



school of  
**SYSTEMS**  
and  
**LOGISTICS**

› education › research › consultation

# Logistics & Cybersecurity

AFIT's School of Systems & Logistics

Ken Hendrick

Capt Brandon Froberg

Guy Fritchman

# Objective

Discuss logistics and cybersecurity

By....

- Surveying challenges & initiatives
- Focused **Unclassified** conversation with you

# Outline

- Why...are we here?
- A Cybersecurity Primer
- The Cyber Challenges to Logistics
  - Examples of Cyber Impacting Logistics
- Cybersecurity Logistics Approaches & Initiatives

The impacts and  
threats of cyber  
incidents are  
seen in the news





**- BREAKING NEWS -**

# Cyber-Physical Attack with Additive Manufacturing


Cornell University, Sep 1, 2016



# - BREAKING NEWS -

Intruder Alert: Industry Experts  
Weigh In on Cybersecurity Risks

APEX (Airline Passenger Experience Assoc.), February 9,  
2017



# - BREAKING NEWS -

Cybersecurity experts tell  
Congress weapons need better  
security

Defense Systems, March 2, 2017

# IoT Platform for Mi Avionics Security

Engineering.com, April 11, 2012

**BREAKING NEWS**

SAS Symposium: FA  
ke On Cyl

MAKING NEWS

UAS Symposium: FAA Can't  
Take On Cybersecurity Alone

Aviation Today

Aviation Today, March 31, 2017

# BREAKING NEWS -

# Senators Reintroduce Aircraft Cyber Security Legislation

and better

March 2, 2015



**BREAKING NEWS**  
Boeing 757 Testing Shows  
Airplanes Vulnerable to  
Hacking, DHS Say

Aviation Today, M  
eering.com

**BREAKING NEWS**  
Securing the E-Enabled  
Aircraft

**- BREAKING NEWS**

Expansion of ban on larger  
electronics on airlines likely  
U.S.

Reuters, May 16, 2

**- BREAKING**

United Airlines cockpit  
access codes leaked online

Help net Security, M

FLATRON  
Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

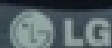
1. Send \$300 worth of Bitcoin to following address:

1Hz7153HHuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

6CiaEy-wM3yRF-XabBVH-w3wJEv-65P8rt-DUS1VU-Cjfe6H-cwG22L-Dqgh6Y-5dQ1Ma

If you already purchased your key, please enter it below.  
Key:





# MAERSK

- The largest Cargo/Shipping Company in the World
- 76 Ports – 17 disabled for 10-14 days
- Approximate damages: \$300 MILLION

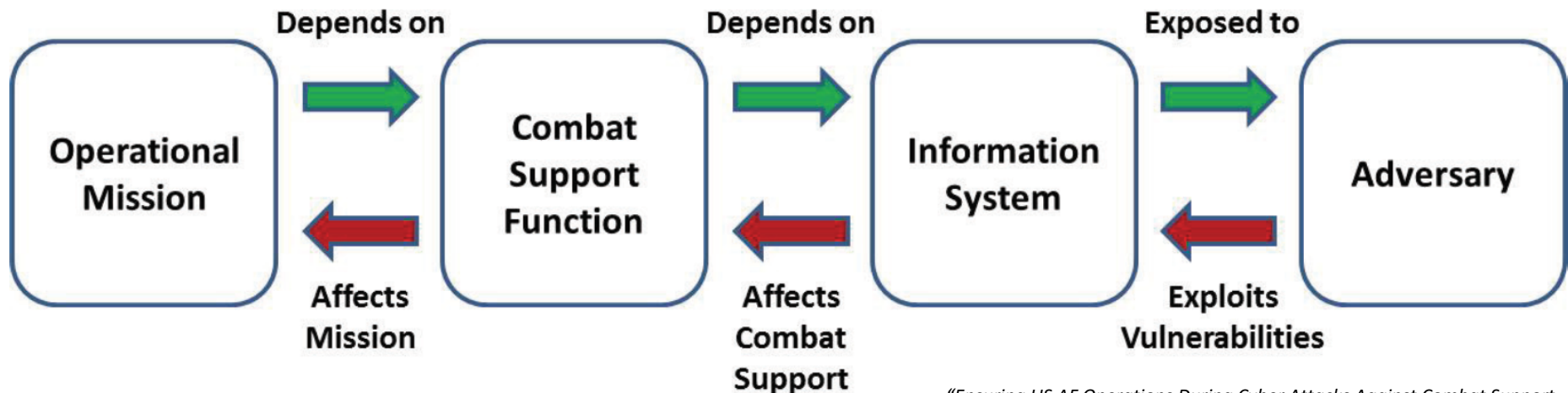
June 2017, the Russian military launched the most destructive and costly cyber-attack in history. The attack, dubbed “NotPetya,” quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas - White House Press Secretary (15 Feb 18)

# Why are We Here?

Cyber a battlefield

# Why are We Here?

Logistics is a target...  
or the path to a weapon  
system/operational target





# Why are We Here?

Cybersecurity is a  
responsibility shared  
by logisticians

# Why are We Here?

**We—as logisticians—need to**

- Understand much more about cyber threats
- How they challenge logistics
- What is being/can be done to defend our operations

# CYBERSPACE

*The interdependent **network of information technology infrastructures**, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.*

Definition from DoDI 8500.01: Cybersecurity  
Referencing the National Information Glossary,  
CNSS Instruction No. 4009

# CYBERSECURITY

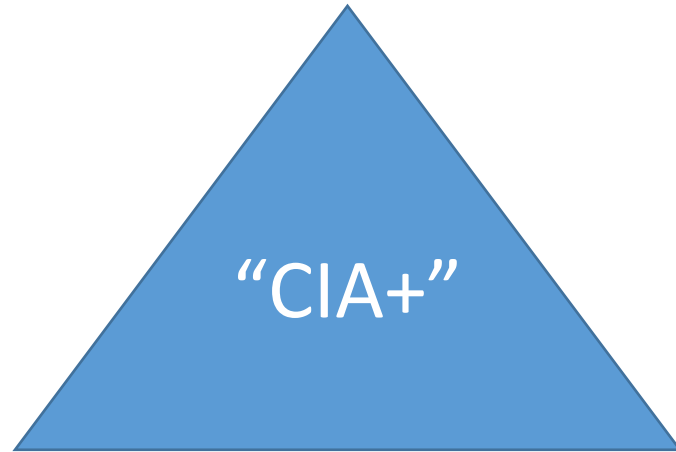
Prevention of damage to, protection of, and restoration of  
*computers, electronic communications systems, electronic communications services, wire communication, and electronic communication*  
including information contained therein,  
*to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation*

Definition from DoDI 8500.01: Cybersecurity  
Referencing the National Information Glossary,  
CNSS Instruction No. 4009

# Other Terms & Definitions

- Malware – Malicious Software
- A Navy Note:
  - The term "cyber attack" is often used by the media, the public, and even U.S. Government (USG) officials (incorrectly) to describe the full range of unauthorized/unlawful actions in cyberspace.
  - Only National Authority should characterize a cyberspace operation as a cyberspace attack ... The term "attack" carries with it significant legal and national security implications.

