SENTAR

INNOVATE.
BUILD.
SECURE.

MISSION CRITICAL
ASSETS

Healthcare as a Cyber-Contested Environment

National Cyber Summit 2019 Lightning Round Presentation

Jeremy B. Blevins, CISSP, CEH

Cybersecurity Analyst

5 June 2019

SENTAR

Jeremy B. Blevins

- Experience
  - 20+ years Information Technology
  - 10+ years Cybersecurity
  - 6 years Army National Guard (Radio/COMSEC Repair)
- Education
  - Bachelor of Business Administration (Faulkner University)
  - Master of Science in Management (Embry-Riddle Aeronautical University)
  - Master of Professional Studies in Cyber Policy Risk Analysis (Utica College)
- Certifications
  - Security+, CompTIA Advanced Security Practitioner (CompTIA)
  - Certified Ethical Hacker (EC Council)
  - Certified Information Systems Security Professional (ISC^2)
- Affiliations
  - Calhoun Community College: Adjunct Instructor
  - InfraGard Huntsville Members Alliance: President
  - North Alabama Chapter Information Systems Security Association: Senior Member

SENTAR

Agenda

- Cyber is a Contested Domain of Warfare
- The Military Health System
- Healthcare is a Cyber-Contested Environment
- Defend Healthcare Systems
- Summary

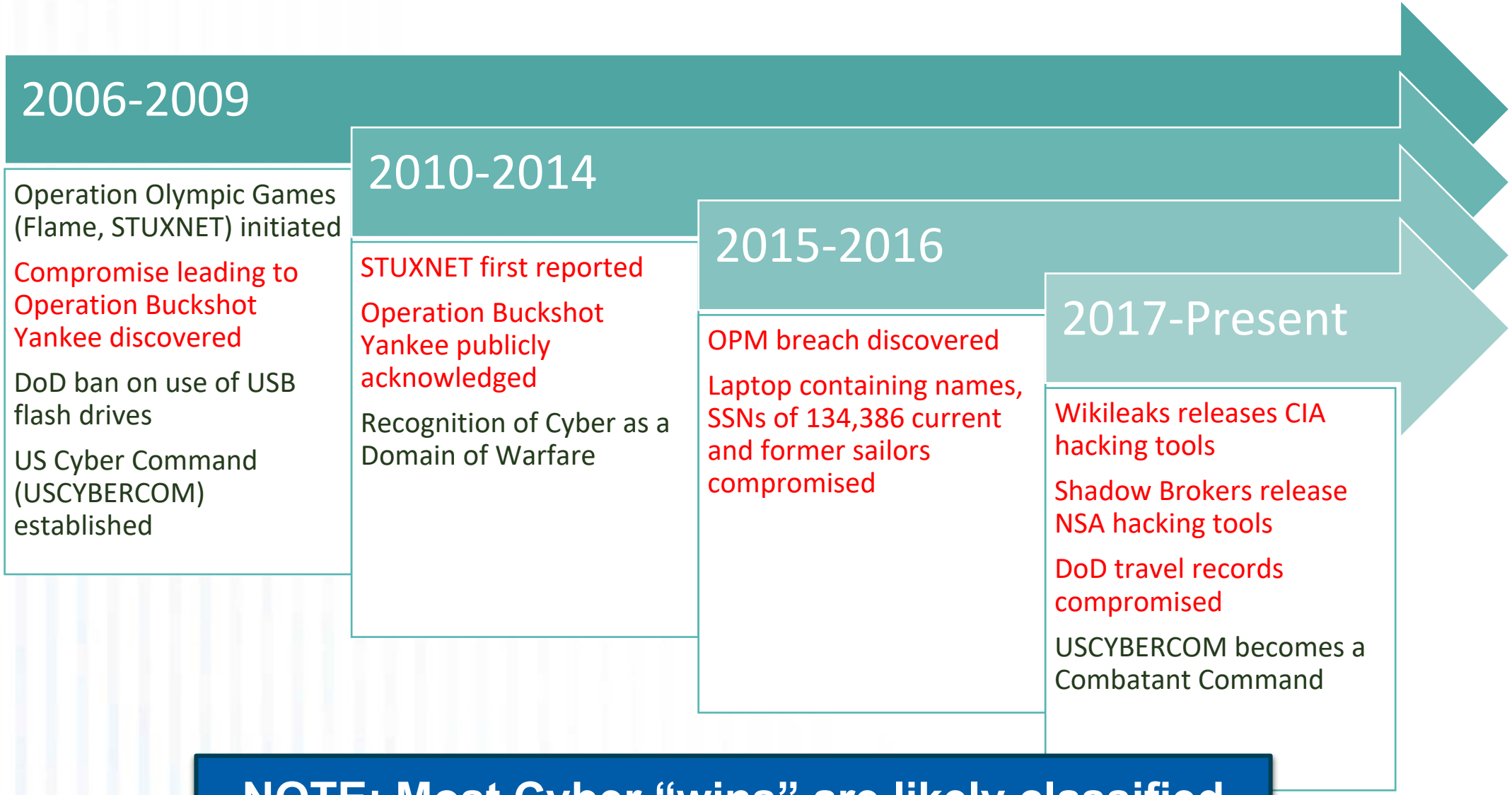
Caveat Emptor: This presentation is given from a defense-centric perspective, but wholly applicable to non-defense health systems.

