

The background is a dark gray gradient. On the left side, there are white circuit-like lines with small circles at the ends, resembling a printed circuit board. The rest of the background is filled with numerous overlapping circles in various shades of purple, blue, and teal, creating a bokeh or bubble effect.

# THE INFORMATION ENVIRONMENT AND YOU

COL BRAD E. RHODES

# AGENDA

- WHOIS
- The Primer
- The Information Environment
- Cyber & The Information Environment
- Information Environment Challenges
- Examples “Ripped” from the Headlines
- IE Parting Thoughts

# 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), 63<sup>rd</sup> 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>



# THE PRIMER

We live in a world dominated by **information**. Unfortunately, that information is under assault every day and we can no longer necessarily **trust** what we see and hear (throw in AI / Machine Learning and all bets are off). Within the cyber domain and the broader information environment it is critical to understand how and why information is **manipulated**, threat actor **intent(s)** when it comes to information, and finally how to educate our users. Let's have a conversation about advanced threat actors who are now starting their information attack sequences using our **personal emails** and text messages. As threat actors continue to look for novel approaches impact our organizations, we need tactics to ensure everyone from leadership to the frontline workers understand risks they face.



# THE INFORMATION ENVIRONMENT

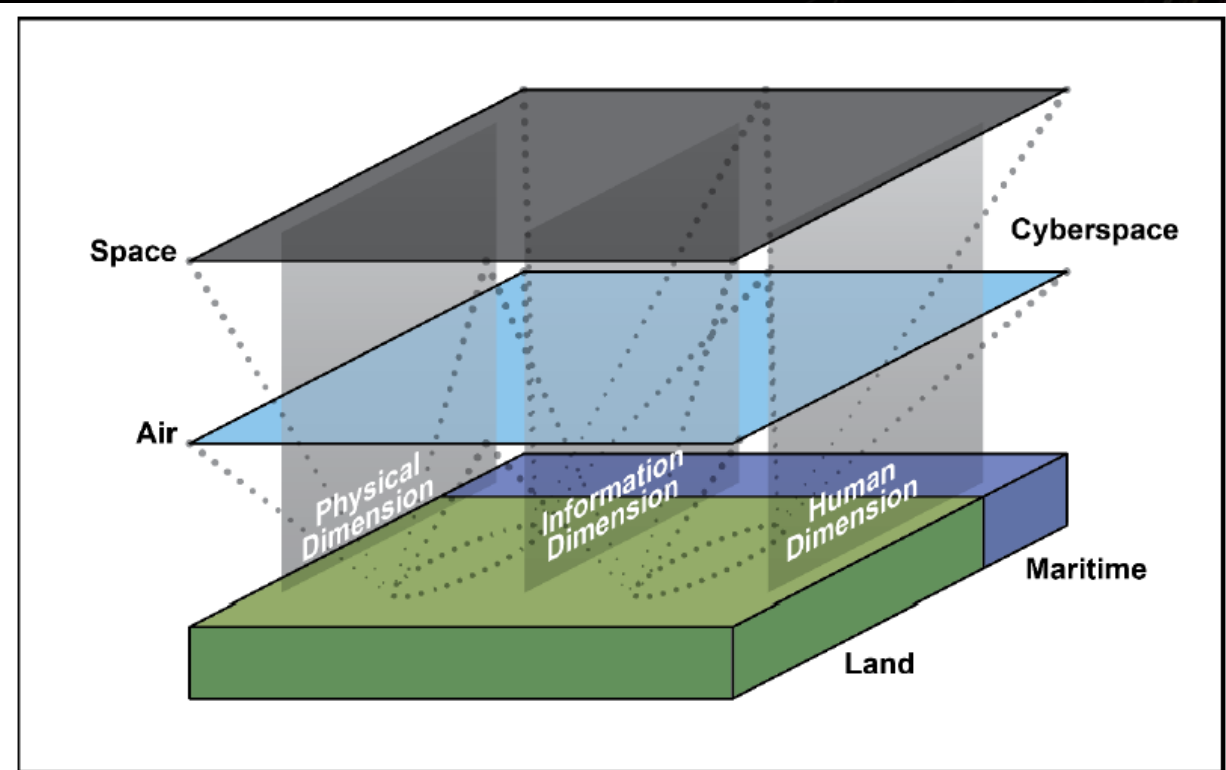
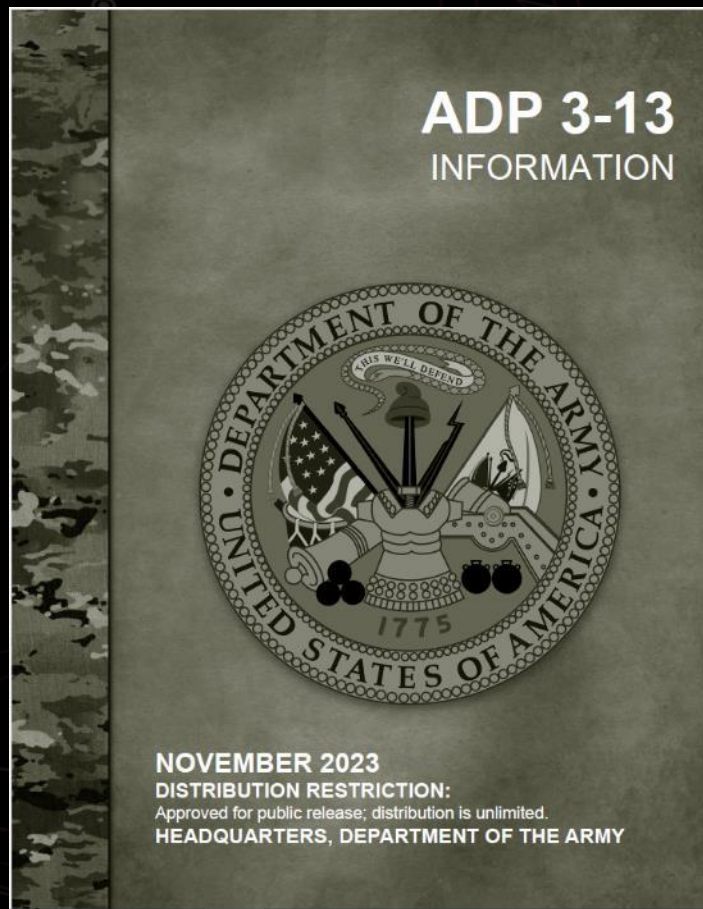
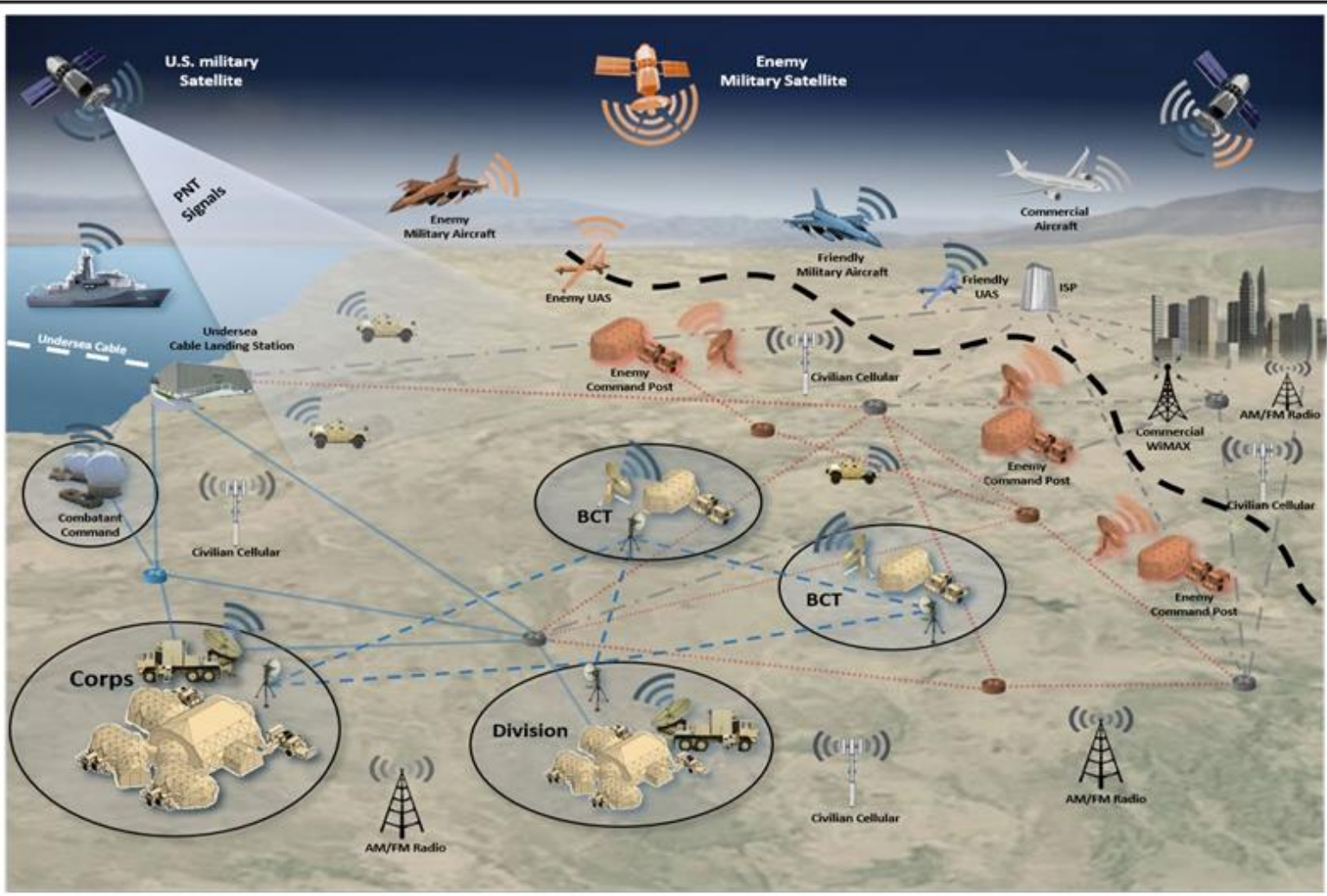


