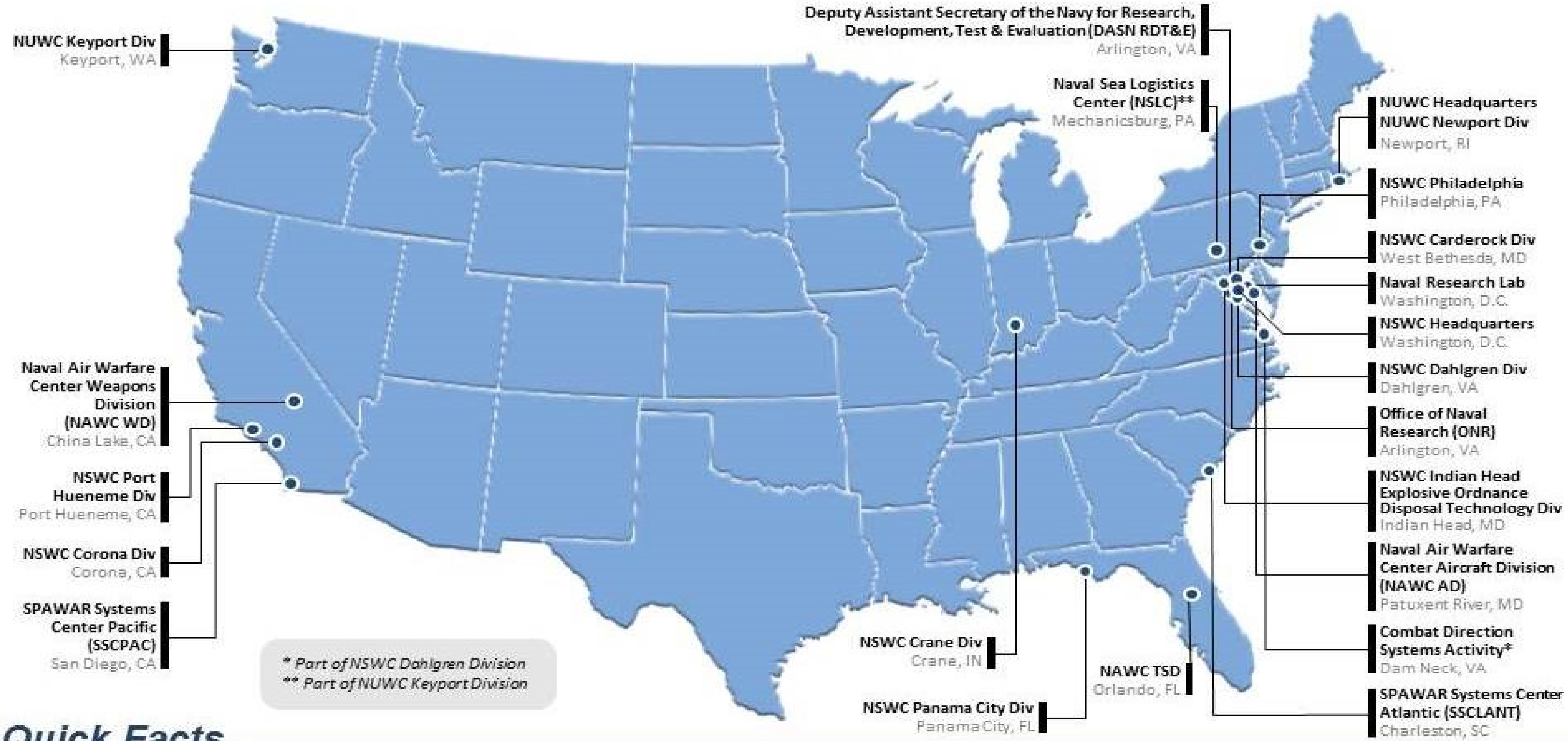
Full Scope Cybersecurity

Dr. Robert Templeman, SSTM
Distinguished Engineer for Cybersecurity

CAPT Mark Oesterreich, USN
Commanding Officer
NSWC Crane

Dr. Brett Seidle, SES
Technical Director
NSWC Crane

Naval Research & Development Establishment



NUWC Keyport Div
Keyport, WA

Naval Air Warfare Center Weapons Division (NAWC WD)
China Lake, CA

NSWC Port Hueneme Div
Port Hueneme, CA

NSWC Corona Div
Corona, CA

SPAWAR Systems Center Pacific (SSCPAC)
San Diego, CA

** Part of NSWC Dahlgren Division*
*** Part of NUWC Keyport Division*

NSWC Crane Div
Crane, IN

NSWC Panama City Div
Panama City, FL

NAWC TSD
Orlando, FL

Deputy Assistant Secretary of the Navy for Research, Development, Test & Evaluation (DASN RDT&E)
Arlington, VA

Naval Sea Logistics Center (NSLC)**
Mechanicsburg, PA

NUWC Headquarters
NUWC Newport Div
Newport, RI

NSWC Philadelphia
Philadelphia, PA

NSWC Carderock Div
West Bethesda, MD

Naval Research Lab
Washington, D.C.

NSWC Headquarters
Washington, D.C.

NSWC Dahlgren Div
Dahlgren, VA

Office of Naval Research (ONR)
Arlington, VA

NSWC Indian Head Explosive Ordnance Disposal Technology Div
Indian Head, MD

Naval Air Warfare Center Aircraft Division (NAWC AD)
Patuxent River, MD

Combat Direction Systems Activity*
Dam Neck, VA

SPAWAR Systems Center Atlantic (SSCLANT)
Charleston, SC

Quick Facts

❑ Diverse and highly educated workforce with 25,000 scientists, engineers, and technicians (with more than 2,000 Ph.D.s)

❑ 20 commands across the NAVAIR/NAVSEA Warfare Centers, SPAWAR Systems Centers, ONR and NRL

❑ Conducts RDT&E for the DoN to discover, develop, transition and field technologically superior naval warfighting capabilities.

❑ Unique Naval RDT&E facilities including laboratories, test facilities and test ranges

❑ Serves as principal R&D agents for Navy and Marine Corps Program Executive Offices

❑ Organizationally aligned to Naval Systems Commands and ONR

- Naval Sea Systems Command (NSWCs, NUWCs)
- Naval Air Systems Command (NAWCs)
- Space and Naval Warfare Systems Command (SSCs)

Aggressive Research, Development, Test & Evaluation for reliable real world solutions.

