#RSAC

RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

MATTERS NOW

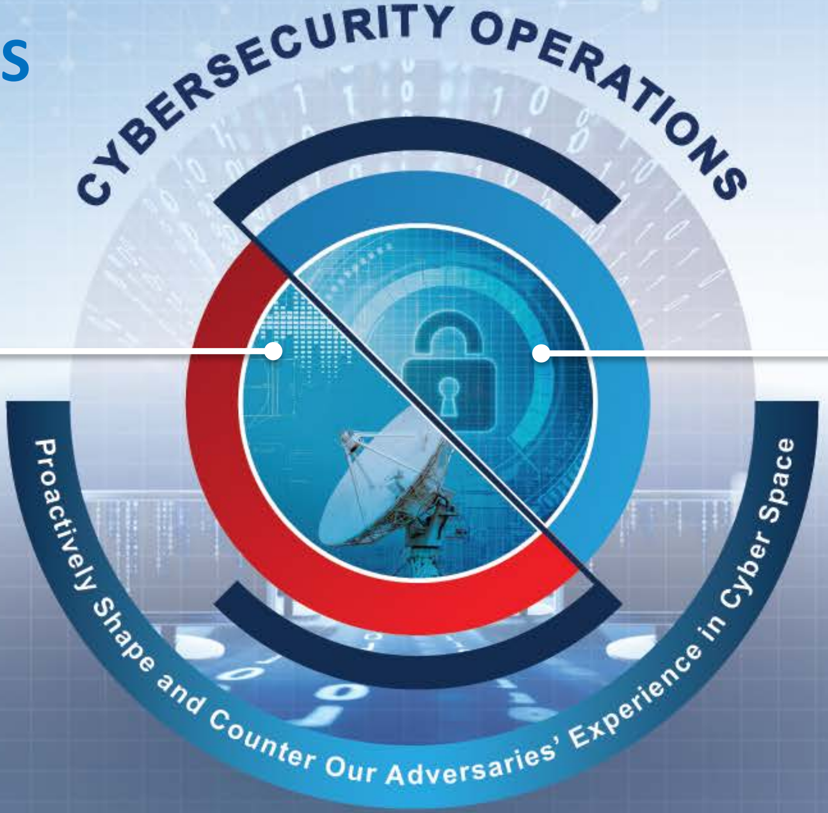
SESSION ID: AIR-T08

INSIGHTS FROM NSA'S CYBERSECURITY THREAT OPERATIONS CENTER

Dave Hogue

Technical Director
National Security Agency's Cybersecurity Threat Operations Center

NEXUS OF
NSA AUTHORITIES


CYBERSECURITY OPERATIONS
Proactively Shape and Counter Our Adversaries' Experience in Cyber Space

