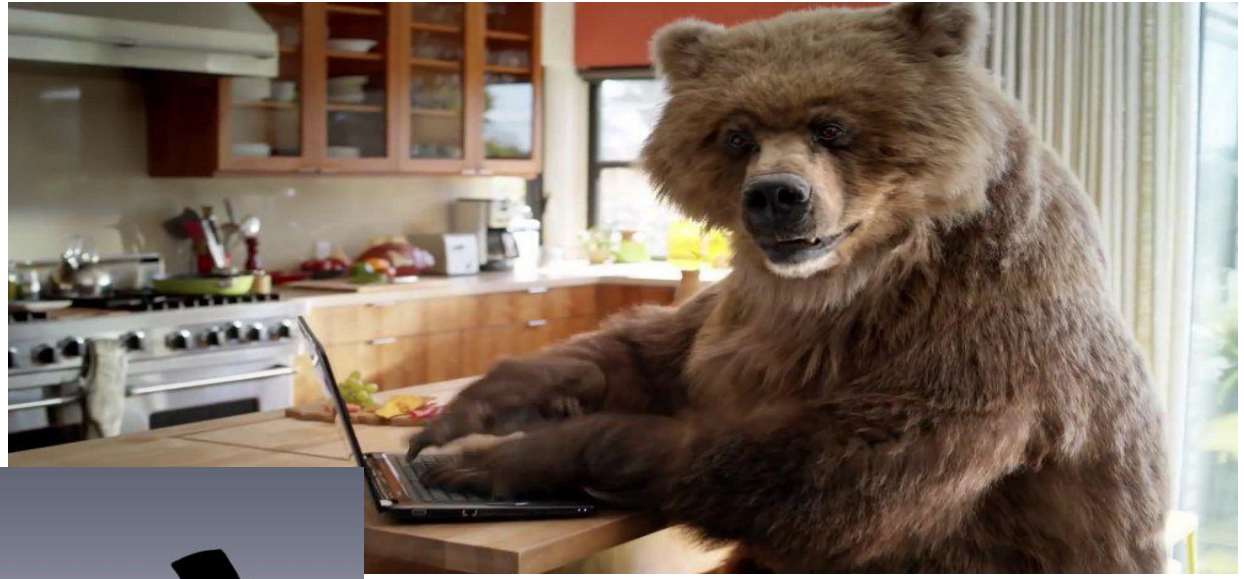
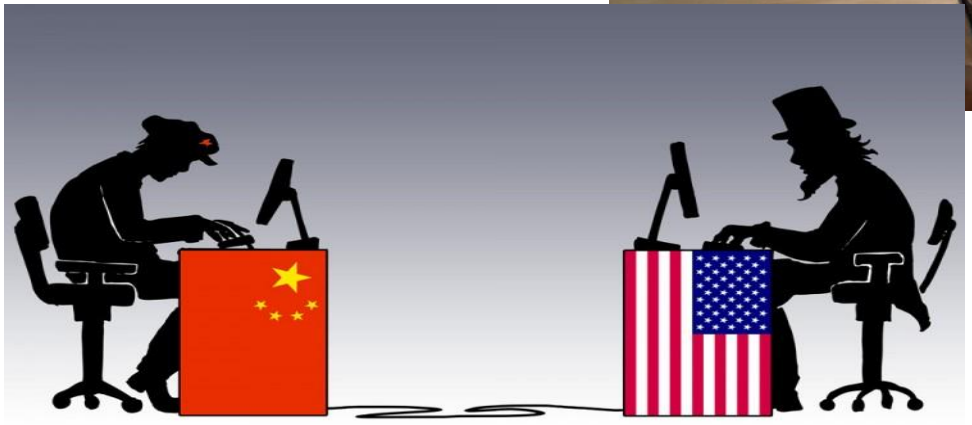
# The New Arms Race – Operations in the Cyber Electromagnetic Domain