Distribution Statement A – Approved for Public Release

Naval Surface Warfare Center, Crane Division

3238
NSWC Crane Employees

67 %
Scientists, Engineers & Technicians

QUICK FACTS

2
DoD Executive Agent Assignments

$1.3B
Business Base

3
Focus Areas

Electronic Warfare
Strategic Missions
Expeditionary Warfare

1
Mission

5
Technical Warrant Holders

87 PhD
584 Masters
1401 Bachelors

Distribution Statement A – Approved for Public Release

Cyber

“There are three professions that beat their practitioners into a state of humility: farming, weather forecasting, and cybersecurity”

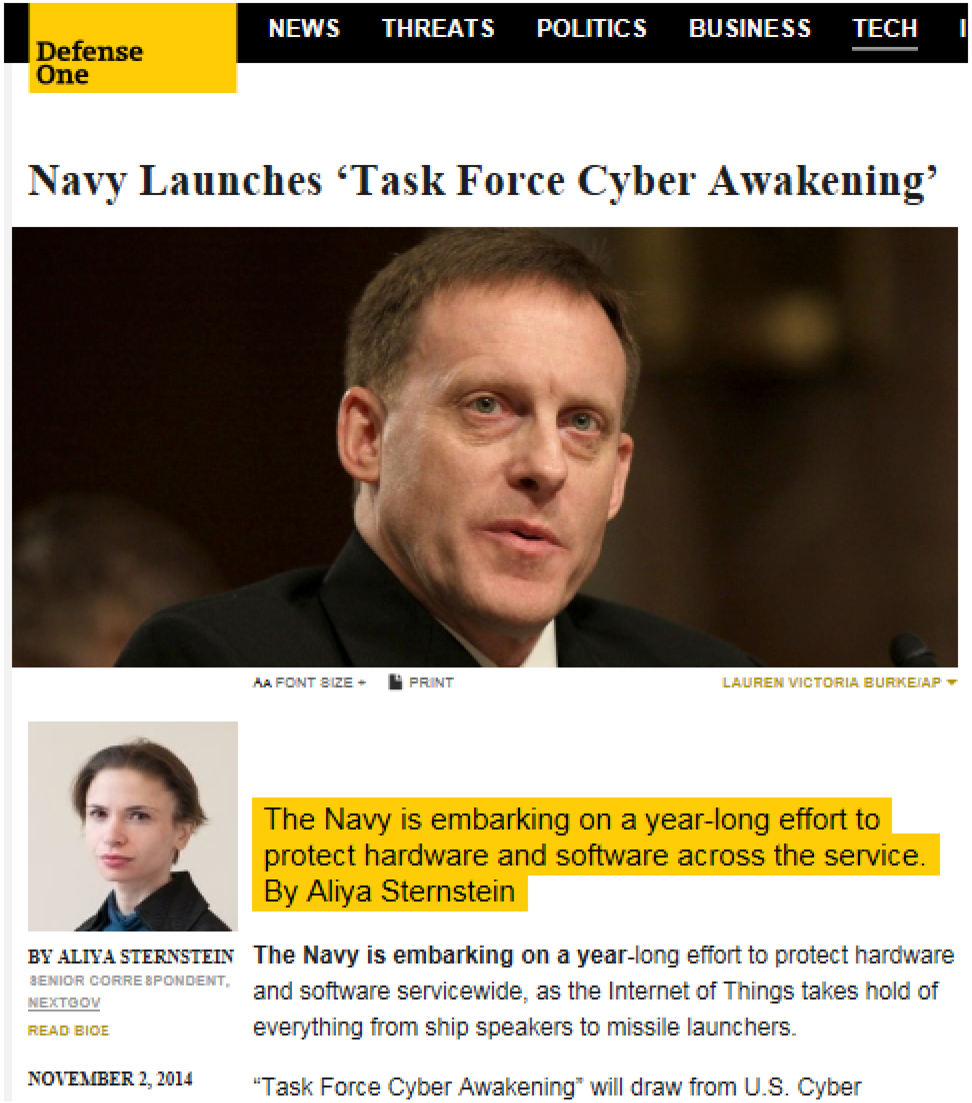
- Dan Geer

Challenging environments

Navy got woke

The 2014 Navy Cyber Awakening was the realization of a new risk calculus in cyber

Cybersecurity is a mission priority in the NAVSEA Campaign Plan



Navy Launches 'Task Force Cyber Awakening'

LAUREN VICTORIA BURKE/AP

The Navy is embarking on a year-long effort to protect hardware and software across the service. By Aliya Sternstein

BY ALIYA STERNSTEIN
SENIOR CORRESPONDENT, NEXTGOV
READ BIO

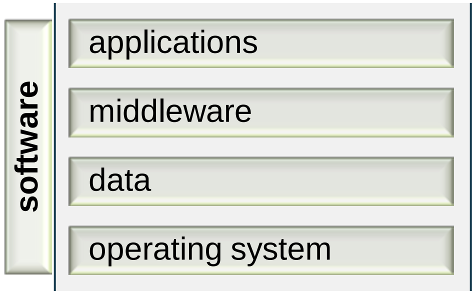
NOVEMBER 2, 2014

The Navy is embarking on a year-long effort to protect hardware and software servicewide, as the Internet of Things takes hold of everything from ship speakers to missile launchers.

"Task Force Cyber Awakening" will draw from U.S. Cyber

Full Scope Cyber

Many organizations hold a limited view of cyber, often limited to threats against software and networks.

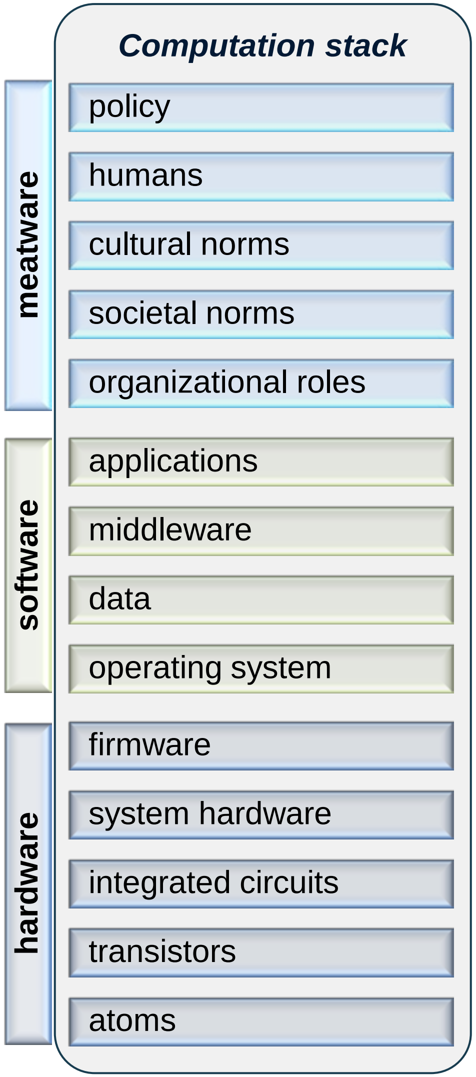


Full Scope Cyber

Many organizations hold a limited view of cyber, often limited to threats against software and networks.

Full-scope cyber recognizes the entirety of the computation stack as terrain that is contested (Talbot 2011).

Cyber terrain is entangled in the other warfighting domains.



