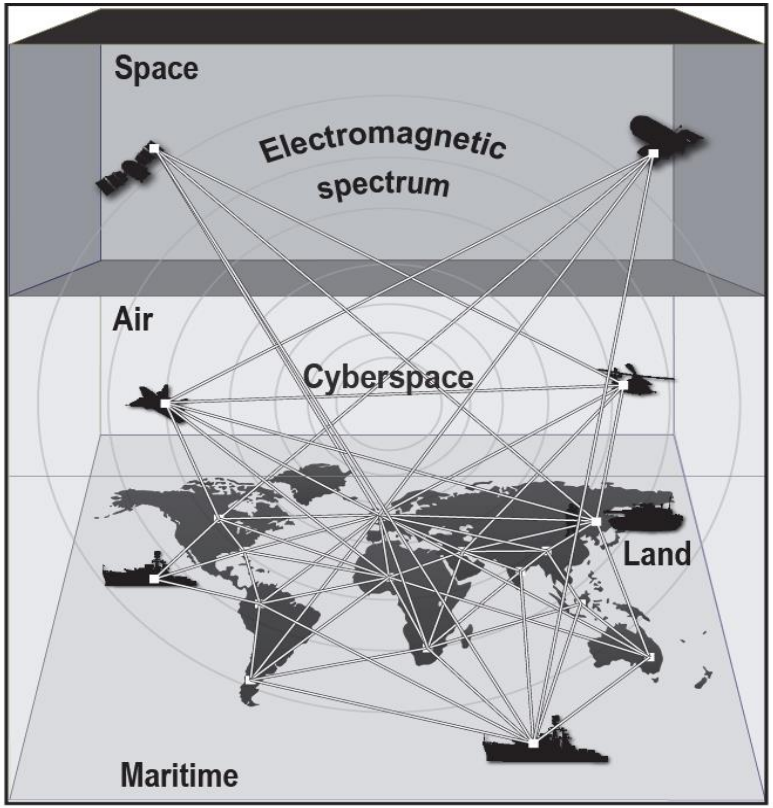
Cyber Threat Awareness

The overall classification of this briefing is:
UNCLASSIFIED

Purpose

To ensure that all Soldiers comprehend the relationship between cyberspace and the electromagnetic spectrum and maintains the necessary protection measures when using personal and government devices on and off duty.



References

FM 3-38 Cyber Electromagnetic Activities (CEMA)

FM 3-36 Electronic Warfare

FM 6-02 Signal Support to Operations

FM 6-02.70 Army Electromagnetic Spectrum Operations

FBI Social Networking Threats

Agenda

- Introduction
- Cyber Electromagnetic Activities (CEMA) Defined
- Cyber Electromagnetic (EM) Vulnerabilities and Threats
- Cyber EM Security and Protection
- Questions