# How the DoD Ensures Cybersecurity



- Confidentiality
- Integrity
- Availability
- Authentication
- Nonrepudiation

## Activities:

- Vulnerability Assessment & Analysis
- Vulnerability Management
- Malware Protection
- Information Security Continuous Monitoring
- Cyber Incident Handling
- User Activity Monitoring for DoD Insider Threat Program
- Warning Intelligence

# Threats in Cyberspace

- Nation State
- Transnational Actor
- Criminal Organization
- Individual or Small Group
- Traditional
- Irregular
- Catastrophic
- Disruptive
- Natural
- Accidental
- Insider





# Some Malware Examples

Delivery
Viruses
Trojan Horses
Worms

Payloads
Logic or Time Bombs
Keyloggers
Ransomware
Rootkit

Persistence/ Capabilities
Backdoors
Spyware
Zombies/Botnets



# Where Cybersecurity is needed



Information  
Systems



Weapon  
Systems



“Others”

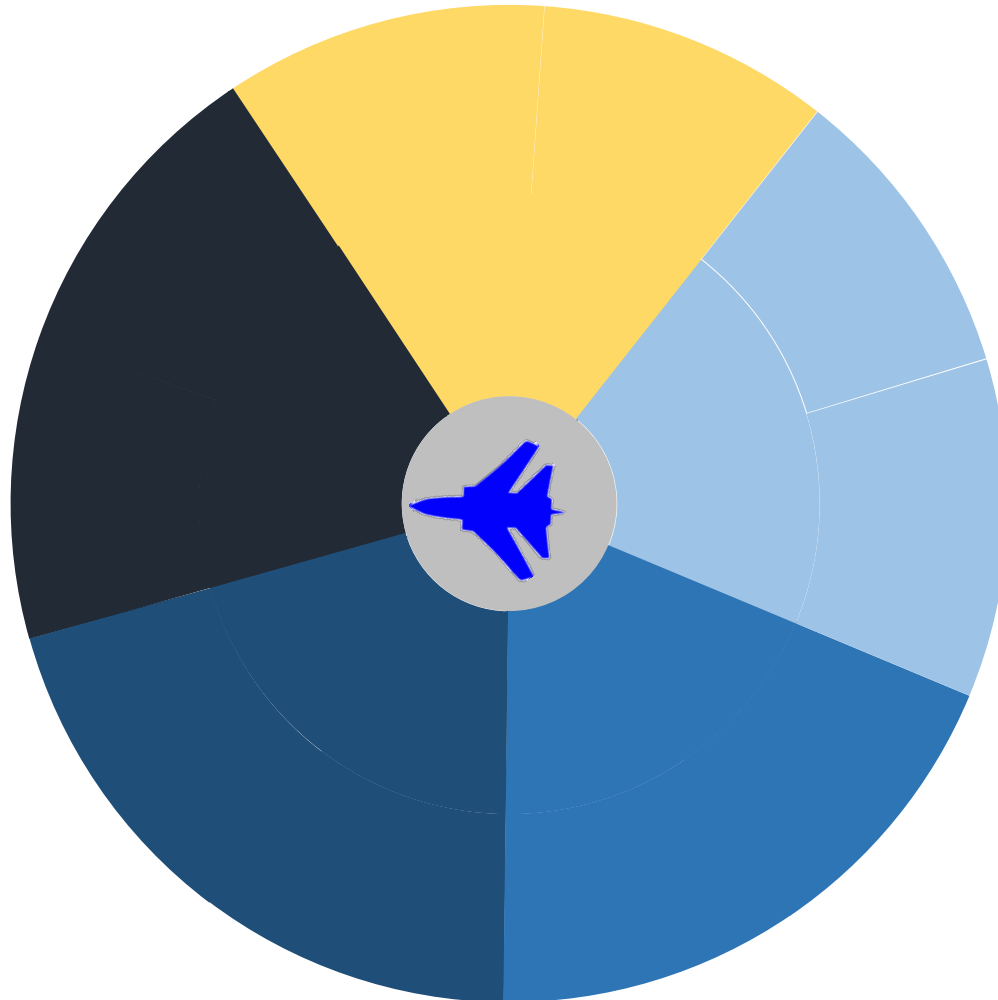
- Critical Infrastructure
- Industrial Control Systems (ICS)
- Supervisory Control and Data Acquisition (SCADA)

# Enemies are using Cyber for Effects

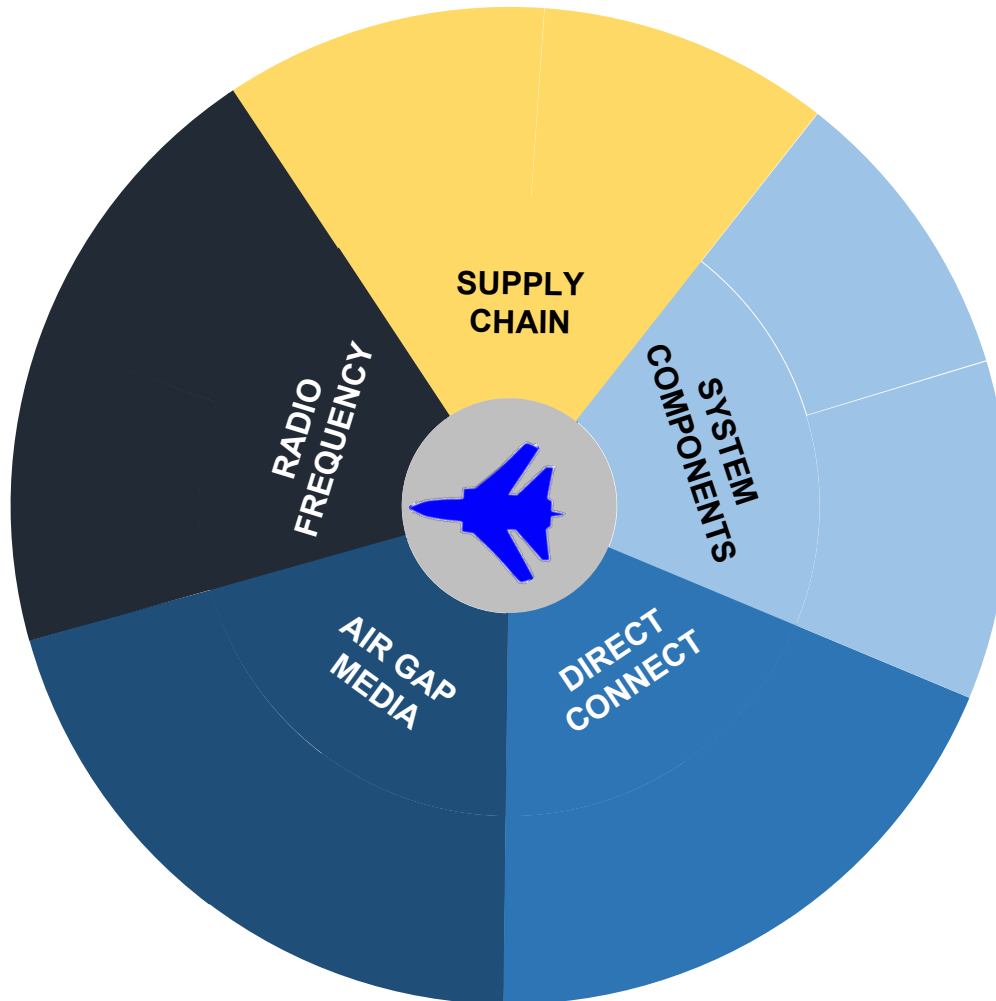
- Deny
- Degrade
- Manipulate (e.g., Deceive)
- Disrupt
- Destroy



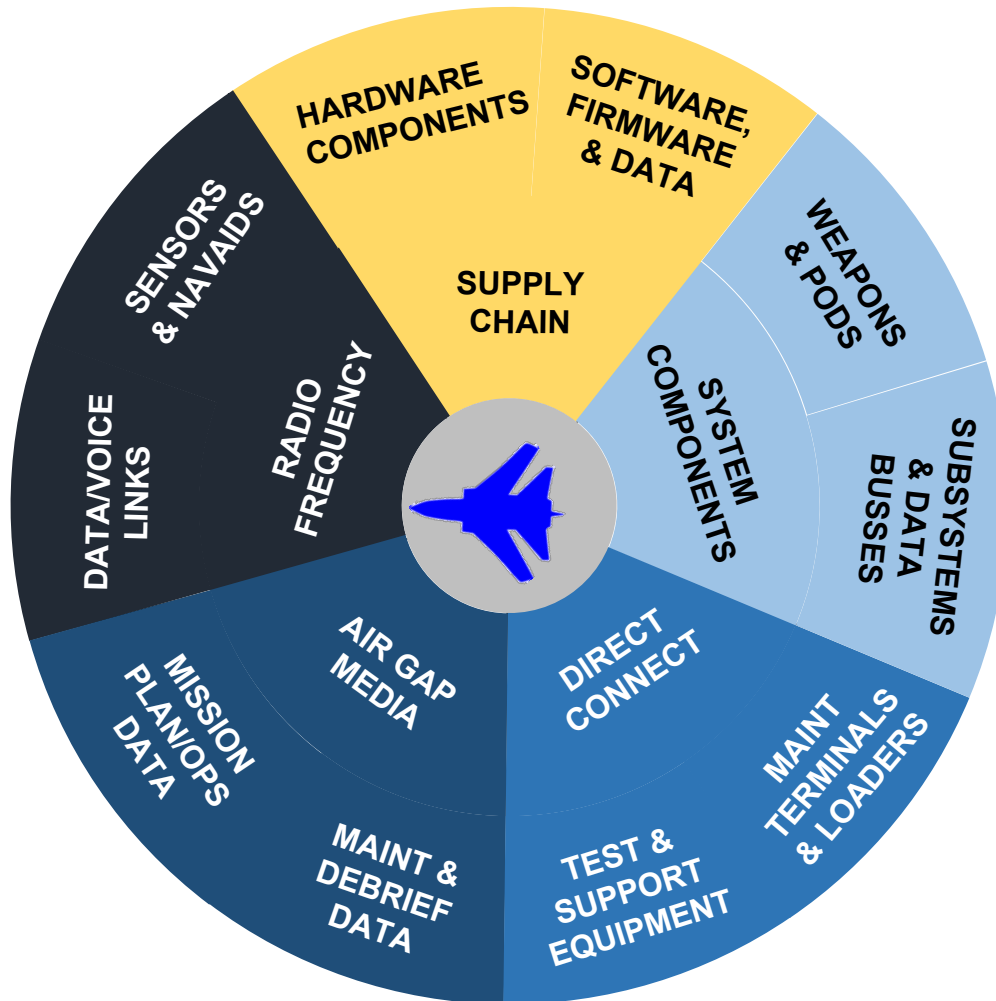
# Wheel of Access (WOA)



