Army Cyber Capabilities and the Changing Threat Landscape

COL BE Rhodes
G6/CIO, 63D Readiness Division

U.S. ARMY

WHOIS: Brad Rhodes

TLDR:

- Deputy Director for Operations, Energy Threat Analysis Center (ETAC)
  Office of Cybersecurity, Energy Security, and Emergency Response (CESER), Department of Energy (DOE)

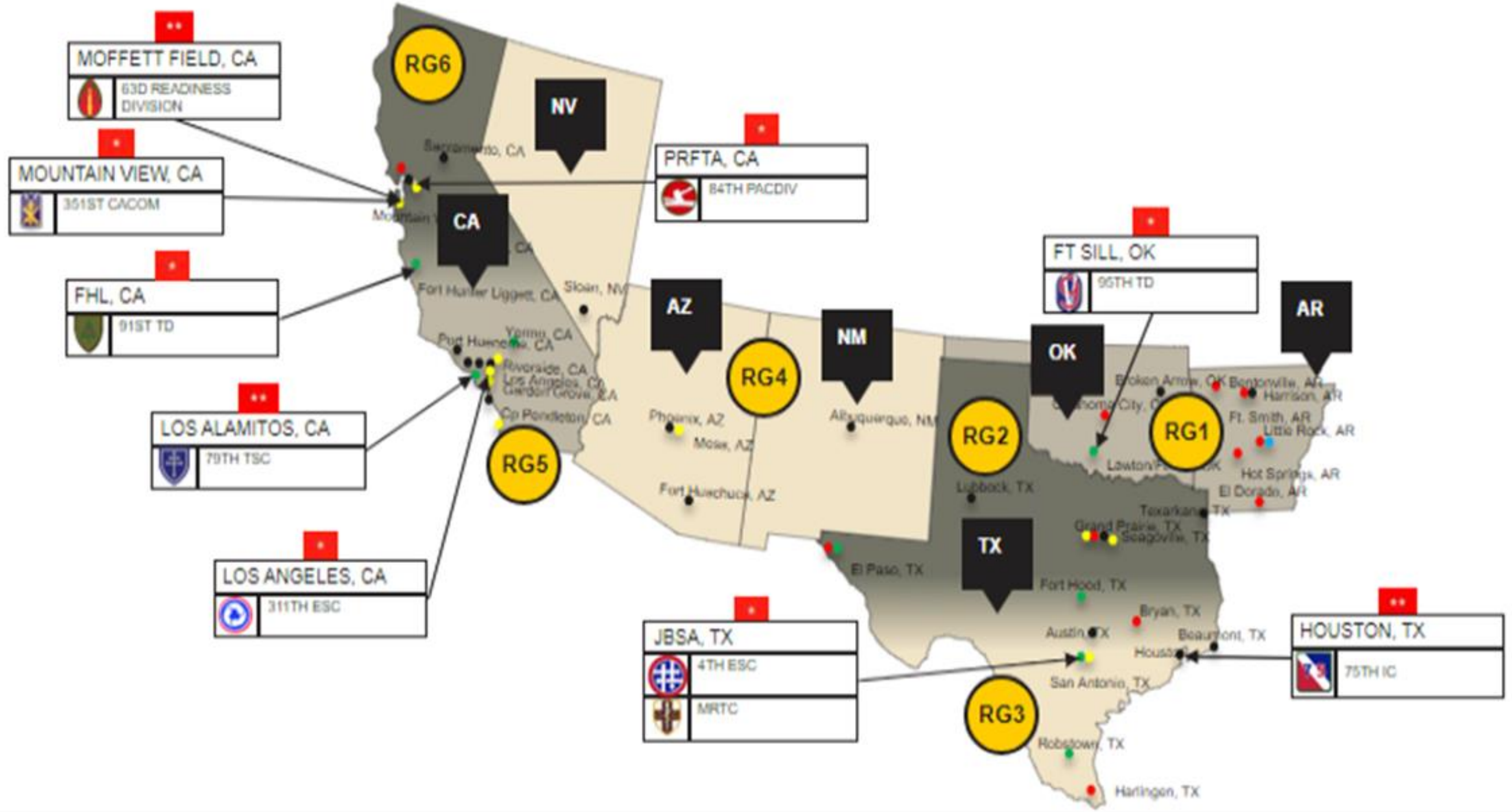
➡ **COL, Cyber (17A), 63rd Readiness Division, G6/CIO**

- Military Cyber Professionals Association, HammerCon Co-Lead
- Speaker, Author, Professor, Coach
- #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, CDPSE, PMP, CEH, GMON, GCIH, Cloud+, CySA+
- Extra Class Amateur Radio (HAM): KG4COS

Feel free to view/listen/grab my previous presentation/articles here: https://github.com/cyberguy514

AREA OF RESPONSIBILITY

ARMY RESERVE



LEGEND	
■	20 - Area Maintenance Support Activities (AMSA)
🟩	9 - Equipment Concentration Site (ECS)
🟥	11 - Branch Maintenance Activity (BMA)
🟪	1 - New Equipment Fielding Facility (NEFF)
🟨	19 - Regional Personnel Action Centers (RPAC)
🟦	1 - Hands on Training (HOT) & Center of Excellence (COE)

AREA OF RESPONSIBILITY (CA & TX MAKE UP 67% OF ALL SITES IN THE RG W/ 89 SITES)

[redacted]	TOT. SITES (FACIDs)	REAL ESTATE SQ FT	SUPPORTED UNITS (UICs)	SUPPORTED SOLDIERS	MFGIs	AR GARRISONS
	131	9,502,927	1883	43,774	2	2

Agenda

Part 1 – Army Cyber Capabilities

- Army Doctrine
  - FM 3-12 - CEMA
  - ADP 3-13 – Information
  - FM 3-14 – Space Operations
- Joint Cyber Forces
- Army Cyber Forces
- Army Cyber Activities
- Army Authorities in Cyber Response
- Innovative Readiness Training

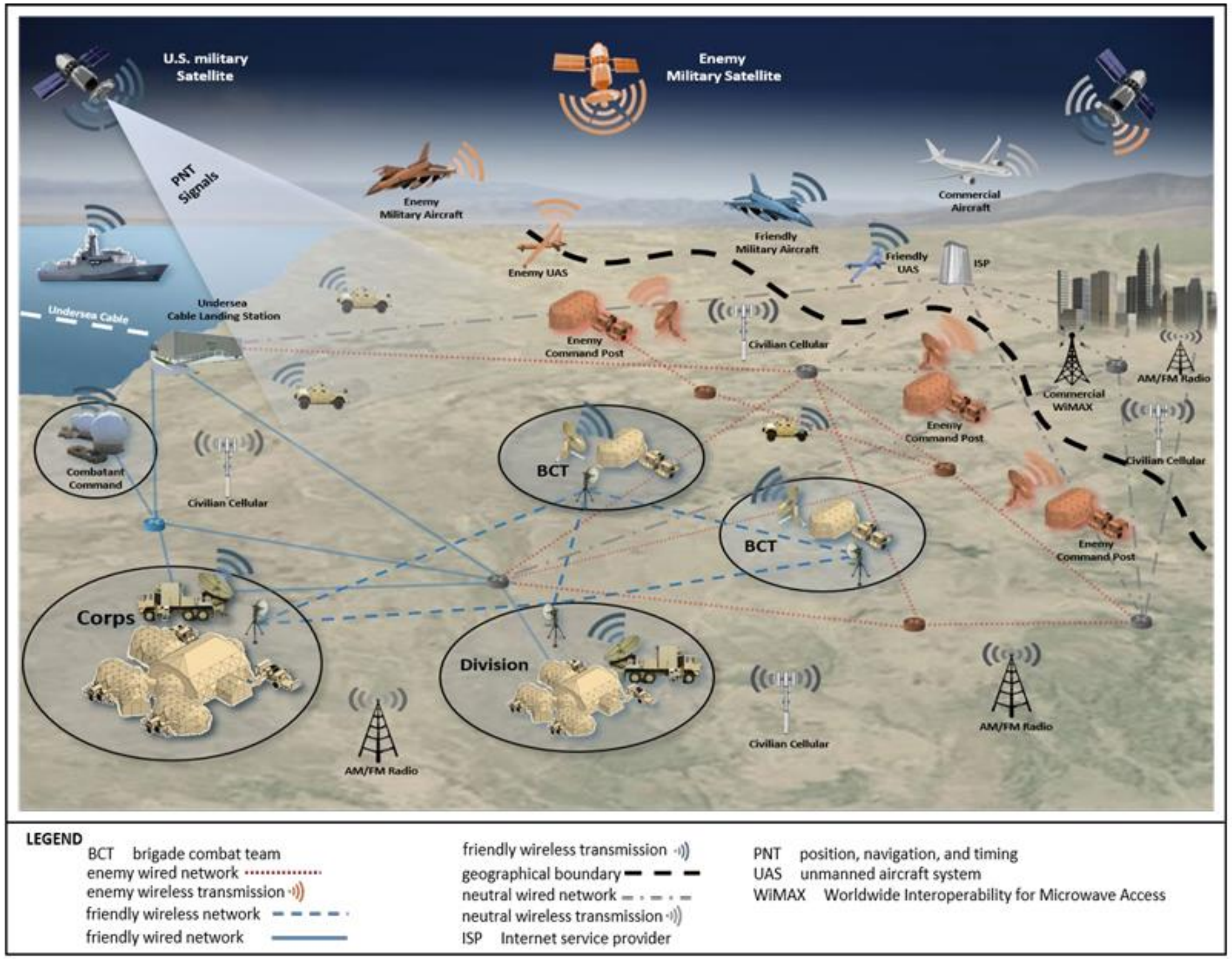
Part 2 – The Changing Threat Landscape

- CISA Critical Infrastructure Sectors
- Cyber Threat Families
- Kimsuky and the Scientists
- CL0p Extortion
- Midnight Blizzard
- Volt Typhoon
- Salt Typhoon
- Mis/Dis/Mal-Information
- TikTok and Influence
- Key Current Threat TTPs
- What can you do “Left of Boom?”

Part 1

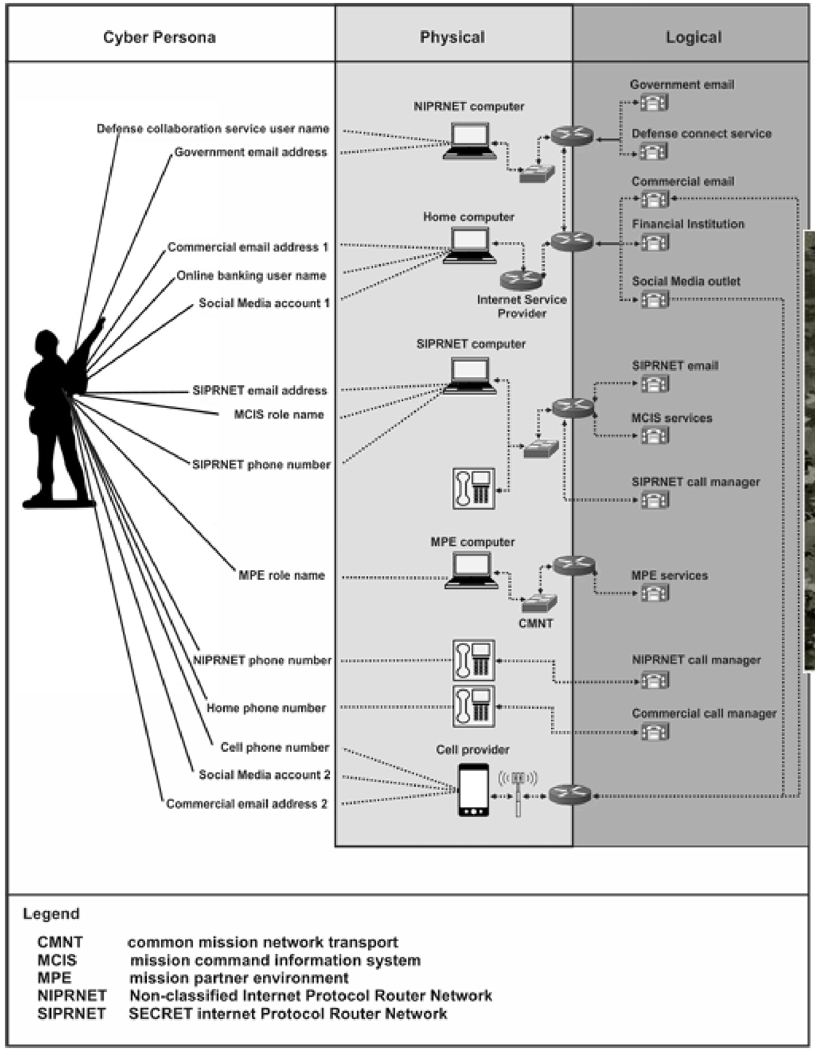
Army Cyber Capabilities

Army Doctrine – FM 3-12: CEMA



LEGEND
BCT brigade combat team
enemy wired network
enemy wireless transmission
friendly wireless network
friendly wired network
friendly wireless transmission
geographical boundary
neutral wired network
neutral wireless transmission
ISP Internet service provider
PNT position, navigation, and timing
UAS unmanned aircraft system
WiMAX Worldwide Interoperability for Microwave Access

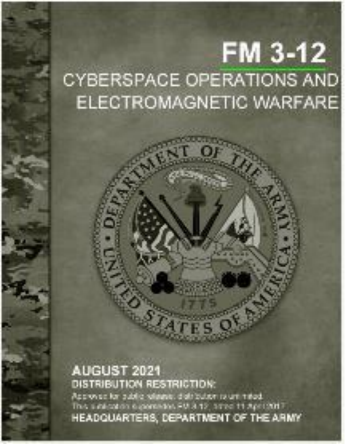
Figure 1-4. Congestion in cyberspace and the electromagnetic spectrum



Legend

CMNT	common mission network transport
MCIS	mission command information system
MPE	mission partner environment
NIPRNET	Non-classified Internet Protocol Router Network
SIPRNET	SECRET internet Protocol Router Network

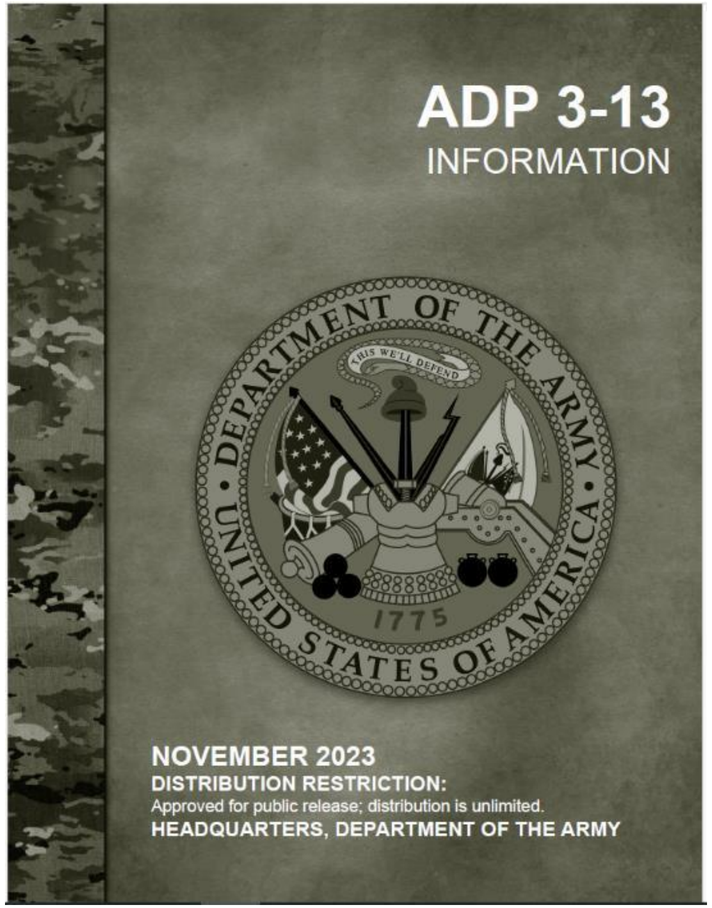
Figure 1-2. Relationship between the cyberspace network layers