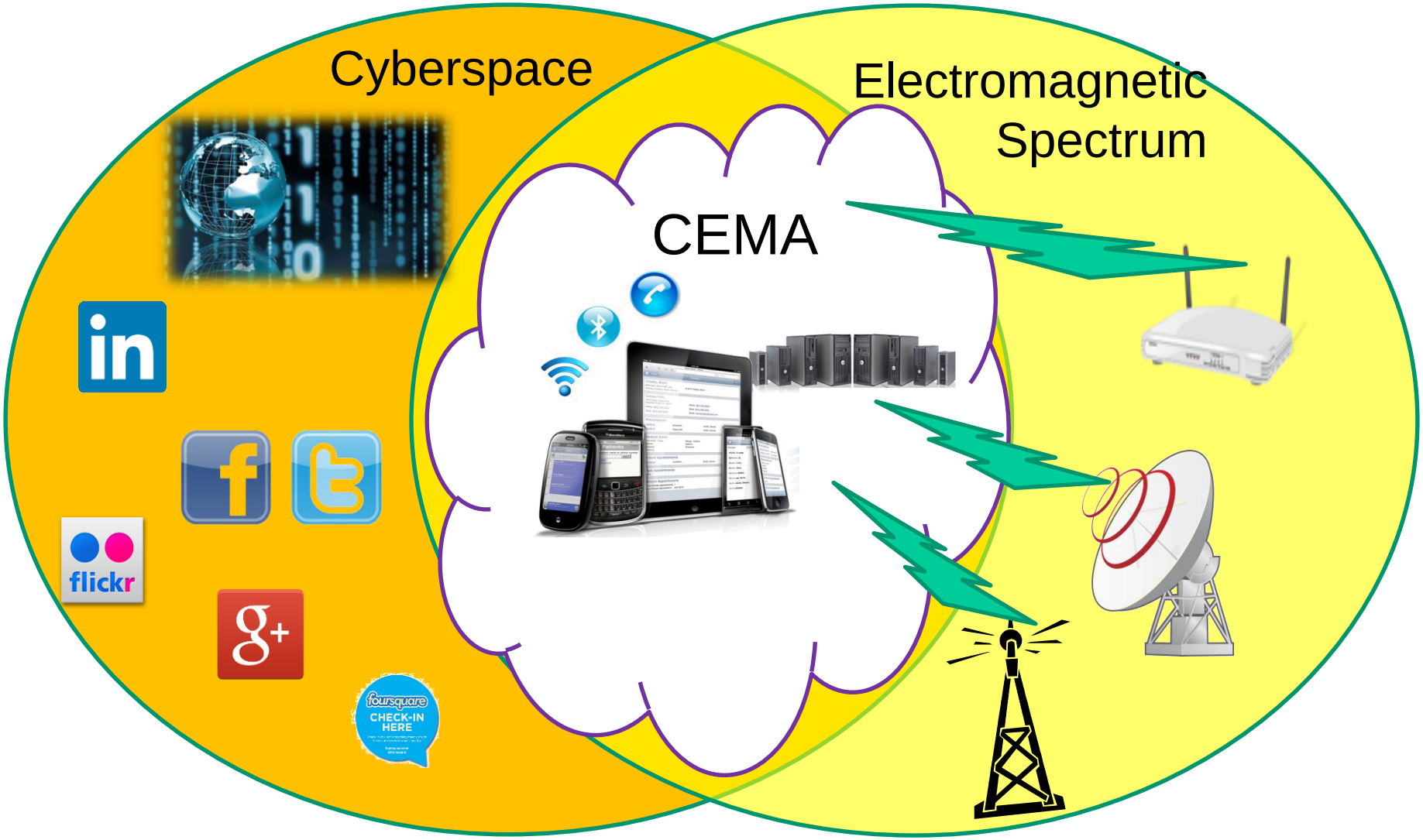
Introduction

"Many of our adversaries lack the ability to confront our forces physically, choosing instead to employ virtual weapons with potentially devastating effect. We must take full advantage of these technologies, building our own capabilities to operate in cyberspace with the same level of skill and confidence we enjoy on the land. We will either adapt to this reality or risk ceding the advantage to future enemies."