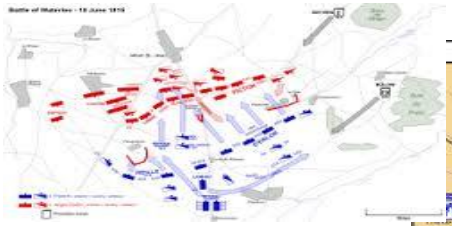
*EW Europe – 7 June 2017*

*Wing Commander Garry Crosby MSc FRAeS RAF (Retd)*

LEONARDO
AIRBORNE & SPACE SYSTEMS










*State on State war using mass, objective and manoeuvre*

*Kinetic war for political objectives*

*Act of force to compel the enemy to do our will*

*Intelligence, Deception*

*Attack the mind of your enemies*

*Subdue the enemy without fighting*

*"Observe, orient, decide and act more inconspicuously, more quickly, and with more irregularity …"*

*Boyd, Patterns of War*

Developed from 'Principles of War for Cyberspace' Lt Col Steven E. Cahinin US Air War College 2011 *www.au.af.mil/au/afri/aspj/digital/pdf/articles/Jan-Feb.../Research-Cahanin.pdf*

## Joint Definitions

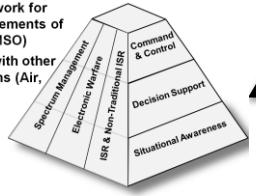
- Electromagnetic Spectrum Control (EMSC)
  - The coordinated execution of joint electromagnetic spectrum operations with other lethal and nonlethal operations that enable freedom of action in the electromagnetic operational environment.
- Joint Electromagnetic Spectrum Operations (JEMSO)
  - Those activities consisting of electronic warfare (EW) and joint electromagnetic spectrum management operations (JEMSMO) used to exploit, attack, protect, and manage the electromagnetic operational environment to achieve the commander's objectives.
- Electromagnetic Battle Management (EMBM)
  - The dynamic monitoring, assessing, planning and directing of JEMSO in support of the commander's scheme of maneuver.

Draft JP 3-13.1 *EW* / JP 6-01 *JEMSMO*

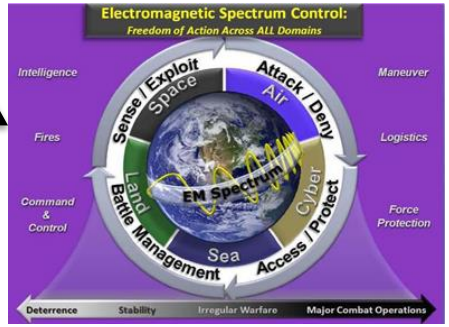
WHAT IS CYBER/EW CONVERGENCE?


## EMBM

- Provides the framework for integrating all the elements of Joint EMS Ops (JEMSO)
- Integrates JEMSO with other aspects of operations (Air, Land, Sea, Space, Cyberspace)
- Provides effective and efficient use of EMS resources and capabilities