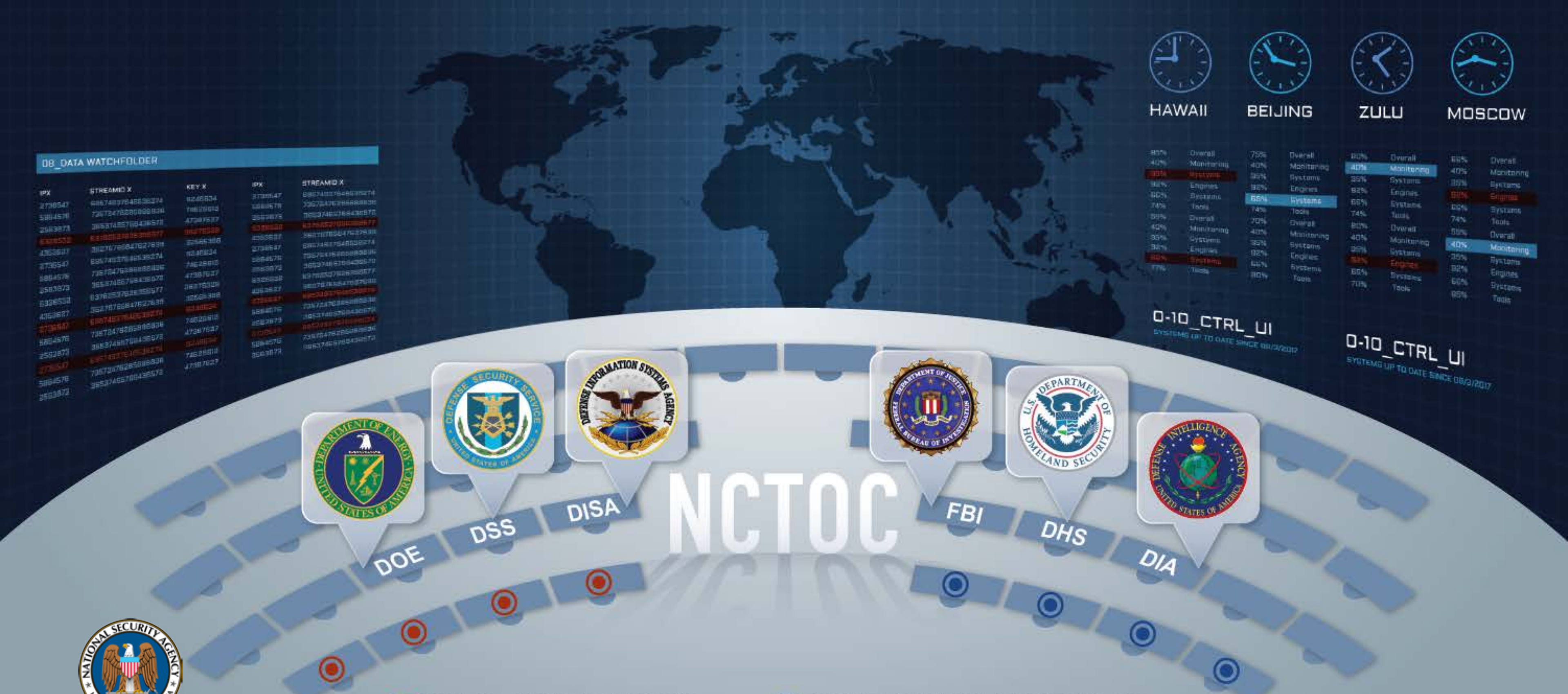
SIGNALS INTELLIGENCE

Intercept and exploit foreign signals

INFORMATION ASSURANCE

Defend National Security Systems

NSA CYBERSECURITY THREAT OPERATIONS CENTER



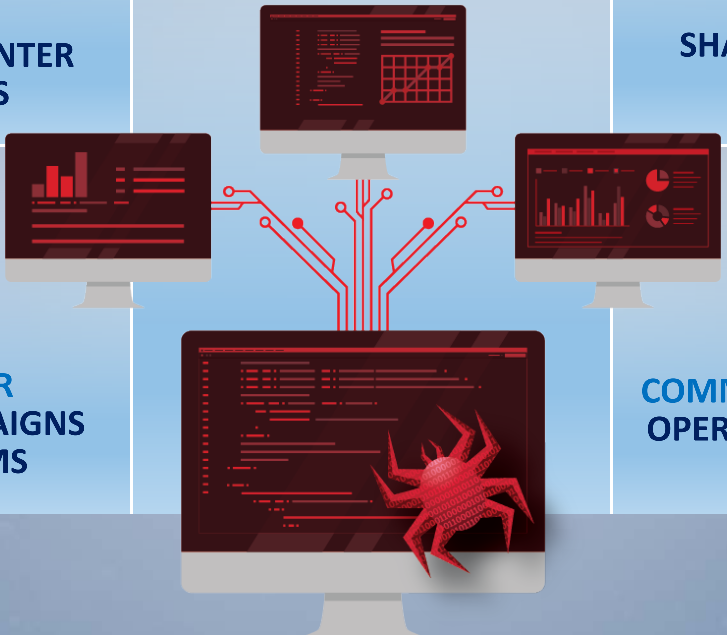
◉ CYBER THREAT ANALYSTS ◉ COUNTERMEASURE ENGINEERS