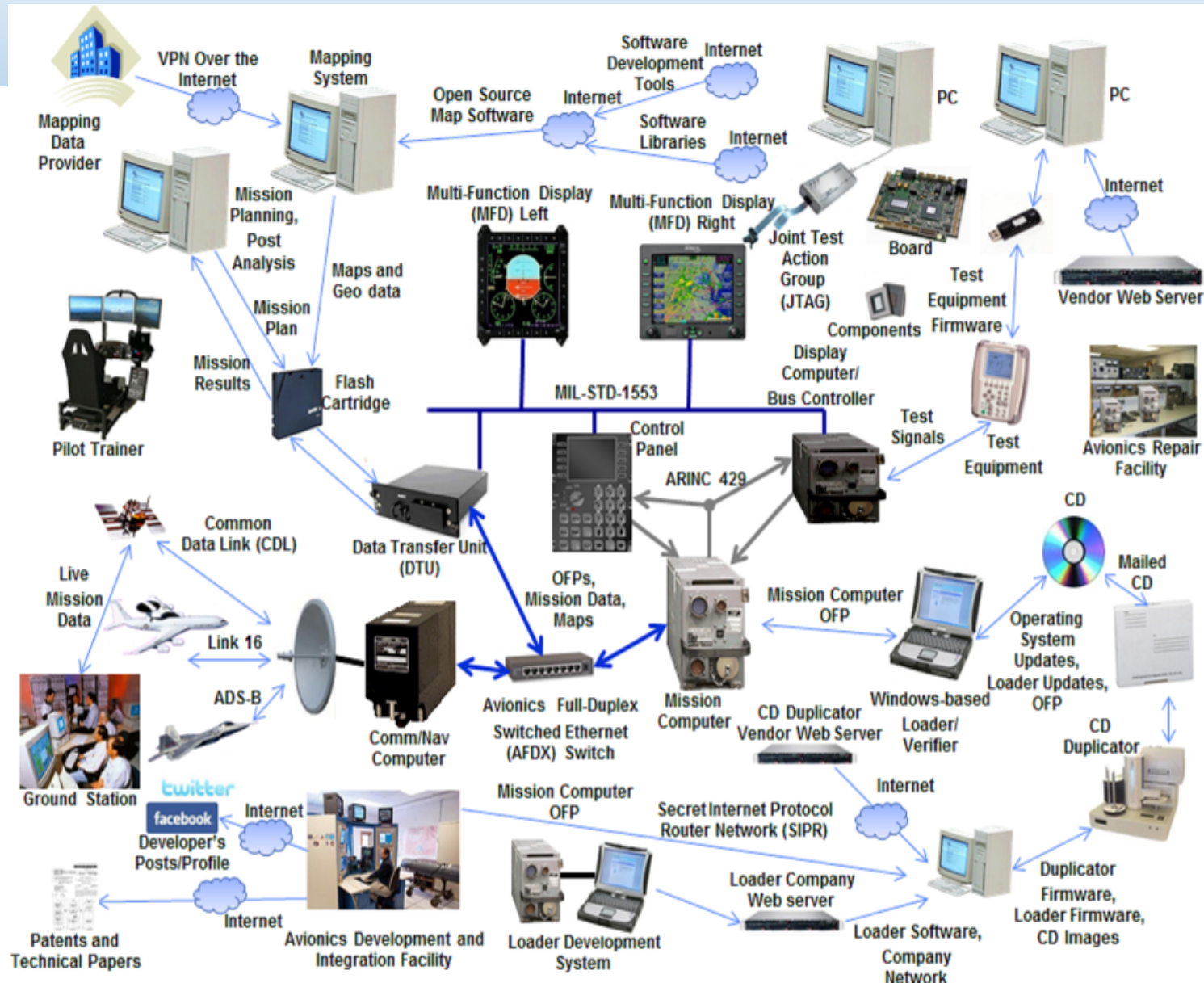
# Wheel of Access (WOA)



