Headquarters U. S. Air Force

Integrity - Service - Excellence

Air Force Cyber Testing

Ms. Tanya Skeen
AF/TE(D)
16 March 2016

U.S. AIR FORCE

U.S. AIR FORCE

Cyber In The News

[China] has specialized units devoted to wage war on computer networks.

The Science of Military Strategy (translated from Chinese), 2015

Chinese doctrinal writings on cyber and asymmetric warfare portend that country's use of cyber-based means to disconnect and disable U.S. C4ISR and DoD fighting elements in the event of a conflict.

Defense Science Board, January 2013

Ukraine's top law enforcement agency, the SBU, has publicly claimed [a recent electricity blackout] was a cyberattack by Russia, part of its ongoing war over the Crimean peninsula.

CNN, January 18, 2016

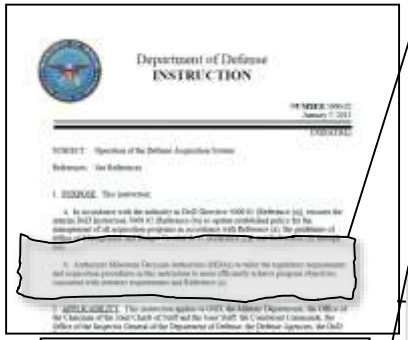
It is the firm determination of the DPRK to wage Korean-style cyber war to hasten the final ruin of the U.S. and the forces following it, who attempted to bring down the former with the cyber war.

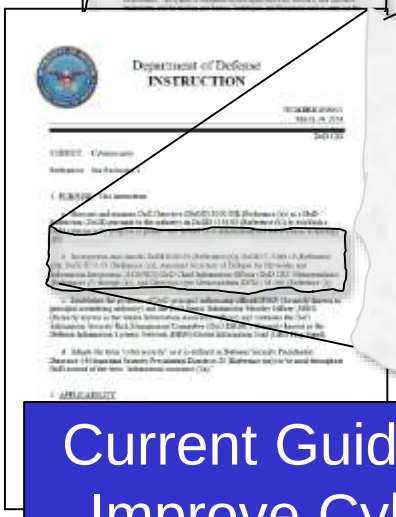
Rodong Sinmun, June 2015, newspaper of the Workers Party of Korea

The hacker "took five minutes to crack the [ACARS] messaging system. It was another couple of days before the same consultant managed to gain access to aircraft control systems."

Les Echoes, October 2015, French newspaper

Current Guidance


Department of Defense
INSTRUCTION


Department of Defense
INSTRUCTION

DoDI 5000.02, January 7, 2015

At a minimum, software in all systems will be assessed for **vulnerabilities**. Mission critical systems or mission critical functions and components will also require **penetration testing** from an emulated threat in an operationally realistic environment during OT&E.

DOT&E Memo, August 4, 2014

…test shall be conducted by a **vulnerability assessment** and **penetration testing** team through document reviews, physical inspection, **personnel interviews, and the use of the automated scanning, password tests, and applicable exploitation tools**.

Operational resilience must be achieved by: DoDI 8500.01, March 14, 2014

- Performing developmental T&E of cybersecurity in accordance with [DoDI 5000.02] and OT&E in accordance with [DOT&E Memorandums], including the **ability to detect and react to penetrations and exploitations and to protect and restore data and information**, in order to inform acquisition and fielding decisions.

Current Guidance Focused on Vulnerability ID & Penetration Test to Improve Cyber Hygiene → AF Moving toward **Resiliency Testing**

Air Force Direction

Air Force Vision & Strategy

"Exploit and defend air, space, and cyberspace, especially in contested environments, while denying our adversaries unrestricted use of the same"

- Air Force Vision 2015

Ensure resiliency … against attack from all domains, especially cyberspace

- Air Force Strategic Master Plan

Cyberspace will no longer be clearly separable from the physical domains, as actions in cyberspace will create effects in all other domains.

- Air Force Future Operating Concept

Future Strategy Demands that we Answer the Question:
"Will the weapon system work in a cyber challenged environment?"

Air Force Cyber Test Vision

- Focus: Move beyond RMF compliance/mitigation to testing wpn sys mission resiliency in an operationally rep cyber environment
  - Legacy Wpn Sys
    - Resiliency must be characterized to provide mission limitations in cyber attacks
    - System upgrades require re-test
  - New Wpn Sys
    - Resiliency must be "baked-in" via thoughtful design & well-defined threat capabilities
    - Lifecycle sustainment includes periodic threat updates & re-test
- Fundament Test Principles still apply in the Cyber domain
  - Instrumentation, Repeatability, Mission Context
  - Independent Trained Testers

Cyber Resiliency Testing Answers the Question:
"Will the weapon system work in a cyber challenged environment?

U.S. AIR FORCE

AF Efforts Underway

- Formalize Cyber Resiliency Testing
  - Mandate resiliency testing across AF DT and OT organizations
  - Develop techniques/tools to test, analyze & characterize wpn sys
- Infrastructure Requirements
  - Instrumented Hardware-in-the-loop weapon systems
  - Instrumented Cyber threat emulation and simulation
  - Visualization tools; response documentation; test data analysis
- Manpower
  - Develop/increase DT/OT personnel to conduct cyber testing
  - Bring test discipline and repeatability to cyber community
  - Improve Intel to characterize cyber threat systems & techniques
- Policy
  - AFI 99-103, 63-119 revisions in work
  - Engagement with OSD test policy efforts