SENTAR

"For decades the United States has enjoyed ***uncontested or dominant superiority*** *in every operating domain. We could generally deploy our forces when we wanted, assemble them where we wanted, and operate how we wanted. Today, every domain is contested—air, land, sea, space, and* ***cyberspace****."*

-2018 National Defense Strategy https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Gains and Losses on the Cyber Battlefront



NOTE: Most Cyber "wins" are likely classified

SENTAR

"We can't operate with the mindset that everything has to be about keeping them out"

-Rich Barger, CIO, ThreatConnect

- Personal information of **22 million** current and former federal employees compromised
- Each of those people have to list contact information for family & references as part of their SF86 application

https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/
https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

SENTAR

"There is hardly a military mission that doesn't incorporate cyber capabilities, and that is both a great strength of the U.S. military and a possible weakness."

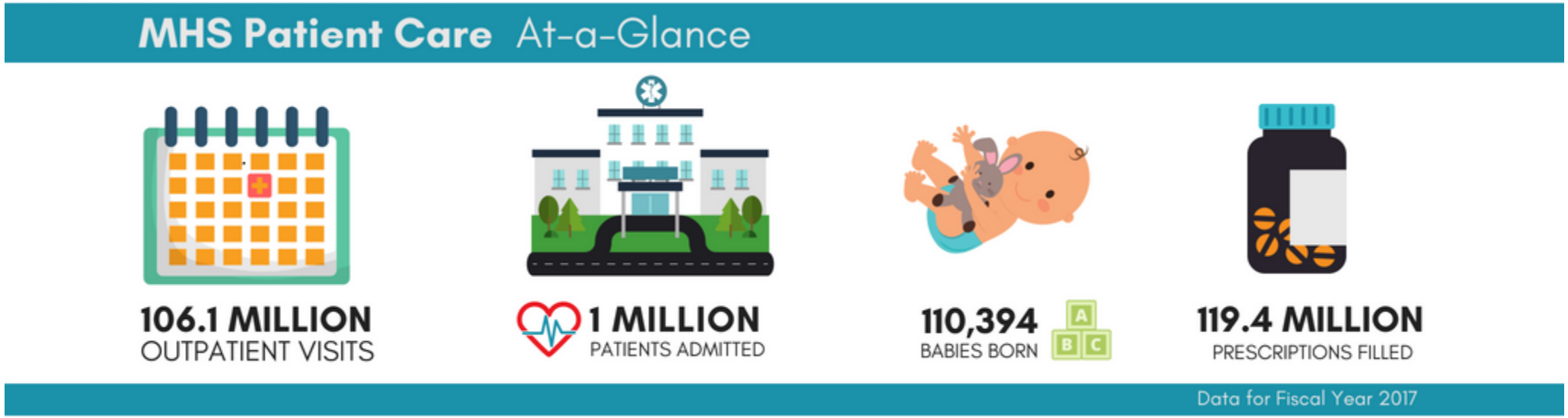
-Maj. Gen. Charles L. Moore Jr. (USAF)