Figure 1-3. Domains and dimensions of an operational environment

# CYBER & THE INFORMATION ENVIRONMENT



AUGUST 2021  
DISTRIBUTION RESTRICTION:  
Approved for public release; distribution is unlimited.  
This document contains information that is not to be released to the public.  
HEADQUARTERS, DEPARTMENT OF THE ARMY

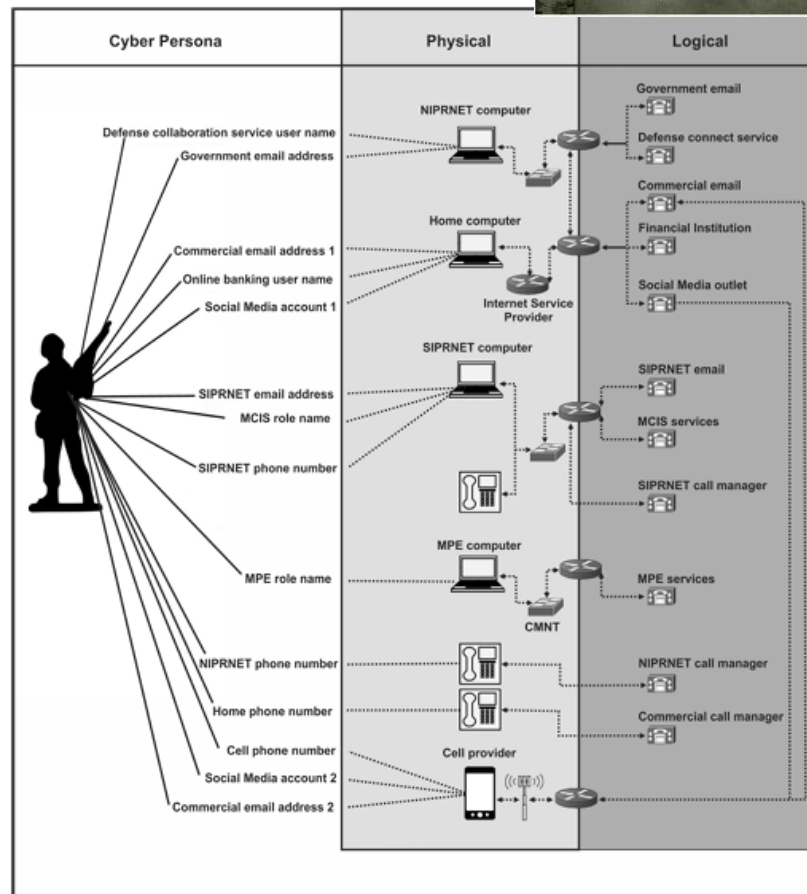


**LEGEND**

BCT brigade combat team  
 enemy wired network .....  
 enemy wireless transmission (signal icon)  
 friendly wireless network - - - - -  
 friendly wired network ————

friendly wireless transmission (signal icon)  
 geographical boundary ————  
 neutral wired network - - - - -  
 neutral wireless transmission (signal icon)  
 ISP Internet service provider

PNT position, navigation, and timing  
 UAS unmanned aircraft system  
 WiMAX Worldwide Interoperability for Microwave Access



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

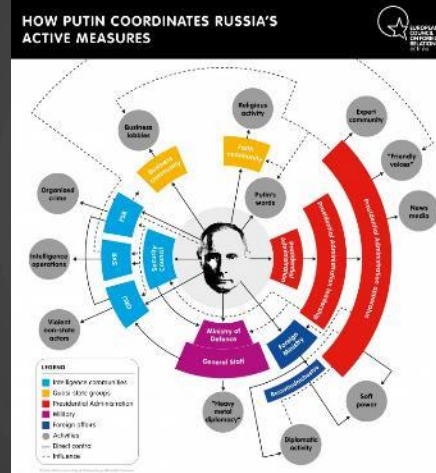
Figure 1-2. Relationship between the cyberspace network layers





# INFORMATION ENVIRONMENT (IE) CHALLENGES

- States Controlling Information & Access
- Election Interference
- The “New” Electronic Warfare Frontier
- Kimsuky and the Scientists
- The TikTok Ban & China’s Campaign to Stop It
- Deep Fakes & AI/ML



### FREEDOM ON THE NET 2023

## Russia

21 /100

NOT FREE

A. Obstacles to Access	10 /25
B. Limits on Content	5 /35
C. Violations of User Rights	6 /40

LAST YEAR'S SCORE & STATUS 23 /100 ■ Not Free

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.

