DIRECTORATE OF
CYBERSECURITY

NSA, CYBERSECURITY AND THE RUBIK'S CUBE: CAN YOU SOLVE THE PUZZLE?

DR. RITA DOERR, NSA

OCTOBER 26, 2021

OUTLINE

CYBERSECURITY

- NSA's Cybersecurity Directorate (CSD) Overview
- CSD's Cybersecurity Collaboration Center (CCC) Overview
- CSD's new (!!) Cybersecurity Summer Internship & NSA Cyber Positions
- Rubik's Cube: Can you solve the puzzle?! ☺

NSA'S CYBERSECURITY DIRECTORATE (CSD)

CYBERSECURITY

[Join the Mission to Prevent and Eradicate Cyberthreats – YouTube]

THE NSA CYBERSECURITY MISSION

Prevent & eradicate cyber threats to U.S. National Security Systems and Critical Infrastructure, focused initially on the Defense Industrial Base (DIB) and the improvement of our weapons' security.

Our comparative advantage is our people, code-making and code-breaking, hard-target access, and our partnerships.

"NSA will establish a Cybersecurity Directorate that redefines its cybersecurity mission."

OFFENSE INFORMING DEFENSE

CYBERSECURITY

SIGNALS INTELLIGENCE

CYBERSECURITY

OUR DIFFERENTIATOR IS OUR ABILITY TO INTEGRATE THE TWO TO DRIVE CYBERSECURITY IMPACTS THAT SCALE

PREVENT & ERADICATE CYBER THREATS

Encryption Production & Solutions

KEYS, CODES, AND CRYPTO

Critical Networks Defense

WEAPONS AND SPACE SYSTEMS

ADVERSARY DEFEAT

NUCLEAR COMMAND, CONTROL, AND COMMUNICATIONS CYBERSECURITY

Cybersecurity Collaboration Center

DIB DEFENSE

KEY AUTHORITIES: NSD-42, EO12333, EO13587, FAA-702, DoDIN and DIB Authorities

STRENGTHS AND OUTCOMES

COMPARATIVE ADVANTAGES

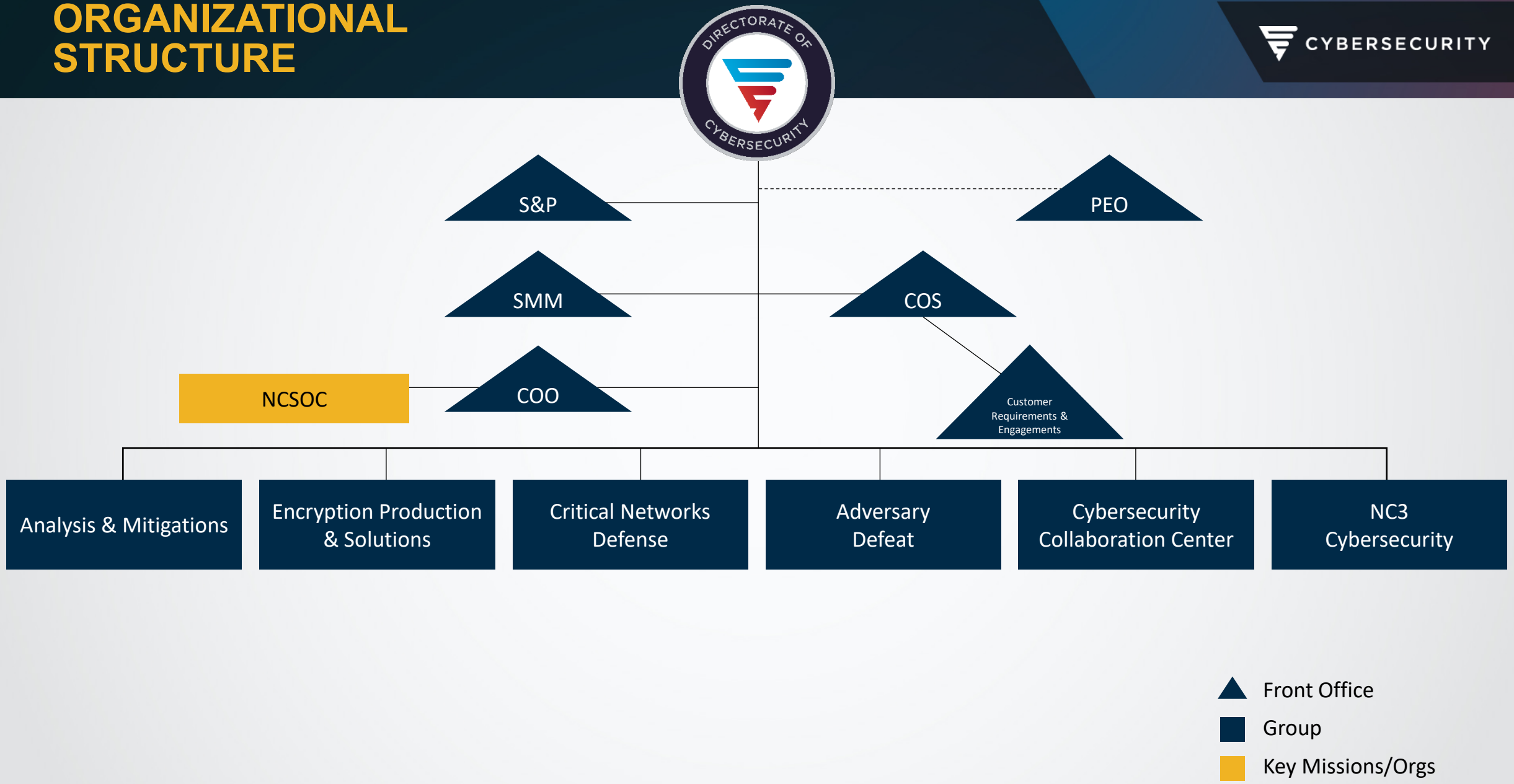
- Expert workforce
- Cyber threat intelligence
- Code-making
- Partnerships with USCYBERCOM and Defense Industrial Base
- Cryptologic Partners
- Offense informs defensive mission

