the US Government must:

- A. Disclose known vulnerabilities
- B. Be software updateable
- C. Avoid hard-coded credentials
- D. Have a coordinated disclosure policy

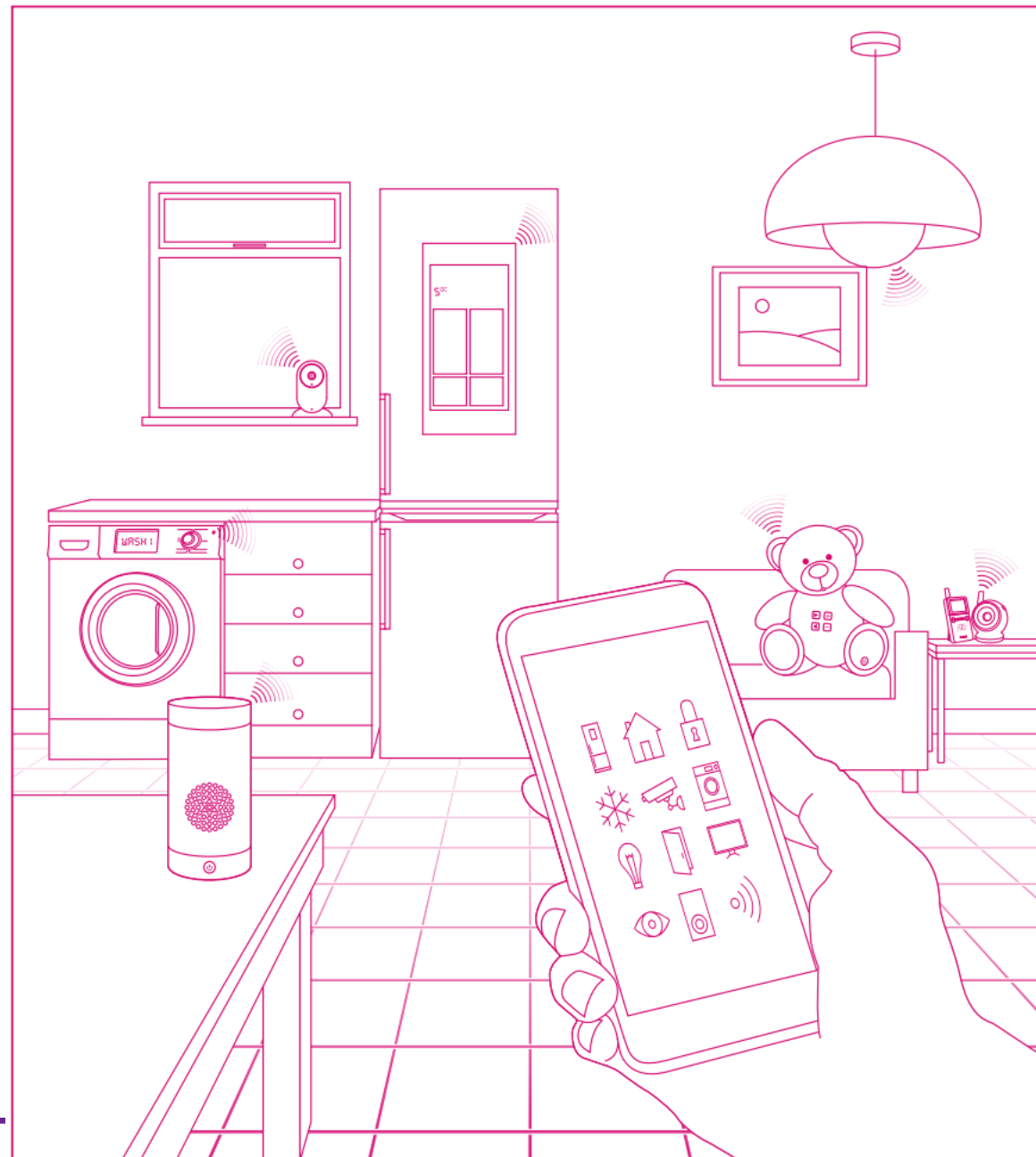


Department for Culture Media & Sport



Code of Practice for IoT Security

1. No default password
2. Coordinated Vulnerability Disclosure Policy
3. Keep devices updated



DoD's Vulnerability Disclosure Policy Results

Coordinated Vulnerability Disclosure

- US Department of Commerce, NTIA Template

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

Total valid reports resolved

2,837

- ISO/IEC 29147 Standard for Vulnerability Disclosure

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

High or critical severity vulnerabilities

100+

- ISO/IEC 30111 Standard for Vulnerability Handling Processes

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

50

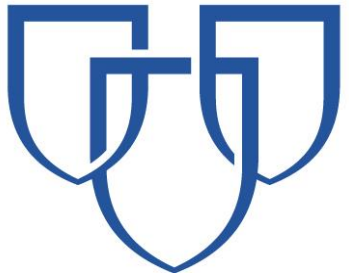
Hackers from countries including: India, Great Britain, Pakistan, Philippines, Egypt, Russia, France, Australia and Canada

hackerone C











@ACScowcroft
@iamthecavalry

MAYO CLINIC



Procurement Guidance

<p>4. System information:</p> <ul style="list-style-type: none"> 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 	<p>Provides more granular information as to how the system is setup and managed within the Mayo Clinic environment.</p>	<p>Provide vendor documentation (i.e. Bill of Materials) for the bulleted items. Template provided.</p>	 Deliverable 4 - System Information T
<p>5. Vulnerability Assessment, including:</p> <ul style="list-style-type: none"> Testing Results Remediation Tracking 	<p>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.</p>	<p>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.</p>	 Vulnerability Assessment Book.pdf  VA Statement of Methodology - mocku  VA Statement of Methodology.docx  Vulnerability Assessment Template
<p>6. Mayo Clinic Information Security Schedule</p>	<p>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.</p>	<ol style="list-style-type: none"> Ensure appropriate vendor internal staff receives Mayo's Information Security Schedule for review. Perform review and prepare any proposed redline items. Provide a vendor contact to the Mayo proponent for the redlined ISS negotiation. 	 Deliverable 6 - Information Security !   @ACSowcroft @iamthecavalry

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



Software Component Transparency (Software Bill of Materials)

<https://www.ntia.doc.gov/SoftwareTransparency>

Coordinated Security Vulnerability Disclosure

<https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities>

Device Upgradeability and Patching

<https://www.ntia.doc.gov/IoTSecurity>

President's Commission Report on Enhancing National Cybersecurity

<https://www.nist.gov/cybercommission>