FM 3-12
CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE

AUGUST 2021
DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited.
This publication supersedes FM 3-12, dated 11 April 2017.
HEADQUARTERS, DEPARTMENT OF THE ARMY

THE Information Environment



ADP 3-13
INFORMATION

NOVEMBER 2023
DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited.
HEADQUARTERS, DEPARTMENT OF THE ARMY

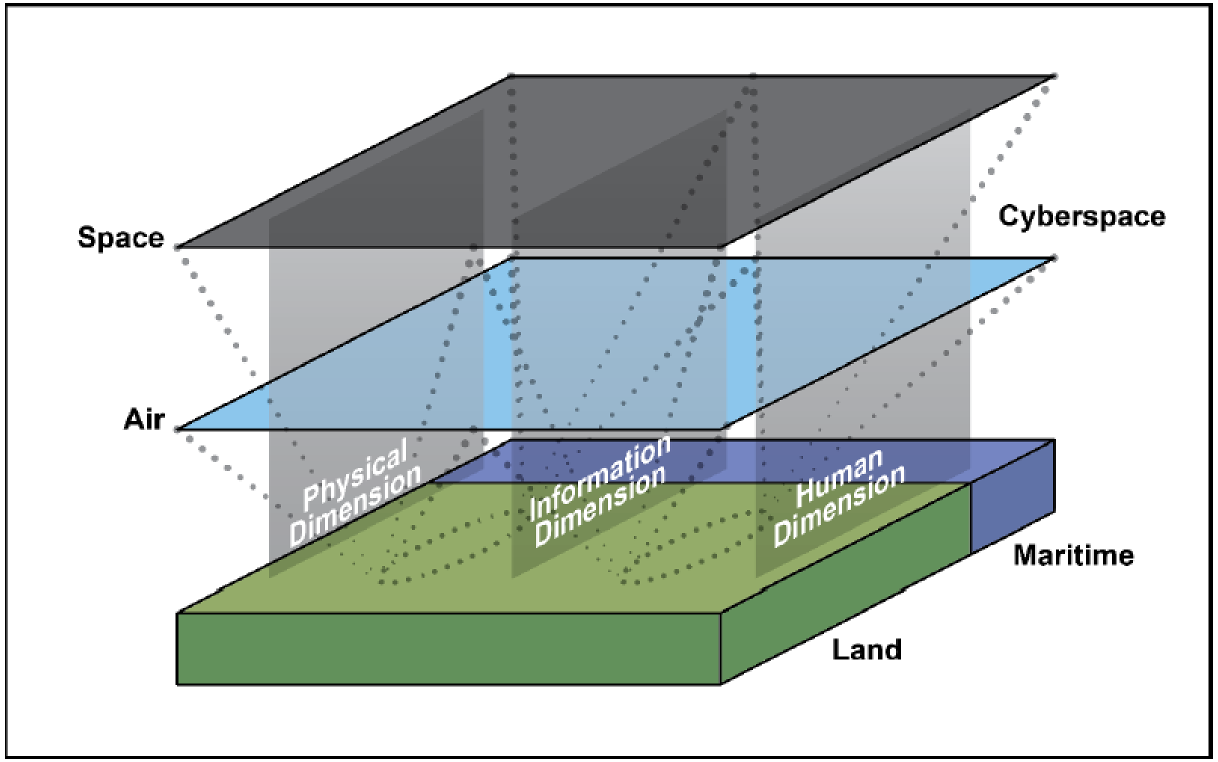
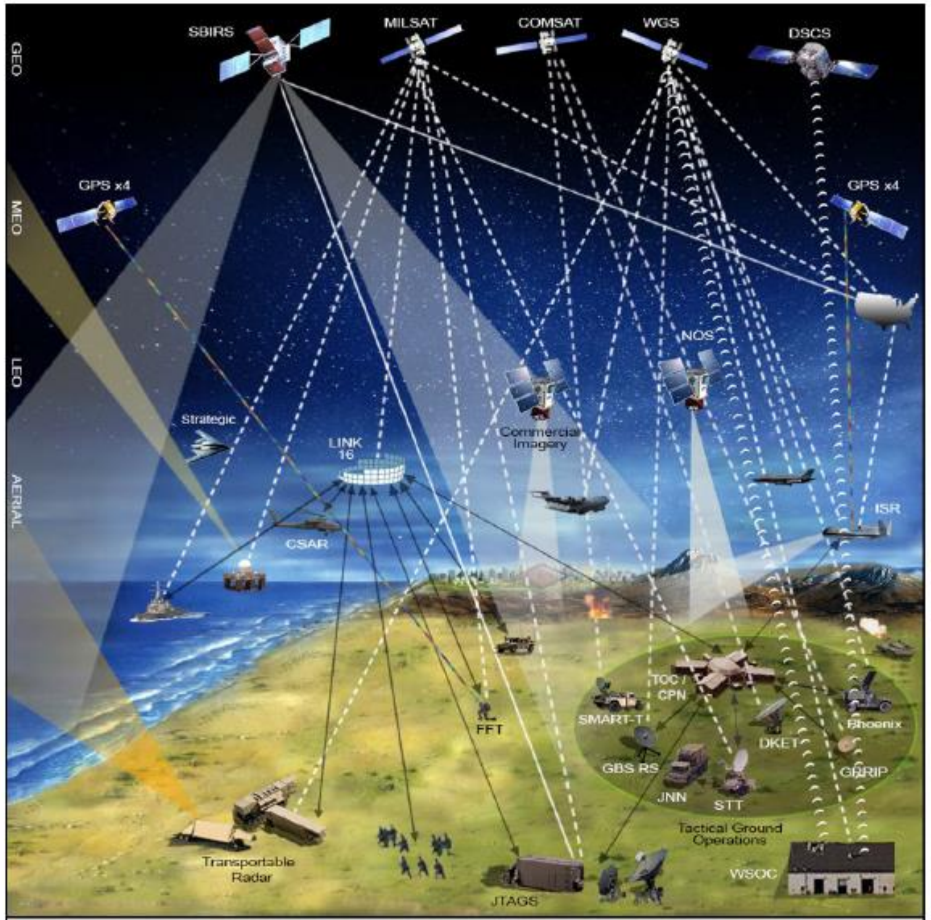


Figure 1-3. Domains and dimensions of an operational environment

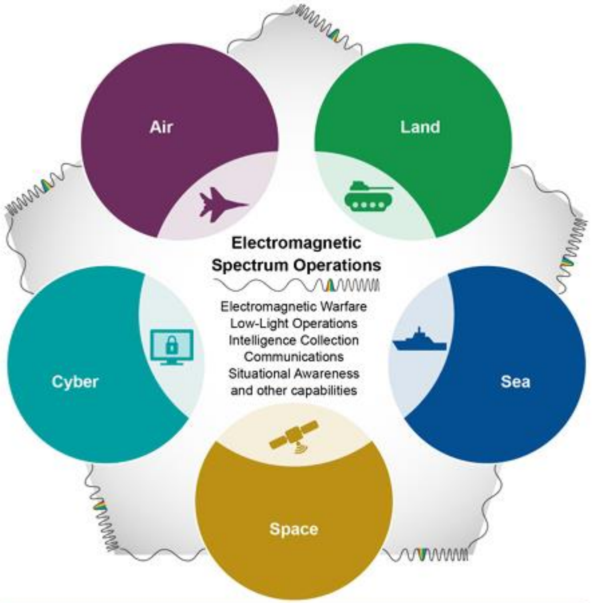
Army Doctrine – FM 3-14: Space Operations



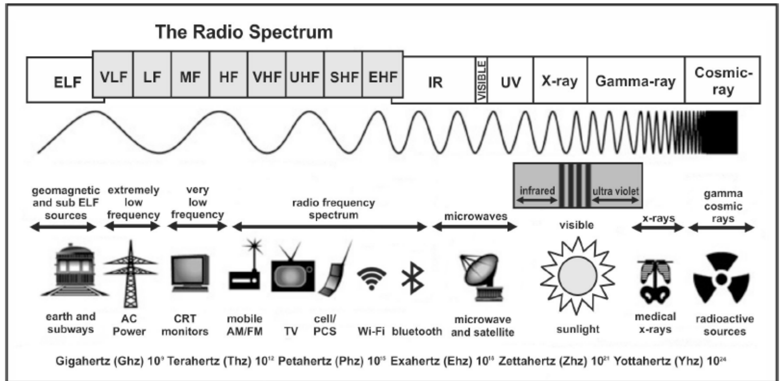
- - - - - Transmission control
⟷ Line of sight communications
——— Direct downlink
)))))) Payload control & Assured access

COMSAT – communications satellite
CSAR – combat search and rescue
DSCS – Defense Satellite Communications System
GBS RS – Global Broadcast System receive suite
GPS – Global Positioning System
ISR – intelligence, surveillance, reconnaissance
JTAGS – joint tactical ground station
MEO – medium Earth orbit
NOS – National Reconnaissance Office (NRO) overhead system
SMART-T – secure, mobile, anti-jam, reliable, tactical terminal
TOC – tactical operations center
WSOC – wideband satellite communications operations center

CPN – command post node
DKET – deployable Ku band Earth terminal
FFT – friendly force tracking
GEO – geosynchronous Earth orbit
GRRIP – global rapid response information package
JNN – joint network node
LEO – low Earth orbit
MILSAT – military communications satellite
SBIRS – space-based infrared system
STT – satellite transportable terminal
WGS – Wideband Global Satellite Communications

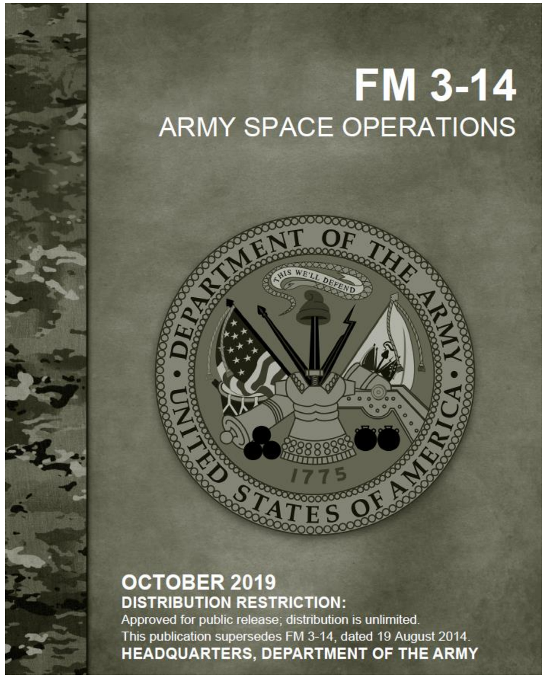


The joint force depends on the electromagnetic spectrum for operations in all domains.



Legend

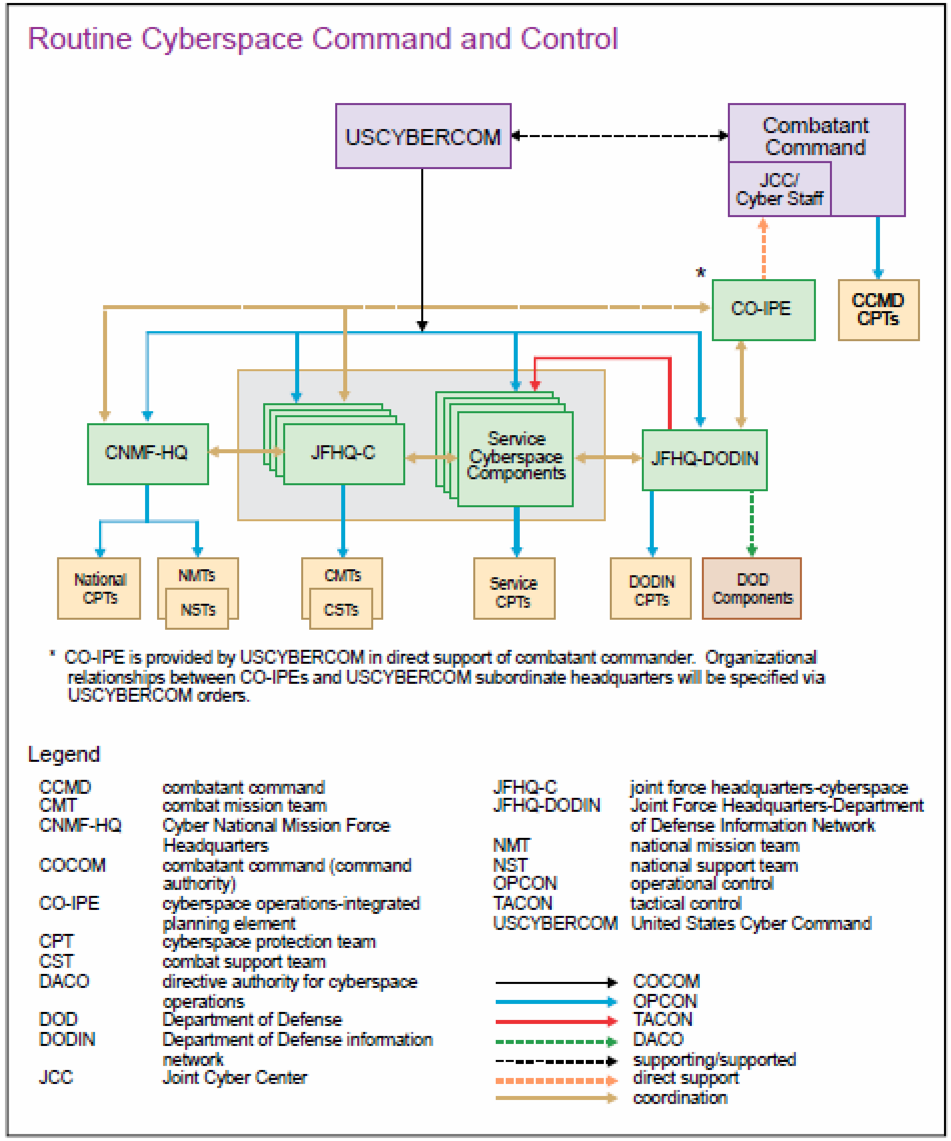
AC	alternating current	FM	frequency modulation	SHF	super high frequency
AM	amplitude modulation	HF	high frequency	TV	television
CRT	cathode ray tube	IR	infrared	UHF	ultra high frequency
EHF	extremely high frequency	LF	low frequency	UV	ultra violet
ELF	extremely low frequency	MF	medium frequency	VHF	very high frequency
EMF	electromagnetic field	PCS	personal communication systems	VLF	very low frequency



FM 3-14
ARMY SPACE OPERATIONS

OCTOBER 2019
DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited.
This publication supersedes FM 3-14, dated 19 August 2014.
HEADQUARTERS, DEPARTMENT OF THE ARMY

Joint Cyber Forces


Routine Cyberspace Command and Control

* CO-IPE is provided by USCYBERCOM in direct support of combatant commander. Organizational relationships between CO-IPEs and USCYBERCOM subordinate headquarters will be specified via USCYBERCOM orders.

