Cyber Security Challenges and Opportunities

An academic perspective of the new DOD Cyber Strategy and how it impacts education, training, and industry
US Cyber Security Challenge

• U.S. prosperity and security depend on open and reliable access to information.

• Nations that are deterred from directly confronting U.S. military strength are using cyberspace operations in day-to-day competition to exploit a perceived advantage and harm our interests.

• China and Russia are engaging in great power competition via persistent, aggressive cyberspace campaigns that pose strategic, long-term risks to the Nation, our allies, and partners.

*The United States cannot afford inaction: our values, economic competitiveness, and military edge are exposed to threats that grow more dangerous every day*
Strategic Competition in Cyberspace

Goals

• **We must ensure the U.S. military’s ability to fight and win wars in any domain, including cyberspace.**
  - This is a foundational requirement for U.S. national security and a key to ensuring that we deter aggression, including cyber attacks that constitute a use of force, against the United States, our allies, and our partners.

• **Preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident**
  - Our primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets. The Department also provides public and private sector partners with indications and warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies.

• **Strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing** in order to advance our mutual interests.
What is the Cyber Threat Landscape

• Cyber threats confronting the US are multifaceted and evolving, ranging from individual hackers to hacktivists to criminals to terrorist organizations to nation-states or those that they sponsor, directly or indirectly.
• Complex threat spectrum affects both public and private sectors, the interface and intersections between them, as well as individual citizens. National security, economic security, and intellectual property are just some of the major interests at stake.
• A differentiation needs to be made among nuisance hacks, acts of espionage & true cyber attacks to proportionately defend against the most egregious threats.
  • Attribution
  • Retribution/retaliation
Key Themes

• Using cyberspace to amplify military lethality and effectiveness;
• Defending forward, confronting threats before they reach U.S. networks;
• Proactively engaging in the day-to-day great power competition in cyberspace;
• Protecting military advantage and national prosperity;
• Recognizing partnerships are key to shared success in protecting cyberspace;
Key Themes

• Actively contesting the exfiltration of sensitive DoD information;
• Embracing technology, automation, and innovation to act at scale and speed;
• Supporting the defense of critical infrastructure;
• Recruiting, developing, and managing critical cyber talent.
DoD Objectives for Cyberspace

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace domain;
2. Enhancing Joint Force military advantages through the integration of cyber capabilities into planning and operations;
3. Deterring, preempting, or defeating malicious cyber activity targeting U.S. critical infrastructure that is likely to cause a significant cyber incident;
4. Securing DoD information and systems, including on non-DoD-owned networks, against cyber espionage and malicious cyber activity;
5. Expanding DoD cyber cooperation with allies, partners, and private sector entities
Cultivate Talent (1 of 2)

• **Embed software and hardware expertise as a core competency:**
  • To make it attractive to skilled candidates, establish a career track for computer science related specialties (including hardware engineers, software developers, and data analysts) that offers meaningful challenges, rotational billets at other Federal departments and agencies, specialized training opportunities tied to retention commitments, and the expansion of compensation incentives for the Cyber Excepted Service (CES).

• **Establish a cyber top talent management program:**
  • Provides most skilled cyber personnel with focused resources and opportunities to develop key skills over the course of their careers.
  • Use competitive processes, including individual and team competitions, to identify the most capable DoD military and civilian cyber specialists and then empower those personnel to solve the Department’s toughest challenges.
• Sustain a ready cyber workforce:
  • Invest in building future talent, identifying and recruiting sought-after talent, and retaining current cyber workforce.
  • Provide ample opportunities for professional development and career progression of cyber personnel.
  • Ensure that cyber requirements are filled by the optimal mix of military service members, civilian employees, and contracted support to serve mission requirements.