Computation stack

meatware

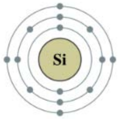
- policy
- humans
- cultural norms
- societal norms
- organizational roles

software

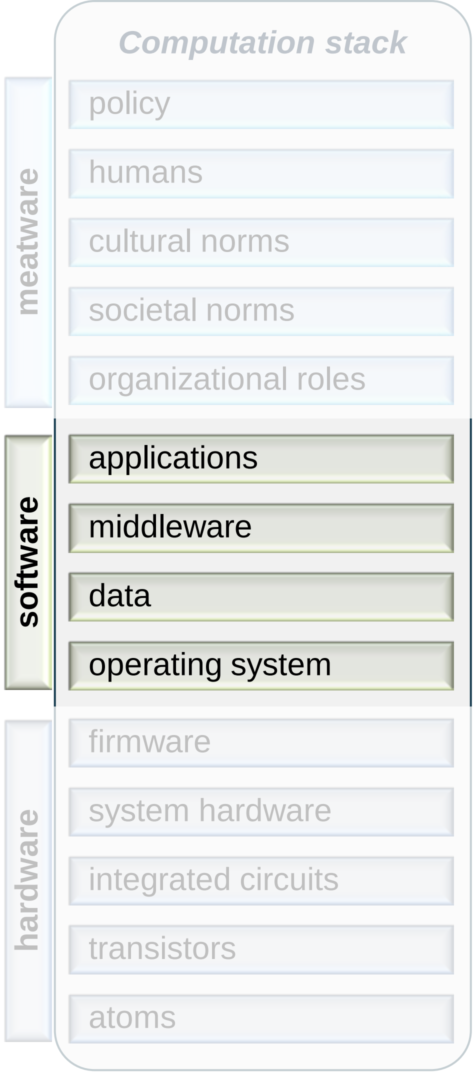
- applications
- middleware
- data
- operating system

hardware

- firmware
- system hardware
- integrated circuits
- transistors
- atoms



Full Scope Cyber Attacks

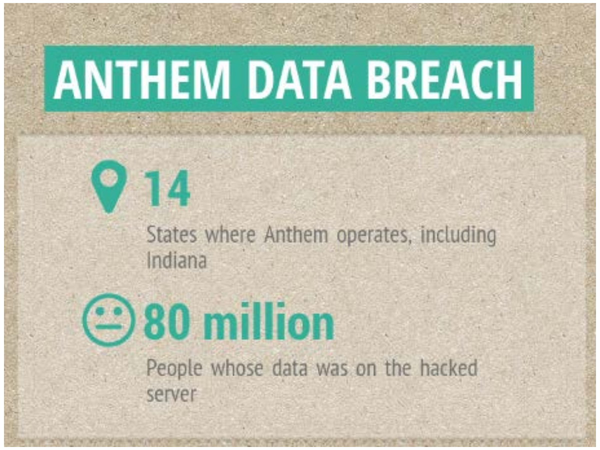


Computation stack

meatware
- policy
- humans
- cultural norms
- societal norms
- organizational roles

software
- applications
- middleware
- data
- operating system

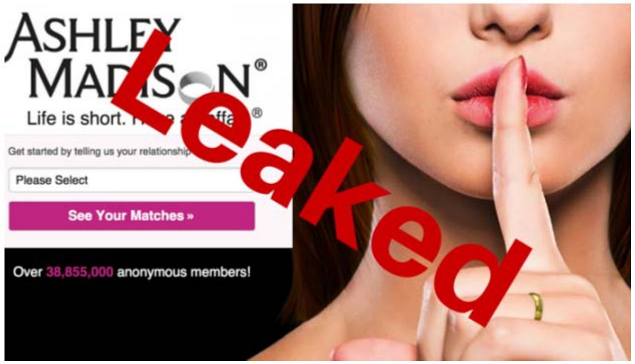
hardware
- firmware
- system hardware
- integrated circuits
- transistors
- atoms



ANTHEM DATA BREACH

14
States where Anthem operates, including Indiana

80 million
People whose data was on the hacked server



ASHLEY MADISON®

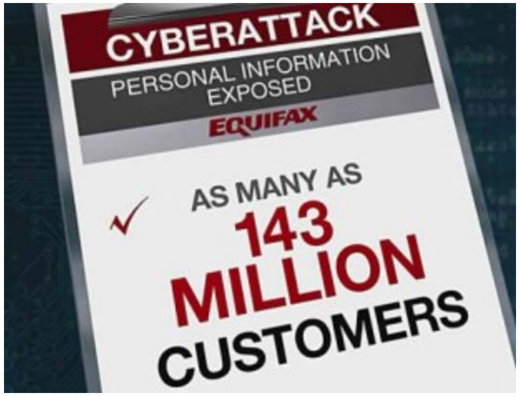
Life is short. Have an affair®

Get started by telling us your relationship

Please Select

See Your Matches »

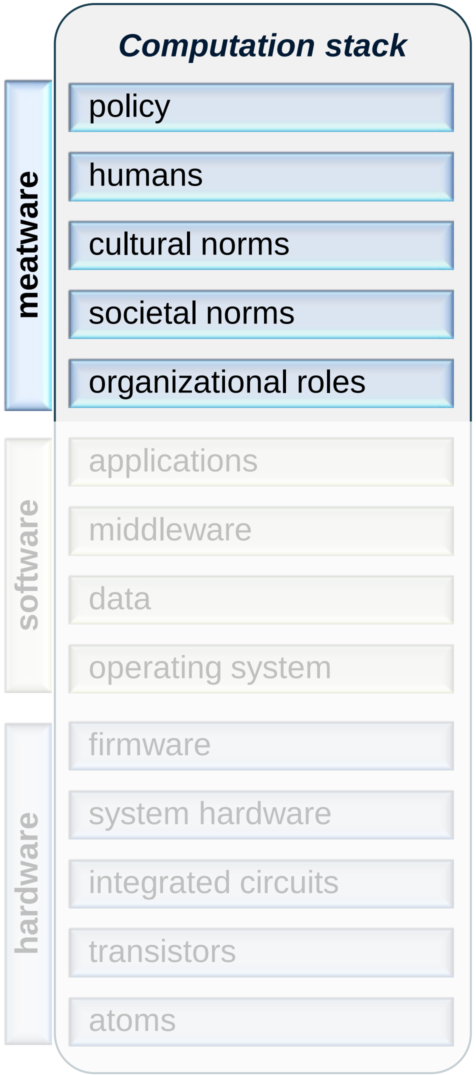
Over 38,855,000 anonymous members!