# Wheel of Access (WOA)



# Cyber Challenges to Logistics

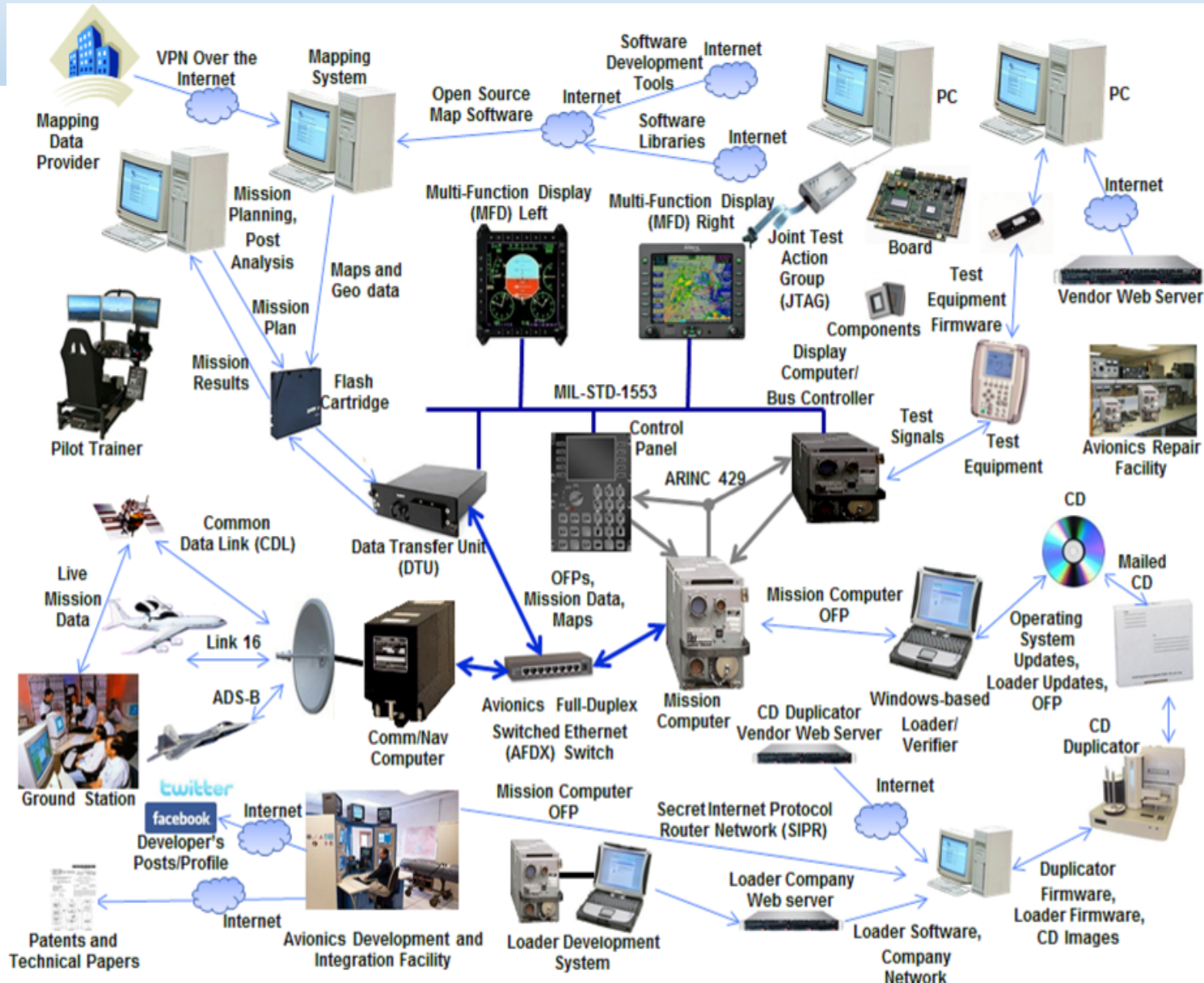




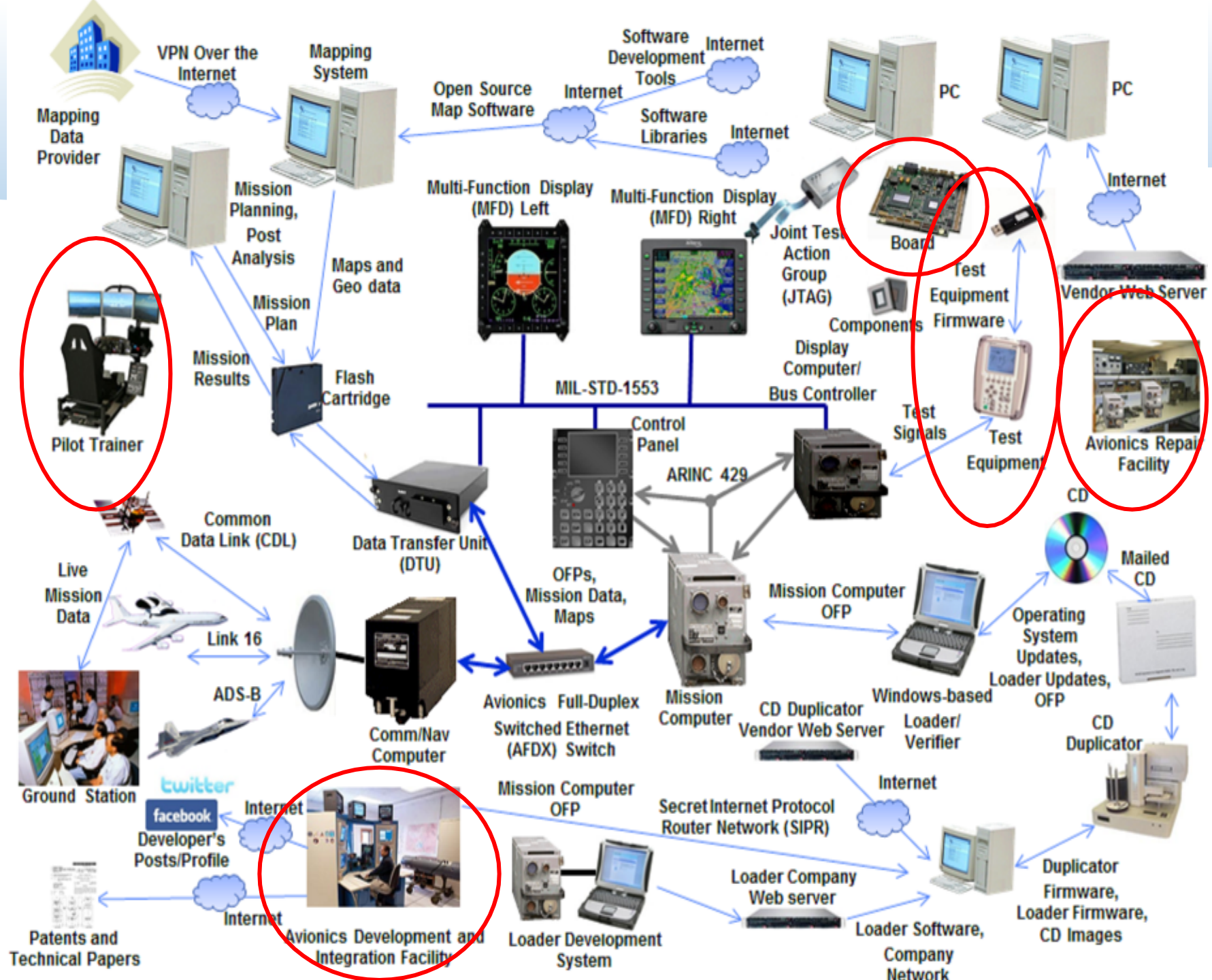


# Cyber Challenges to Logistics

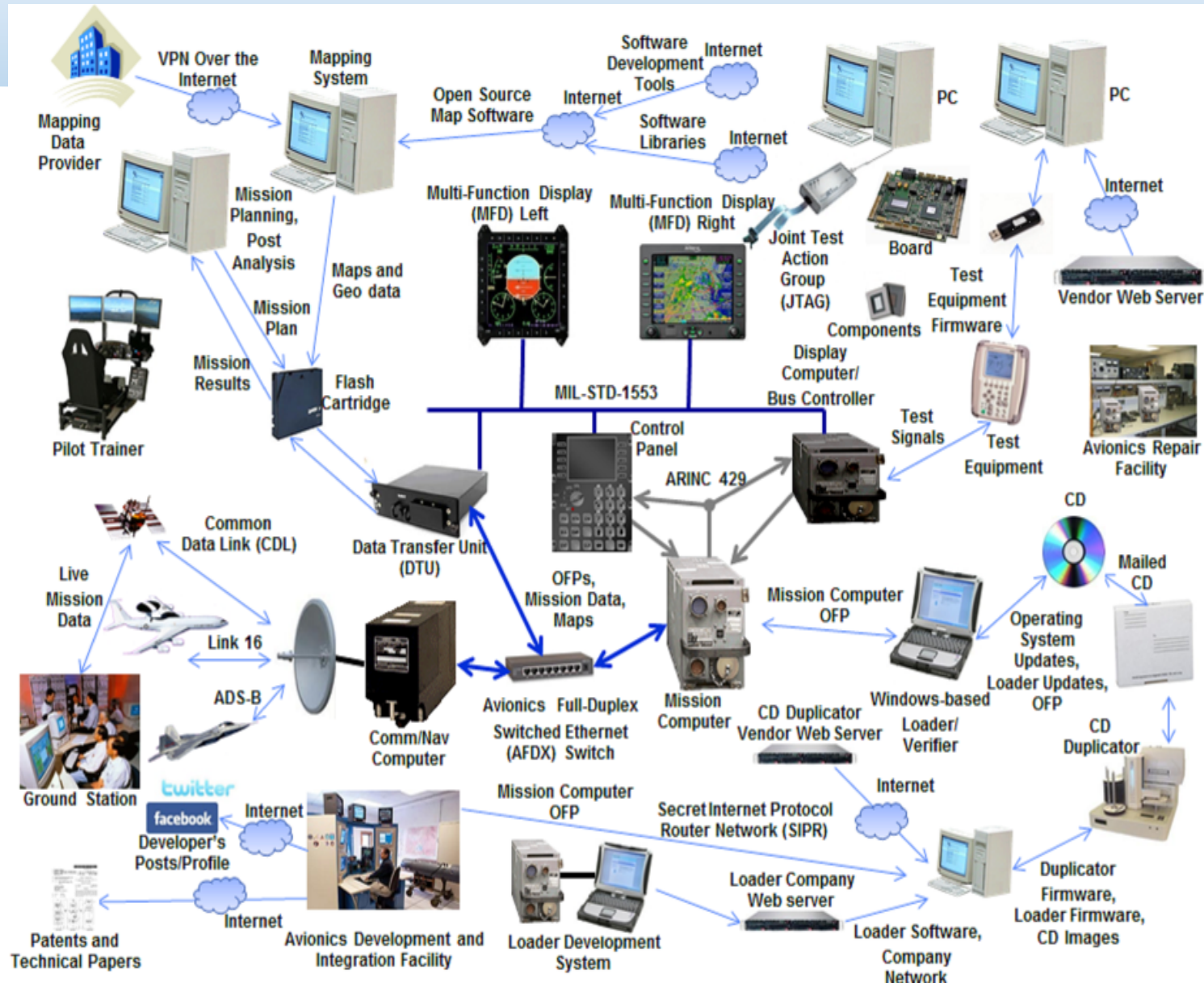
Complexity







# Interconnectivity



# Cyber Challenges to Logistics

Everything that connects to an Aircraft acts like an USB Port

