UNITED STATES CYBER COMMAND
9800 Savage Road Fort George G. Meade, Maryland 20755

MAR 23 2012

Reply to:
USCYBERCOM/CDR

MEMORANDUM FOR RECORD

Subject: United States Cyber Command (USCYBERCOM) Commander's Strategic Assessment for Operating in Cyberspace – Preventing a Pearl Harbor Environment

1. The United States (U.S.) is vulnerable to the accelerated pace of cyberspace "events." The U.S. must immediately act through several cyber initiatives to ensure we avoid a cyber Pearl Harbor.

2. The President identified cyber security as one of the most serious threats we face as a nation. Events in cyberspace continue to accelerate as Nation States and non-state actors seek to exploit asymmetrical advantages in the cyber domain. Examples include:

a. Recent Google, RSA, Lockheed Martin, Booz Allen Hamilton, and NASDAQ, exploits.

b. Disruption of networks (Estonia, banks, etc.)

c. Development of Cyber attack tools by Nation States (Russia, China, and Iran)

d. Recent reports of AQ intent to use Cyber Attack tools

e. Critical loss of Intellectual Property (greatest transfer of wealth in history)

f. UAV virus

3. The risks of failure in the cyber domain are widespread, cascading, and potentially catastrophic.

a. The nation relies on the cyber domain for its major activities (military, commerce, utilities, governing), posing risks to the value of the entire U.S. investment in military capabilities, intellectual property, critical infrastructure, and diplomatic relationships.

b. The cyber domain poses unique challenges because it is a globally connected domain without traditional borders; the enabling infrastructure is owned and operated by military and civilians alike; activities occur at cyber speed making synchronization of national-level responses essential.

c. The attacker currently has the advantage over the defender because the defender must defend everywhere across the network while the attacker merely needs to find a single point of vulnerability.

d. The U.S. as a society is extraordinarily vulnerable because we rely on highly interdependent networks with ubiquitous access points that are unsecure, sensitive to interruption, and lack resiliency.

4. Adversaries leverage their comparative advantages and exploit our vulnerabilities.

a. Our capabilities continue to grow with increasing access into other countries, but others have access into our networks.

b. They are preparing future battlefields now by stealing intellectual property and exploiting networks across the defense, financial, and communication sectors.

c. We know adversaries are actively conducting reconnaissance, surveillance, penetration, and establishing persistence.

5. The USCYBERCOM Commander's Assessment.

a. We can prevent some attacks but we cannot prevent a major cyber attack against the U.S. now because:

(1) We have a multitude of asset types with various configurations and more gravely have multiple organizations enacting inconsistent policies, capabilities, and configurations, preventing unified approaches to cyber security.

(2) We cannot see across all networks which allows adversaries to operate in uncontested areas as they seek to penetrate our defenses.

(3) We lack authorities and policy to act in defense of the nation as a whole.

(4) We have insufficient trained and ready forces to act.

(5) We rely on an inherently indefensible architecture built for availability, functionality, and ease of use, with security bolted on as an afterthought.

(6) We have immature operational concepts.

(7) Commercial industry is reluctant to divulge penetrations/attacks due to perceived vulnerability, lack of technical competency, and loss of share holder confidence which could negatively impact future business relationships.

b. What must an adversary have to conduct a cyber Pearl Harbor?

(1) Strategy to drive goals and objectives.

(2) Operational Concept on how they will fight.

(3) Capabilities to achieve the effects required to meet those objectives.

(4) Training to ensure their forces can employ capabilities effectively.

(5) Knowledge and access to vulnerabilities in our networks.

(6) Catalyst for the decision to attack.

(7) An opponent susceptible to surprise or unwilling/unable to proactively defend itself.

c. Today we are seeing:

(1) Cyber development is following the traditional path from commercial innovations to war fighting capabilities much like that of aviation.

(2) Russian operations in Estonia and Georgia demonstrated how cyber could be employed and provided lessons learned for cyber operations.

(3) China and others have been thinking about cyber doctrine for years at senior military schools and think tanks.

(4) The U.S. has already observed the cyber equivalents of the sinking of a battleship at Taranto and the practice for using torpedoes in shallow waters.