CYBERATTACK
PERSONAL INFORMATION EXPOSED
EQUIFAX

AS MANY AS
143 MILLION
CUSTOMERS

Full Scope Cyber Attacks

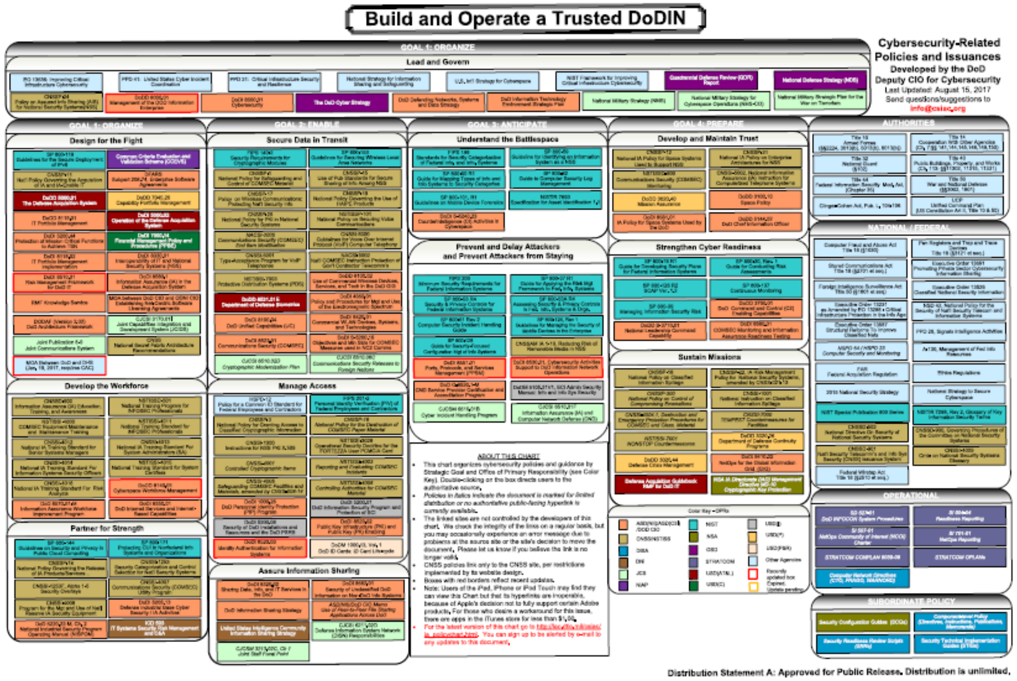


Computation stack

meatware
- policy
- humans
- cultural norms
- societal norms
- organizational roles

software
- applications
- middleware
- data
- operating system

hardware
- firmware
- system hardware
- integrated circuits
- transistors



Build and Operate a Trusted DoDIN

GOAL 1: ORGANIZE

Lead and Govern

EO 13636 Improving Critical Infrastructure Cybersecurity | PPD 41 United States Cyber Incident Coordination | PPD 21 Critical Infrastructure Security and Resilience | National Strategy for Information Sharing and Safeguarding | U.S. Int'l Strategy for Cyberspace | NIST Framework for Improving Critical Infrastructure Cybersecurity | Quadrennial Defense Review (QDR) Report | National Defense Strategy (NDS)

CNSSP 24 Policy on Assured Info Sharing (AIS) for National Security Systems (NSS) | DoDD 8000.01 Management of the DOD Information Enterprise | DoDI 8500.01 Cybersecurity | The DoD Cyber Strategy | DoD Defending Networks, Systems and Data Strategy | DoD Information Technology Environment Strategic Plan | National Military Strategy (NMS) | National Military Strategy for Cyberspace Operations (NMS-CO) | National Military Strategic Plan for the War on Terrorism

GOAL 1: ORGANIZE — Design for the Fight; Develop the Workforce; Partner for Strength

GOAL 2: ENABLE — Secure Data in Transit; Manage Access; Assure Information Sharing

GOAL 3: ANTICIPATE — Understand the Battlespace; Prevent and Delay Attackers and Prevent Attackers from Staying

GOAL 4: PREPARE — Develop and Maintain Trust; Strengthen Cyber Readiness; Sustain Missions

AUTHORITIES

NATIONAL / FEDERAL

OPERATIONAL

SUBORDINATE POLICY

Cybersecurity-Related Policies and Issuances Developed by the DoD Deputy CIO for Cybersecurity
Last Updated: August 15, 2017
Send questions/suggestions to
info@csiac.org

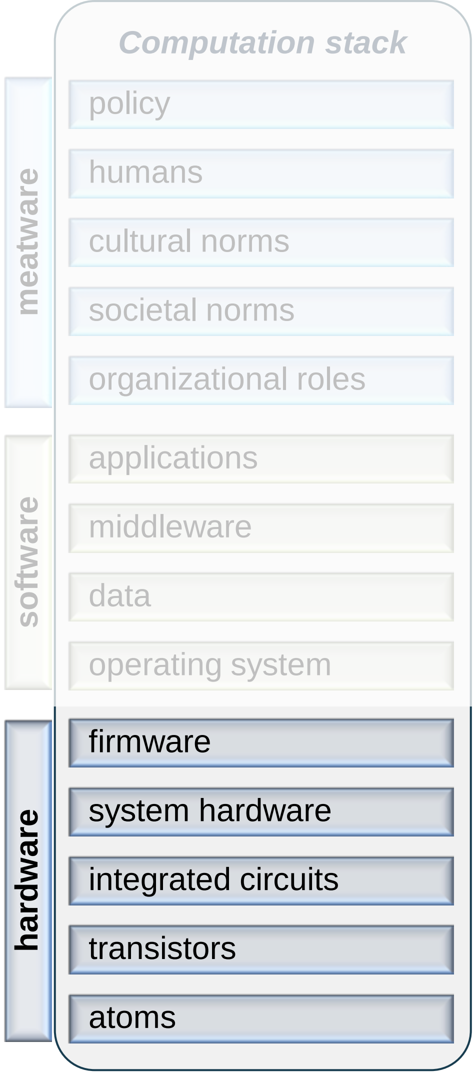
ABOUT THIS CHART
- This chart organizes cybersecurity policies and guidance by Strategic Goal and Office of Primary Responsibility (see Color Key). Double-clicking on the box directs users to the authoritative source.
- *Policies in italics indicate the document is marked for limited distribution or no authoritative public-facing hyperlink is currently available.*
- The linked sites are not controlled by the developers of this chart. We check the integrity of the links on a regular basis, but you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.
- CNSS policies link only to the CNSS site, per restrictions implemented by its website design.
- Boxes with red borders reflect recent updates.
- Note: Users of the iPad, iPhone or iPod Touch may find they can view this Chart but that its hyperlinks are inoperable, because of Apple's decision not to fully support certain Adobe products. For those who desire a workaround for this issue, there are apps in the iTunes store for less than $1.00.
- For the latest version of this chart go to http://iac.dtic.mil/csiac/ia_policychart.html. You can sign up to be alerted by e-mail to any updates to this document.

Color Key – OPRs

Distribution Statement A: Approved for Public Release. Distribution is unlimited.