• Enhance the Nation’s cyber talent:
  • DoD plays an essential role in enhancing the Nation’s pool of cyber talent in order to further the goal of increasing national resilience across the private and public sectors.
  • Increase efforts to promote science, technology, engineering, mathematics, and foreign language (STEM-L) disciplines at the primary and secondary education levels throughout the United States.
  • DoD will also partner with industry and academia to establish standards in training, education, and awareness that will facilitate the growth of cyber talent in the United States.
Interpreting the new DOD Strategy

- Persistence...
  - Persistent Engagement
  - Persistent Presence in adversaries’ cyberspace
  - Persistent Innovation – faster than adversaries
- Must maintain constant contact with our adversaries
- Superiority in this domain is dynamic (...and tenuous)
- Must adjust to the new environment
Efforts to Define Cyber Education & Training
Fundamental “truths” of cyberspace operations:

1. Humans are more important than hardware.
2. Quality is more important than quantity.
3. Cyber forces cannot be mass produced.
4. Competent cyber forces cannot be created after an emergency occurs.
5. Most cyberspace operations will require support from non-cyber forces.
Bounding Cyber Security
Cyber-related Academic Credentials

• Two existing and new areas to link cyber studies:
  • ABET:
    • Nonprofit, non-governmental accrediting agency for programs in applied and natural science, computing, engineering and engineering technology
    • New Cybersecurity criteria
  • NSA and DHS sponsored National Centers of Academic Excellence in Cyber Defense (CD) and Cyber Operations (CO)
ABET New Cybersecurity Criteria

• Applies to computing programs using cybersecurity, computer security, cyber operations, information assurance, information security, or similar terms in their titles.
• At least 45 semester credit hours (or equivalent) of computing and cybersecurity course work.
• The course work must cover:
  • Application of the crosscutting concepts of confidentiality, integrity, availability, risk, and adversarial thinking.
  • Advanced cybersecurity topics that build on crosscutting concepts and fundamental topics to provide depth.
• At least 6 semester credit hours (or equivalent) of mathematics that must include discrete mathematics and statistics.
ABET New Cybersecurity
Fundamental topics

- **Data Security**: protection of data at rest and in transit.
- **Software Security**: development & use of software that reliably preserves security properties of information and systems.
- **System Security**: establishing & maintaining security properties of systems, including those of interconnected components.
- **Human Security**: protecting individuals’ personal data and privacy; threat mitigation combined with the study of human behavior as it relates to cybersecurity.
- **Organizational Security**: protecting organizations from cybersecurity threats & managing risk to support successful accomplishment of the organizations’ missions.
- **Societal Security**: aspects of cybersecurity that can broadly impact society as a whole for better or for worse.
National Centers of Academic Excellence in Cybersecurity

• Cyber Defense (CAE-CD):
  • NSA & DHS jointly sponsored
  • Goal: reduce vulnerability in national information infrastructure by promoting higher ed and research in cyber defense and producing professionals with cyber defense expertise

• Cyber Operations (CAE-CO)
  • Emphasis on technologies & techniques related to specialized cyber operations, to enhance the National security posture; critical to intelligence, military and law enforcement organizations authorized to perform these specialized operations.
US Naval Academy Cyber Education

Turning Midshipmen into Cyber Warriors
Importance of Cyber Education at USNA

• The Cyber Domain is a warfighting domain...just like Sea, Land, Air, and Space
  • Adversaries and threats are not going away, they are adapting, becoming asymmetric, more challenging
• All of our graduates will serve as officers in units and fields which will all rely on...depend on...Cyber Operations and Cyber Security
  • Mission Assurance and Success depend on it
• We must ensure our future officers and leaders understand this complex domain as they do all others
  • While our incoming student body is highly technical, their understanding of this domain is limited in scope
USNA Strategic Challenges

• Educate **all of** our students on the importance of Cyber Security and the Cyber Domain as a warfighting area

• Develop cyber-related course(s) of study

• Create a viable path for accessions of junior officers into the Information Warfare Community
Programs and Facilities
- Cyber Internships
- Cyber Competitions
- International Exposure
- Cyber related Clubs
- Cyber Lecture series

Curricular Elements
- Cyber Operations major
- Cyber Semesters Abroad
- Innovative/Creative Design projects
- Single/multi-disciplinary electives
- Two required Cyber core courses for All Midshipmen