STRATEGIC COMPETITION

- Denied, Degraded, Disrupted Adversary Capabilities
- Reduced Cyber-Attack Surface
- Next-Gen Encrypted US Gov't Comms, Data, & Networks
- Hardened Defense Systems
- Whole of US Gov't Cyber Countermeasures

ORGANIZATIONAL STRUCTURE

CYBERSECURITY



SUCCESS STORIES

ADVERSARY DEFEAT THROUGH PUBLIC EXPOSURE

Reshaping the cyber landscape by frustrating our adversaries' activities in cyberspace by forcing them to retool.

Russia

DROVORUB CSA: Exposed proprietary Linux malware developed for use by Russian actors

SolarWinds: CSD published multiple products on Russian techniques used in this breach and how to mitigate vulnerabilities

China

Released a series of advisories that detailed how Chinese state-sponsored actors are exploiting U.S. and allied networks and how to stop them

CYBERSECURITY COLLABORATION CENTER (CCC)

Bidirectional info sharing with the Defense Industrial Base (DIB).

- Industry partnerships enabled rapid understanding of cyber threats to prevent future compromise
- Bi-directional exchanges with hundreds of industry analysts expedited mitigations across DIB, DoD, and USG
- Accelerated the eradication of known Chinese and Russian malicious activity from DIB networks
- Disclosed significant vulnerabilities such as a critical cryptographic flaw in WIN10 and a series of critical Microsoft Exchange Server Vulnerabilities

STRENGTHENING CYBERSECURITY AT SCALE

CSD made significant progress in rebuilding NSA's cybersecurity mission.

Reducing obsolete encryption

Across the Department of Defense and military services. This ensures our nation's most critical secrets are protected from the eventuality of quantum computing.