Legend

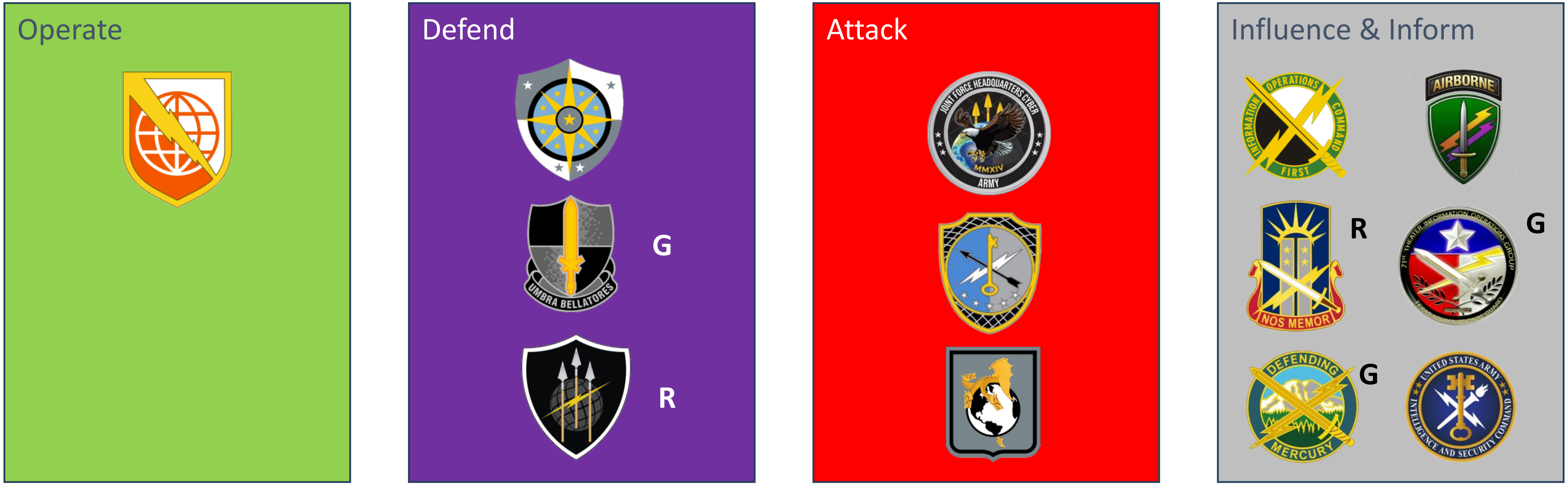
CCMD	combatant command
CMT	combat mission team
CNMF-HQ	Cyber National Mission Force Headquarters
COCOM	combatant command (command authority)
CO-IPE	cyberspace operations-integrated planning element
CPT	cyberspace protection team
CST	combat support team
DACO	directive authority for cyberspace operations
DOD	Department of Defense
DODIN	Department of Defense information network
JCC	Joint Cyber Center
JFHQ-C	joint force headquarters-cyberspace
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network
NMT	national mission team
NST	national support team
OPCON	operational control
TACON	tactical control
USCYBERCOM	United States Cyber Command

→ COCOM
→ OPCON
→ TACON
⇢ DACO
⇢ supporting/supported
⇢ direct support
→ coordination

Figure IV-1. Routine Cyberspace Command and Control

Army Cyber Forces

U.S. ARMY
CYBER COMMAND



Operate

Defend

G

R

Attack

Influence & Inform

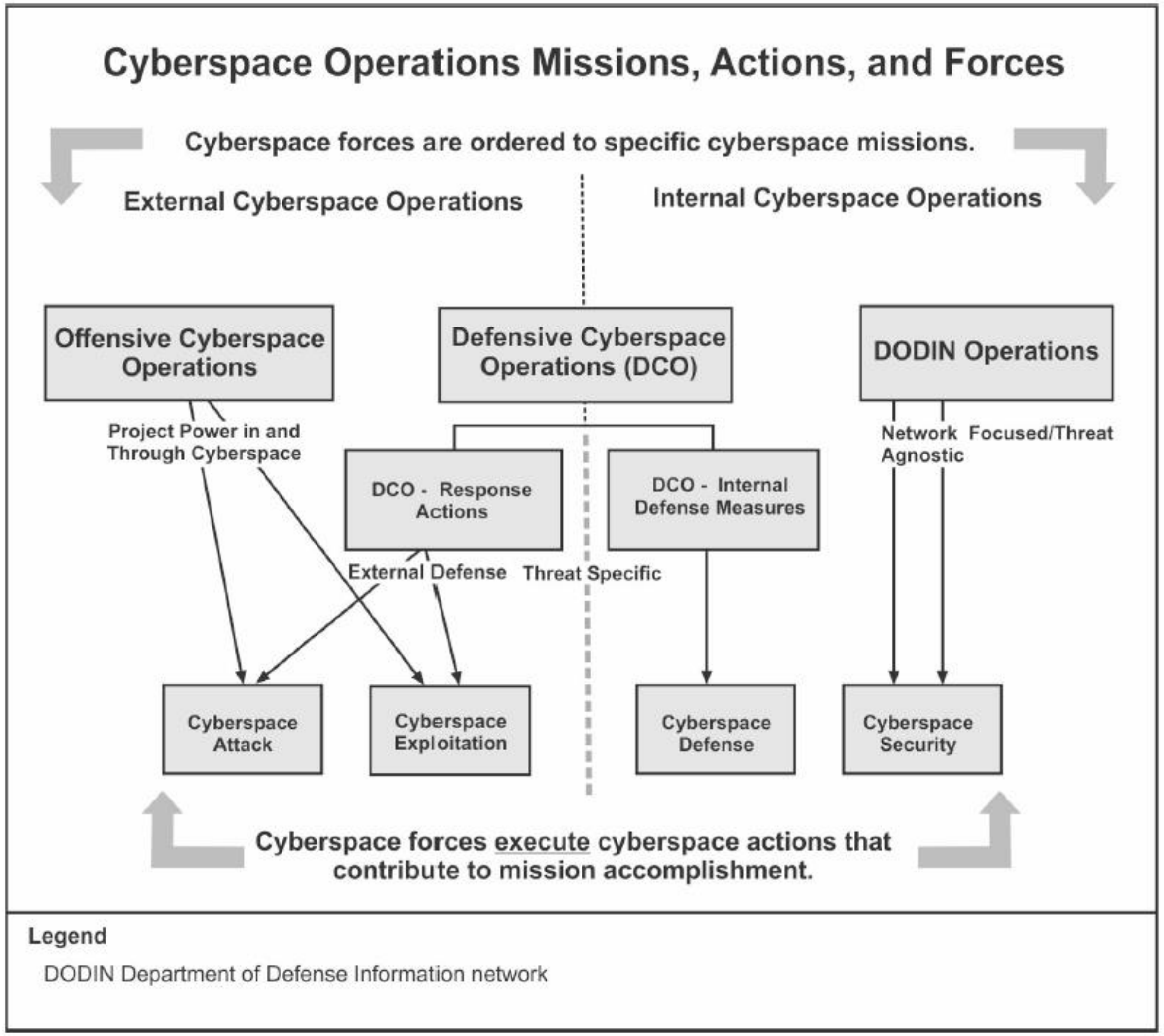
R

G

G

https://www.arcyber.army.mil/Organization/Units/

Army Authorities in Cyber Response



Cyberspace Operations Missions, Actions, and Forces

Cyberspace forces are ordered to specific cyberspace missions.
External Cyberspace Operations
Internal Cyberspace Operations
Offensive Cyberspace Operations
Defensive Cyberspace Operations (DCO)
DODIN Operations
Project Power in and Through Cyberspace
DCO - Response Actions
DCO - Internal Defense Measures
Network Agnostic
Focused/Threat
External Defense
Threat Specific
Cyberspace Attack
Cyberspace Exploitation
Cyberspace Defense
Cyberspace Security
Cyberspace forces execute cyberspace actions that contribute to mission accomplishment.

Legend

DODIN Department of Defense Information network

State Active Duty (NG-only)

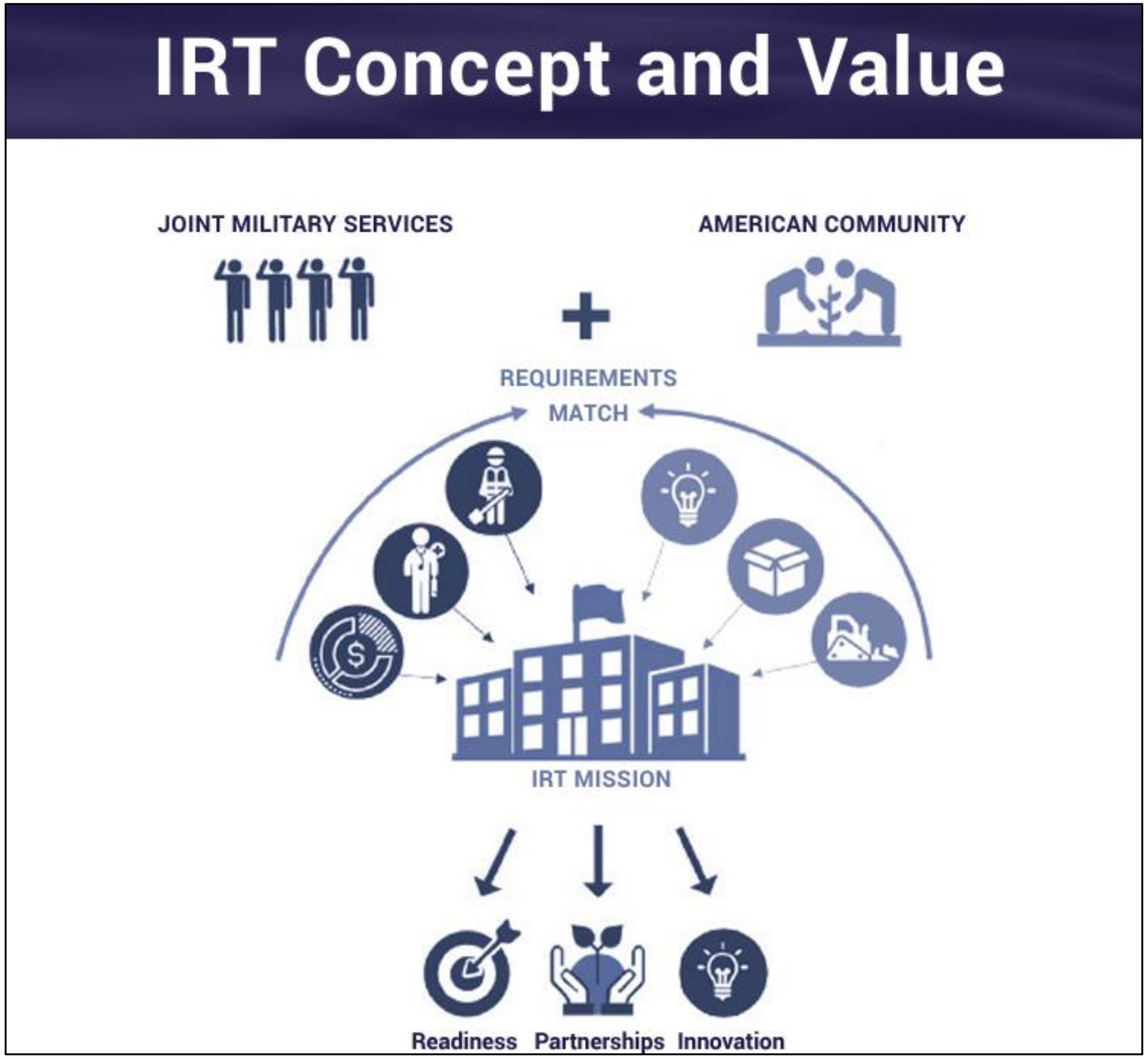
Title 32 (NG-only)

Title 10 (Reserve)

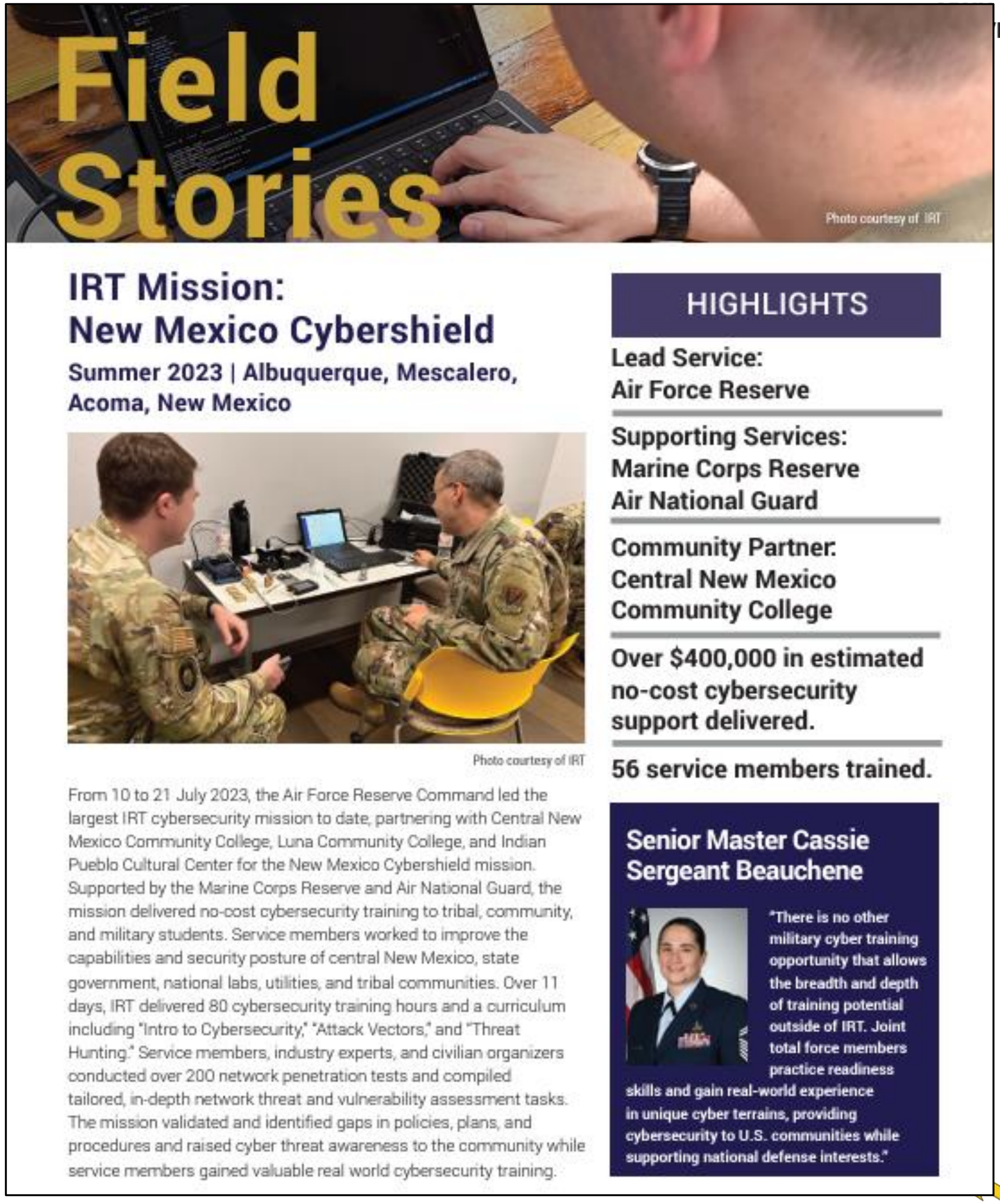
Title 10 (Active)

Immediate Response Authority (72 hrs)

Innovative Readiness Training



IRT Concept and Value



Field Stories
Photo courtesy of IRT

IRT Mission: New Mexico Cybershield

Summer 2023 | Albuquerque, Mescalero, Acoma, New Mexico

Photo courtesy of IRT

From 10 to 21 July 2023, the Air Force Reserve Command led the largest IRT cybersecurity mission to date, partnering with Central New Mexico Community College, Luna Community College, and Indian Pueblo Cultural Center for the New Mexico Cybershield mission. Supported by the Marine Corps Reserve and Air National Guard, the mission delivered no-cost cybersecurity training to tribal, community, and military students. Service members worked to improve the capabilities and security posture of central New Mexico, state government, national labs, utilities, and tribal communities. Over 11 days, IRT delivered 80 cybersecurity training hours and a curriculum including "Intro to Cybersecurity," "Attack Vectors," and "Threat Hunting." Service members, industry experts, and civilian organizers conducted over 200 network penetration tests and compiled tailored, in-depth network threat and vulnerability assessment tasks. The mission validated and identified gaps in policies, plans, and procedures and raised cyber threat awareness to the community while service members gained valuable real world cybersecurity training.