*Not just IT systems!*

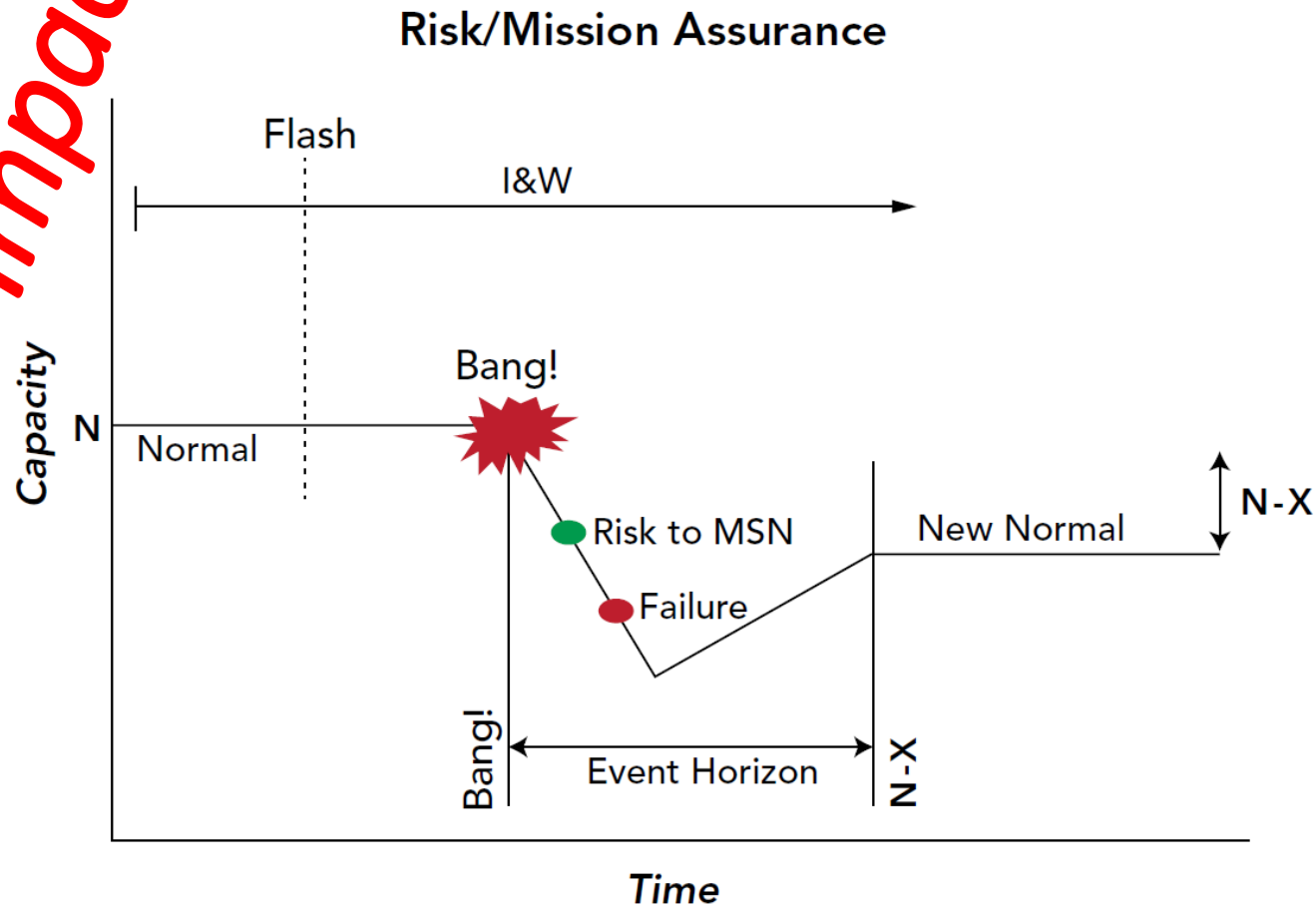


- All Access points need to be considered
- Need to ensure chain of trust and confidence



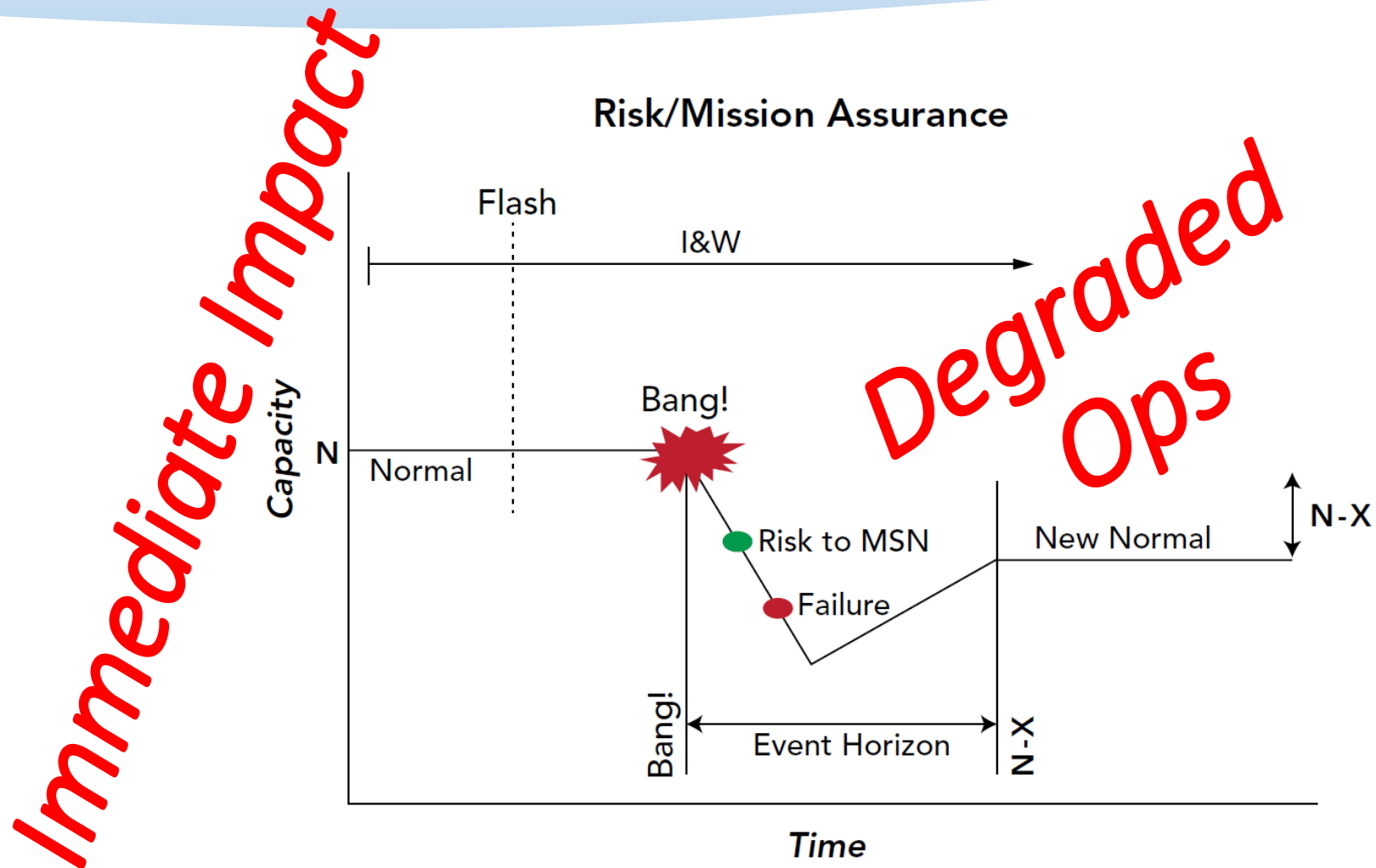
# Cyber Challenges to Logistics

*Immediate Impact*



Robert Allardice & George Topic, "Battlefield Geometry in Our Digital Age," PRISM 7, No. 2, 2017

