FEBRUARY 27, 2014

U.S. STRATEGIC COMMAND AND U.S. CYBER COMMAND

U.S. SENATE, COMMITTEE ON ARMED SERVICES

ONE HUNDRED THIRTEENTH CONGRESS, SECOND SESSION

HEARING CONTENTS:

OPENING STATEMENT:

Carl Levin *[view PDF]*
Chairman, Senate Committee on Armed Services

WITNESSES:

Admiral Cecil D. Haney, USN *[view PDF]*
Commander, U.S. Strategic Command

General Keith B. Alexander, USA *[view PDF]*
Commander, U.S. Cyber Command

AVAILABLE WEBCAST(S):*

Link to full hearing webcast (duration 02:35:45):

- *http://www.armed-services.senate.gov/hearings/watch?hearingid=5a1e1cef-5056-a032-5287-157157e68450*

COMPILED FROM:

- *http://www.armed-services.senate.gov/hearings/14-02-27-us-strategic-command-and-us-cyber-command*

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

Levin opening statement, Senate Armed Services Committee hearing with U.S. Strategic Command and U.S. Cyber Command

Thursday, February 27, 2014

Good morning. Today we begin our annual posture hearings with the combatant commands by receiving testimony from the U.S. Strategic Command and the U.S. Cyber Command, a sub-unified command of the U.S. Strategic Command. Let me welcome Admiral Cecil Haney, in his first appearance before the committee as the Commander of the U.S. Strategic Command, and General Keith Alexander, in his final appearance before the committee as Commander of U.S. Cyber Command. General Alexander also serves as the Director of the National Security Agency and when he retires at the end of next month he will by far be the longest serving NSA Director in history. We thank you both for your service.

This hearing comes at a time of reduced budgets across the U.S. Government, including the Department of Defense. Even though this hearing comes in advance of the 2015 budget request, we will want to hear from our witnesses about the impact the overall budget situation and the expected 2015 budget submission are likely to have on the programs and operations under their oversight and direction.

Admiral Haney, I hope you will address the full range of issues impacting Strategic Command today, including the status of our nuclear deterrent; the impact of the recent ICBM cheating scandal; any potential efficiencies and cost savings that could reduce the $156 billion that DOD projects it will need to maintain and recapitalize our nuclear triad over the coming decade; steps that may be needed to ensure that we can protect or reconstitute our space assets in any future conflict; and concerns about the adequacy of DOD's future access to communications spectrum as pressure builds to shift more and more spectrum to commercial use.

For most of the last year, General Alexander has been at the center of both the crisis over the loss of intelligence sources and methods from the Snowden leaks and the controversy over aspects of the

Recent News

- Senate Floor Statement of Sen. Carl Levin on the Paycheck Fairness Act – 04-09-2014
- Senate floor statement on the introduction of the MotorCities National Heritage Area Extension Act – 04-08-2014
- Levin opening statement, Senate Armed Services Committee hearing on Army active and reserve force structure – 04-08-2014
- Levin floor statement on the need to renew emergency unemployment benefits – 04-07-2014
- Levin leads Great Lakes senators in pushing for funding for the lakes in Congressional spending bills – 04-04-2014

View more press »

Related Issues

- National Security and Veterans
- A Balanced Approach to Deficit Reduction
- Federal Budget and Fiscal Policy

intelligence activities established after 9/11 to address the terrorist threat.

We look forward to hearing your views about the changes to the NSA collection programs directed by the President; the impact on the military of the Snowden leaks; the capability of the personnel that the military services are making available for their new cyber units; the services' ability to manage the careers of their growing cadre of cyber specialists; and steps that can be taken to ensure that the Reserve Components are effectively integrated into the Department's cyber mission.

In addition, I hope you will provide us with your analysis of the Chinese campaign to steal the intellectual property from U.S. businesses. The committee has almost completed a report on cyber intrusions into the networks of some of the defense contractors on whom DOD may rely to conduct operations. I hope that you will give us your assessment as to whether China has shown signs of altering its cyber behavior subsequent to Mandiant Corporation's exposure of the operations of one of its military cyber units.

Senator Inhofe.

###

Senator Levin's Offices

Washington D.C.	Lansing
Detroit	Traverse City
Escanaba	Saginaw
Grand Rapids	Warren

Washington D.C.