(a) The attack by British airplanes using modified torpedoes validated the concept that air dropped torpedoes could be effective in shallow waters.

(b) The Japanese carefully studies the attack and openly practiced the techniques months prior to the attack on Pearl Harbor.

(c) The tactics and planning that enabled the Pearl Harbor attacks were a direct result of the lessons learned from the Battle of Taranto.

(d) Lessons learned from Russian operations in cyberspace are being turned into tactics and planning by future adversaries today.

(5) Cyber capabilities already exist that can attack systems and render them inoperable even when basic security measures are employed.

(a) Capabilities are being developed and deployed for foreign intelligence, commercial espionage, and criminal activity to penetrate networks.

(b) Advance Persistent Threats can maintain access undetected for long durations ready to act.

(6) Adversaries are only 12-18 months away from having the capability to conduct a cyber Pearl Harbor against the U.S.

(a) Once they have the capability to conduct the attack all that remains is a catalyst before they would act.

(b) They must develop the ability to prevent or mitigate that possibility or we will be left waiting for the adversary to decide when to strike.

d. What we need to do to prevent a cyber Pearl Harbor?

(1) At a minimum, prevent attacks; if that fails, stop attacks, and if that fails, reduce their effect on the nation as they occur, regardless of the attacker, target, means of attack, and launch point and quickly recover from their effects sustained.

(2) The U.S. needs to publicly debate the roles of the DoD and the Intelligence Community (IC) in the protection of the Nation's critical cyber resources.

(a) If the DoD and the IC are going to be operating in cyberspace, their roles and functions must be understood and generally approved by the public.

(b) Part of this discussion should be: What critical infrastructures are serious enough to require DoD/IC involvement?

(c) Being open about our strategy puts our adversaries on notice and removes the possibility of false expectations on the part of the U.S. public.

(3) Global Visibility Enabling Action.

(a) We need to be able to see cyberspace (red, blue, and gray) and provide situational awareness for our decision makers and cyber operators.

(b) Build the capability to recognize early indications of an attack.

(4) Defensible Architecture.

(a) We need a defensible infrastructure with clear identification of critical systems.

(b) Information Technology (IT) efficiencies will support the DoD initiatives to implement defensible architecture that will:

i. Streamline IT capabilities.

ii. Enable shared control of limited resources.

iii. Increase ability to outmaneuver threats.

iv. Support single organizational direction and technical configuration.

(5) Authorities to Act in Defense of the Nation.

(a) We need the authorities to defend designated networks by creating effects outside of the defended network (Computer Network Defense-Response Action).

(b) Long term response should be led by the Executive Branch, but DoD must be capable of stopping attacks while in progress – or before.

i. Pre-approve Standing Rules of Engagement (SROE) response options so they can be immediately implemented at each level of command from tactical to strategic.

ii. Establish processes to rapidly approve additional response options in a crisis, analogous to nuclear Command and Control options.

(6) Command and Control of Cyber Forces.

(a) Immediately co-locate needed authorities with designated cyber operators in the form of operators empowered to act on behalf of their parent organizations at an Integrated Cyber Center.

(b) Integrate and leverage interagency, commercial industry, allies, and foreign partners.

i. Supported by policies for exchanging intelligence on threats and capabilities.

ii. Expand defensive capabilities to critical infrastructure and key sectors.

(c) Incorporate cyber as a flexible option for consideration by U.S. Government decision makers during shaping and deterrence phase ops.

(d) Further build out the Cyber Support Elements with trained cyber analysts and planners and fully integrate them into the Combatant Commands (COCOMs).

(e) Develop the Joint Communications Control Centers and enable them to fully support the COCOMs.

(7) Trained and Ready Cyber Forces.

(a) We need a standing cyber force that is prepared to act immediately and is capable of fighting and winning in cyberspace.

(b) USCYBERCOM should set and enforce uniform training and certifications standards across all services and DoD.

i. Lead USCYBERCOM components should lead Service efforts to organize. train and equip cyber forces to meet training and readiness standards.

ii. Assign Service Cyber Components proponency for cyber functional areas.