https://dod.defense.gov/News/Article/Article/810009/us-militarys-cyber-capabilities-provide-strength-challenges-official-says/

SENTAR

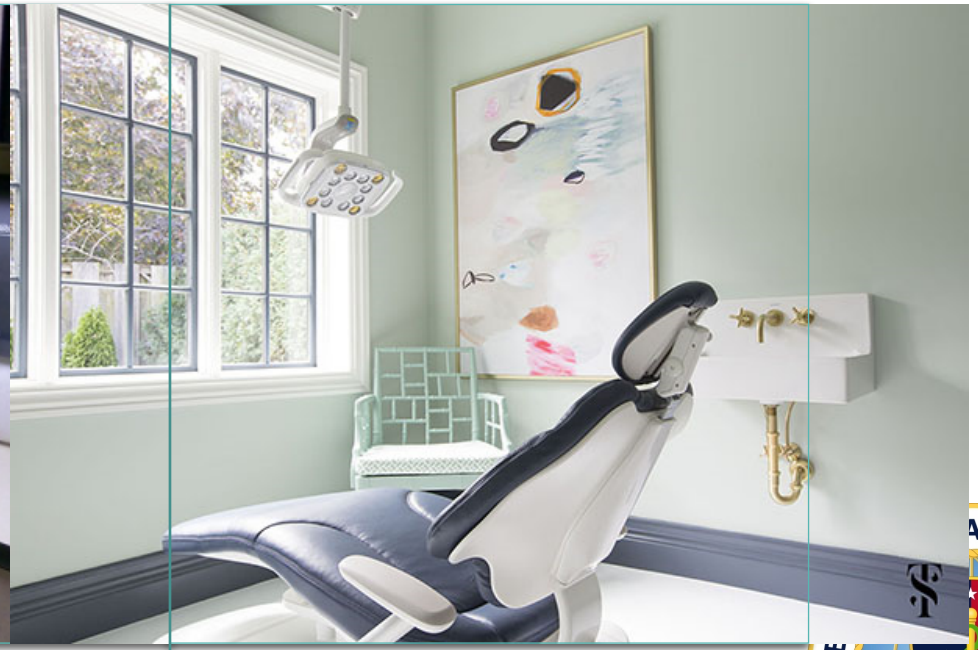
This Includes the Military Health System

Military Health System



- 1.4 Million Active Duty
- 331,000 Reserve Components
- 9.4 Million Active Duty, Military Retirees & Families