### FREEDOM ON THE NET 2023

## China

9 /100

NOT FREE

A. Obstacles to Access	7 /25
B. Limits on Content	2 /35
C. Violations of User Rights	0 /40

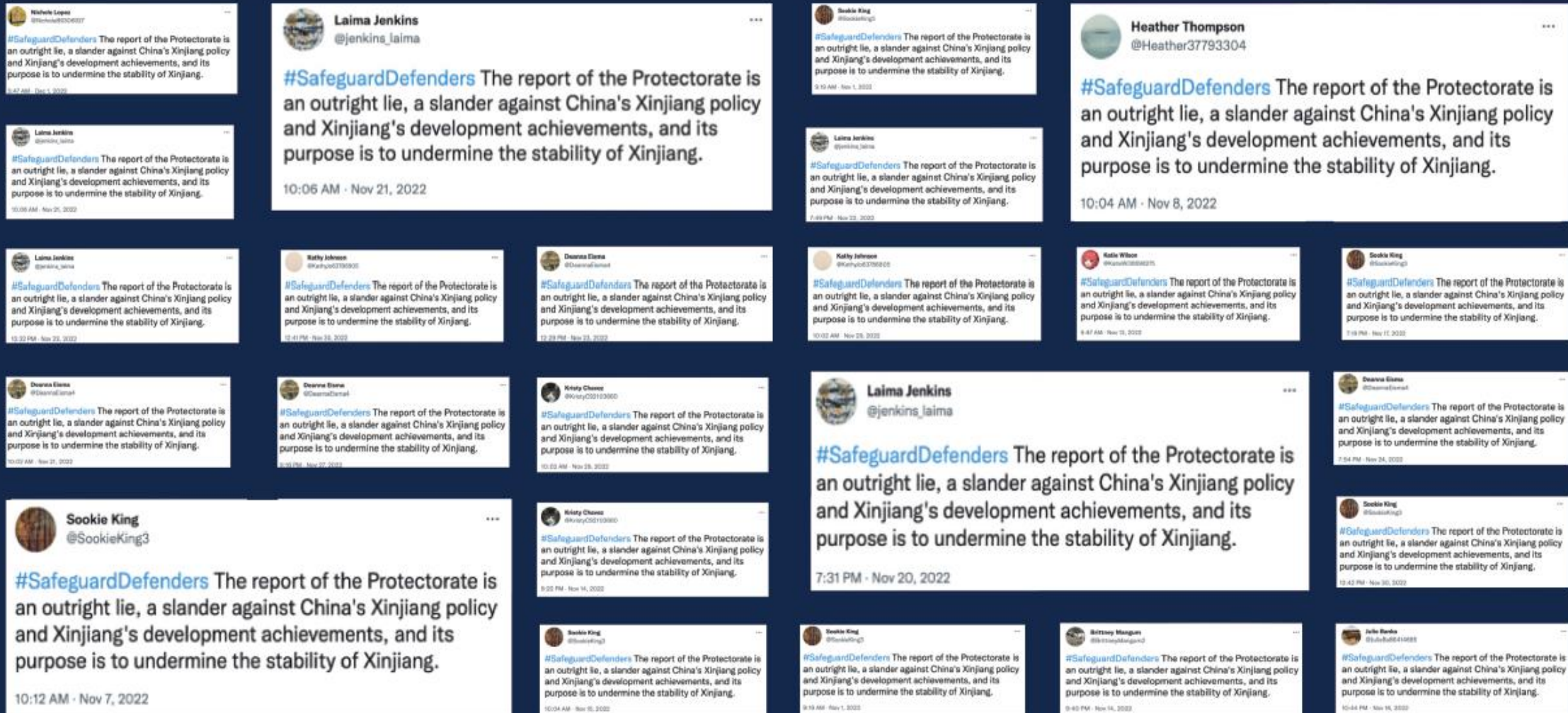
LAST YEAR'S SCORE & STATUS 10 /100 ■ Not Free

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.





# Imposter Accounts Flood Twitter to Drown Out Criticism of the PRC

As of August 2023, at least 265 accounts are targeting @SafeguardDefend in a coordinated information manipulation operation