HIGHLIGHTS

Lead Service:
Air Force Reserve

Supporting Services:
Marine Corps Reserve
Air National Guard

Community Partner:
Central New Mexico
Community College

Over $400,000 in estimated no-cost cybersecurity support delivered.

56 service members trained.

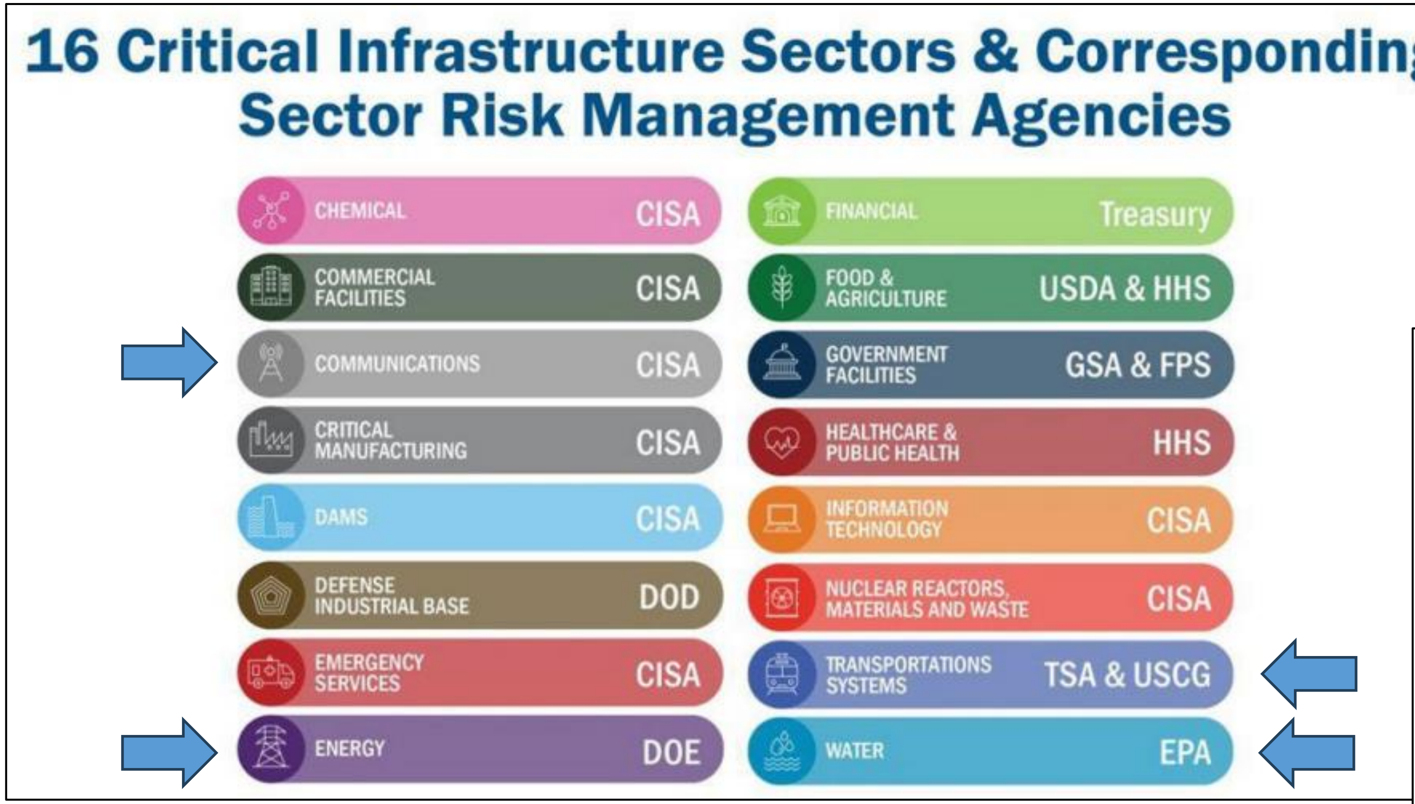
Senior Master Cassie
Sergeant Beauchene

"There is no other military cyber training opportunity that allows the breadth and depth of training potential outside of IRT. Joint total force members practice readiness skills and gain real-world experience in unique cyber terrains, providing cybersecurity to U.S. communities while supporting national defense interests."

Part 2

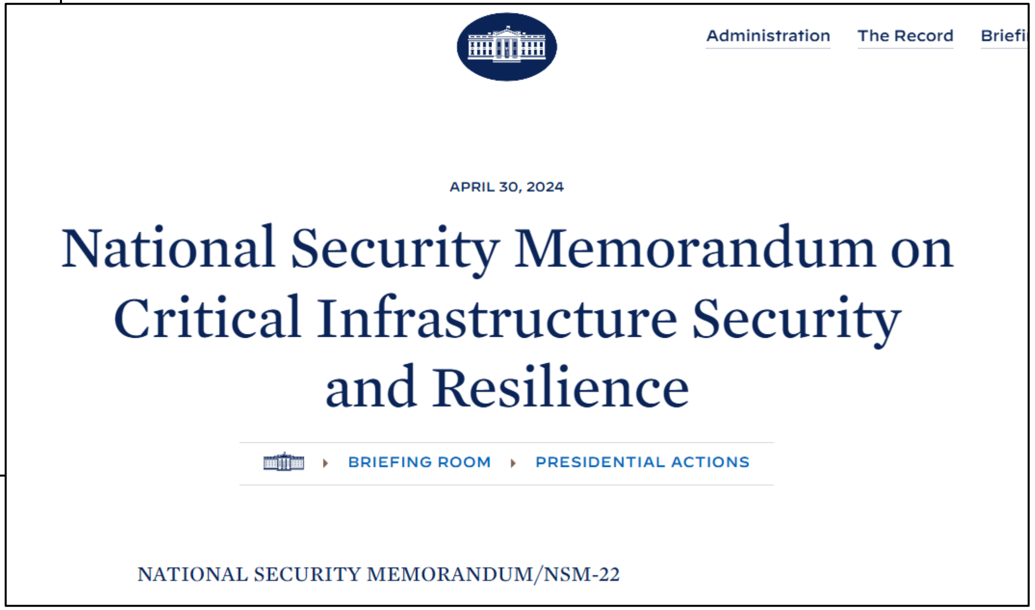
The Changing Threat Landscape

CISA Critical Infrastructure Sectors



16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

CHEMICAL	CISA	FINANCIAL	Treasury
COMMERCIAL FACILITIES	CISA	FOOD & AGRICULTURE	USDA & HHS
COMMUNICATIONS	CISA	GOVERNMENT FACILITIES	GSA & FPS
CRITICAL MANUFACTURING	CISA	HEALTHCARE & PUBLIC HEALTH	HHS
DAMS	CISA	INFORMATION TECHNOLOGY	CISA
DEFENSE INDUSTRIAL BASE	DOD	NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
EMERGENCY SERVICES	CISA	TRANSPORTATIONS SYSTEMS	TSA & USCG
ENERGY	DOE	WATER	EPA



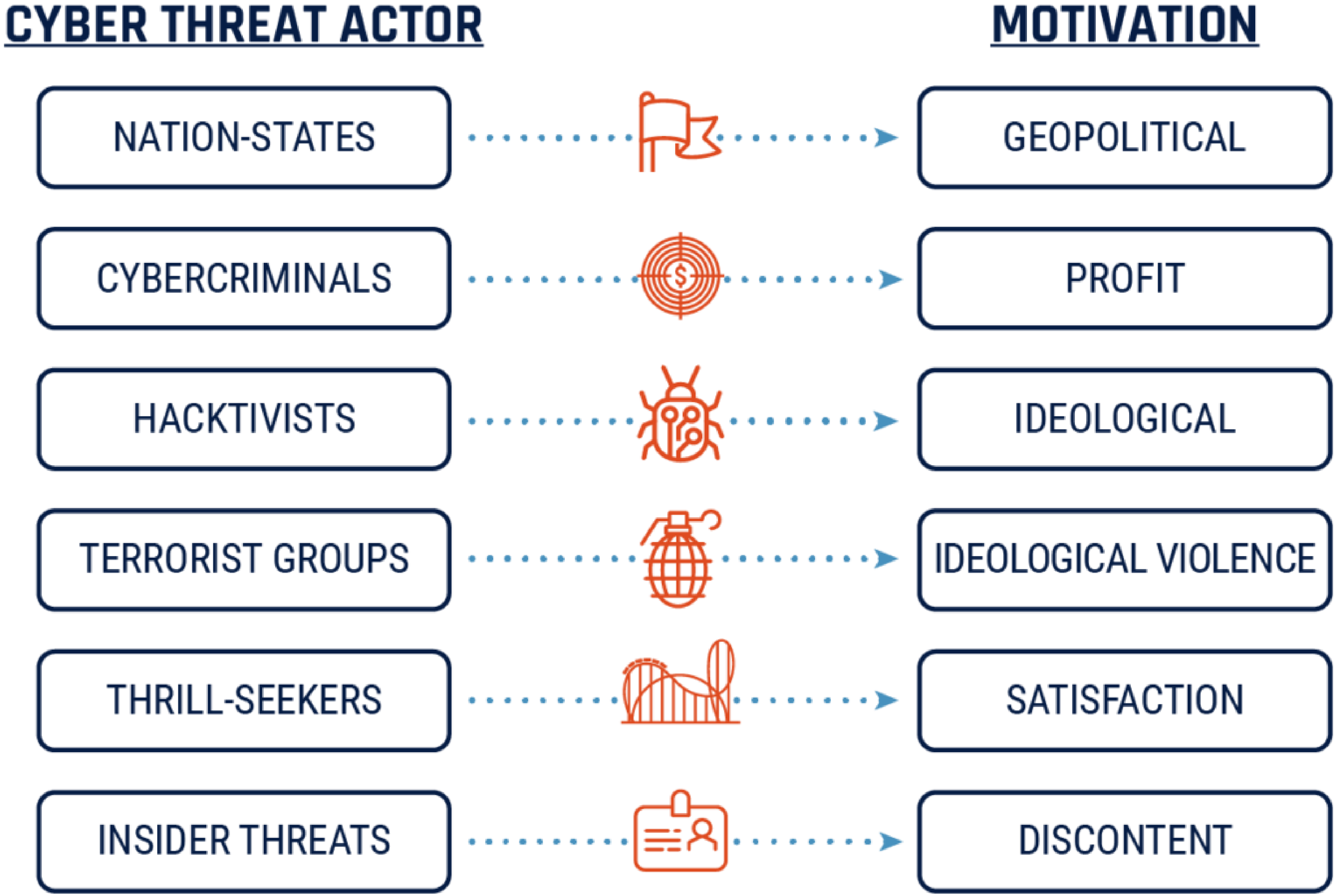
APRIL 30, 2024

National Security Memorandum on Critical Infrastructure Security and Resilience

NATIONAL SECURITY MEMORANDUM/NSM-22

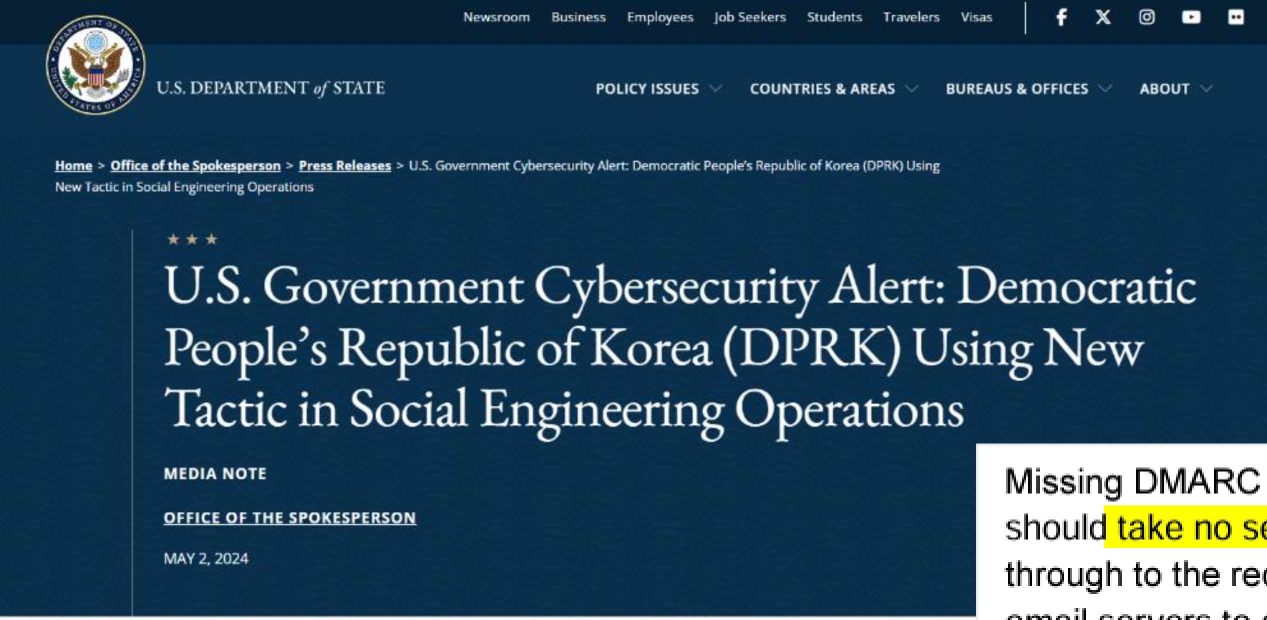
https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

Cyber Threat Families



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

Kimsuky and THE Scientists


Newsroom | Business | Employees | Job Seekers | Students | Travelers | Visas

U.S. DEPARTMENT *of* STATE

POLICY ISSUES | COUNTRIES & AREAS | BUREAUS & OFFICES | ABOUT

Home > Office of the Spokesperson > Press Releases > U.S. Government Cybersecurity Alert: Democratic People's Republic of Korea (DPRK) Using New Tactic in Social Engineering Operations