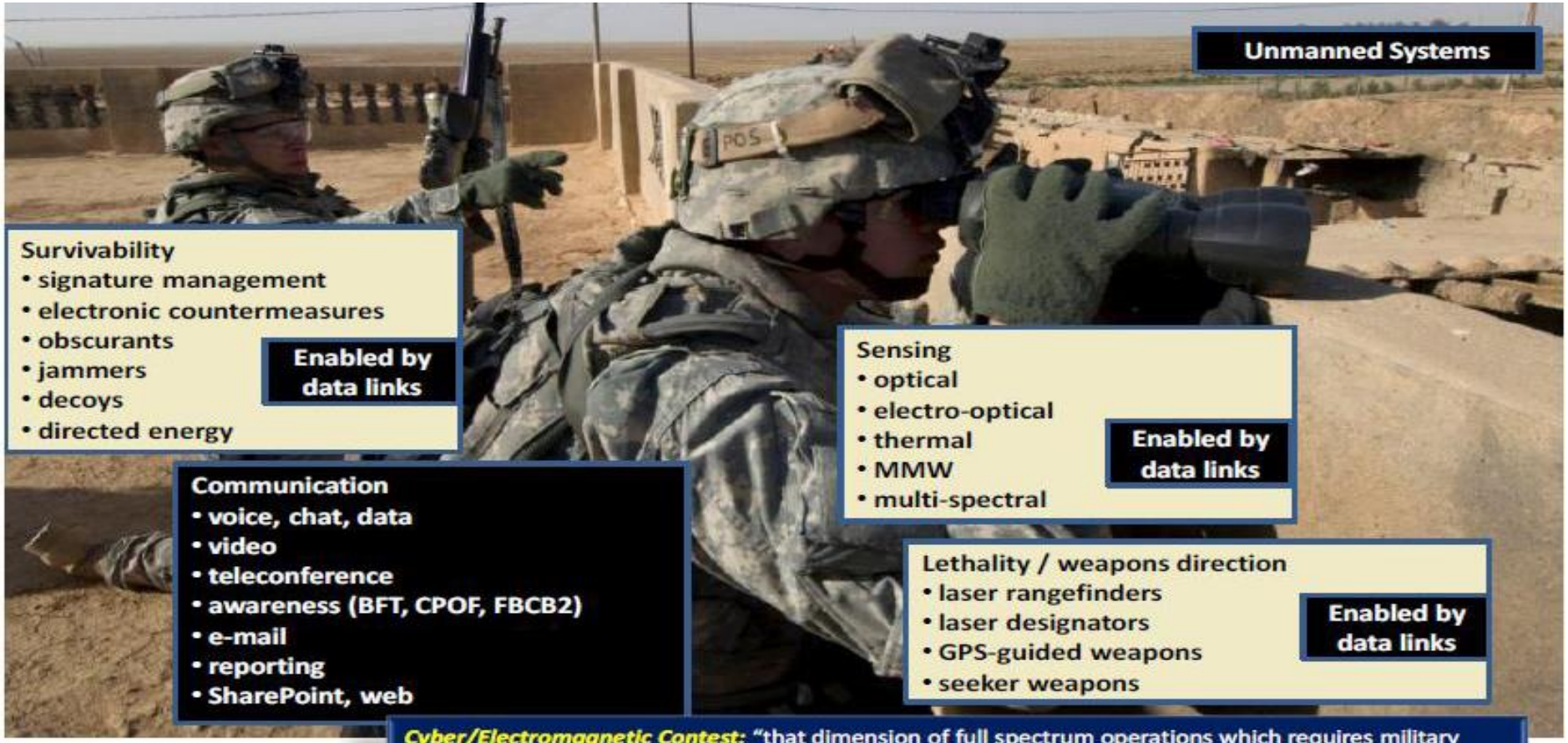
General Raymond Odierno
Chief of Staff of the Army (CSA)
Foreign Policy Magazine
4 February 2013

CYBER ELECTROMAGNETIC ACTIVITIES (CEMA) DEFINED

Cyberspace Electromagnetic Activities (CEMA) Defined



Cyberspace Electromagnetic Activities (CEMA) Application



CYBER ELECTROMAGNETIC (CEMA) VULNERABILITIES AND THREATS

Vulnerabilities and Threats

- **Physical vulnerabilities:** Loss of individual CAC, compromising/sharing Personally Identifiable Number (PIN), leaving your computer or device logged-on and unattended, allowing someone else to use your log-in credentials, being overheard while talking on a phone or over a video chat

- **Insider threats:** individuals acting suspiciously (odd work habits, unexplained communication with foreign or questionable organizations), requesting access to information that is outside the scope of their responsibility or need to know