269 Russell Office Building
U.S. Senate
Washington, DC 20510-2202
Phone (202) 224-6221
Fax (202) 224-1388
TTY (202) 224-2816
Get Directions

STATEMENT OF

ADMIRAL C. D. HANEY

COMMANDER

UNITED STATES STRATEGIC COMMAND

BEFORE THE

SENATE COMMITTEE ON ARMED SERVICES

27 FEBRUARY 2014

INTRODUCTION

Mr. Chairman and distinguished members of the committee, I am honored to join you today. This is my first appearance before you as the Commander of United States Strategic Command (USSTRATCOM), and I appreciate the opportunity to testify about the importance of strategic deterrence in the 21st century and on how USSTRATCOM is responding to today's complex global security environment. Following my confirmation late last year, I reviewed USSTRATCOM's missions, priorities, and capabilities. I found an organization executing a diverse set of global responsibilities that directly contribute to national security, and I am pleased to report that today USSTRATCOM remains capable and ready to meet our assigned missions. We are blessed to have a talented, dedicated, and professional cadre of military and civilian men and women to address the significant national security challenges facing our nation. I thank Congress and this committee for your support and I look forward to working alongside you throughout my tour of duty.

USSTRATCOM carries responsibility for nine mission areas as assigned by the Unified Command Plan (UCP). These mission areas are critical to national security and strategic stability. The more significant challenge to sustaining excellence in these mission areas for the foreseeable future remains how we balance national priorities and fiscal realities given the outlook for future Department of Defense (DOD) budgets under current law spending constraints. This requires that we take a strategic approach to understanding and prioritizing near term and future threats in a systematic manner that ultimately involves balancing risks. My USSTRATCOM team and I are fully engaged in this work helping to not only execute missions and conduct detailed planning, but providing insight to inform our national decision making process regarding these critical strategic national security issues. Even in the current fiscal

environment, and given the complex strategic security environment, we must ensure the necessary strategic capabilities are adequately resourced.

GLOBAL SECURITY ENVIRONMENT

The current security environment is more complex, dynamic and uncertain than at any time in recent history. Advances of significant nation state and non-state military capabilities continue across all air, sea, land, and space domains—as well as in cyberspace. This trend has the potential to adversely impact strategic stability. Nation states such as Russia and China are investing in long-term and wide-ranging military modernization programs to include extensive modernization of their strategic capabilities. Nuclear weapons ambitions and the proliferation of weapon and nuclear technologies continues, increasing risk that countries will resort to nuclear coercion in regional crises or nuclear use in future conflicts. A number of actors are improving their existing Weapons of Mass Destruction (WMD) capabilities while others are pursuing new capabilities along with the technologies to deliver deadly agents against targets of their choice. These include nations as well as non-state Violent Extremist Organizations (VEOs).

While we have increased our own cyber capabilities, the worldwide cyber threat is growing in scale and sophistication, with an increasing number of state and non-state actors targeting U.S. networks on a daily basis. Due to cyberspace's relatively low cost of entry, cyber threats range from state-sponsored offensive military operations and espionage activities, to VEOs intent on disrupting our way of life, to cyber criminals and recreational hackers seeking financial gain and notoriety. Additionally, the U.S. supply chain and critical infrastructure remains vulnerable to cyber attack, and even as we detect and defeat attacks, attribution remains a significant challenge.

Developed nations rely heavily on space systems to enable a wide range of services which provide vital national, military, civil, scientific and economic benefits. The space domain is becoming ever more congested, contested and competitive but the number of space-faring nations continues to grow. The U.S. still retains a strategic advantage in space as other nations are investing significant resources—including developing counterspace capabilities—to counter that advantage. These threats will continue to grow over the next decade.

Finally, uncertainty continues to manifest in a number of other ways such as terrorist threats, social unrest and turmoil, and regional competition for scarce resources and economic opportunities.

PRINCIPLES OF OUR DETERRENT

In the broadest sense, **USSTRATCOM's mission is to deter and detect strategic attacks against the U.S. and our allies, and to defeat those attacks if deterrence fails**. Strategic attacks are those which have decisive negative outcomes—and they are not all nuclear in nature. They may impact many people or systems, affect large physical areas, act across great distances, persist over long periods of time, disrupt economic and social systems, or change the status quo in a fundamental way. While nuclear attack will always remain unique in its potential for devastation, today's strategic attacks can occur through a variety of mechanisms across multiple domains and are defined by the magnitude of their effect versus a specific weapon or means of delivery. As a nation, we must continue our efforts toward deterring both nuclear and non-nuclear strategic threats to global security.