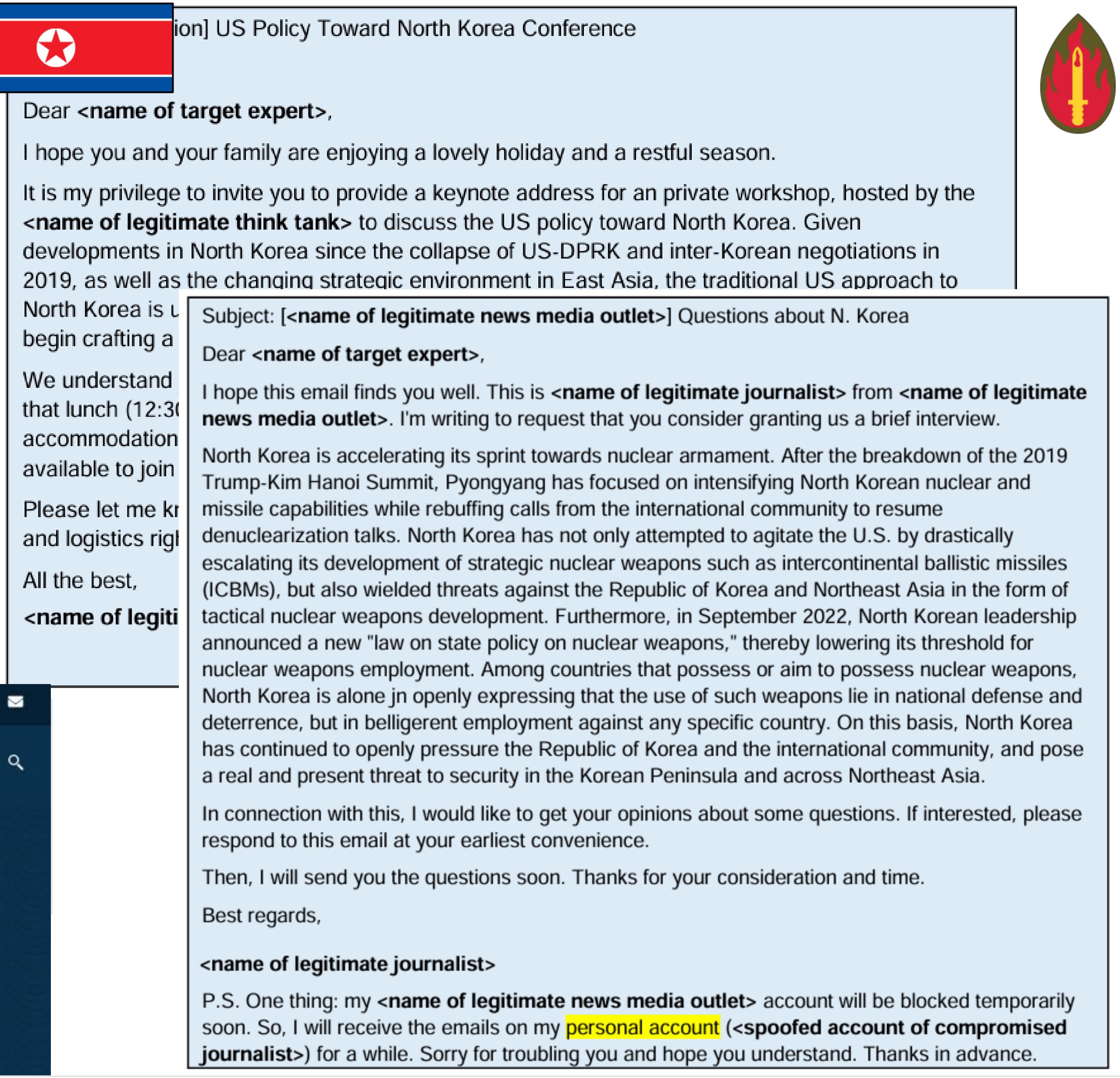
★ ★ ★

U.S. Government Cybersecurity Alert: Democratic People's Republic of Korea (DPRK) Using New Tactic in Social Engineering Operations

MEDIA NOTE

OFFICE OF THE SPOKESPERSON

MAY 2, 2024


ion] US Policy Toward North Korea Conference

Dear **<name of target expert>**,

I hope you and your family are enjoying a lovely holiday and a restful season.

It is my privilege to invite you to provide a keynote address for an private workshop, hosted by the **<name of legitimate think tank>** to discuss the US policy toward North Korea. Given developments in North Korea since the collapse of US-DPRK and inter-Korean negotiations in 2019, as well as the changing strategic environment in East Asia, the traditional US approach to North Korea is u
begin crafting a

We understand
that lunch (12:3
accommodation
available to join

Please let me kı
and logistics rigl

All the best,

<name of legiti

Subject: [**<name of legitimate news media outlet>**] Questions about N. Korea

Dear **<name of target expert>**,

I hope this email finds you well. This is **<name of legitimate journalist>** from **<name of legitimate news media outlet>**. I'm writing to request that you consider granting us a brief interview.

North Korea is accelerating its sprint towards nuclear armament. After the breakdown of the 2019 Trump-Kim Hanoi Summit, Pyongyang has focused on intensifying North Korean nuclear and missile capabilities while rebuffing calls from the international community to resume denuclearization talks. North Korea has not only attempted to agitate the U.S. by drastically escalating its development of strategic nuclear weapons such as intercontinental ballistic missiles (ICBMs), but also wielded threats against the Republic of Korea and Northeast Asia in the form of tactical nuclear weapons development. Furthermore, in September 2022, North Korean leadership announced a new "law on state policy on nuclear weapons," thereby lowering its threshold for nuclear weapons employment. Among countries that possess or aim to possess nuclear weapons, North Korea is alone jn openly expressing that the use of such weapons lie in national defense and deterrence, but in belligerent employment against any specific country. On this basis, North Korea has continued to openly pressure the Republic of Korea and the international community, and pose a real and present threat to security in the Korean Peninsula and across Northeast Asia.

In connection with this, I would like to get your opinions about some questions. If interested, please respond to this email at your earliest convenience.

Then, I will send you the questions soon. Thanks for your consideration and time.

Best regards,

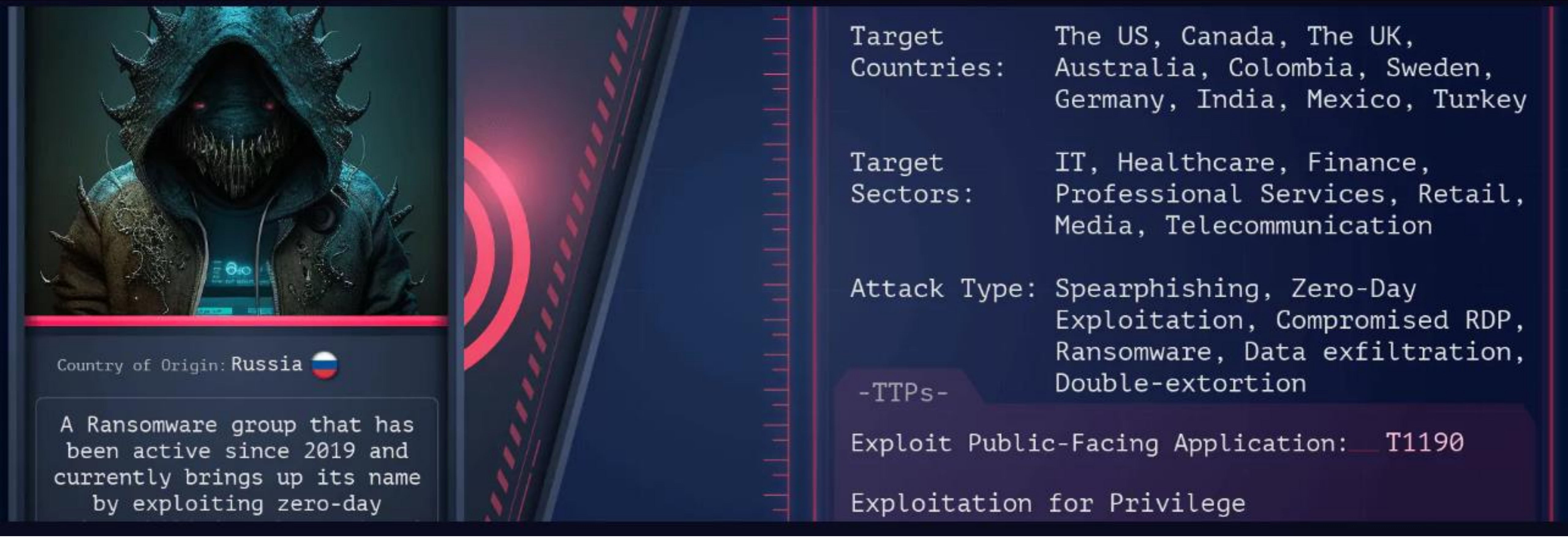
<name of legitimate journalist>

P.S. One thing: my **<name of legitimate news media outlet>** account will be blocked temporarily soon. So, I will receive the emails on my personal account (**<spoofed account of compromised journalist>**) for a while. Sorry for troubling you and hope you understand. Thanks in advance.

Missing DMARC policies or DMARC policies with "p=none" indicate that the receiving email server should take no security action on emails that fail DMARC checks and allow the emails to be sent through to the recipient's inbox. In order for organizations to make their policy stricter and signal to email servers to consider unauthenticated emails as spam, the authoring agencies recommend

CLOp Extortion (1 of 2)

CLOP is a ransomware variant associated with the FIN11 threat actor group and the double extortion tactic, it has previously been used to target several U.S. HPH organizations. Researchers have also identified the CLOP operators combining the "spray and pray" approach to compromising targets with a more targeted approach, suggesting that the operators have some discretion when selecting victims.



Country of Origin: Russia

A Ransomware group that has been active since 2019 and currently brings up its name by exploiting zero-day

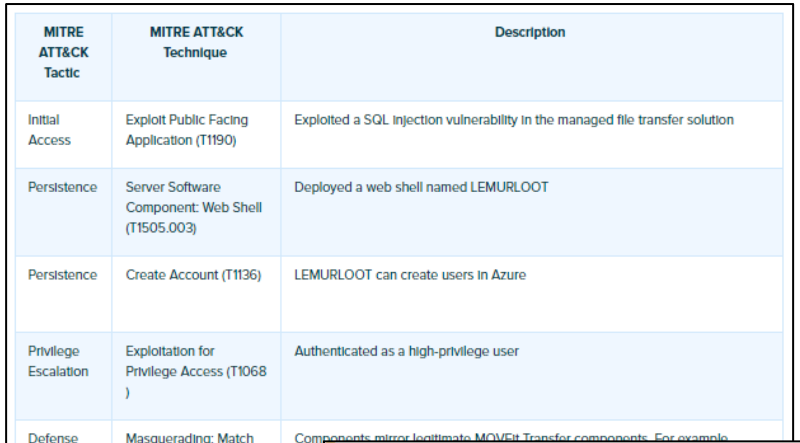
Target Countries:	The US, Canada, The UK, Australia, Colombia, Sweden, Germany, India, Mexico, Turkey
Target Sectors:	IT, Healthcare, Finance, Professional Services, Retail, Media, Telecommunication
Attack Type:	Spearphishing, Zero-Day Exploitation, Compromised RDP, Ransomware, Data exfiltration, Double-extortion

-TTPs-

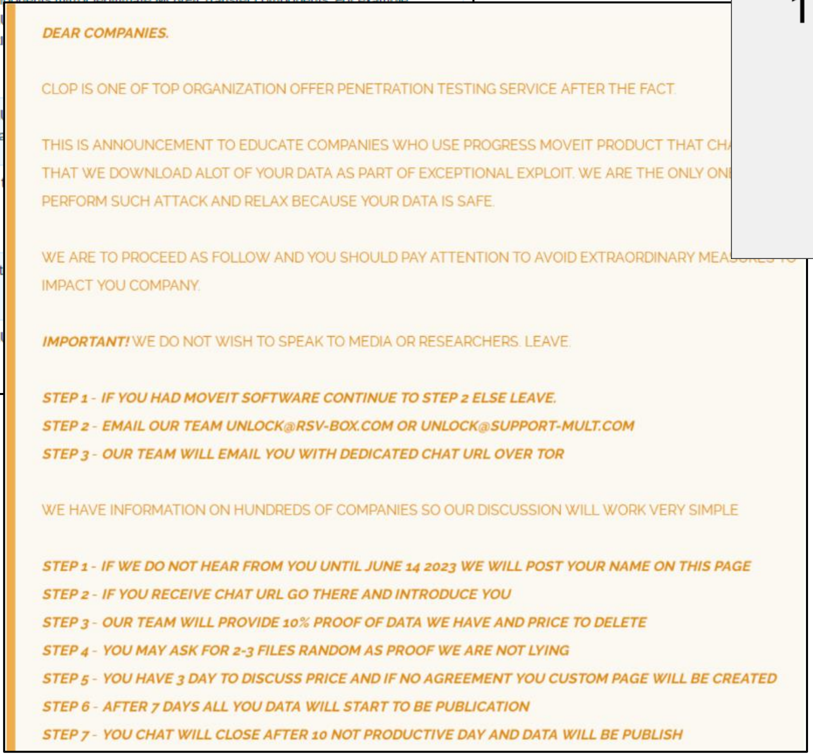
Exploit Public-Facing Application: T1190

Exploitation for Privilege

CL0p Extortion (2 of 2)



MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Description
Initial Access	Exploit Public Facing Application (T1190)	Exploited a SQL injection vulnerability in the managed file transfer solution
Persistence	Server Software Component: Web Shell (T1505.003)	Deployed a web shell named LEMURLOOT
Persistence	Create Account (T1136)	LEMURLOOT can create users in Azure
Privilege Escalation	Exploitation for Privilege Access (T1068)	Authenticated as a high-privilege user
Defense Evasion	Masquerading: Match Legitimate Name or Location (T1036.005)	Components mirror legitimate MOVEit Transfer components. For example LEM legit
Discovery	Cloud Storage Object Discovery (T1619)	LEM Stora
Command and Control	Application Layer Protocol: Web Protocols (T1071.001)	The
Exfiltration	Exfiltration over C2 Channel (T1041)	Exfilt
Impact	Account Access Removal (T1531)	LEM



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHA
THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE
PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

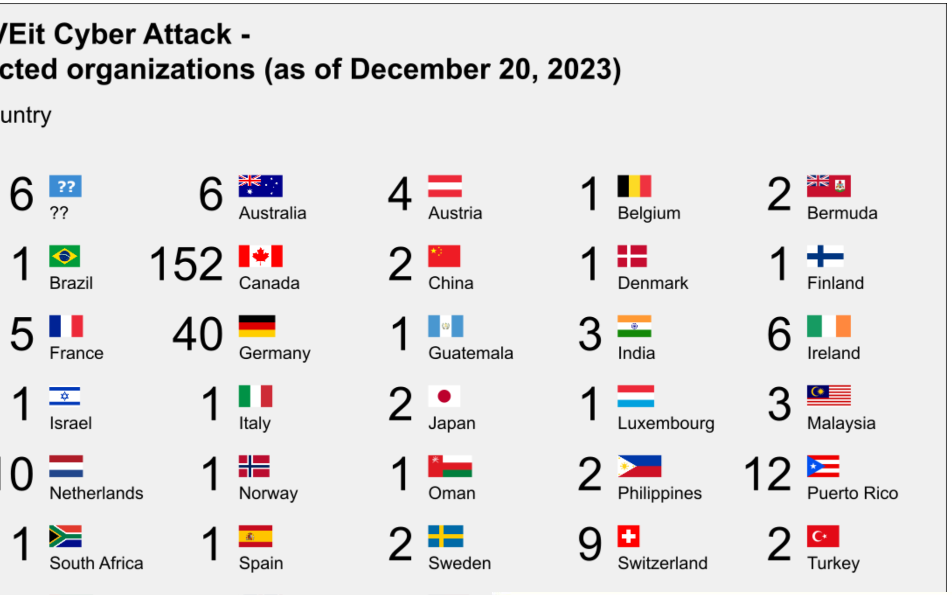
WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