- **Virtual threats:** viruses, Trojans, malware, web crawlers, identity theft

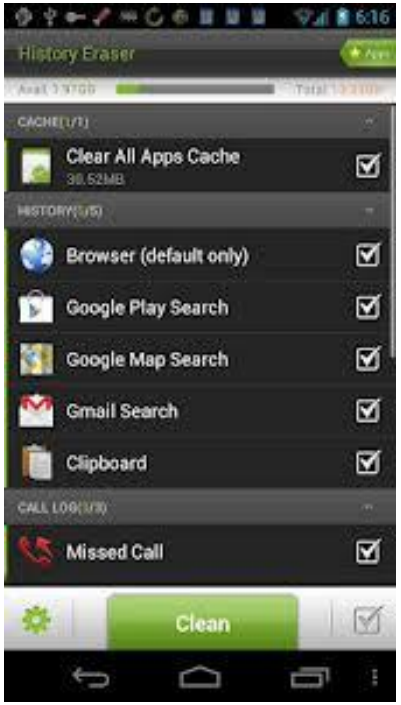
Mobile Technology: Vulnerabilities

Mobile/Cellular devices use a wireless signal from the mobile unit to the base station/cell tower, and from the base station to the base station controller. Wireless signals can be highly vulnerable to recording, interception, tracking, and data mining.

Mobile Technology: Vulnerabilities

Eavesdropping and "Wiretapping".

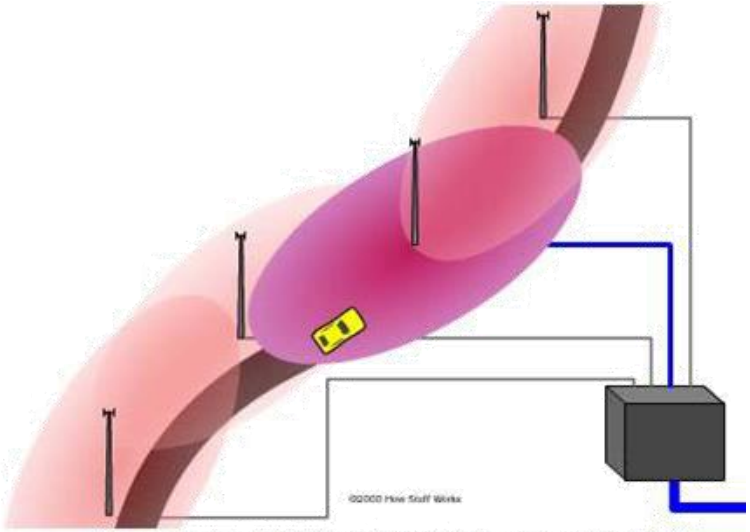
Recording Devices



Traffic Analysis and Cached Information

Environmental microphones.

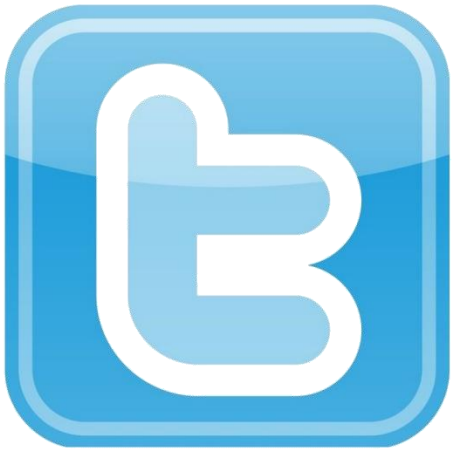
Mobile Technology: Vulnerabilities



As you travel, the signal is passed from cell to cell.

Geolocation and Tracking.