# Cyber Challenges to Logistics

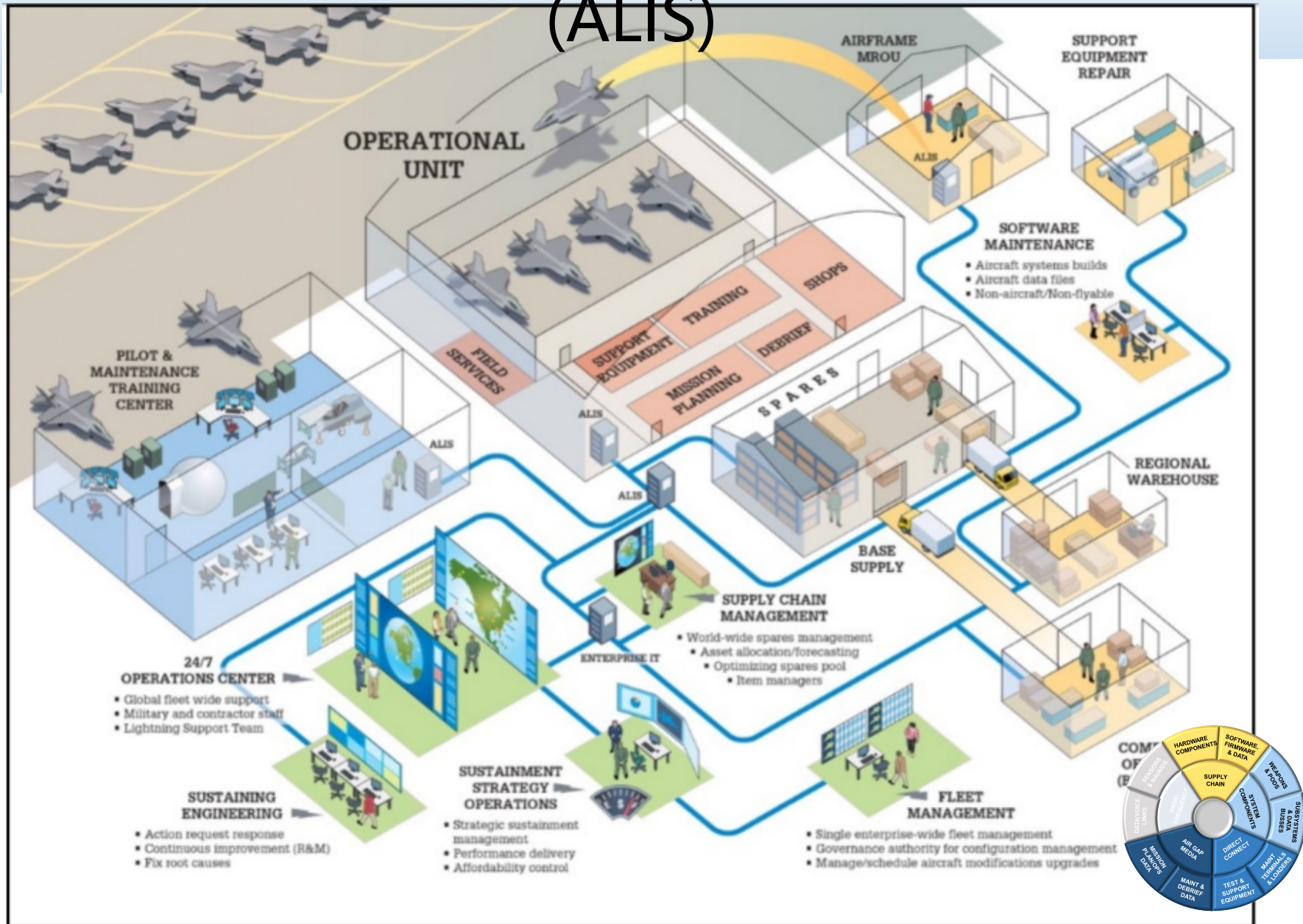


Robert Allardice & George Topic, "Battlefield Geometry in Our Digital Age," PRISM 7, No. 2, 2017

# Examples of Cyber Impacting Logistics


- Operations – ALIS
- Acquisitions – PPP & ATO
- Cyber Vulnerability Assessments
- Supply Chain
- Life Cycle Logistics – 12 IPS Elements
- MX Hygiene

# Autonomic Logistics Information System (ALIS)





# Recent Strategic Initiatives

- 
1. DoD to Make Security the Fourth Acquisition Pillar
  2. Combatting Supply Chain Risk (Section 881 NDAA)
  3. Strengthening Cybersecurity Requirements
  4. DoD Confirms Existence of “Do Not Buy” Software List
  5. Cybersecurity Reviews



# Protect against foreign espionage



# Weapons Systems Acquisition Initiatives



DEPARTMENT OF THE AIR FORCE  
WASHINGTON, DC

FEB 02 2017

OFFICE OF THE SECRETARY

MEMORANDUM FOR MAJCOMS AND PROGRAM EXECUTIVE OFFICERS  
SUBJECT: Weapons System Cybersecurity Guidance – Operational Cyber Hygiene

1. The USAF's ability to fly, fight, and win is reliant upon the operational readiness of our weapon systems. Recently, several cyber events on weapons system support equipment highlighted that cyber threats present a real risk to weapon system operational readiness. Therefore, the Air Force must address fundamental changes to operational cyber hygiene approaches.

2. Cyber threats are more than just network intrusion or traditional malware; they also affect our weapon systems, presenting a clear and present danger to successful mission assurance. To address these risks, the Cyber Resiliency Office for Weapon Systems, in collaboration with Air Force Task Force Cyber Secure, identified five cyber hygiene best practices (ref. Table 1). These activities should be completed where feasible and in accordance with appropriate risk management procedures in order to reduce the risk of cyber effects impacting the operational readiness of our weapon systems.

3. The cyber contested environment is a complex combination of individual systems acquisition (design and development), operational systems of systems applications (planning and execution), and systems sustainment (maintenance and training). These complexities, combined with the inherent vulnerabilities, external factors, and adversary tactics create a set of dependencies requiring diligence from across the Air Force in a holistic manner in order to effectively and affordably combat cyber risks. In short, we, collectively, must securely:

- a. Design and develop our capabilities;
- b. Operate our systems/missions;
- c. Sustain our capabilities; and
- d. Educate and train our Air Force communities to be vigilant of cyber risks at all times.

4. Program Executive Officers (PEO) and MAJCOMs need to work together to ensure the activities in Table 1 are implemented across all Air Force weapon systems, where feasible, as recommended by both the Air Force Chief Information Officer and the Principal Deputy Assistant Secretary of the Air Force (Acquisition & Logistics) in support of initial implementation of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) Directive-1vne Memorandum (YTMD) 17-001 *Cybersecurity in the Defense*

AT&L Memo, 2 Feb 2017

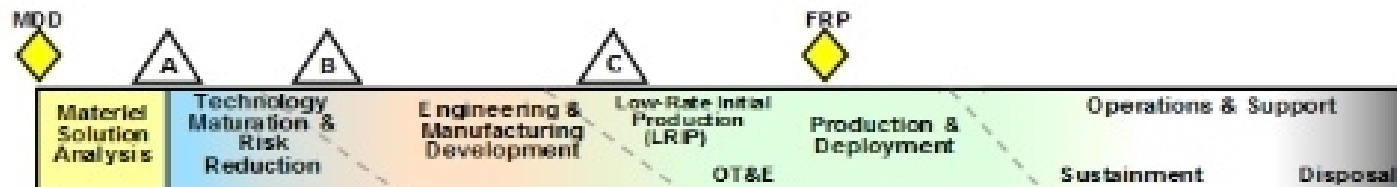
SUBJECT: Weapons System Cybersecurity Guidance – Operational Cyber Hygiene

1. The USAF's ability to fly, fight, and win is reliant upon the operational readiness of our weapon system. Recently, several cyber events on weapons system support equipment highlight that cyber threats present a real risk to weapon system operational readiness. Therefore, the Air Force must address fundamental changes to operations cyber hygiene approaches.