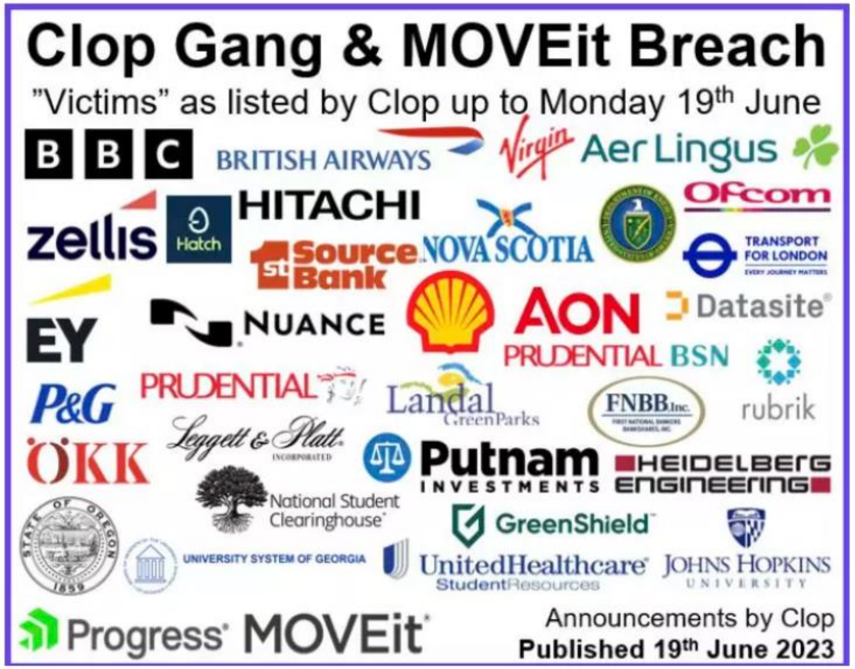
STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH



MOVEit Cyber Attack -
Affected organizations (as of December 20, 2023)

By country

6	??
6	Australia
4	Austria
1	Belgium
2	Bermuda
1	Brazil
152	Canada
2	China
1	Denmark
1	Finland
5	France
40	Germany
1	Guatemala
3	India
6	Ireland
1	Israel
1	Italy
2	Japan
1	Luxembourg
3	Malaysia
10	Netherlands
1	Norway
1	Oman
2	Philippines
12	Puerto Rico
1	South Africa
1	Spain
2	Sweden
9	Switzerland
2	Turkey
1	UAE
25	UK
2290	USA

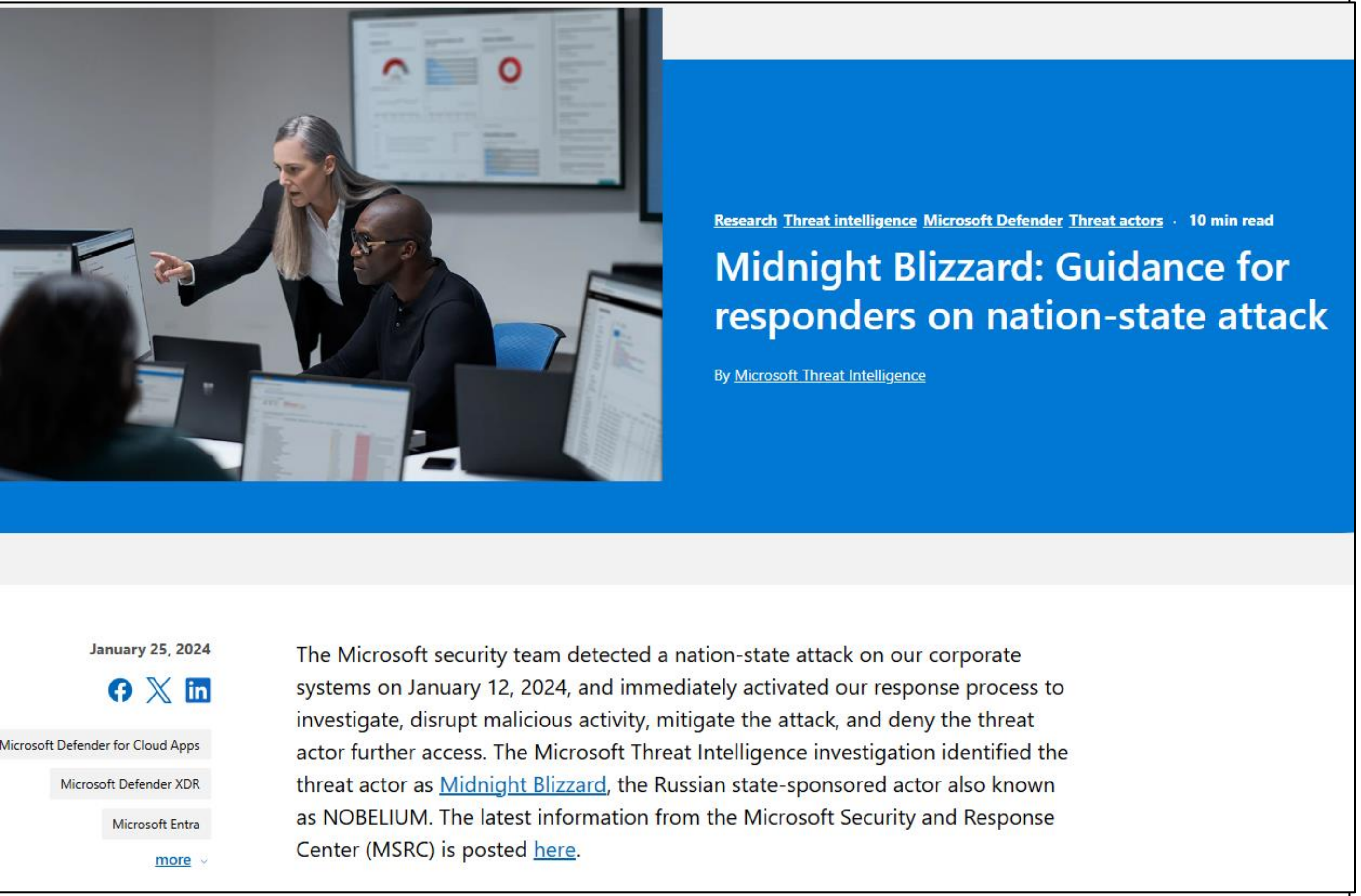


Clop Gang & MOVEit Breach

"Victims" as listed by Clop up to Monday 19th June

Announcements by Clop Published 19th June 2023

Midnight Blizzard RDP



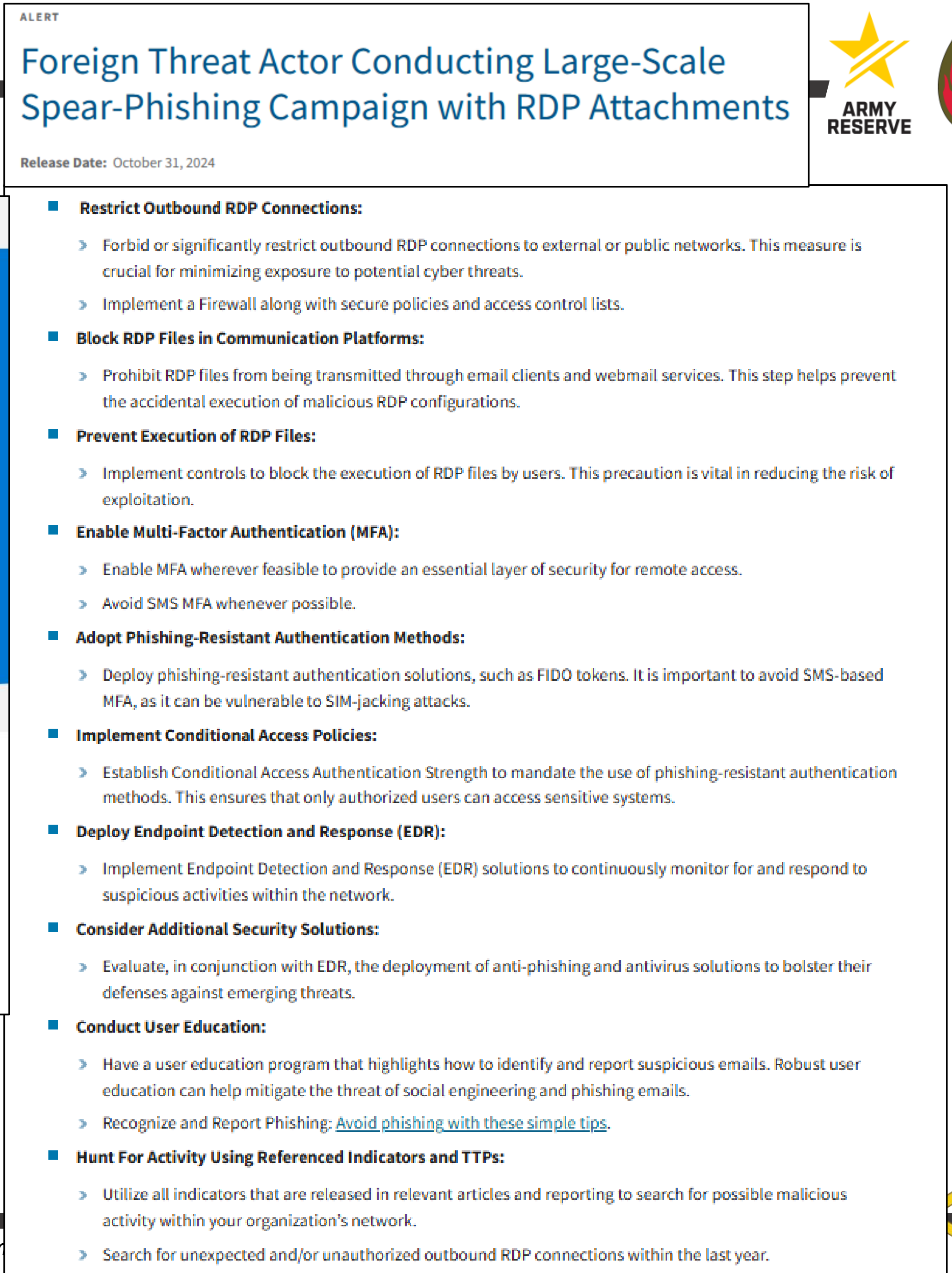
Research Threat intelligence Microsoft Defender Threat actors · 10 min read

Midnight Blizzard: Guidance for responders on nation-state attack

By Microsoft Threat Intelligence

January 25, 2024

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. The Microsoft Threat Intelligence investigation identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as NOBELIUM. The latest information from the Microsoft Security and Response Center (MSRC) is posted here.



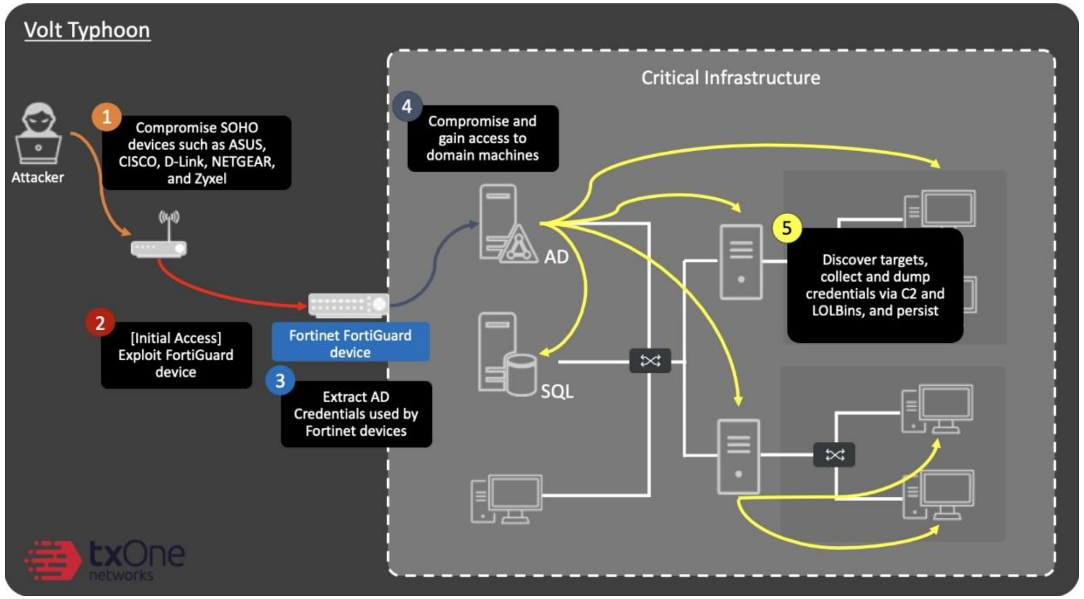
ALERT

Foreign Threat Actor Conducting Large-Scale Spear-Phishing Campaign with RDP Attachments

Release Date: October 31, 2024

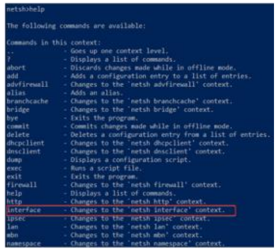
- **Restrict Outbound RDP Connections:**
  - Forbid or significantly restrict outbound RDP connections to external or public networks. This measure is crucial for minimizing exposure to potential cyber threats.
  - Implement a Firewall along with secure policies and access control lists.
- **Block RDP Files in Communication Platforms:**
  - Prohibit RDP files from being transmitted through email clients and webmail services. This step helps prevent the accidental execution of malicious RDP configurations.
- **Prevent Execution of RDP Files:**
  - Implement controls to block the execution of RDP files by users. This precaution is vital in reducing the risk of exploitation.
- **Enable Multi-Factor Authentication (MFA):**
  - Enable MFA wherever feasible to provide an essential layer of security for remote access.
  - Avoid SMS MFA whenever possible.
- **Adopt Phishing-Resistant Authentication Methods:**
  - Deploy phishing-resistant authentication solutions, such as FIDO tokens. It is important to avoid SMS-based MFA, as it can be vulnerable to SIM-jacking attacks.
- **Implement Conditional Access Policies:**
  - Establish Conditional Access Authentication Strength to mandate the use of phishing-resistant authentication methods. This ensures that only authorized users can access sensitive systems.
- **Deploy Endpoint Detection and Response (EDR):**
  - Implement Endpoint Detection and Response (EDR) solutions to continuously monitor for and respond to suspicious activities within the network.
- **Consider Additional Security Solutions:**
  - Evaluate, in conjunction with EDR, the deployment of anti-phishing and antivirus solutions to bolster their defenses against emerging threats.
- **Conduct User Education:**
  - Have a user education program that highlights how to identify and report suspicious emails. Robust user education can help mitigate the threat of social engineering and phishing emails.
  - Recognize and Report Phishing: Avoid phishing with these simple tips.
- **Hunt For Activity Using Referenced Indicators and TTPs:**
  - Utilize all indicators that are released in relevant articles and reporting to search for possible malicious activity within your organization's network.
  - Search for unexpected and/or unauthorized outbound RDP connections within the last year.