Distribution Statement A – Approved for Public Release

Full Scope Cyber Attacks

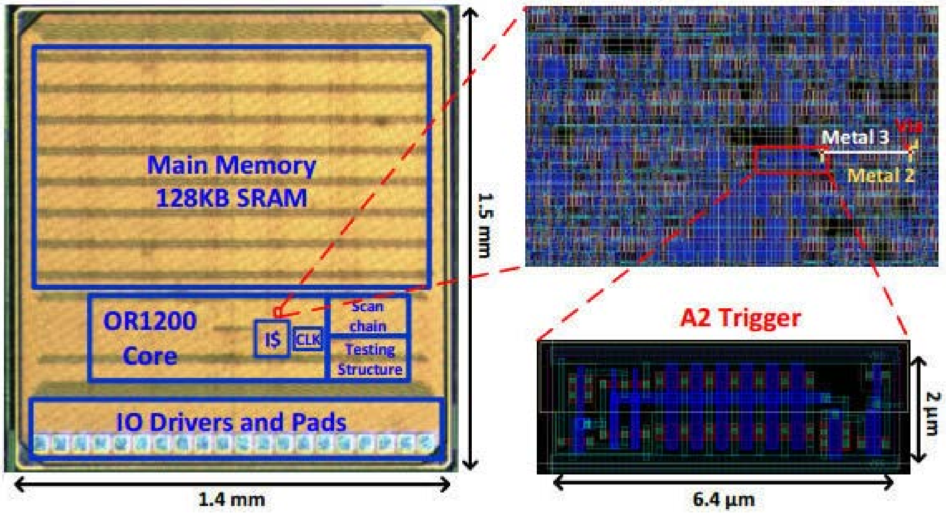


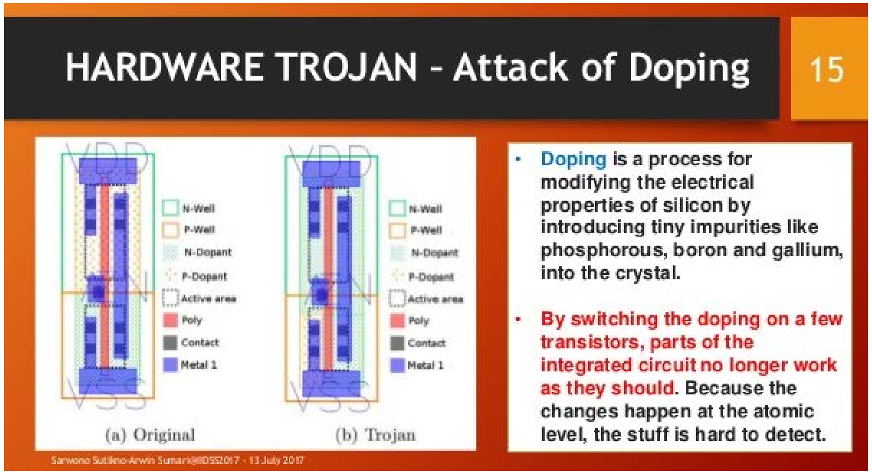
Computation stack

meatware
- policy
- humans
- cultural norms
- societal norms
- organizational roles

software
- applications
- middleware
- data
- operating system

hardware
- firmware
- system hardware
- integrated circuits
- transistors
- atoms





HARDWARE TROJAN - Attack of Doping

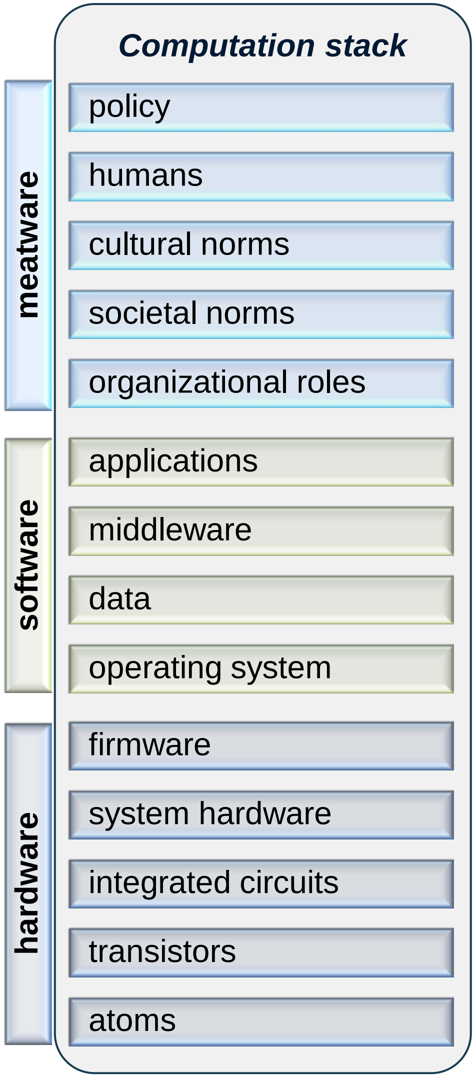
15

- **Doping** is a process for modifying the electrical properties of silicon by introducing tiny impurities like phosphorous, boron and gallium, into the crystal.
- **By switching the doping on a few transistors, parts of the integrated circuit no longer work as they should.** Because the changes happen at the atomic level, the stuff is hard to detect.

Sarwono Sutikno-Arwin Sumari@IDSS2017 - 13 July 2017

Distribution Statement A – Approved for Public Release

Full Scope Cybersecurity


Computation stack

meatware
- policy
- humans
- cultural norms
- societal norms
- organizational roles

software
- applications
- middleware
- data
- operating system

hardware
- firmware
- system hardware
- integrated circuits
- transistors
- atoms

Our adversaries are maneuvering over the cyber terrain to exploit weaknesses in systems and organizations.

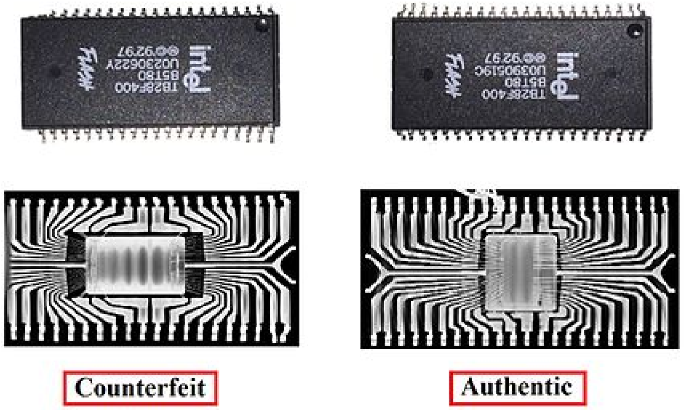
Critical systems require a full scope approach to cybersecurity.

Naval Surface Warfare Center Crane Division and other NAVSEA warfare center divisions have numerous efforts underway to develop capabilities where gaps currently exist.