2. Cyber threat are more than just network intrusion or traditional malware; they also affect our weapon system, present a clear and present danger to successful mission assurance. . .

# Program Protection in DoDI 5000.02 Acquisition Policy

- DoDI 5000.02 requires Program Managers to employ system security engineering practices and prepare a Program Protection Plan (PPP) to manage the security risks to the program and system elements that are vulnerable and can be exposed to targeting
  - Critical Program Information
  - Mission-critical functions and critical components
  - Information about the program and within the system
- PPPs are required at all major milestones
  - PPPs inform program acquisition strategies, engineering, and test and evaluation plans
  - PMs incorporate appropriate PPP requirements into solicitations



# Program Protection Plan

- Supply Chain Risk Management
- Cybersecurity
- Hardware Assurance
- Anti-tamper
- Software Assurance
- Defense Exportability





# Authorizing Official

## Authority to Operate (ATO)

- Usually defined by Focus Area (e.g. Weapons, Logistics)
- Air Force has 26 AO's including Aircraft and Industrial Depot Maintenance
- Insertion of new, innovative technology is dependent on obtaining successful Cybersecurity assessment and Interim Authority to Test (IATT) or Authority to Operate (ATO) on a timely basis



# Cyber Vulnerability Assessments



An F-22 Raptor pilot from the 95th Fighter Squadron based at Tyndall Air Force Base, Fla., gets situated in his aircraft



# Supply Chain Risk + Cybersecurity

**Bloomberg  
Businessweek**

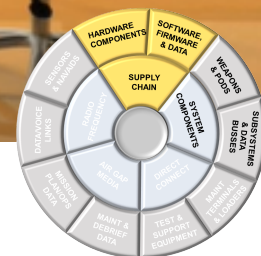
October 8, 2018

## The Big Hack

How China used  
a tiny chip to  
infiltrate America's  
top companies

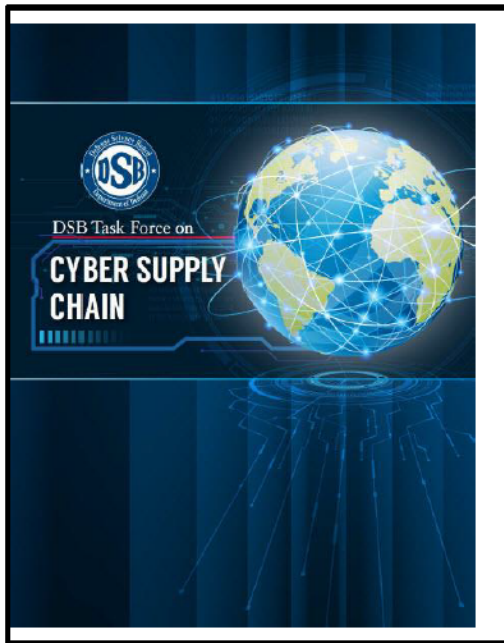
“More than natural disaster, financial instability, or political upheavals, what keeps me up at night is the fear the bad guys are injecting into products bad stuff that can disrupt, bring down, or steal confidential information from networks.”

**Dennis Omaoff served a McAfee's senior vice president , chief supply chain officer**





# Supply Chain Attack

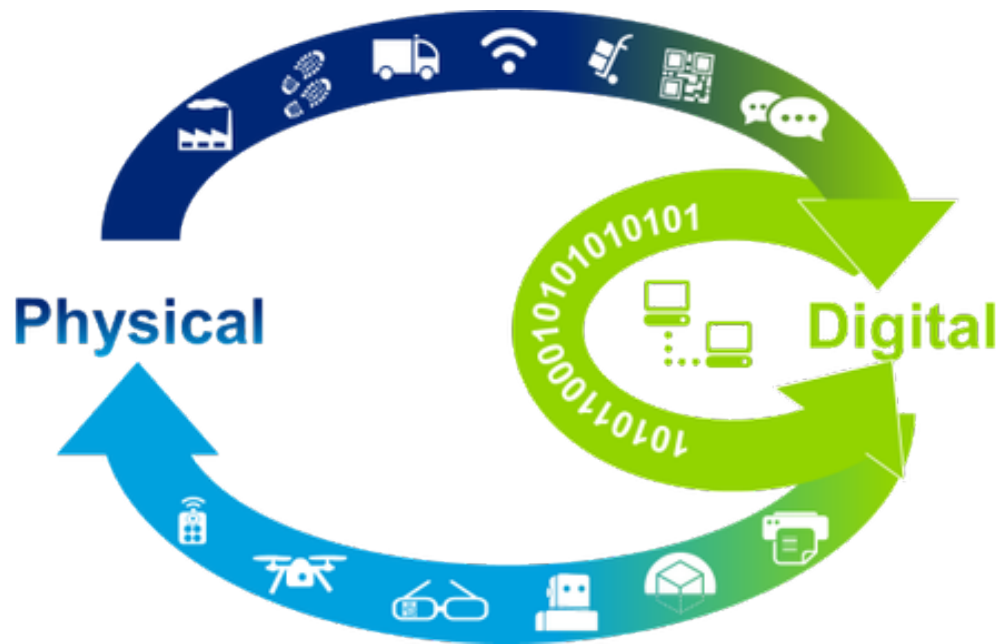


Approved for public release  
February 6, 2017

***“Of particular concern are the weapons the nation depends upon today; almost all were developed, acquired, and fielded without formal protection plans.”***

- The task force concluded that USD(AT&L): must strengthen lifecycle protection policies, enterprise support, and R&D programs so that weapons systems are designed, fielded, and sustained to reduce risk of cyber supply chain attacks.
- But How?
  - Example Platform: 16K+ Components
  - 50 Safety Critical
  - 3K+ Mission Critical
  - SW vs HW in Supply Chain

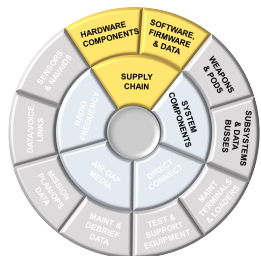
# Supply Chain's digital information loops



**Physical-to-digital:** Examples: sensors, controls, GPS, 3D scanning)

**Digital-to-digital:** Examples: predictive analytics, artificial intelligence, machine learning.

**Digital-to-physical:**  
Examples: autonomous robots and control systems, real-time geospatial visualizations, driverless trucks, drones, remote maintenance, 3D printing.

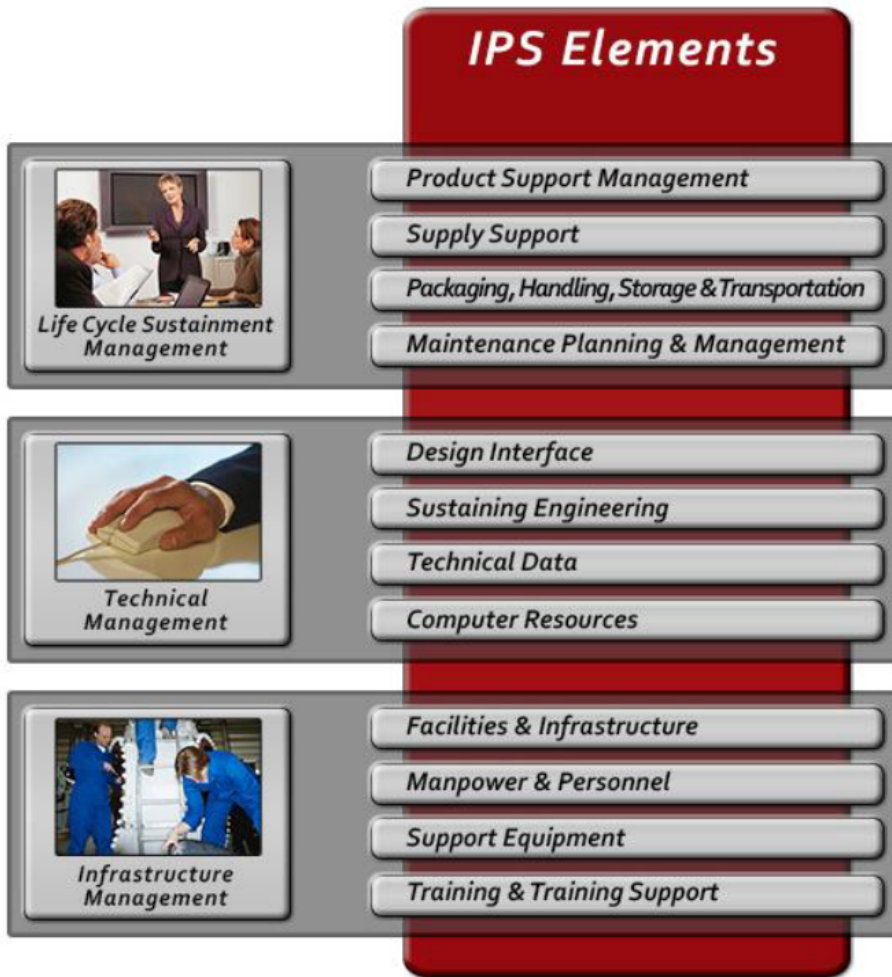




*“Traditionally, we think of sustaining the force as maintaining hardware or ‘bending metal.’ If you consider the highly digitized, interconnected Air Force of tomorrow, we will instead manipulate ones and zeroes.”*