Volt Typhoon (1 of 2)



Volt Typhoon
Critical Infrastructure
Attacker
1
Compromise SOHO devices such as ASUS, CISCO, D-Link, NETGEAR, and Zyxel
2
[Initial Access] Exploit FortiGuard device
Fortinet FortiGuard device
3
Extract AD Credentials used by Fortinet devices
4
Compromise and gain access to domain machines
AD
SQL
5
Discover targets, collect and dump credentials via C2 and LOLBins, and persist
txOne networks

Active Directory



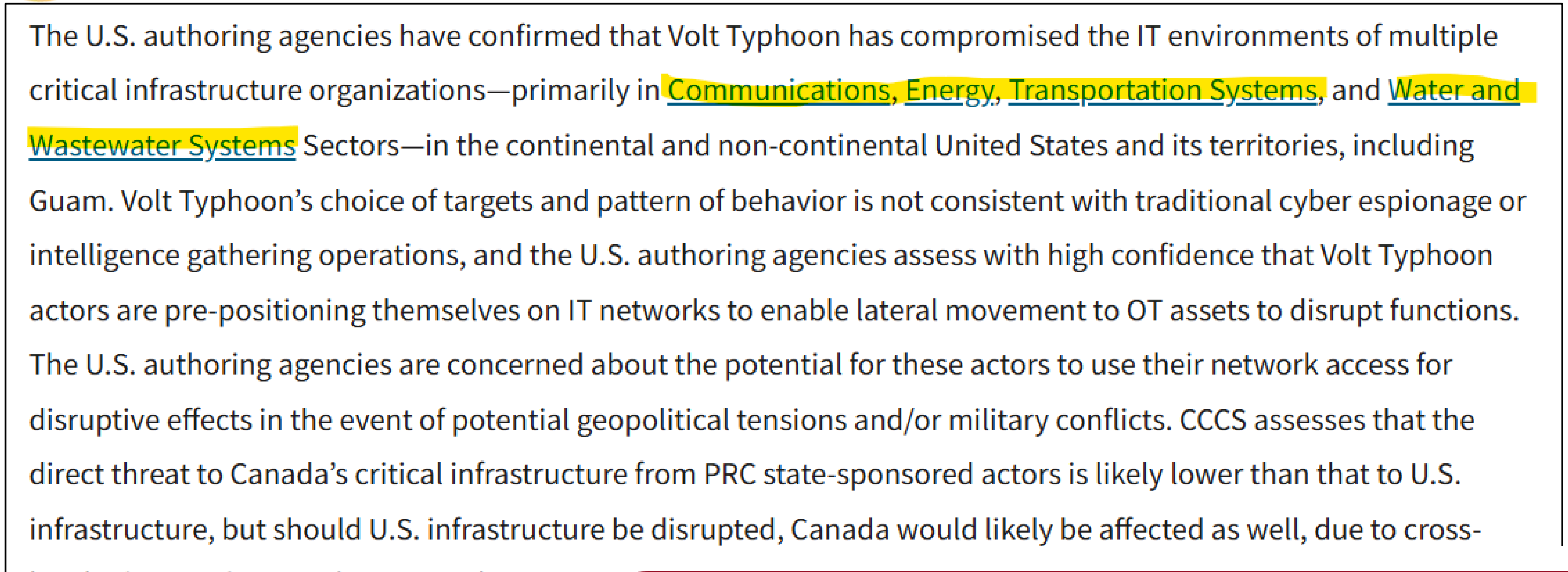
```
netsh>help

The following commands are available:

Commands in this context:
..             - Goes up one context level.
?              - Displays a list of commands.
abort          - Discards changes made while in offline mode.
add            - Adds a configuration entry to a list of entries.
advfirewall    - Changes to the `netsh advfirewall' context.
alias          - Adds an alias.
branchcache    - Changes to the `netsh branchcache' context.
bridge         - Changes to the `netsh bridge' context.
bye            - Exits the program.
commit         - Commits changes made while in offline mode.
delete         - Deletes a configuration entry from a list of entries.
dhcpclient     - Changes to the `netsh dhcpclient' context.
dnsclient      - Changes to the `netsh dnsclient' context.
dump           - Displays a configuration script.
exec           - Runs a script file.
exit           - Exits the program.
firewall       - Changes to the `netsh firewall' context.
help           - Displays a list of commands.
http           - Changes to the `netsh http' context.
interface      - Changes to the `netsh interface' context.
ipsec          - Changes to the `netsh ipsec' context.
lan            - Changes to the `netsh lan' context.
mbn            - Changes to the `netsh mbn' context.
namespace      - Changes to the `netsh namespace' context.
```

WMI Windows Management Instrumentation

PsExec

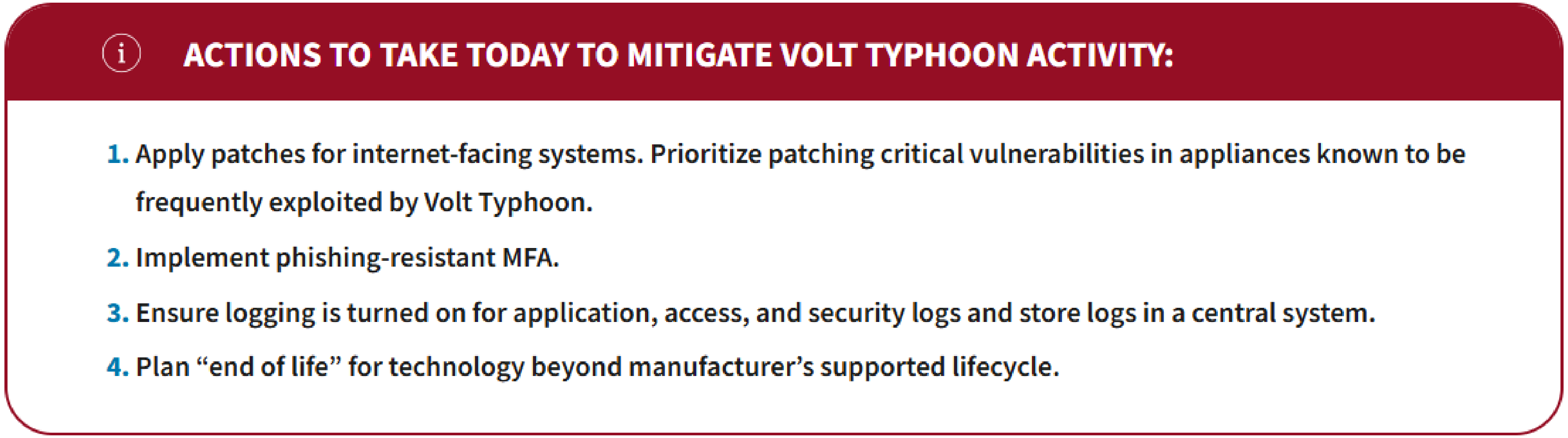
RESOURCE DEVELOPMENT	INITIAL ACCESS	EXECUTION	PERSISTENCE	CREDENTIAL ACCESS	DISCOVERY	COLLECTION	COMMAND AND CONTROL
Compromised SOHO devices	Unknown Fortinet exploit	WMIC, PowerShell, and CLI	Valid accounts	LSASS process memory dumping	Virtualization evasion	Local browser data	Internal proxy
				Domain controller installation media creation	Remote system discovery	Data staging	
					Local system information discovery		

Volt Typhoon (2 of 2)



The U.S. authoring agencies have confirmed that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations—primarily in Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors—in the continental and non-continental United States and its territories, including Guam. Volt Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions. The U.S. authoring agencies are concerned about the potential for these actors to use their network access for disruptive effects in the event of potential geopolitical tensions and/or military conflicts. CCCS assesses that the direct threat to Canada's critical infrastructure from PRC state-sponsored actors is likely lower than that to U.S. infrastructure, but should U.S. infrastructure be disrupted, Canada would likely be affected as well, due to cross-border integration. ASD's ACSC and NCSC-I

could be vulnerable to similar activity from



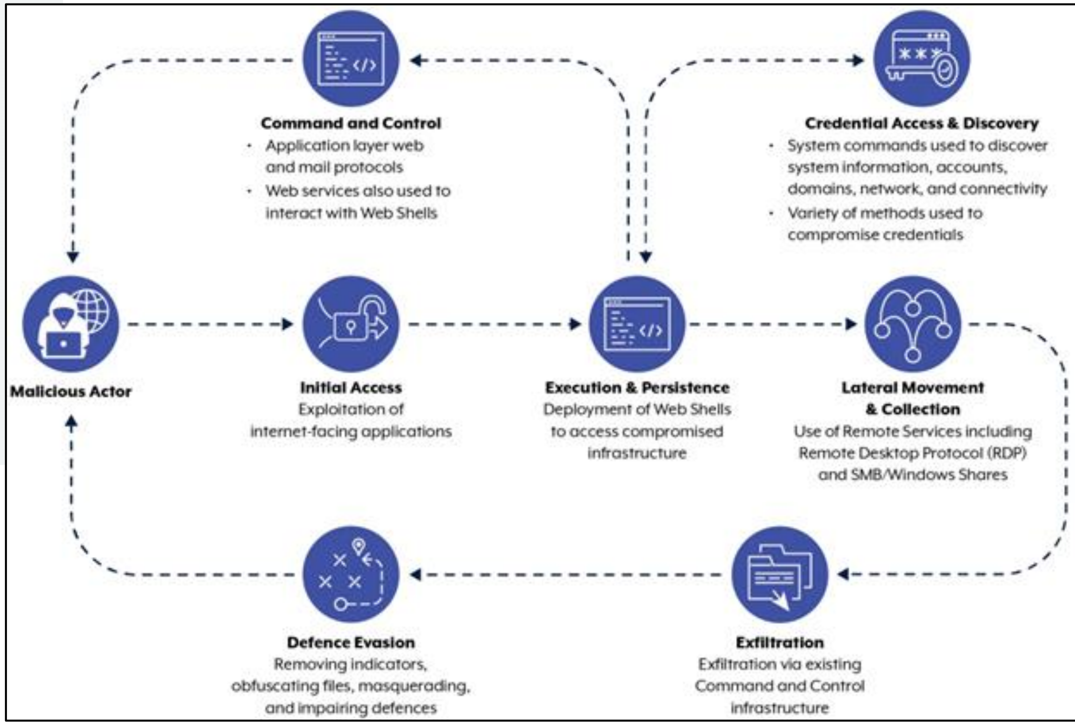
ⓘ ACTIONS TO TAKE TODAY TO MITIGATE VOLT TYPHOON ACTIVITY:

1. Apply patches for internet-facing systems. Prioritize patching critical vulnerabilities in appliances known to be frequently exploited by Volt Typhoon.
2. Implement phishing-resistant MFA.
3. Ensure logging is turned on for application, access, and security logs and store logs in a central system.
4. Plan "end of life" for technology beyond manufacturer's supported lifecycle.

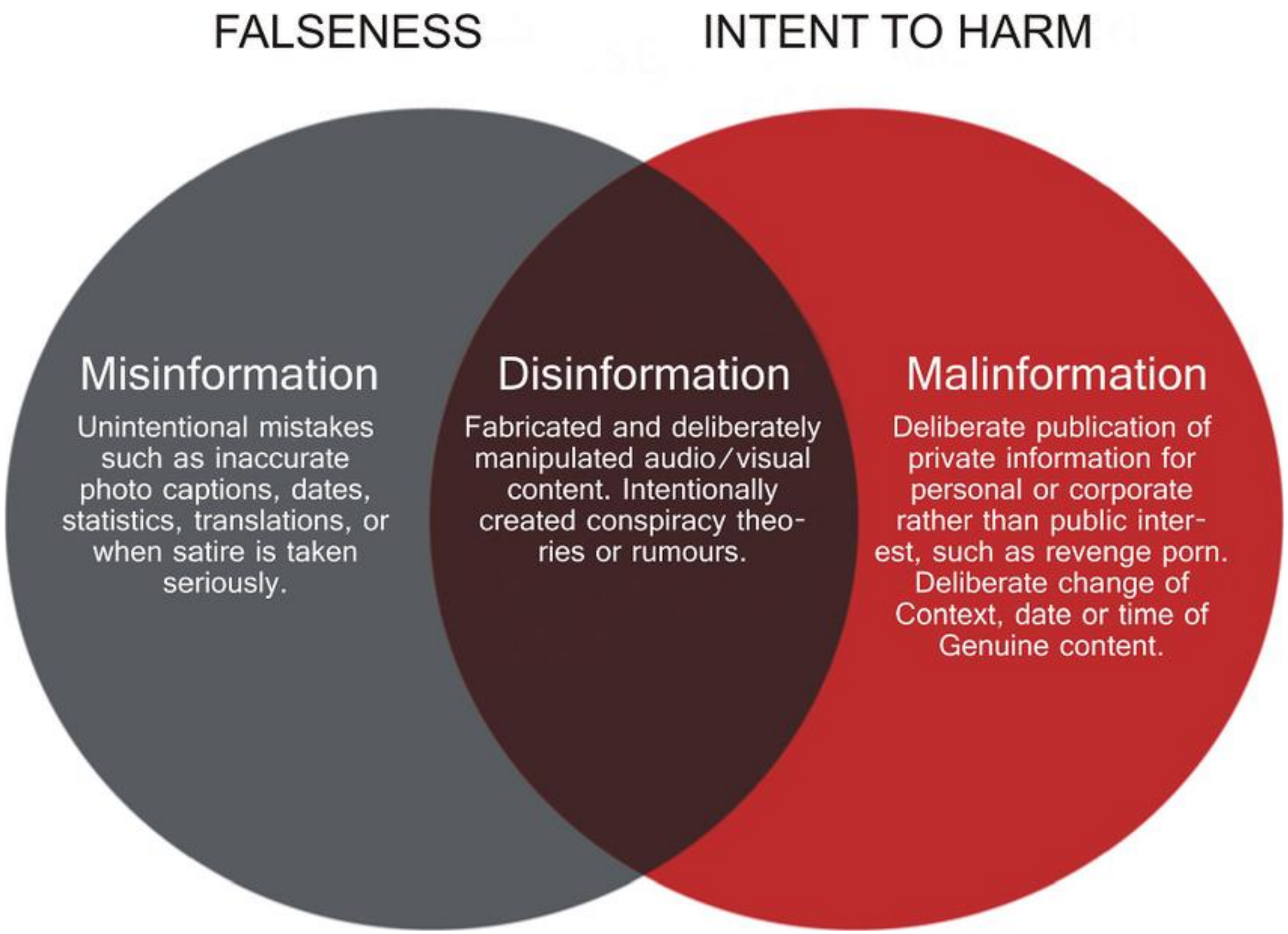
Salt Typhoon

SALT TYPHOON: TARGETING ISPS AND DATA PERSISTENCE

While Salt Typhoon has not garnered as much publicity as other APT groups, it has been linked to significant intrusions within U.S. Internet Service Providers (ISPs). Salt Typhoon's campaign has focused on compromising routers and other network devices to establish persistent access. Their activities have been primarily espionage-oriented, to collect sensitive data, such as authorized wiretaps, from ISP networks while maintaining a low profile. This threat actor mirrors some tactics from other Typhoon groups, especially using LOTL techniques to prolong their foothold in target environments.