Supports CC's EMS Scheme of Maneuver
Takes the Fight to the Adversary



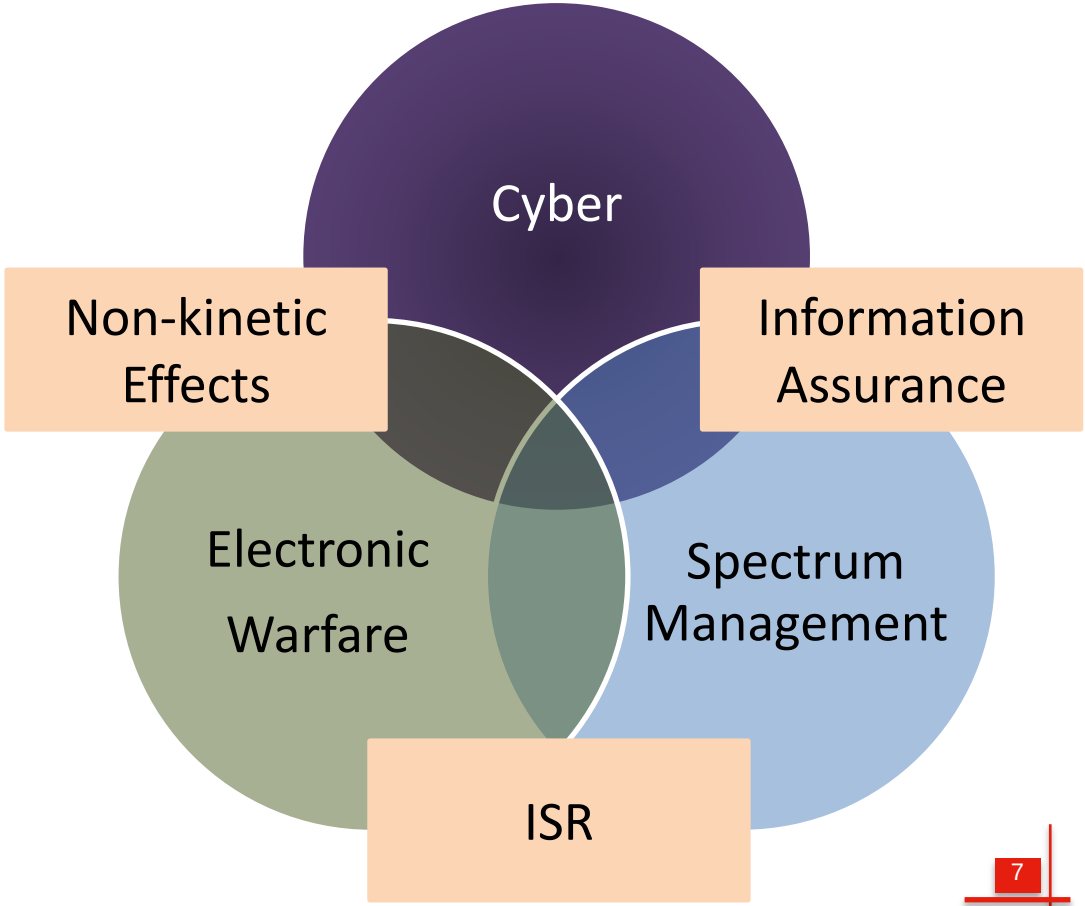

"United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries."

| Electronic Warfare | Cyberspace Operations |
|---|---|
| Electronic Surveillance | Cyberspace ISR |
| Electronic Defence | Defensive Cyber Operations |
| Electronic Attack | Offensive Cyber Operations |

**'The use of EM energy for offensive purposes'**

**'Activities that project power to achieve military objectives in, or through, cyberspace'**

PARTICULARLY ON 'DISCONNECTED ENTITIES'?



# Cyber Effect on Disconnected Entities

**JDN 3-16 - EA and Cyberspace Attack**

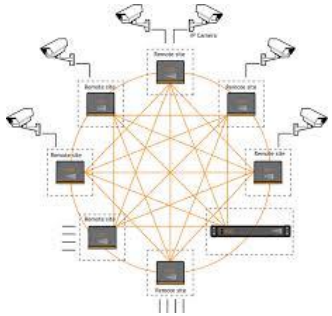
EA can be used to facilitate cyberspace attack objectives and, conversely, cyberspace attack can be used to facilitate EA objectives.

When combined, EA is used for injection of an autonomous or interactive executable CO payload into a system. This combination is characterized by deterministic effects within data-based components.

'We're able to touch a target and manipulate a target…from an aircraft'
'[We can] touch a network that in most cases might be closed'
*Maj Gen Burke Wilson, Cmdr 24th AF*