Testimony to the Senate Armed Service Committee  
TO THE LIEUTENANT GENERAL LEE K. LEVY, II  
COMMANDER , AIR FORCE SUSTAINMENT CENTER (APRIL  
2018)

# Cyber and the 12 IPS Elements



Now...Consider the IPS Elements for any system--

What are potential Cyber risks & Consequences?

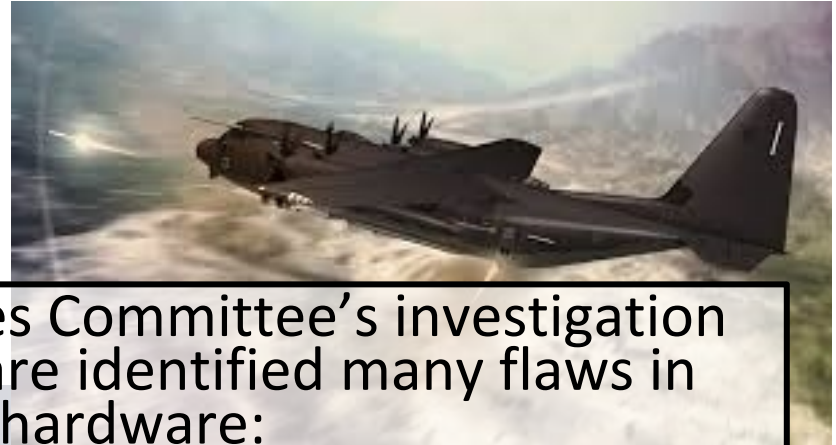
- Improper Labeling / Transport
- Maintenance Data Integrity
- Inadequate Tech Data Rights for Cybersecurity Assessment
- False Supply Trends
- Incorrect Interface Documentation
- Faulty Tech Pubs
- Access to Classified Weapon Systems & Critical Infrastructure
- Improper Maintenance Procedures
- Access to Personnel Data
- Inadequate Response to Cyber Incident





# Counterfeit hardware

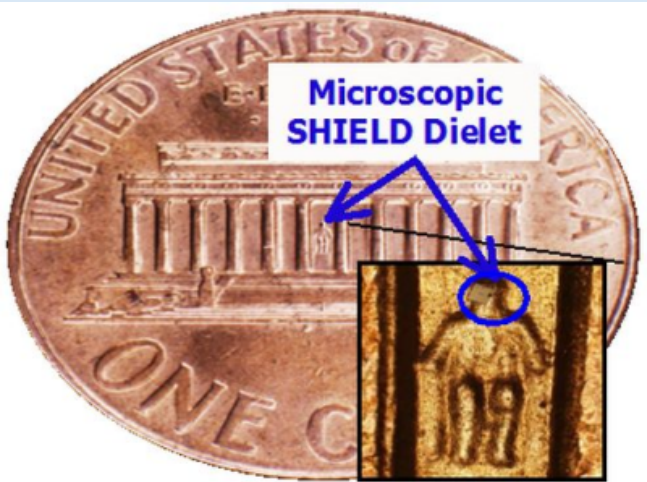
Product  
Support  
Management



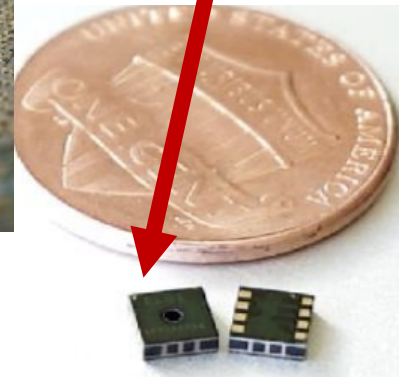
A Senate Armed Services Committee's investigation into counterfeit hardware identified many flaws in current mission-critical hardware:

- the U.S. Army's Terminal High Altitude Area Defense anti-ballistic missile system,
- the Navy's Integrated Submarine Imaging System
- and the Air Force's C-130J aircraft, among other systems.





"Dielets"



**The global growth of the supply chain that lets electronics manufacturers tap less-expensive suppliers in China, Japan, Singapore, South Korea and Taiwan has proved very difficult to police.**



# Supply Chain Cyber-Attacks

## Manufacturing and Development

### Mx Planning and Management

#### Supply Chain attacks ...

...could contain a cyber vulnerability at the time they are received.

...may introduce a vulnerability to create a specific effect that impacts a mission and designed in such a way as to avoid being detected.

...may degrade performance, cause erratic behavior, or cause premature failures.

Option: require suppliers to show evidence of good security controls

# Cybersecurity Logistics Approaches & Initiatives

Your turn...

What ideas do you have  
to enhance cybersecurity  
protection in the logistics  
arena?

# Cybersecurity Logistics Approaches & Initiatives

## Life Cycle Log/Supply Chain

- Approved Vendor Lists
- Program Protection Plans
- Product Support Elements
- Contract Clauses

# Cybersecurity Logistics Approaches & Initiatives

## All Logistics Communities

- Hygiene
- Redundancy
- Alternative Practices

# Cybersecurity Logistics Approaches & Initiatives

## All Logistics Communities

- Hygiene
- Redundancy
- Alternative Practices

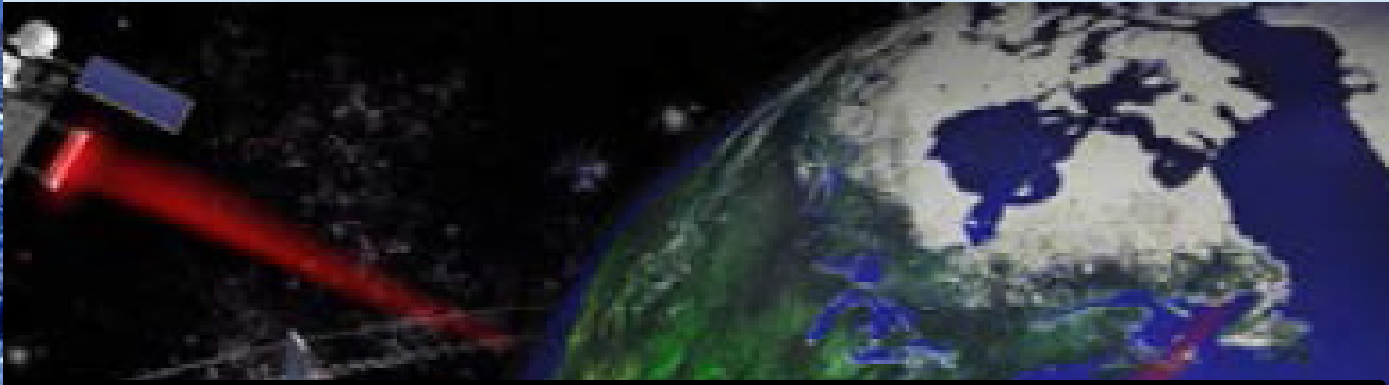


# Cybersecurity Logistics Approaches & Initiatives

## All Logistics Communities

- Risk Assessments
- Data Analytics
- Tiered Responses
- Focused Education

# Cyber is a battlefield



## ... And you are on the battlefront



The bottom line is:

A **cyber attack** **WILL**  
impact your life and  
work **if it hasn't already**