Securing Hardware

Counterfeit microelectronics

http://cdn2.hubspot.net/hub/399101/file-1820289621-jpg/counterfeit_electronic_components-1.jpg

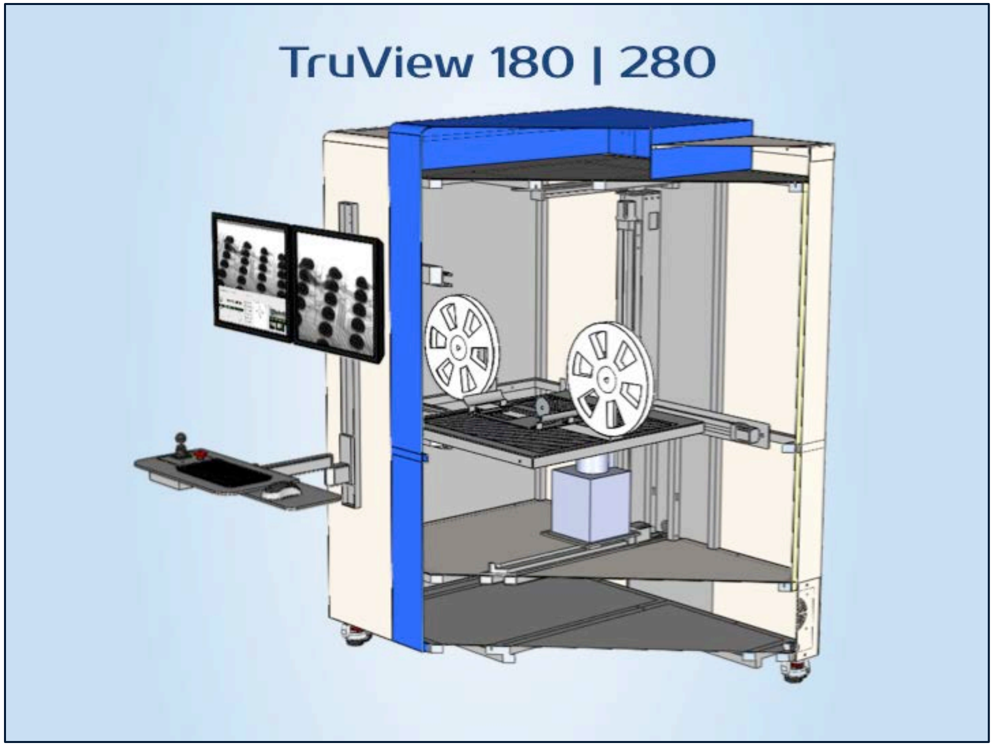


https://upload.wikimedia.org/wikipedia/commons/thumb/6/65/Using_X-ray_for_authentication_and_quality_control_in_electronics_industry.jpg/440px-Using_X-ray_for_authentication_and_quality_control_in_electronics_industry.jpg

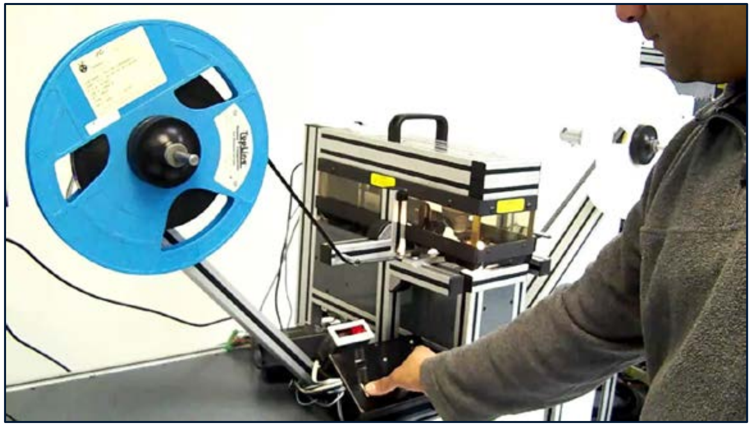
"Experts have estimated that as many as 15 percent of all spare and replacement semiconductors purchased by the Pentagon are counterfeit. Overall, we estimate that counterfeiting costs US-based semiconductor companies more than $7.5 billion per year, which translates into nearly 11,000 lost American jobs."

SIA President Brian Toohey SASC Hearing
November, 2011

Detecting counterfeits



http://creativeelectron.com/wp-content/uploads/2014/06/Slide3.png



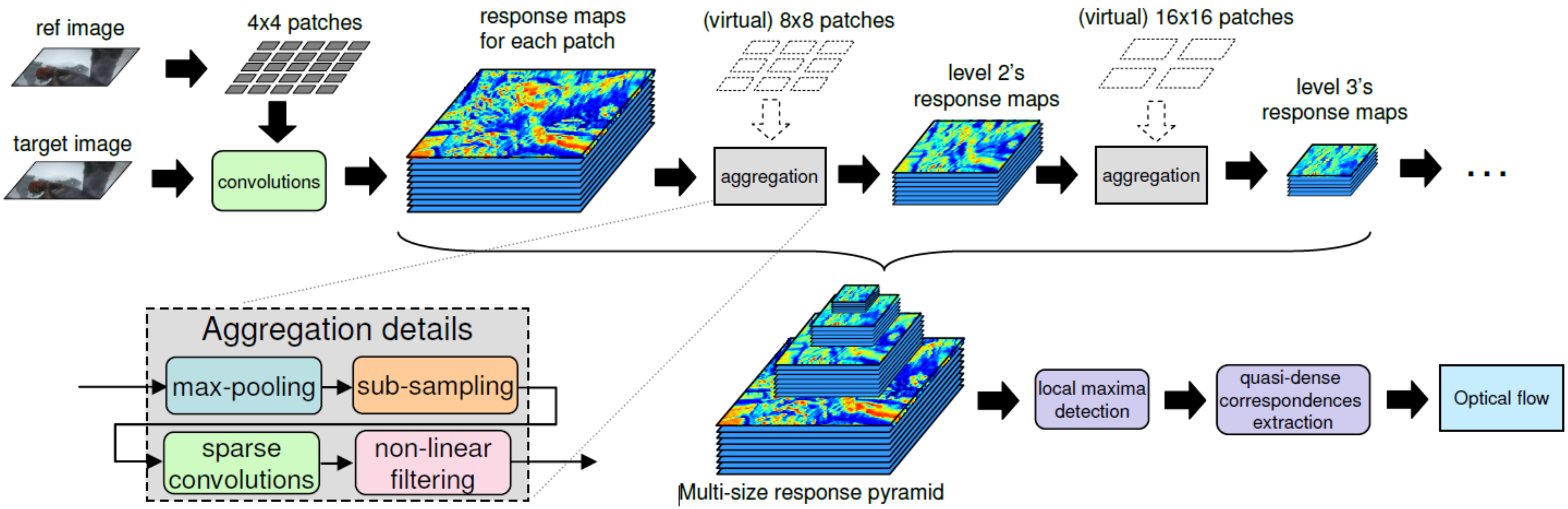
https://i.ytimg.com/vi/BjWpAIFgiMA/maxresdefault.jpg