https://www.health.mil/About-MHS
https://www.health.mil/About-MHS/MHS-Elements



54
Hospitals

377
Medical
Clinics

270
Dental
Facilities

https://www.health.mil/About-MHS

SENTAR

Advances Post-GWOT

Advanced Prosthetics

Identifying & Treating Traumatic Brain Injury

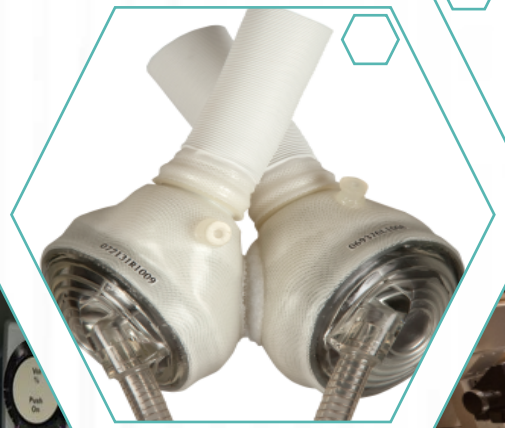
Regenerative Medicine

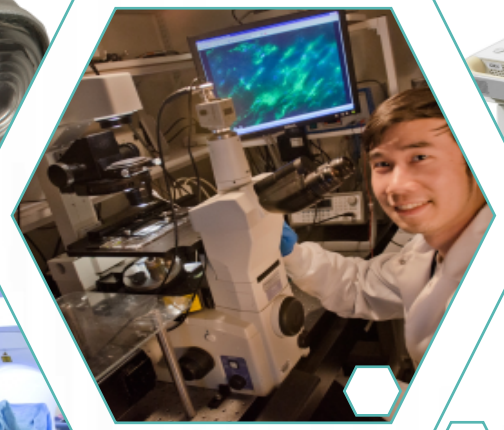
Medical Devices

INNOVATE. BUILD. SECURE.

https://taskandpurpose.com/10-medical-advancements-from-the-iraq-and-afghanistan-wars

SENTAR





INNOVATE. BUILD. SECURE.

SENTAR

Both Healthcare Systems and Medical Devices are Potential Targets for Cyber Attacks

INNOVATE. BUILD. SECURE.

This Photo by Unknown Author is licensed under CC BY-ND

SENTAR

MHS GENESIS [Health Record System] is not survivable in a cyber-contested environment.

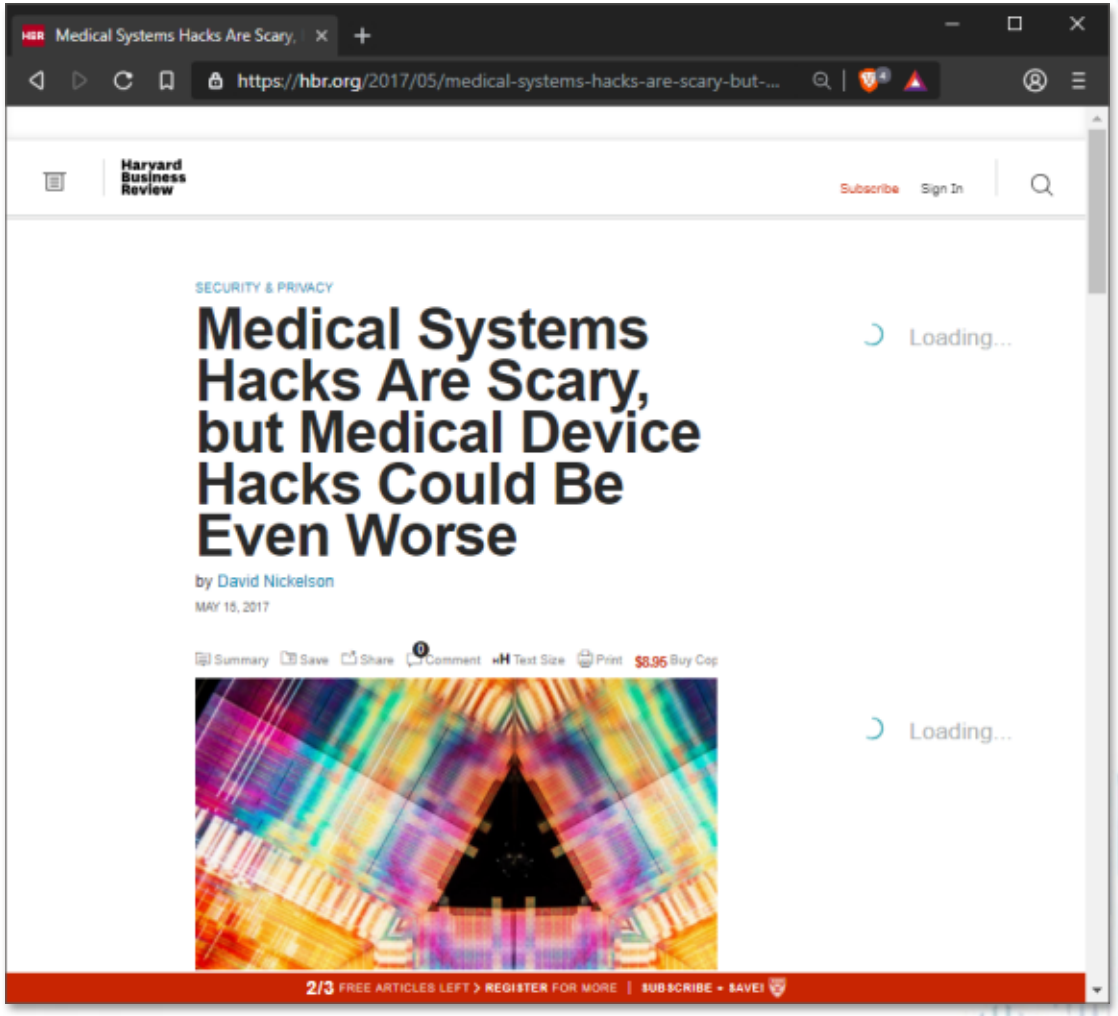
JITC and the SPAWAR Red Team successfully executed three cybersecurity attacks against the system as an insider, near-sider, and outsider.