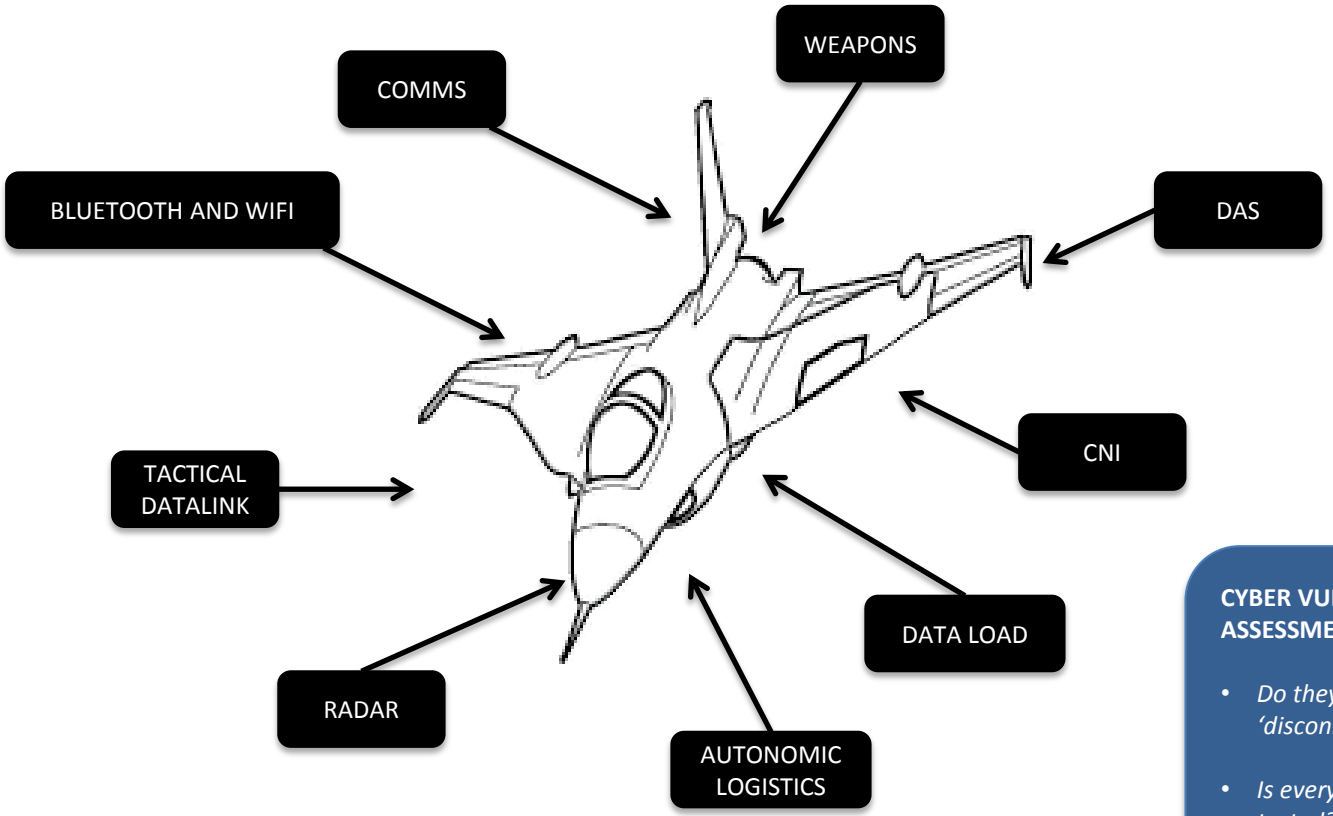
"Radio frequency and Computer Network Exploitation and Attacks can no longer be viewed as separate activities or actions within the spectrum"

Rohret and Jimenez 'Convergence of Electronic Warfare and Computer Network Exploitation/Attakcs with the RF Spectrum'



- IP over Radio system denial of service
- ID SATCOM ground station and jam
- Degradation of mesh network (without triggering alerts)

RF-INDUCED CYBER EFFECTS (RICE)