The technology exists to photograph or x-ray components at scale (100% collection), but requires manual inspection

Addressing supply chain risks through computer vision

- 3-year Navy contract with Indiana University (Professor David Crandall, SICE)
- Computationally inferring hardware configurations
- Detecting counterfeit devices

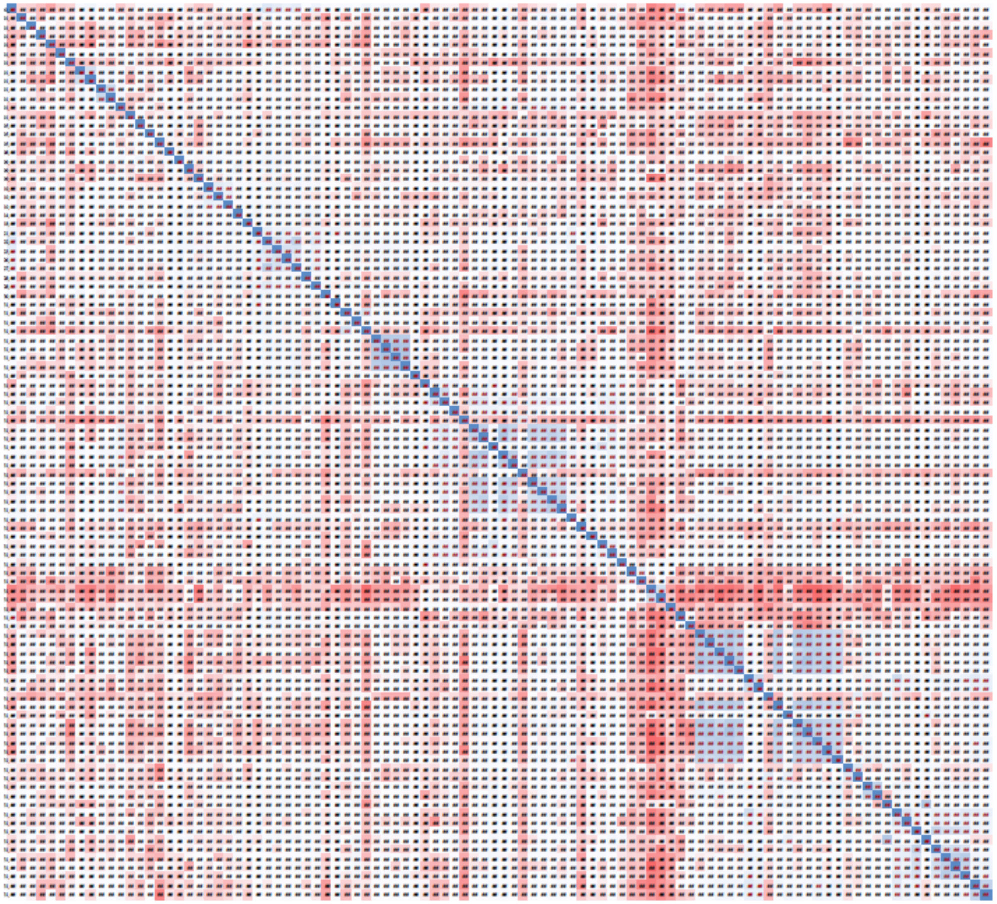
Enter deep learning

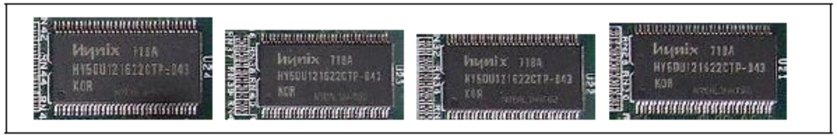


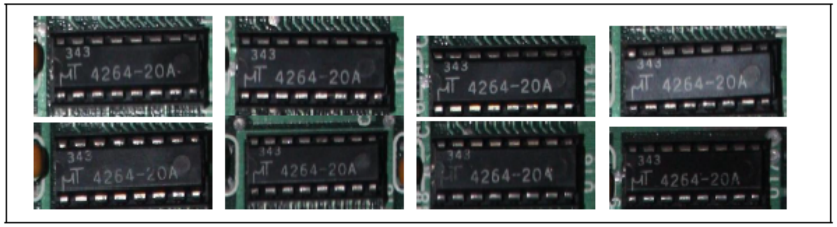
P. Weinzaepfel, J. Revau, Z. Harchaou, and C. Schmid. "Deepflow: Large displacement optical flow with deep matching." In the Proceedings of the International Conference on Computer Vision, 2013.

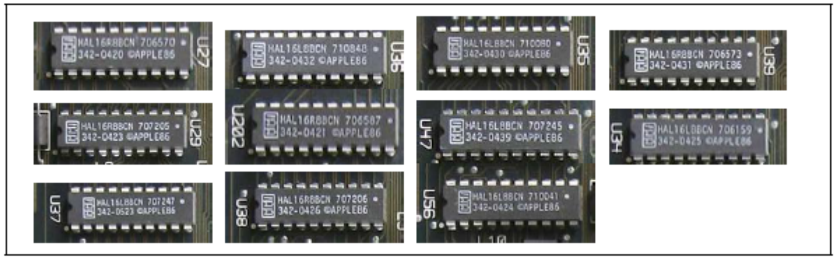
Distribution Statement A – Approved for Public Release

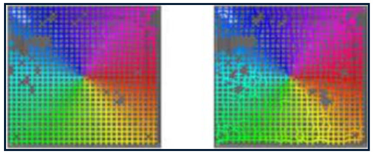
IU contribution – computer vision

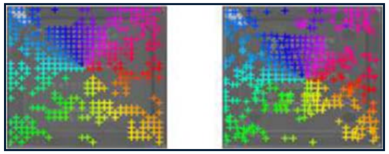












Zhenua Chen, Tingyi Wanyan, Ramya Rao, Benjamin Cutelli, James Sowinski, David Crandall, and **Robert Templeman**. “Addressing supply chain risks of microelectronic devices through computer vision.” Proceedings of the 47th Annual Applied Imagery Pattern Recognition (AIPR) Workshop, 2017.

Securing Meatware

protecting our systems from our users

Phishing

"Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials (APWG 2017, Lastdrager 2014)."