- https://www.dote.osd.mil/pub/reports/FY2018/pdf/dod/2018dhmsm.pdf

https://fcw.com/articles/2019/02/04/mhs-genesis-cyber-probe.aspx

SENTAR

Researchers in Belgium and the UK have demonstrated that it's possible to transmit life-threatening (if not fatal) signals to implanted medical devices such as pacemakers, defibrillators, and insulin pumps.



https://hbr.org/2017/05/medical-systems-hacks-are-scary-but-medical-device-hacks-could-be-even-worse

SENTAR

That's pretty bad!

*We **must** defend healthcare systems.*

SENTAR

How Do We Defend Healthcare Systems?

- Device manufacturers must harden devices and provide updates for the full lifecycle
- Healthcare systems must be secured like other critical assets
- The Risk Management Framework must be applied
- Trained Cyber professionals must be staffed

What are we doing about it NOW?

- All DoD medical facilities are being migrated to the DHA Medical Community of Interest (Med-COI) network enclave
- Naval Information Warfare Center (NIWC) serves as the Cyber Security Service Provider (CSSP) for DHA
- Systems and medical devices are being secured in accordance with RMF

Sentar is on the forefront of this effort

- 2014 - Sentar Awarded Over $31 Million in Multiple Task Orders Under SPAWARSYSCEN Atlantic ICO Preferred Pillar Contract
- 2016 - Sentar to Provide Information Assurance, Cyber Security (IA/CS) And Cyber Services Under Sentar's SPAWAR Prime Contract
- 2018 - Sentar Awarded Fedhealthit Innovation Award Winner for its Work on the Defense Health Agency (DHA) Mitigation and Remediation Support (MARS) Team
- 2019 - Sentar Proudly Announces it has been Selected by FedHealthIT as an Innovation Award Winner for its Work on hhe Defense Health Agency (DHA) Cybersecurity Operations Center (CYOC)

SENTAR

Summary

- We must recognize that healthcare is a cyber-contested environment
- We must have trained Cyber professionals in place to defend
- We must win because of the kinetic, real-world impact of failing

The National Cyber Summit's Best Kept Secret

Hacker Prohibition Night

Straight to Ale Speakeasy at Campus 805

2610 Clinton Ave., Huntsville, AL 35805

Wednesday, June 5th, 5:30 - 8:30 PM

SENTAR

mission multiplier