(c) We need to create joint cyber designators to track military/civilian cyber workforce.

i. Standardize Cyber Work Roles across DoD and the IC.

ii. Track officer. Enlisted and DoD Civilians cyber career paths and assignments to ensure our success.

(d) Repurpose IT personnel not needed as a result of IT efficiencies.

(e) Recruit cyber warriors including use of non-traditional recruiting sources.

(f) Make greater use of reserve and guard component forces - cyber units. but also cyber joint planning teams to work on lower-priority missions that are below the active components' cut lines.

6. Recommendations for Improving DoD's Cyber Defenses.

a. Strengthen Network Defenses:

(1) Reduce the number of individual DoD networks and network owners to a minimum necessary to provide required services.

(2) Architect the remaining networks to be more robust. resilient. and defensible. Develop global visibility of red. blue. and gray.

(a) Cyber Pilot

(b) National Security Agency (NSA) Infrastructure

(c) Op Center connectivity

(3) Leverage global cryptologic platform to identify threats (exploits and attacks) before they are launched against us, and enable USCYBERCOM to deploy defenses in advance of their use.

(4) Leverage partnerships with commercial entities (.com, Defense Industrial Base (DIB), etc.) as a means of strengthening our defenses and also gathering information about enemy actions, exploitations, and attacks.

(5) Leverage cloud computing to store critical information where it can be most easily protected by emerging attribute based access protocols.

(6) Share classified signatures and other information with Tier 1 Internet Service Providers, DIB, and Critical Infrastructure and Key Resources to strengthen National defense beyond the Global Information Grid (GIG).

(7) Expand boundary defenses: employ reconnaissance, counter-reconnaissance, and countermeasures beyond the GIG to prevent attacks on our networks.

(8) Neutralize adversary capabilities affecting DoD systems at the point of origin (without necessarily destroying the adversary system or network), regardless of the capability (surveillance, reconnaissance, attack).

b. Assume our networks are compromised, improve Operations Security and Rear Area Security.

(1) Employ hunter teams to patrol inside the wire, searching for signs of enemy exploits or intrusions.

(2) Build insider protection tools and practices.

(3) Architect networks to be robust and resilient to enemy action.

c. Deter attacks in the long term.

(1) Build capability to ensure rapid and reliable attribution.

(2) Establish credible commitment to respond to attacks in proportional fashion.

(3) Signal clear political will to act in response to credible threats of planned aggression.

(a) National boundaries have less meaning in cyberspace; the virtual cyber battle may take place on servers physically located anywhere around the world.

(4) Continually build accesses into adversary networks to gain critical intelligence for active defense and to enable the U.S. to project power through cyberspace.

d. Respond smartly.

(1) Rapid response options in place (Standing Rules Of Engagement) – proportional to escalatory; cyber to kinetic.

(2) Assess second. third order effects of both the attack and proposed responses.

(3) Deconflict with partners: assess consequences of targeting key cyber terrain on military operations. effects and intelligence.

(4) Maximize pre-planning. pre-authorization. and automation of cyber operations.

(5) Streamline approval processes to act. to enable us the ability to act at "net speed"

c. Treat the network as a weapons platform. and train they way we will fight in cyberspace.

(1) Cyber forces across all components (active. reserve. guard. DoD civilians) must be trained to common baseline standards.

(2) Having all Lines of Operation under the same chain of command provides unity of effort and provides the synergy necessary to make them stronger.

(3) Partner between NSA and USCYBERCOM to build accesses that support contingency planning and COCOM deliberate planning objectives and desired effects.

(4) Develop streamlined targeting procedures that allow us to operate at "net speed."

(5) Grow a cyber training center in which cyber warriors practice their tradecraft in a realistic, stressful environment.

(a) Focus cyber training at the individual, collective, Joint Task Force and COCOM staff level.

(b) Track and evaluate via exercises/real world operations.

(6) Establish common Tactics. Techniques. and Procedures (TTPs) for fighting in cyberspace.

(a) This would take the form of a Cyber Field Manual analogous to the Counter Insurgency manual.

(b) Think beyond one-off attacks: develop tactics that are generally applicable to a variety of situations.

(7) Be prepared to execute cyber missions as part of a larger national response to attacks against the nation.

KEITH B. ALEXANDER
General. U.S. Army
Commander