Although the likelihood of major conflict with other nuclear powers is remote today, the existential threat posed by a nuclear attack requires the U.S. to maintain a credible and capable deterrent force. While total deterrence against any particular adversary is never guaranteed, I am

confident in our ability to deter nuclear attack. Arms control treaties have and continue to reduce the likelihood of nuclear conflict with Russia, but the possibility of regional nuclear conflict strains U.S. alliances and global security commitments.

USSTRATCOM is taking appropriate steps to mitigate these strategic risks by actively executing a tailored deterrence and assurance campaign plan against specific strategic threats on a daily basis and by updating contingency plans that account for deterrence failure. Our campaign and contingency plans employ the breadth of USSTRATCOM capabilities in concert with other U.S. capabilities and the regional combatant commands.

Increased interdependence between organizations (to include other combatant commands, the interagency, and allies and partners) and across domains will be a hallmark of future military operations. Our military forces must exercise the ability to operate in degraded environments, and future conflicts are not likely to be limited to a single domain or by geographic boundaries. Our planning leverages robust integration with other combatant commands and applies the breadth of USSTRATCOM capabilities to pursue national objectives. Combatant commands, the whole of the U.S. government, and allies and partners will need to train, exercise and operate together using all the instruments of national power. This will require increased linkages and synergies at all levels to bring the appropriate integrated capabilities to bear through synchronized planning, simultaneous execution of plans, and coherent strategic communications. The Combatant Command Exercise and Engagement Fund supports USSTRATCOM's needs by addressing our joint training requirements and is integral to improving joint context and enabling capabilities that enrich our training environment. Adequate funding is essential to maintaining USTRATCOM's ability to train, exercise and operate together.

USSTRATCOM MISSION & PRIORITIES

USSTRATCOM provides an array of global strategic capabilities to the Joint Force through its nine UCP assigned missions: **Strategic Deterrence**; **Space Operations**; **Cyberspace Operations**; **Joint Electronic Warfare**; **Global Strike**; **Missile Defense**; **Intelligence, Surveillance and Reconnaissance**; **Combating Weapons of Mass Destruction**; and **Analysis and Targeting**. These diverse missions are strategic in nature, global in scope, and intertwined with capabilities of the Joint Force, the interagency and the whole of government.

While executing our UCP missions, USSTRATCOM efforts are guided by my five overarching priorities. **My number one priority is to provide a safe, secure and effective nuclear deterrent force** as directed by the 2010 *Nuclear Posture Review* (NPR). It is my responsibility to ensure our nuclear deterrent force remains viable and credible now and as long as nuclear weapons exist.

Second, we will partner with other combatant commands to win today. Future conflicts are not likely to be limited by conventional constraints characteristic of 20th century warfare or by geographic boundaries; thus our planning leverages robust integration with other combatant commands and applies the breadth of USSTRATCOM capabilities to synchronize efforts in pursuit of national objectives. Toward this end, we are shifting from geography-based to adversary-based thinking and are reevaluating our planning assumptions to more accurately reflect the threats, our goals, partner capacity, and both adversary and ally military capabilities.

Third, we must continue to address challenges in space. The National Security Space Strategy identifies space as contested, congested and competitive. The space domain, along with cyberspace, is simultaneously more critical to all U.S. operations yet more vulnerable than ever to hostile actions. Today, the U.S. continues to hold an advantage in space. We must maintain

that advantage as we move deeper into the 21st century and other nations continue to invest heavily in offensive, defensive, and commercial space capabilities. Key to these efforts will be securing assured access to space and developing a robust situational awareness of the space environment across the dimensions of time, space, and spectrum.

Fourth, we must continue to build cyberspace capability and capacity. Cyberspace operations extensively support all of my other mission areas and there are significant negative impacts if that support becomes uncertain. Along with the need to protect U.S. critical infrastructure and intellectual property, information assurance is a critical facet of national power that underpins our ability to identify national security risks and to hold those threats in check. This means we must simultaneously strengthen our internal information security safeguards and protect against a maturing set of external cyber threats.