- World Wide Threat (APWG 2017)
  - Lowest infection rate: Sweden – 20.03%
  - Highest infection rate: China – 47.09%
- Affects governments, industry, and individuals
  - "IRS Paid $5.8 Billion in Fraudulent Refunds, Identity Theft Efforts Need Work (Forbes 2015)"
  - Average estimated cost per attack per employee is $188.4 (Ponemon Institute 2015)
    - 48% of that loss comes from productivity loss

Mitigating phishing

- Email filtering
- Deactivating hyperlinks
- Preventing drive-by downloads
- User literacy and training
  - But how well does training work?
  - Measuring educational outcomes is complex, programmatic, and context dependent (Rychetnik, Frommer, Hawe, and Shiell 2002)

Mitigating phishing

Measuring Phishing Education: A Protocol

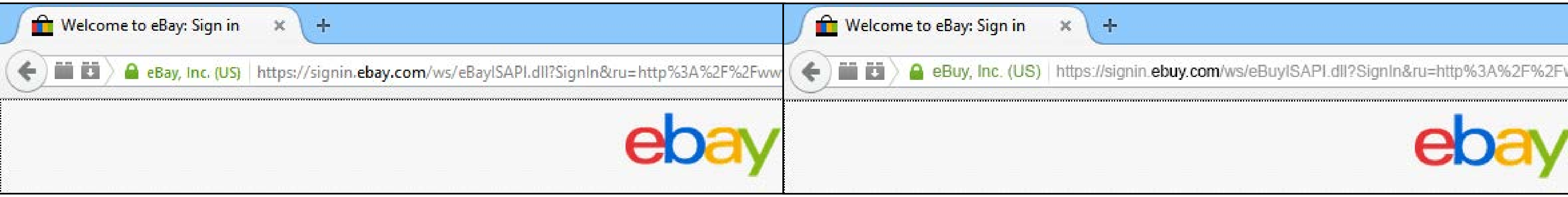
- Indiana University, Army, and Navy collaboration
- A study was performed
  - **Threat Detection Task**: Participants categorize web sites as malicious or benign by utilizing technical knowledge and familiarity with affected websites
  - **Methods**:

    Sample size: 172 participants; Data collected with Amazon’s Mturk

    Procedure: Visit 3 spoof and 3 no-spoof websites; decide whether to login or leave website by clicking on login or back buttons; bonus pay is dependent on response speed & accuracy
  - **Measures**: Survey data (Demographic, practical and technical security knowledge); accuracy scores based on logins to secure sites; and real-time measures of decision making (mouse tracking and response time)

    Area Under the Curve (AUC): area formed by connecting the mouse trajectory and the straight-line trajectory beginning at the start and finishing at the end points of the observed trajectory

    Sample Entropy: Variability in the trajectory measures the disorder of a time series


Welcome to eBay: Sign in
eBay, Inc. (US)
https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&ru=http%3A%2F%2Fww
ebay
Welcome to eBay: Sign in
eBuy, Inc. (US)
https://signin.ebuy.com/ws/eBuyISAPI.dll?SignIn&ru=http%3A%2F%2F
ebay

Securing Systems

A brief history of (DoD) Cyber

- TCSEC/CC
- DITSCAP
- DIACAP
- RMF (NIST-based)

In general, we use compliance regimes to authorize operation.

Policy and controls are often additive devolving to large checklists.

As-applied problems

1. **Expensive / Time-Consuming**. The SANS 2016 IT Security Spending Trends Survey reported regulatory compliance as a much more significant driver for spending than, e.g., reducing attack surface, improving visibility (detection), new, advanced threats and techniques, and improving incident response.
2. **Distracting**. Defenders' focus becomes compliance, not security.
3. **Inflexible**. Good security needs to imbue experts and decision makers with flexibility/discretion based on specific context.
4. **Stifles innovation**. Strict compliance regimes discourage any variance from "checking the box." There's a cost to tailoring with "compensating controls.

Credit: Craig Jackson, Indiana University Center for Applied Cybersecurity Research

Information Security Practice Principles

Comprehensivity (“*Am I seeing the whole field, playing the long game?*”)

Identify and account for all relevant systems, actors, and risks in the environment.

Opportunity (”*Am I taking advantage of my environment?*”)

Take advantage of the actor relationships, material resources, and strategic opportunities available in the environment.

Rigor (”*What is correct behavior, and how am I ensuring it?*”)

Specify the expected state, behavior, and evaluation and accountability criteria of the relevant systems and actors, then enforce the same.

Minimization (”*Can this be a smaller target?*”)

Minimize the size and quantity of what is to be protected, system complexity, and the number and proliferation of externally facing points of attack.

Compartmentation (“*Is this made of distinct parts with limited interfaces?*”)

Isolate and control system elements to allow only the accesses and functions essential for their intended purposes.

Fault Tolerance (”*What happens if this fails?*”)

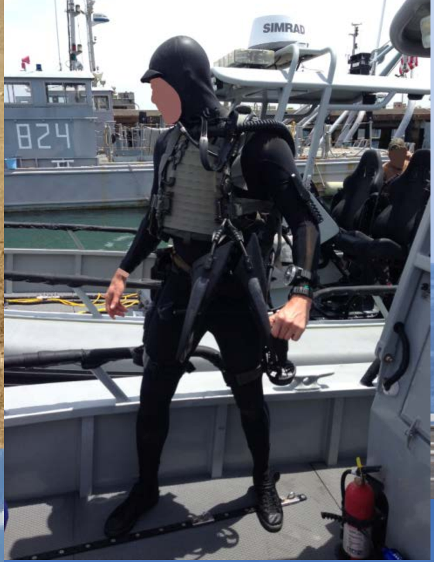
Anticipate and address the potential compromise of system elements and the failure of security controls.

Proportionality (”*Is this worth it?*”)

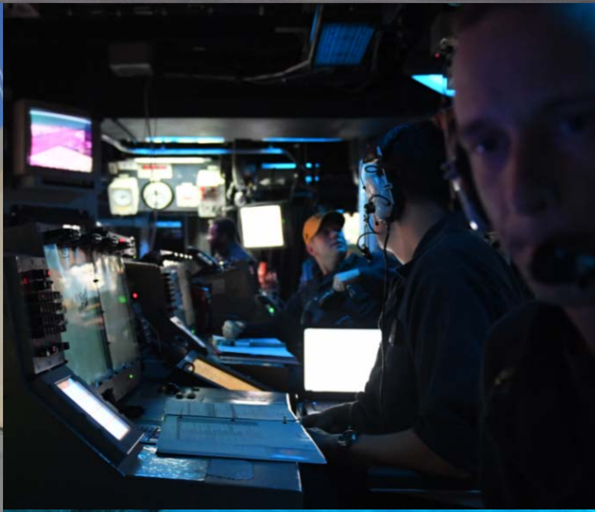
Tailor security strategies to the magnitude of the risks, accounting for the practical constraints imposed by the mission and the environment.

Summary

- We must adopt a full scope cybersecurity approach for our critical systems
- There are great improvements to be made in the areas of hardware assurance and behavioral cybersecurity
- NSWC Crane is working actively with government, industry, and academia to expand our Navy’s advantage by securing national defense systems


SIMRAD
824

AJ



MAERSK
MAERSK
MAERSK
MAERSK SARNIA