NSA SECURITY OPERATIONS CENTER FUNCTIONS

DISCOVER,
PURSUE, AND COUNTER CYBER THREATS

MANAGE
CYBERSECURITY SYSTEMS AND CAPABILITIES

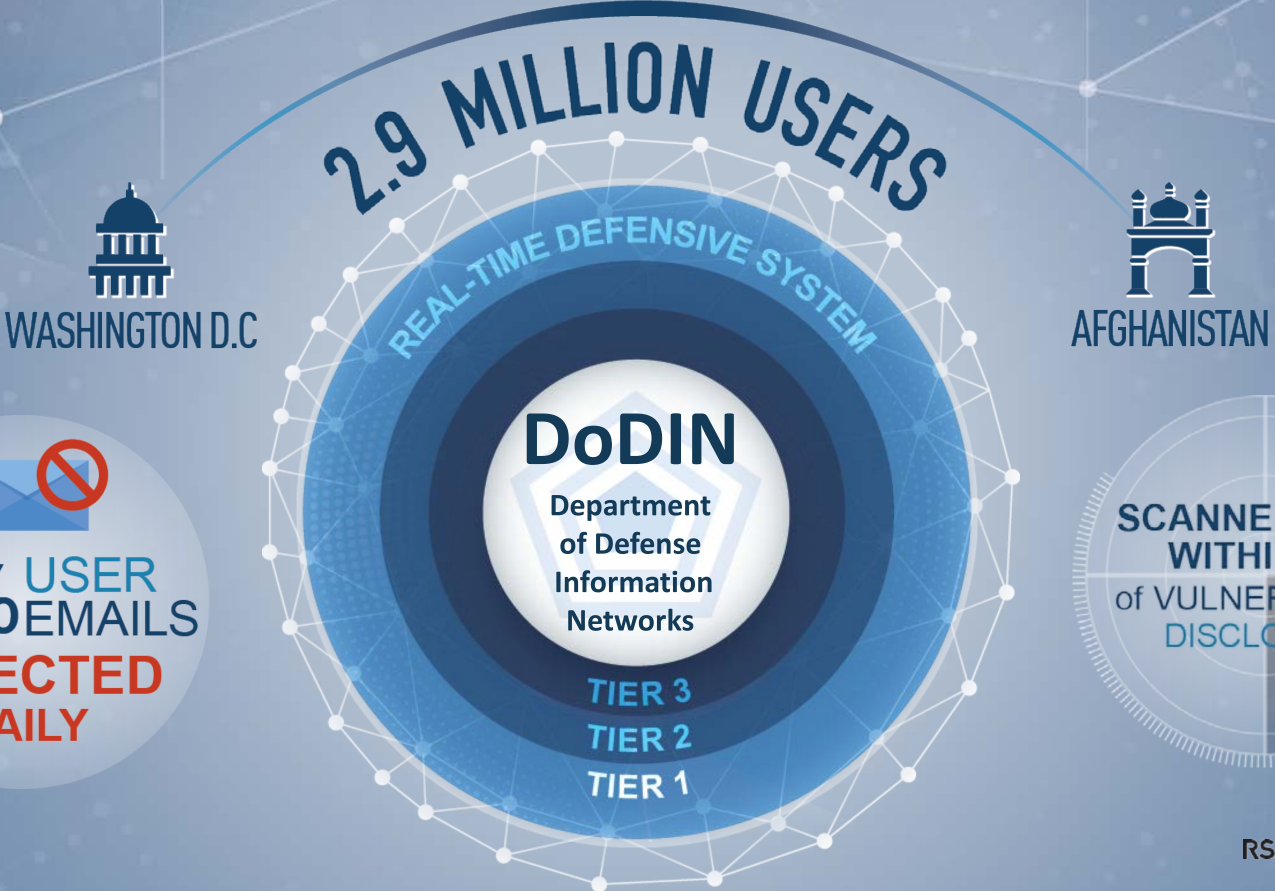
PROMOTE
SHARED SITUATIONAL AWARENESS



DISRUPT CYBER
ADVERSARY CAMPAIGNS AND PROGRAMS

COMMAND AND CONTROL
OPERATIONS AND EVENTS

NSA NETWORK DEFENSE



2.9 MILLION USERS

WASHINGTON D.C

AFGHANISTAN

REAL-TIME DEFENSIVE SYSTEM

DoDIN

Department of Defense Information Networks

TIER 3

TIER 2

TIER 1

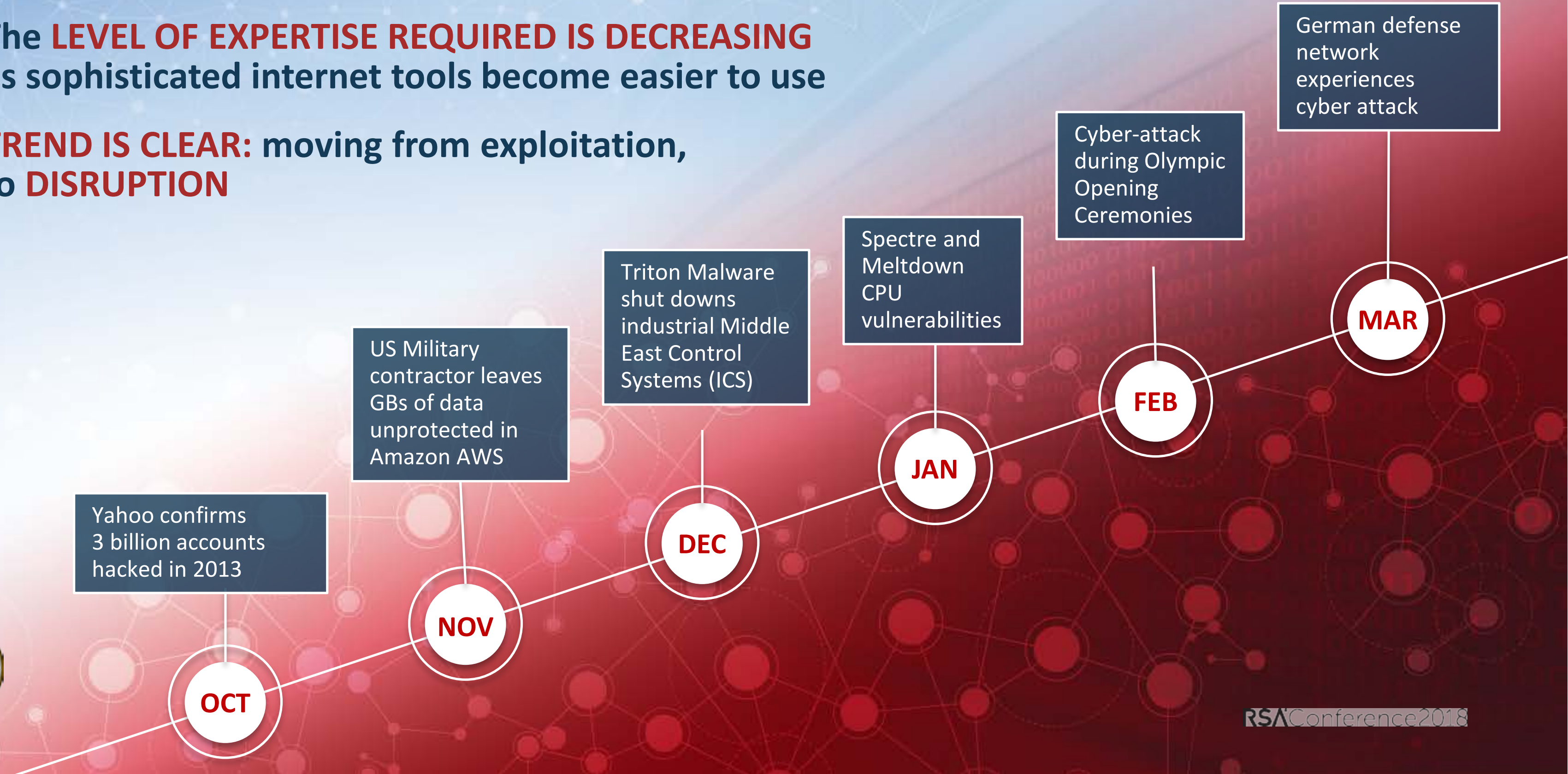
36 MILLION EMAILS EACH DAY

85% USER EMAILS REJECTED DAILY

SCANNED WITHIN 24 HOURS of VULNERABILITY DISCLOSURE

2018 ESCALATING CYBER THREATS

- Cyber activity continues to become **MORE SOPHISTICATED**
- The **LEVEL OF EXPERTISE REQUIRED IS DECREASING** as sophisticated internet tools become easier to use
- **TREND IS CLEAR:** moving from exploitation, to **DISRUPTION**



OCT: Yahoo confirms 3 billion accounts hacked in 2013

NOV: US Military contractor leaves GBs of data unprotected in Amazon AWS

DEC: Triton Malware shut downs industrial Middle East Control Systems (ICS)

JAN: Spectre and Meltdown CPU vulnerabilities

FEB: Cyber-attack during Olympic Opening Ceremonies

MAR: German defense network experiences cyber attack

Fundamental Shifts in Nation State Activity

Geopolitical events have drastically altered the operating profile of sophisticated Nation state adversaries

RUSSIA **Their aggressive cyber behavior** resembles the show of force we have seen displayed **in their geopolitical actions**

IRAN **Remains very sensitive to international political events,** which can influence target selection **and level of malicious activity**

DPRK Has always viewed cyber as an effective tool of state power, **every conflict will have a cyber dimension**

CHINA **Continues to use cyber espionage** as a prime enabler to acquire transformative technologies, as **part of their long-term plan to be a global superpower**