Executive Order

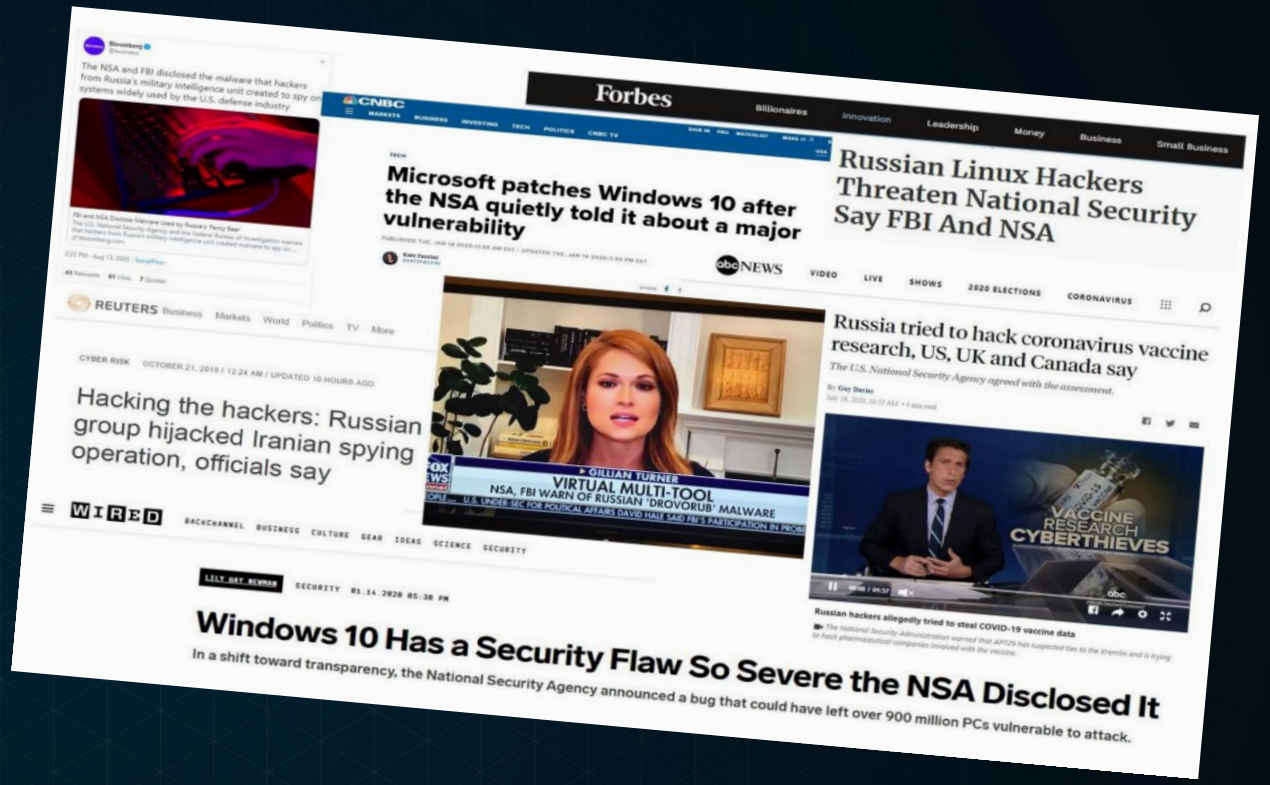
CSD worked with the White House and National Security Council on a cybersecurity Executive Order designed to improve the cybersecurity of federal networks at scale.

Strategic Cybersecurity Program

Protect key weapons and space systems from adversary cyber intrusions by hardening vulnerable systems.

CYBERSECURITY MISSION IN ACTION

- Release of 50+ unique, actionable, and timely cybersecurity products
- Cybersecurity Collaboration Center
- Award-winning vulnerability discoveries and disclosures



Community Feedback

- "This team has dramatically changed the game. It's not hyperbolic to state that the tide has most definitely turned and, through CSD's efforts, the deeply troubling existential threats….are now receding…" Senior DOD leader
- "[NSA's] report is excellent. The level of detail, context, and advance warning prior to any public release is exactly what we need." DIB Prime CISO
- "Thank you for your team sharing the information on [Russian cyber threats]. We are scouring our logs for any data that can be helpful and we plan to share it back. We will also quietly update our system to protect our customers." Leading cloud provider

CYBERSECURITY COLLABORATION CENTER

CYBERSECURITY

NSA's Cybersecurity Collaboration Center – YouTube

ABOUT: CYBERSECURITY COLLABORATION CENTER

CYBERSECURITY

- Provides NSA the ability
  - to develop open, robust, and **collaborative relationships**
  - with **private industry**
  - to **prevent and eradicate foreign cyber threats** from the U.S.'s most critical networks.

- We execute this mission through
  - **bi-directional cyber threat intelligence** sharing
  - and joint **analytic tradecraft development**.

VISION: CYBERSECURITY COLLABORATION CENTER

CYBERSECURITY

- Create cybersecurity solutions with **industry, academia, and other government partners** to identify and disrupt foreign adversaries.

- Leverage **unclassified data sources** (e.g., VirusTotal) to identify foreign cybersecurity threats and publish findings **to effect adversary TTP changes**.

- **Host analytic exchanges** to address cybersecurity issues of National importance including sector-specific threats and critical infrastructure concerns.