**CYBER VULNERABILITY ASSESSMENTS**

- *Do they include 'disconnected entities'?*
- *Is every attack surface tested?*

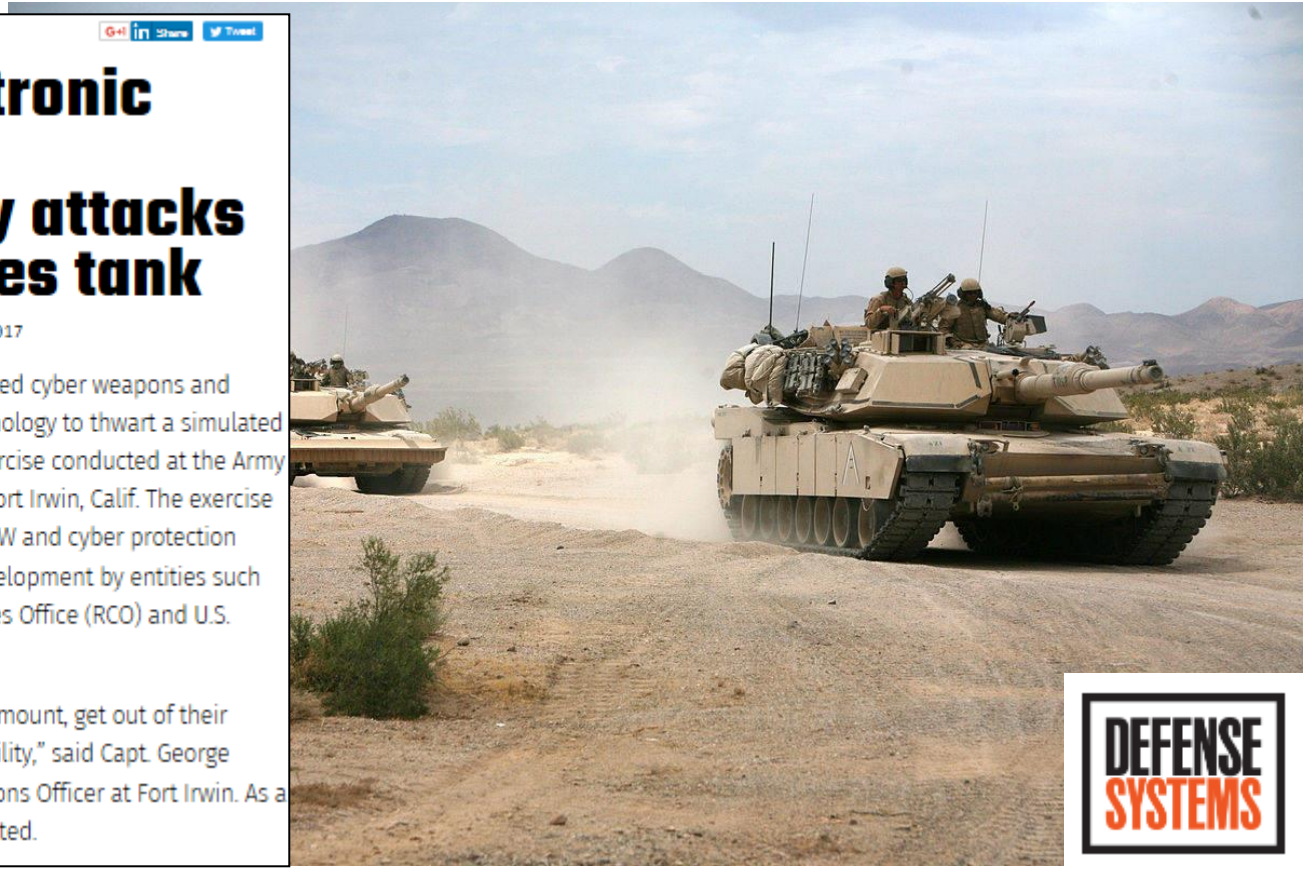
CYBER DEFENSE

# Army electronic warfare technology attacks and disables tank

BY KATHERINE OWENS • JUN 05, 2017

Army trainers successfully used cyber weapons and electronic warfare (EW) technology to thwart a simulated tank assault at a training exercise conducted at the Army National Training Center at Fort Irwin, Calif. The exercise reinforced the need for the EW and cyber protection technology that is under development by entities such as the Army Rapid Capabilities Office (RCO) and U.S. Cyber Command.

"These tanks had to stop, dismount, get out of their protection, reduce their mobility," said Capt. George Puryear, an Irregular Operations Officer at Fort Irwin. As a result, they were easily defeated.



DEFENSE SYSTEMS

| Likely Outcomes |
| --- |
| Future operations will take place in the presence of ‘eyewatering’ EW |
| Adversary cyber capabilities are advancing rapidly, state and non-state |
| Attribution will be difficult |
| The whole force will come under attack, wherever it operates |
| Rapid digitalisation may improve capability, but it will increase vulnerability |
| An adversary who can combine OCO and EA will be a formidable opponent |

SO WHAT?

# YOU NEED TO:

IDENTIFY VULNERABILITIES

WHOLE FORCE | ADVERSARY

DENY ATTACK VECTORS

BUILD A SUSTAINABLE EW AND CYBER FORCE

ATTACK

**Wing Commander Garry Crosby MSc FRAeS RAF (Retd)**

*Head of Studies and Research*
*Leonardo Airborne and Space Systems Division*

**garry.crosby@leonardocompany.com**

LEONARDO
AIRBORNE & SPACE SYSTEMS