The Cyber Threat

Dr. Jeff McNeil

January 29, 2015

What keeps me up at night?

- Adversaries already present in our networks
- Lack of information sharing and coordination with partners
- Cyber response capability and authority
- The role of third parties to exploit political conditions and technological advances
- ***Adversaries poised to exploit vulnerabilities in C2 and weapons systems; Convergence of Insider/EW/Cyber/Physical System threats***

All of these limit capability and options to defend the nation

Adversaries in our networks

The series of cyber attacks that repeatedly knocked major U.S. banking websites offline in the past nine months has been more powerful than the general public realizes…the distributed denial-of-service (DDoS) attacks … took down the websites of more than a dozen U.S. banks for hours or even days at a time…

-Reuters, Cyber attacks against banks more severe than most realize, May 18, 2013
www.reuters.com

"A successful cyber attack on a telecommunications operator could disrupt service for thousands of phone customers, sever Internet service for millions of consumers, cripple businesses, and shut down government operations.

And there's reason to worry: Cyber attacks against critical infrastructure are soaring. For instance, in 2012, the US Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security, processed approximately 190,000 cyber incidents involving US government agencies, critical infrastructure, and the department's industry partners. This represents a 68% increase over 2011."

"Security risks and responses in an evolving telecommunications industry"
PricewaterhouseCoopers Communications Review, Vol 18, No 2 at
http://www.pwc.com/

Adversaries in our networks

"America's air traffic control systems are vulnerable to cyber attacks, and support systems have been breached in recent months to allow hackers access to personnel records and network servers ... although most of the attacks disrupted only support systems, they could spread to the operational systems that control communications, surveillance and flight information used to separate aircraft."

NBC News, May 6, 2009

Hackers claiming allegiance to the Islamic State took control of the social media accounts of the U.S. military's Central Command on Monday, posting threatening messages and propaganda videos, along with some military documents.

-Washington Post, January 12, 2015

"In 2014, my office conducted 16 cybersecurity assessments in conjunction with Combatant Command and service exercises ... Despite the improved defenses, my office found that at least one assessed mission during each exercise was at high risk to cyber-attack from beginner to intermediate cyber adversaries."

-DOT&E FY14 Annual Report, January 16, 2015

Information Sharing and Coordination

In a cyber attack, are information sharing agreements and operational procedures in place to react and respond?

—Cyber Blitz his U.S., Korea,‖ *Wall Street Journal*, July 9, 2009.

5 ½ Years Later…
U.S.-United Kingdom Cybersecurity Cooperation, January 16, 2015

The United States and the United Kingdom agree that the cyber threat is one of the most serious economic and national security challenges that our nations face…Both leaders additionally recognized that the inherently international nature of cyber threats requires that governments around the world work together to confront those threats.
-http://www.whitehouse.gov/

Cyber Response Capability and Authority

- What options can I provide the SECDEF/POTUS?
- Are my cyber forces prepared to respond? Have their capabilities been proven?
- ***Are my forces resilient?***
- Are my alternatives a choice between ineffective or potentially overly escalatory options? Must I accept unnecessary risk?

Third Party Confounding Activities

- Potentially uncoordinated, but complicating activities of politically-motivated or opportunistic actors stress our defensive forces, processes and technologies
- Exacerbate attribution efforts and response options

C2 and Weapon System Resiliency

- Systems Engineering – Was my Design and PPP developed with cyber threats in mind?
- Test & Evaluation – Did I execute rigorous cybersecurity T&E to validate security controls and identify residual risks?
- Knowledge Management – Do I have access to program and evaluation data to rapidly research and mitigate exposed vulnerabilities?

- Defense in Depth?