METHODOLOGY: CYBERSECURITY COLLABORATION CENTER

CYBERSECURITY

- Detect the adversary by leveraging **signals intelligence, commercial data and bi-directional threat sharing**.
- Innovate by **creating new tradecraft** for discovering and tracking the adversary.
- Mitigate by developing, sharing, and amplifying guidance to **National Security Systems, DoD, and the Defense Industrial Base (DIB).**

NEW (!!) CYBERSECURITY SUMMER INTERNSHIP

CYBERSECURITY

- 1169435 Job Description | IC Candidate Portal (intelligencecareers.gov)
- **Job Summary:** Are you a cyber professional with the drive and expertise to be on the forefront of the cyber fight; tackling NSA's complex mission to defend against cyber threats of today and tomorrow? NSA, the nation's leading cyber agency, has exciting and challenging positions in Cyber Security Engineering and Cyber and TEMPEST vulnerability analysis/mitigation. Are you ready to help secure our Nation's critical Infrastructure? If so, NSA is the place for you!
- **Qualifications:** To be accepted into the NSA Summer Internship - Cybersecurity, candidates must: - Be a U.S. citizen; - Be eligible to be granted a TS/SCI/TK security clearance after successfully completing a background investigation that includes passing a Full-Scope Polygraph and a Psychological Evaluation; - Preferred cumulative GPA of 3.0 or higher for all college work completed; - Be a currently enrolled college student (undergraduate, graduate or doctorate program) at time of application. Those entering their final year of a degree program cannot be considered unless they are immediately entering graduate school in the Fall of 2022; - Be available and in the U.S. for operational and technical interviews and other applicable processing, both in-person and via telephone/internet, between the months of November 2021 and March 2022; - Be pursuing a major in Cybersecurity, Psychology or closely related field.
- **DEADLINE: October 31, 2021**

FULL-TIME CYBER POSITIONS

CYBERSECURITY

- Digital Network Exploitation Analyst – 1155796 Job Description | IC Candidate Portal (intelligencecareers.gov)

- Other positions – National Security Agency for Intelligence Careers (intelligencecareers.gov/NSA)

  - Click on “Search NSA Jobs”

    - Location = Ft. Meade
    - Roles = Cyber
    - Job Type = Full-time
    - Date Posted = Last 90 days

HASHING ACTIVITY

PROPERTIES OF A GOOD HASH FUNCTION … TRANSLATED

CYBERSECURITY

1. Can be applied to any size data
2. Regardless of input size, produces a fixed-length output
3. It should be [computationally] easy to compute the hash of any input
4. If all you have is a hash value, it should be very hard to find an input that hashes to that value **(ONE-WAY FUNCTION)**
5. It should be difficult to find two different inputs that generate the same hash **(WEAK COLLISON RESISTANT)**
6. It should be difficult to take a hash value and an input that hashes to it, and engineer from the first input another input that hashes to the same value **(STRONG COLLISON RESISTANT)**

HASHING ACTIVITY

CYBERSECURITY

- **Prediction Scenario:** "*The Voice*"

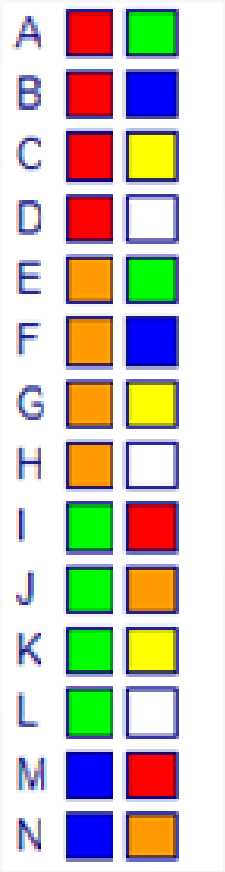
- **Beforehand:**
  - gives no information before or during the season about your prediction
  - after the season provides indisputable evidence that you predicted the real winner (or, if you failed, that you didn't)

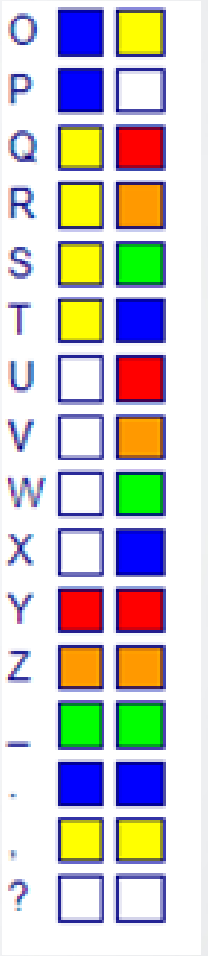
- Need something to guarantee that we haven't modified the message since before "*The Voice*" season started; hashing provides this something for **Integrity**

HASHING ACTIVITY

CYBERSECURITY

- Let's use a 3x3 Rubik's Cube





Source: [SI110: Cryptographic Hashing & Passwords (usna.edu)]

QUESTIONS?

CYBERSECURITY

Thank you for your time!

rita.doerr@cyber.nsa.gov

NSA_CSD_Hiring@nsa.gov