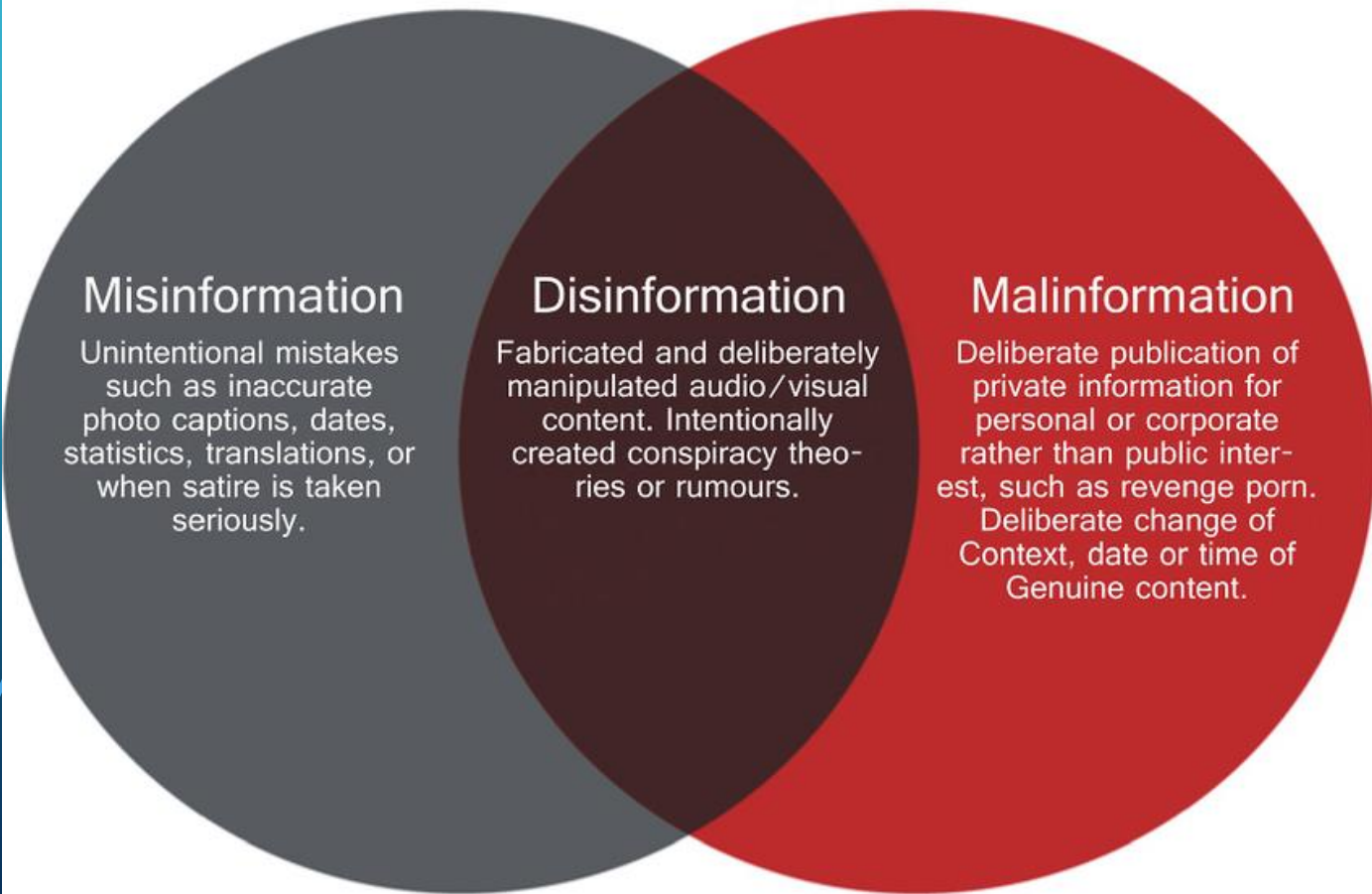


# ELECTION INTERFERENCE

2016	2020	2024
	 	  




FALSENESS

INTENT TO HARM



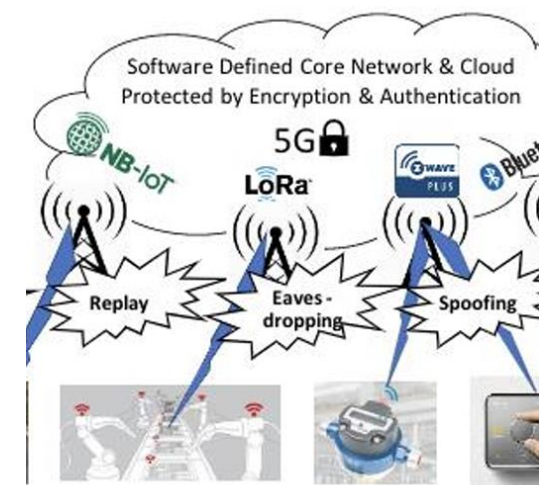
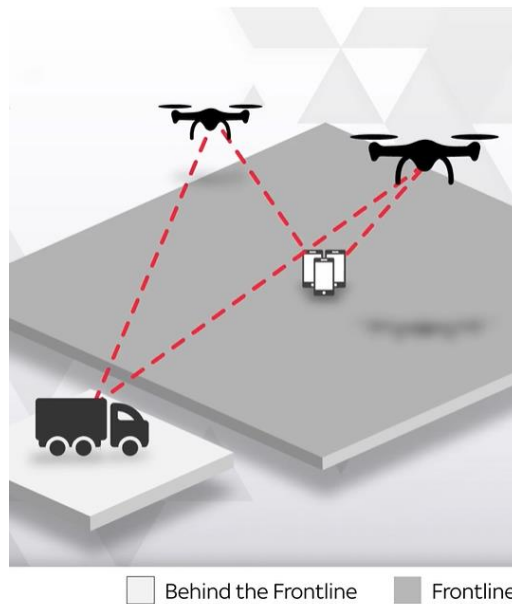
## Blinken tells CNN the US has seen evidence of China attempting to influence upcoming US elections