A Worst-Case Scenario

…(One Version)…

- Political Event Leads to Regional Crisis; Increase Alert Levels and Diplomacy
- Cyber Attacks on Regional Networks and US Critical Infrastructure; Complex Attribution
- Inability to Coordinate with Relevant Actors (Other Agencies, Foreign Partners, etc.)
- Lack of Cyber Response Options … Alternatives Become Moribund or Escalatory
- **Successful Cyber Attacks on USTRANSCOM and Forward Edge ISR and Strike Platforms; Loss of Confidence in US Military Resiliency and Effectiveness**

Adversary Momentum Becomes Political Fait-Accompli

The Vignette

- Leading edge ISR assets are commandeered and lost
- Combat Air Patrol aircraft and ships maneuver to engage incoming aircraft…
- …no aircraft appear in the vicinity of the track; adversary aircraft approach carrier battle group undetected
- Rapid analysis identifies the first of potentially many previously unidentified supply chain and software vulnerabilities
- Catastrophic failure of carrier engineering plant

"On 4 December 2011, an American RQ-170 Sentinel UAV was captured by Iranian forces. The Iranian government announced that the UAV was brought down by its cyberwarfare unit which commandeered the aircraft and safely landed it…"

-"Exclusive: Iran Hacked US Drone, Iranian Engineer Says", csmonitor.com, 15 Dec 2011

Stuxnet

"Israel's attack on the alleged Syrian nuclear reactor involved disabling that nation's radar/anti-aircraft defenses... ...the Israelis had used a built-in kill switch to shut down the radar...the attack had been the work of Israel's equivalent of America's National Security Agency..."

-N.Y. Times: "IDF Unit 8200 Cyberattack Disabled Syrian Anti-Aircraft Defense", September 27, 2010

Resiliency

- Have we designed systems with cybersecurity as a driving consideration?
- Have we fundamentally tested new and legacy systems against both IP and non-IP-based attacks?
- Have identified vulnerabilities and risks been mitigated through design, sensors, indicators, TTP, defense in depth CONOPS, etc?

Why PPP?


Усовершенствованный F-16
компоновочная схема

SCALE GUIDE
COLOR & DECAL
キャノピーガラスはモデルのままでも良いですが、実機のように緑がかったスモークブラウンにすると更に良いでしょう。
参考C101(95%)+C49(5%)等
フレーム:C2
C305(80%)+C306(20%)
主翼・水平尾翼・垂直尾翼前縁及びインティークリップ
C305(80%)+C306(20%)
C3
C6
C28(内側:C62)
C305
C2(垂直尾翼外側は艶有りの黒)
◆細部塗装
●兵装庫内 :C62
●各脚収納部 :C62
●各脚柱 :C62
●ホイール :C62
●オレオ :C8
●各タイヤ部 :C33
●コックピット内部・シート:C308
●計器パネル・カバー:C33
C8
C35
内部はC1
内部はC1(リフトファンはC8)
■ AIM-9L/M Sidewinder
サイドワインダー空対空ミサイル
■ AIM-120C AMRAAM
アムラーム空対空ミサイル
◆右のネームは切り取って飾り台にネームプレートとしてお使い下さい。デカールの右下も同じ。
F-35B LIGHTNING II
ロッキードマーチン F-35Bライトニング II
F-35B LIGHTNING II
JOINT STRIKE FIGHTER F-35B
■COLOR GUIDE
C1 白 WHITE
C2 黒 BLACK
C3 赤 RED
C4 黄 YELLOW
C5 青 BLUE
C6 緑 GREEN
C8 銀 SILVER
C28 黒鉄色 STEEL
C33 艶消し黒 FLAT BLACK
C35 明白色(三菱系) IJN GRAY
C49 クリアーオレンジ CLEAR ORANGE
C62 艶消し白 FLAT WHITE
C101 スモークグレー SMOKE GRAY
C303 グリーンFS34102 GREEN FS34102
C305 グレーFS36118 GRAY FS36118
C306 グレーFS36270 GRAY FS36270
C308 グレーFS36375 GRAY FS36375
◆F-35B 性能表
全長 : 15.41m
全幅 : 10.97m
全高 : 4.60m
機体重量 : 13,888kg
最大離陸重量 : 22,680kg
エンジン : P&W製 F135ターボファンエンジン×1基
最大速度 : マッハ1.6
戦闘行動半径 : 830km
実用上昇限度 : 19,240m
固定装備 : 無し
乗員 : 1名
■サービスデカール
仮に航空自衛隊に導入された時の日の丸を付属しています。ご自由にお使い下さい。
● 主翼上下面用 30 + 31
● 胴体両側面用 32 + 33

The Cyber Threat

Dr. Jeff McNeil
jjmcnei@clemson.edu
Jeffrey.j.mcneil.ctr@mail.mil