Goal: Prepare Graduates to Lead in an Evolving Cyber Domain
Other Thoughts

• Educate, educate, educate...train, train, train
  • The *human in the loop* continues to be the weak link in the majority of all attacks

• Cyber Security is not a “fad”, all levels of the workforce, from the top down/bottom up, need increased awareness and better understanding

• Enable better information sharing with private sector, industry, government – that can’t be mandated, must be “owned” by all parties

• When cyber attacks can be attributed...attribute them publicly, let others know of the threat
Director, NSA: What Keeps Him Up At Night

1. **Cyber attacks that do infrastructure damage**: "It is only a matter of 'when' that someone users cyber as a tool to do damage to the critical infrastructure of our nation, I'm watching nation states, groups within some of that infrastructure. At the moment, it seems to be really focused on reconnaissance and attempting to understand the characteristics of the structure, but it's only a matter of time I believe until someone actually does something destructive."

2. **Data manipulation**: "Historically, we've largely been focused on stopping the extraction of data and insights, whether for intellectual property for commercial or criminal advantage, but what happens when suddenly our data is manipulated and you no longer can believe what you're physically seeing? As a military guy, who's used to the idea that, 'I can look at a display, I can look at a set of data, and I can very quickly draw conclusions and start to make risk-based decisions quickly,' what happens if that gets called into question? I believe that's going to happen."

3. **Non-state actors**: "What happens when a non-state actor, who literally has no interest in the status quo — take ISIL for an example, whose vision of the world is diametrically opposed to ours — starts viewing the web as not just a vehicle to generate revenue, to recruit, to spread the ideology, but instead they view it as a weapon system?"
Questions
Back up slides
Safeguarding your Home Network

Secure Your Wireless Router: Unless you secure your router, you’re vulnerable to people accessing information on your computer, using your Internet service for free and potentially using your network to commit cybercrimes. Here are ways to secure your wireless router:

• **Ensure your WiFi encryption is on:** When choosing your router’s level of security, opt for **WPA2**, if available, or WPA...WEP is weak and breakable (~30-seconds to break with free software).

• **Change the default name of your router:** The default ID - called a service set identifier” (SSID) or “extended service set identifier” (ESSID ) – is assigned by the manufacturer. Change your router to a name that is unique/obscure (...not “GoNavy”) and won’t be easily guessed by others. You can also disable your SSID broadcast so

• **Change the default password on your router:** When creating a new password, make sure it is long and strong, using a mix of numbers, letters and symbols.

• **Use a firewall:** Firewalls help keep hackers from using your computer to send out your personal information without your permission. While anti-virus software scans incoming email and files, a firewall is like a guard, watching for attempts to access your system and blocking communications with sources you don’t permit. Your operating system and/or security software likely comes with a pre-installed firewall, but make sure you turn on these features.

• **Create a guest password:** Some routers allow for guests to use the network via a separate password. If you have many visitors to your home, it’s a good idea to set up a guest network.
Safeguarding your Online Activity

- **Keep a clean machine:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

- **Protect all devices that connect to the Internet:** Along with computers, smart phones, gaming systems, & other web-enabled devices need protection.

- **Plug & scan:** “USBs” and other external devices can be infected by viruses & malware. If you must use them (...DOD doesn’t allow USB drives...), scan them first.

- **Protect your $$:** When banking & shopping, check to be sure the sites is security enabled. Look for web addresses with “https://” which means the site takes extra measures to help secure your information. [“http://” is not secure it has no s]

- **Back it up locally (...not in a cloud):** Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

- **Free WiFi...is not free:** Free and/or Public networks should never be assumed to be secure.
Define/Declare Priorities
- Define the assets, capabilities, and conditions the US is prepared to defend in and through cyberspace
  - Private components yield internal clarity and coherence
  - Public components (messaging) yields deterrence in adversaries and confidence in partners
  - The delta between public and private yields uncertainty for the adversary and maneuver advantage for the US