Command and Control
Application layer web and mail protocols
Web services also used to interact with Web Shells
Credential Access & Discovery
System commands used to discover system information, accounts, domains, network, and connectivity
Variety of methods used to compromise credentials
Malicious Actor
Initial Access
Exploitation of internet-facing applications
Execution & Persistence
Deployment of Web Shells to access compromised infrastructure
Lateral Movement & Collection
Use of Remote Services including Remote Desktop Protocol (RDP) and SMB/Windows Shares
Defence Evasion
Removing indicators, obfuscating files, masquerading, and impairing defences
Exfiltration
Exfiltration via existing Command and Control infrastructure

Mis/Dis/Mal-Information



FALSENESS

INTENT TO HARM

Misinformation

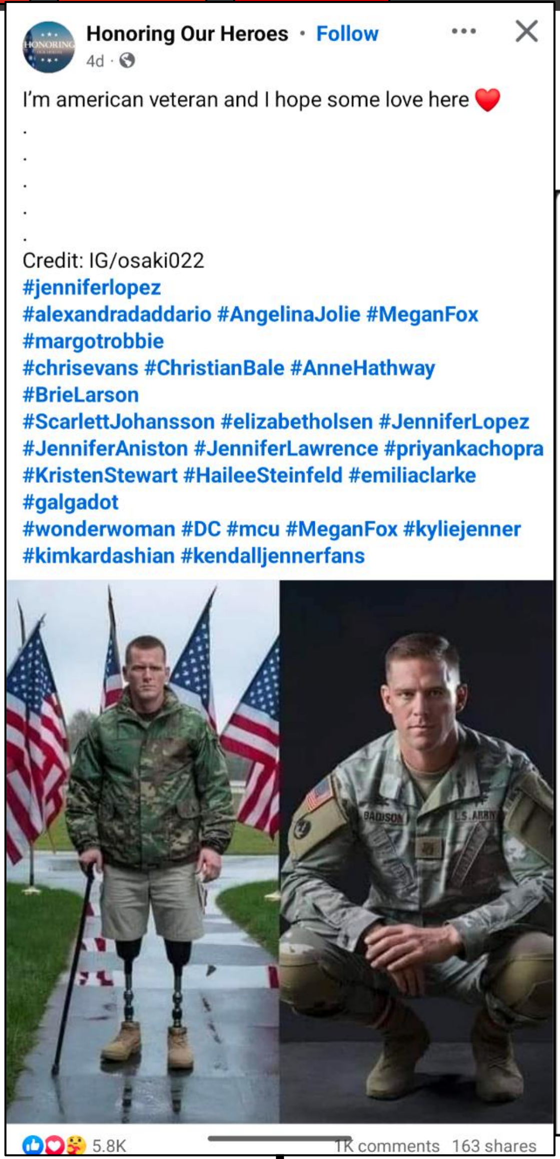
Unintentional mistakes such as inaccurate photo captions, dates, statistics, translations, or when satire is taken seriously.

Disinformation

Fabricated and deliberately manipulated audio/visual content. Intentionally created conspiracy theories or rumours.

Malinformation

Deliberate publication of private information for personal or corporate rather than public interest, such as revenge porn. Deliberate change of Context, date or time of Genuine content.



Honoring Our Heroes · Follow

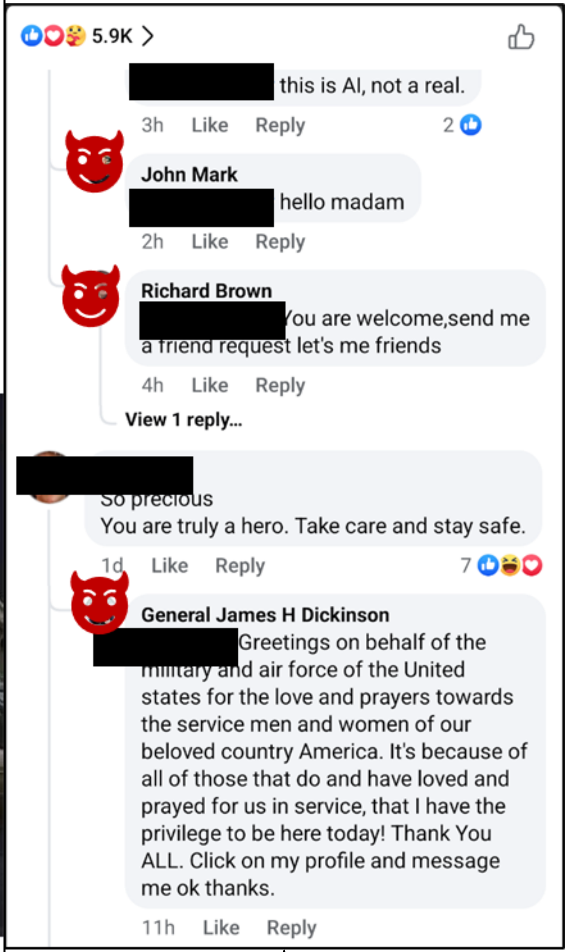
4d

I'm american veteran and I hope some love here ❤

.
.
.
.
.

Credit: IG/osaki022
#jenniferlopez
#alexandradaddario #AngelinaJolie #MeganFox
#margotrobbie
#chrisevans #ChristianBale #AnneHathway
#BrieLarson
#ScarlettJohansson #elizabetholsen #JenniferLopez
#JenniferAniston #JenniferLawrence #priyankachopra
#KristenStewart #HaileeSteinfeld #emiliaclarke
#galgadot
#wonderwoman #DC #mcu #MeganFox #kyliejenner
#kimkardashian #kendalljennerfans

5.8K   1K comments 163 shares



5.9K

[redacted] this is AI, not a real.

3h Like Reply 2

John Mark

[redacted] hello madam

2h Like Reply

Richard Brown

[redacted] You are welcome,send me a friend request let's me friends

4h Like Reply

View 1 reply...

[redacted] So precious
You are truly a hero. Take care and stay safe.

1d Like Reply 7

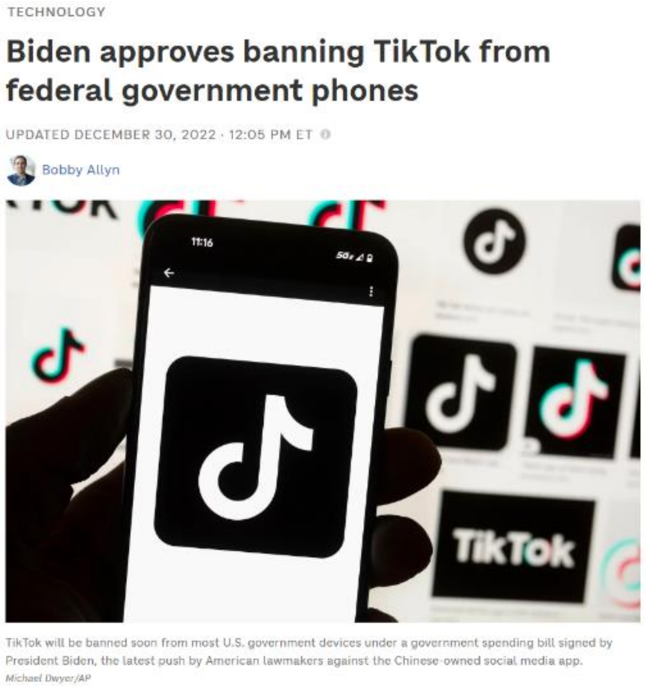
General James H Dickinson

[redacted] Greetings on behalf of the military and air force of the United states for the love and prayers towards the service men and women of our beloved country America. It's because of all of those that do and have loved and prayed for us in service, that I have the privilege to be here today! Thank You ALL. Click on my profile and message me ok thanks.

11h Like Reply

TikTok and Influence

2022



TECHNOLOGY

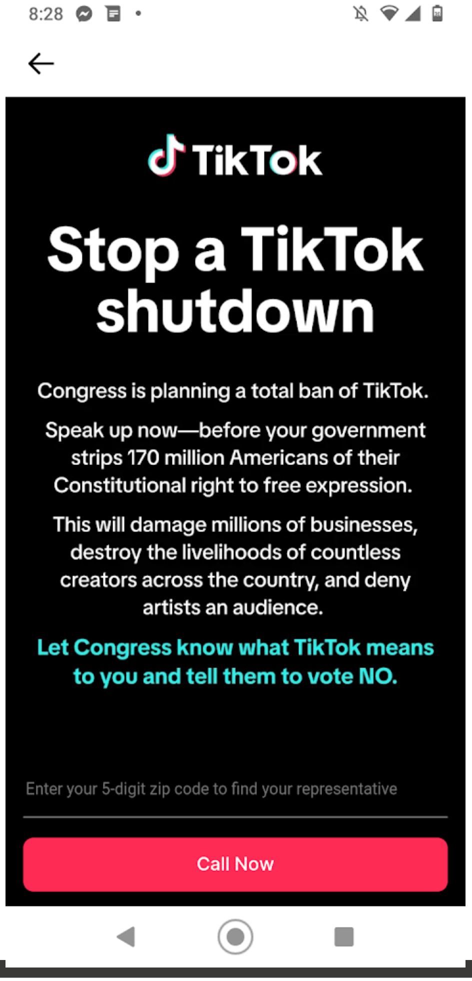
Biden approves banning TikTok from federal government phones

UPDATED DECEMBER 30, 2022 · 12:05 PM ET

Bobby Allyn

TikTok will be banned soon from most U.S. government devices under a government spending bill signed by President Biden, the latest push by American lawmakers against the Chinese-owned social media app.
Michael Dwyer/AP

2024



TikTok

Stop a TikTok shutdown

Congress is planning a total ban of TikTok.

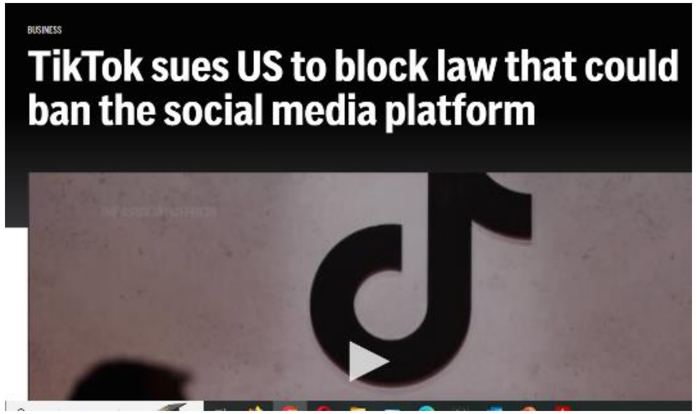
Speak up now—before your government strips 170 million Americans of their Constitutional right to free expression.

This will damage millions of businesses, destroy the livelihoods of countless creators across the country, and deny artists an audience.

Let Congress know what TikTok means to you and tell them to vote NO.

Enter your 5-digit zip code to find your representative

Call Now



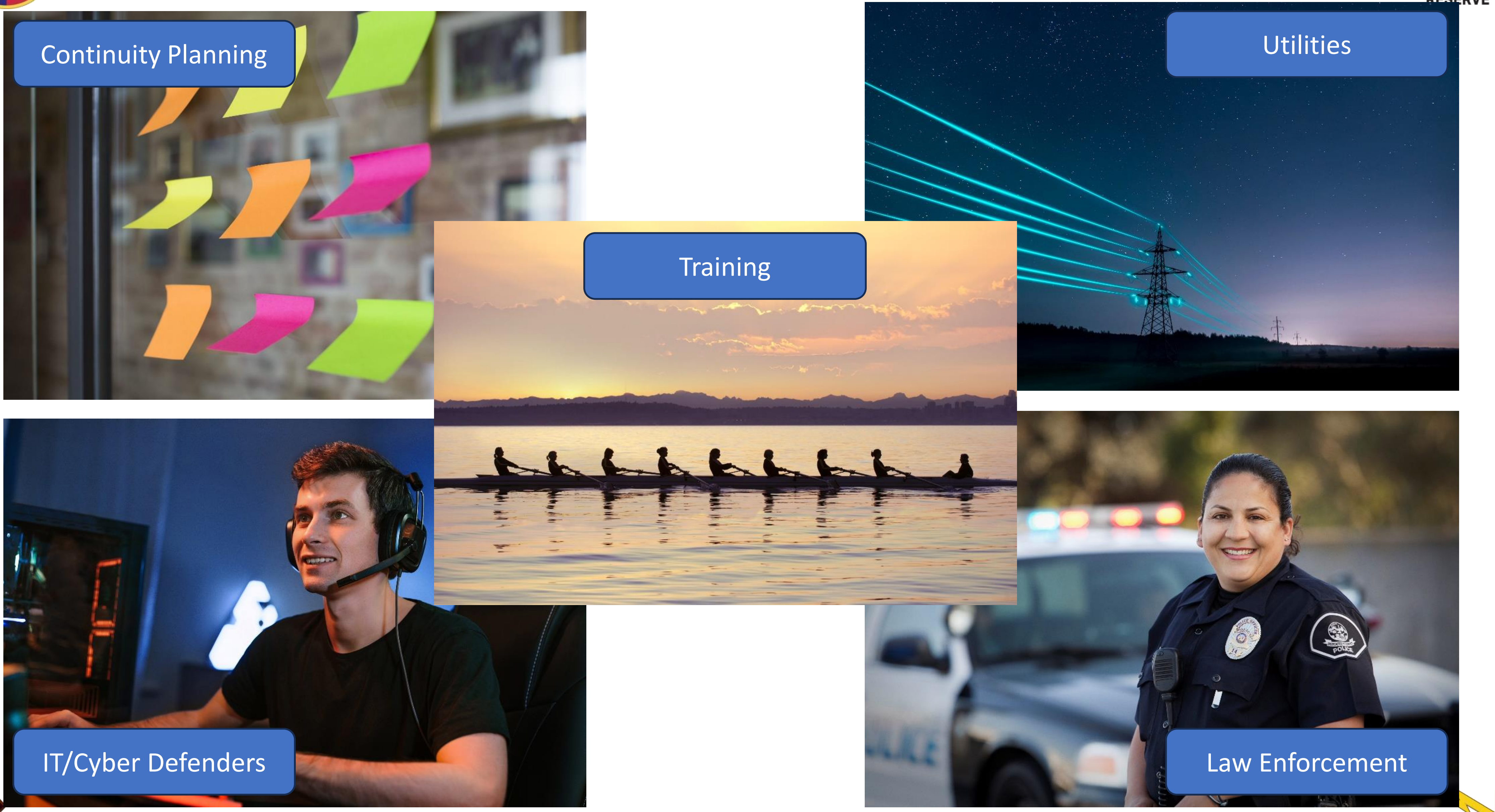
BUSINESS

TikTok sues US to block law that could ban the social media platform

Key Current Threat TTPs

- Internet Exposed Infrastructure
- End-of-Life Systems
- Web Shells
- Phishing and Attachments

What can you do “Left of Boom?”



Continuity Planning

Utilities

Training

IT/Cyber Defenders

Law Enforcement

THANK YOU: AFCEA Silicon Valley Cyber & IT Summit!

Q & A & Discuss!

Happy to connect: https://www.linkedin.com/in/brad-e-rhodes-the-terminal-colonel/