NSA CYBER THREAT | CURRENT TRENDS

FREQUENCY OF AGGRESSIVE & ESCALATORY DISRUPTIVE CYBER BEHAVIOR

In the last year alone, multiple data destruction and ransomware campaigns

USERNAME: Administrator

PASSWORD: •••••••

CONTINUOUS TECHNIQUES TO OVERCOME DEFENSIVE MEASURES

‘Legitimate’ credentials or services rather than relying on traditional malware

ASYMMETRIC DAMAGE INFLICTED

Correlations exist between major geopolitical events and malicious cyber activity

A RETURN TO CYBER DEFENSE BASICS

NSA has not responded to an intrusion using a 0-day exploit in the last 24 months

90% of cyber incidents due to human error

93% OF 2017

INCIDENTS WERE PREVENTABLE WITH

BEST PRACTICES

WHAT'S OLD IS NEW AGAIN

With 'Outdated' Defense Practices such as:

1. Application White-Listing
2. Role based access controls
3. 2-Factor Authentication

HOW CAN WE BE MORE PREDICTIVE AND PREVENTATIVE?

EFFECTIVE PARNTERSHIPS

INNOVATIVE APPROACHES

IMPLEMENTING STRONG DEFENSE POSTURE

TO DEVELOP THE FUTURE OF CYBERSECURITY WORKFORCE

INNOVATION COMES IN MANY FORMS

INNOVATIVE APPROACHES

UK's National Cyber Security Center (NCSC) establishes a singular focal point for cyber and demonstrates that 'simple things, done at scale, can have a positive and measurable effect.'

POLICY

Artificial Intelligence / Machine Learning – parses vast quantities of data to enable NSA Operations Teams to form a predictive and preventive defensive posture, rather than waiting for alerts to fire.

TECHINCAL

Bug Bounties – DoD leverages talent and expertise of the broader cyber community ; 'Hack the Air Force' served as economical and proactive means of eliminating previously undiagnosed flaws

COMMUNITY EXPERTISE

NSA recruits from many disciplines. Data and information may become so highly automated that we will need great thinkers to ask questions of data that computers cannot automate

PEOPLE

NSA TOP 5 ACTIONABLE SOC PRINCIPLES

1. INSTITUTE **WELL-MANAGED** & **DEFENDABLE** PERIMETERS & GATEWAYS

2. ENSURE **VISIBILITY & CONTINUOUS MONITORING OF THE NETWORK** TO INCLUDE TRAFFIC & ENDPOINTS

3. **HARDEN NETWORKS, ENDPOINTS, & SERVICES** TO BEST PRACTICES

4. USE **COMPREHENSIVE & AUTOMATED** THREAT INTELLIGENCE SOURCES

5. **CREATE & FOSTER** A CULTURE OF **CURIOSITY** & EMBRACE **INNOVATIVE APPROACHES**

Top 5 Actionable SOC Principles from NSA

- **#1 Establish a defendable perimeter**
  - Route traffic through a very finite number of Internet-facing gateways
  - Reduce the potential attack surface an adversary can potentially exploit
  - Utilize a combination of IOCs and behavioral/heuristics across host and network-based platforms to see and act upon cyber activity in real time
- **#2 Ensure visibility across the network**
  - Must encompass all levels of the network to include gateway, midpoint, and endpoints
  - Pinpoint and isolate actual victims within minutes, not hours
  - Architect solutions for visibility on sophisticated threats blending into legitimate and encrypted activity

Top 5 Actionable SOC Principles from NSA

#3 Harden to best practices

- Accelerate software and hardware updates ; remove applications/protocols that are no longer vendor-supported
- Reminder – NSA has not responded to an intrusion that used a zero-day in over 24 months

#4 Use comprehensive threat intelligence and machine learning

- Tailor to the network environment – i.e. DoD may encounter different cyber threat activity than a hospital network
- Less can be more – use data science and machine learning to reduce SOC alert fatigue
- Reserve capacity to proactively hunt for undetected threat activity

Top 5 Actionable SOC Principles from NSA

#5 Create a culture of curiosity

- Seek a holistic understanding of threat activity – avoid basing success on how fast tickets are closed
- Think like the adversary and preemptively position defensive actions
- Rotate SOC positions and functions – invigorate new advances by challenging and disrupting the status quo

NSA's Top 5 Security Operations Center (SOC) Principles Link:

https://www.nsa.gov/resources/cybersecurity-professionals/assets/files/top-5-soc-principles.pdf

Questions?