Planning
- Tailoring the components of deterrence to deter extant (known threats), anticipated (projected threats), and prospective actors (vulnerabilities)

Establish Inherent Resilience
- Analogous to traditional Information Assurance
- Establishing technology, doctrine, and procedures that yield defensible architectures
  - Expectation, norms, and accountability for creating defensible architectures

Establish Vigilance and Cognizance as a basis for action
- Vigorous and comprehensive intelligence
- Assessing readiness and taking action(s) to redress
- Redteaming, hunting
- Exercises, COOP drills
- Warning
- Alliances, international law, collective action

[re]Active Defense – the local, close in, fight
- Active engagement of adversaries
- Hackback
- Public and Private sector roles

Impose Consequences – the away fight
- All instruments of power – far more than cyber

Deterrence by Deny Benefits
Requires Attribution
Requires Detection

Deterrence by Impose Costs

Building Blocks of Deterrence

JCI – September 2015
DO YOU KNOW YOUR THREATS, VULNERABILITIES, AND IMPACTS...
DO YOU KNOW YOUR THREATS, VULNERABILITIES, AND IMPACTS…

Vulnerabilities:
• Discoverable: How easy is it for an adversary to discover the vulnerability?
• Exploitable: How easy is it for an adversary to exploit the vulnerability?
• Awareness: How well known is the vulnerability?
• Detectable: How likely is an exploit to be detected?
DO YOU KNOW YOUR THREATS, VULNERABILITIES, AND IMPACTS…

Threats:
• Capability: How technically skilled is an adversary?
• Opportunity: What resources and opportunities are required for an adversary to find and exploit a vulnerability?
• Intent: How motivated is an adversary to find and exploit a vulnerability? Does the actor performing the exploit intend harm?
DO YOU KNOW YOUR THREATS, VULNERABILITIES, AND IMPACTS...

- Impacts:
  - To what extent are personnel in physical danger if vulnerability exploited?
  - To what extend is equipment in physical danger if vulnerability exploited?
  - To what extent will the success of operations be endangered?
  - To what extent will the capabilities of the organization be damaged?
  - To what extent will the organizations reputation be damaged?
  - What will the financial damage to the organization be?
DO YOU KNOW YOUR THREATS, VULNERABILITIES, AND IMPACTS…

“Danger Zone”
ANATOMY OF AN ATTACK:
ONE VIEW OF THE CYBER “KILL CHAIN”

Attacker average time in a network well over 100 days... and then another 100+ days to detect attack

ANOTHER VIEW OF THE KILL CHAIN OR ATTACK CYCLE*

Figure 2. Cyber attack lifecycle.

Initial Recon: Identify exploitable vulnerabilities
Initial Compromise: Gain initial access into target
Establish Foothold: Strengthen position within target
Escalate Privileges: Steal valid user credentials
Internal Recon: Identify target data
Complete Mission: Package and steal target data

M-TRENDS® A View From the Front Lines 2017 – FireEye www.FireEye.com
ONE VIEW OF CYBER ATTACKS YOU’RE LIKELY TO FACE

• Social Engineering attack – tricking end user into installing malware/trojan
• Password phishing attacks – tricking end user via cleverly crafted email to reset password at false site (...DNC Hack)
• Unpatched software – is your network patched & updated? How about all of the devices connected? Do you allow BYOD? How to plan for IOT?
• Social media threats – Personal info can be used to gain access or additional info (Facebook, LinkedIn, Organization Website, etc.)
• Advanced persistent threats – Sophisticated intrusion via malware, network/system vulnerability, end-user clicking something

https://www.entrepreneur.com/article/252028
AN INTERCONNECTED WORLD: NATURE AND DIMENSIONS OF THREATS

• What is the nature and dimensions of the threats deriving from the interconnected world?
  • Intelligence Gathering/Information Operations
  • Military use of the Cyber Domain
  • State Actors
  • Criminal & Economic
    • Theft of Intellectual Property
  • Critical Infrastructure
  • Non-state Actors (Sub-state actors)