By Simone McCarthy, CNN  
6 minute read · Updated 6:38 PM EDT, Fri April 26, 2024







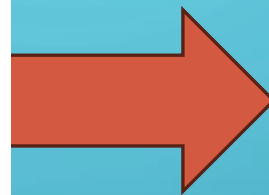
RF Open Attack Surface in today's wireless networks

## THE “NEW” ELECTRONIC WARFARE FRONTIER



## UKRAINIAN ARMY ORDER

1. Leave your own SIM card at home.
2. The best place to get a SIM card is in the zone of conflict itself.
3. If you plan to make a phone call, walk at least 400-500 m away from squad positions.
4. Don't walk away alone, take an armed friend with you to cover you.
5. The best place to make a phone call is in locations with a lot of civilians, preferably in recently liberated towns.
6. Always keep your phone off. Your life depends on it. Grad missiles will hit your whole squad.
7. Do not accept refill codes or cards from the locals. The young woman that brought you a refill card from the neighbouring village may be working for the enemy. Right now FSB and SBU have to process enormous amounts of data to identify the mobile phones of our own people and of the enemy. Do not make their job easier.
8. Watch over your comrades – a friend calls his girlfriend and an hour or so later your position gets shelled or attacked.
9. Remember, the enemy could be listening to your conversations regardless of which SIM card or which telecom operator you are using.



Uncle Sam says, “Don’t Take  
Your Cell Phone to War!”

# THE “NEW” ELECTRONIC WARFARE FRONTIER

# KIMSUKY AND THE SCIENTISTS



U.S. DEPARTMENT of STATE

Newsroom Business Employees Job Seekers Students Travelers Visas



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

Subject: [Invitation] 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 North Korea is unlikely begin crafting a new

We understand you that lunch (12:30- 1 accommodations to available to join in p

Please let me know and logistics right a

All the best,  
<name of legitimate

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 in 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



# TIKTOK BAN + CHINA'S CAMPAIGN TO STOP IT

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



8:28

←

 **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.

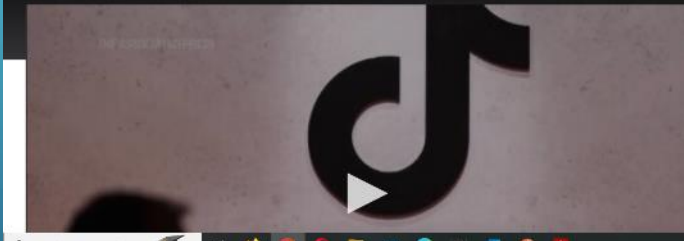
**Let Congress know what TikTok means to you and tell them to vote NO.**

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








 **FakeYou** AI Tools ▾

[★ Pricing](#) [Login](#) [Sign Up](#)



## AI Music, Text to Speech, and Voice to Voice

Use FakeYou's deepfake technology to generate audio or videos of your favorite characters saying anything you want.

[Get Started Free →](#)

Select a Voice

[Rick](#) [Mickey](#) [Eric](#) [Stan](#) [Zelda](#) [Angry Male](#)

What would you like to say? [Randomize Text](#)

[▶ Speak](#)

**NEWS** 9 MAY 2024

# AI-Powered Russian Network Pushes Fake Political News

DEEP FAKES + ML/AI



# IE PARTING THOUGHTS

- LSCO & DSCA - Information as **FIRES**
- In the West: You and your data is the **PRODUCT!**
- Elsewhere: You and your data + intellectual property is the **TARGET!**
- China and Russia leverage the IE for **EFFECTS** in/through cyberspace
- Are you thinking about the IE? In an era where we have may/may not have **MASS**, it is imperative we win the **INFORMATION** fight!



**Thank you,  
Peak Cyber Symposium!**

**Q & A & Discuss!**

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