Social Media



CYBER ELECTROMAGNETIC (CEMA) SECURITY AND PROTECTION

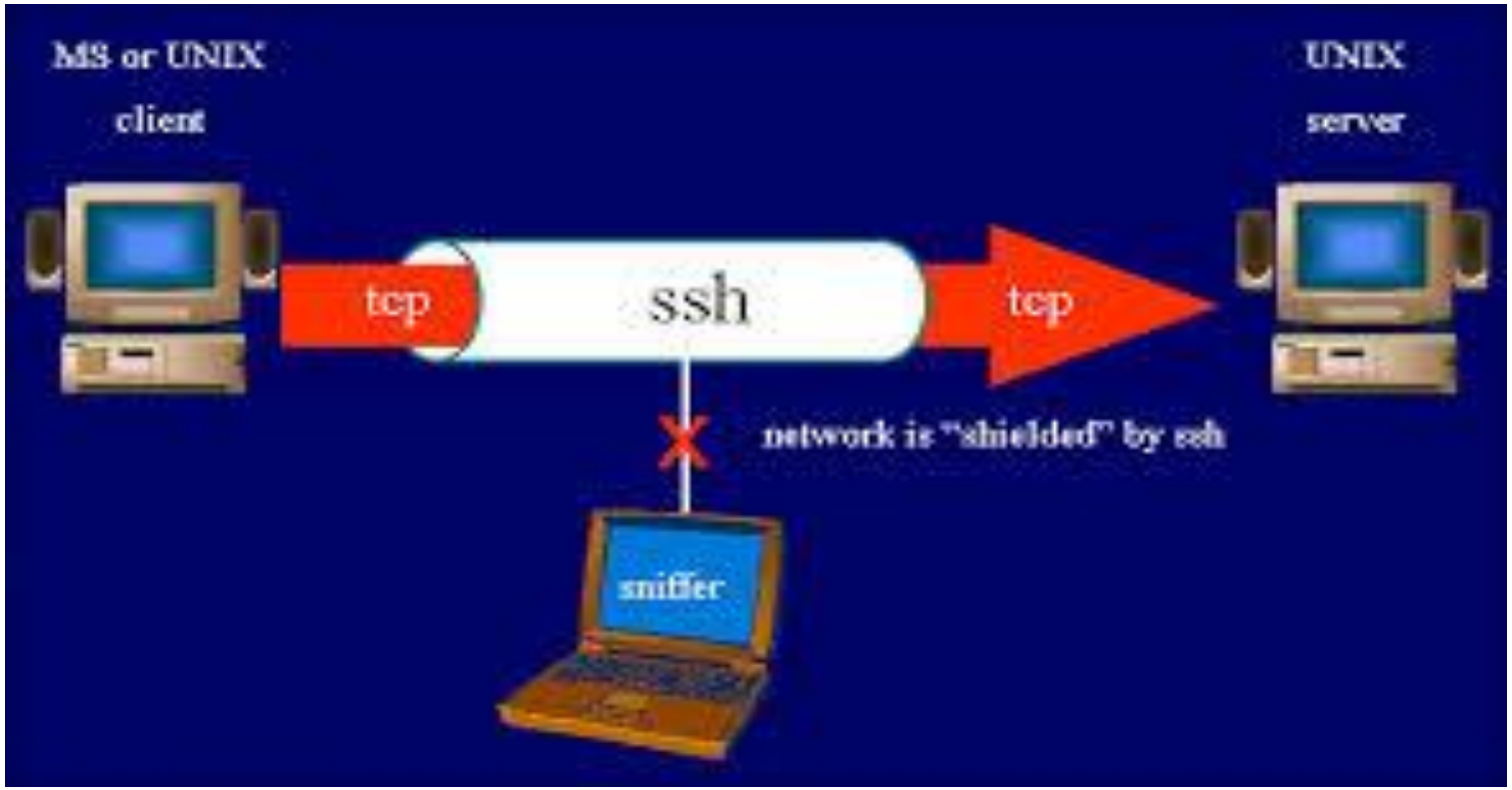
Secure Data and Connectivity

Physical Security

Data Security

Internet Security

Secure Data and Connectivity



Incident Response: What the Doctrine Says

Every organization should have processes in place and the people to contact in case of an incident whether it is a security breach, information spillage, or disclosure of Personally Identifiable Information (PII). Guidelines on reporting processes are defined in AR 25-2.

US CERT has a <u>one hour</u> reporting requirement for PII related incidents. Ensure your IA team's response plan meets this requirement.

Cyber Training

All Soldiers must complete the appropriate cyber and operational security related training required for their position.

Training Topics:

- Annual DoD Cyber Awareness Challenge Training
- Phishing Training
- Operational Security and Social Networking Training

- https://ia.signal.army.mil/

Questions?