Finally, geopolitical and fiscal realities demand that we prepare for uncertainty. We need the right information in the right hands at the right time to make correct assessments and decisions. We are critically dependent on the Intelligence Community's (IC) foundational, data-based intelligence on adversary underground facilities, physical vulnerabilities, command and control, military force analysis, defense resources and infrastructure, and WMD facilities. We also rely on the IC's in-depth analysis of adversary national defense strategy doctrine and military leadership. Decision-making will also require predictive analysis to prioritize our activities along with flexible, agile, adaptable thinking and systems. Since predictive analysis of the future will never be error free, we must maintain adequate readiness to address uncertainty. We must align our posture to the threat while acknowledging that the threat itself will continue to evolve. Uncertainty also requires us to conduct a penetrating analysis of our capabilities and resources to clearly identify where we are taking risk and where we cannot accept further risk.

MISSION AREA CAPABILITIES & REQUIREMENTS

Prioritizing resources to meet our goals requires a thoughtful assessment of national priorities in the context of fiscal realities. Today's budget environment remains a concern as we look to sustain and modernize our military forces. We appreciate the passage of the two-year Bipartisan Budget Act of 2013 and the 2014 omnibus appropriations, as they reduce near-term budget uncertainty.

Although these recent actions provide us with some relief, the sequestration-level reductions in FY 2013 have impacted our readiness and have the potential to impact our capabilities in the future. While our Service components realigned limited resources toward strategic missions to preserve our strategic deterrence capabilities in the short term, those same organizations took on significant additional risk in our ability to address long term requirements. Many procurement and research, development, testing and evaluation (RDT&E) investment accounts have experienced delays and we anticipate future programmatic challenges as a result. At this point it is also difficult to fully discern the impact of sequestration in FY 2013 on our people, but the combined effects of a hiring freeze, furlough, and other force reduction measures continue to stress the human element of USSTRATCOM's capabilities.

Nuclear Deterrent Forces

America's nuclear deterrent force provides enduring value to the nation. It has been a constant thread in the geopolitical fabric of an uncertain world, providing a moderating influence on generations of world leaders. Today, our strategic nuclear capabilities—a synthesis of dedicated sensors, assured command and control, the triad of delivery systems, nuclear weapons and their associated infrastructure, and trained ready people—remain foundational to our national security apparatus. As stated in the 2010 NPR, "as long as nuclear weapons exist, the

United States will maintain a safe, secure, and effective nuclear arsenal, both to deter potential adversaries and to assure U.S. allies and other security partners that they can count on America's security commitments." We are working across the Department to implement the President's new guidance for aligning U.S. policies to the 21st century security environment. This includes revising Office of the Secretary of Defense and Joint Staff guidance as well as updating our own plans.

Although our nuclear arsenal is smaller than it has been since the late 1950s, today's nuclear weapon systems remain capable and will serve the U.S. well into their fourth decade. In recent years the percentage of spending on nuclear forces has gradually declined to only 2.5% of total DOD spending in 2013—a figure near historic lows.

Today's nuclear forces remain safe, secure and effective despite operating well beyond their original life expectancies. The nation faces a substantive, multi-decade recapitalization challenge, and we must continue investing resources toward that effort. Our planned investments are significant, but are commensurate with the magnitude of the national resource that is our strategic deterrent. If we do not commit to these investments, we risk degrading the deterrent and stabilizing effect of a strong and capable nuclear force. I fully support planned and future sensor improvements, upgrades for nuclear command, control and communications (NC3) capabilities, strategic delivery system recapitalization efforts, weapon life extension programs, stockpile surveillance activities, and nuclear complex infrastructure modernization. Together these efforts provide the necessary investments to ensure our triad of nuclear forces remains viable and credible.

Sensors. Our Integrated Tactical Warning and Attack Assessment (ITW/AA) network of sensors and processing facilities provides critical early warning and allows us to select the most

suitable course of action in rapidly developing situations. While the Defense Support Program (DSP) is approaching the end of its life, the Space Based Infrared System (SBIRS) program is on track to provide continued on-orbit capability. The survivable and endurable segments of these systems, along with Early Warning Radars, are being recapitalized and are vital to maintaining a credible deterrent. I fully support continued investment in this critical area.

Nuclear Command, Control and Communications. Assured and reliable NC3 is critical to the credibility of our nuclear deterrent. The aging NC3 system continues to meet its intended purpose, but risk to mission success is increasing. Our challenges include operating aging legacy systems and addressing risks associated with today's digital security environment. Many NC3 systems require modernization, but it is not enough to simply build a new version of the old system—rather; we must optimize the current architecture while leveraging new technologies so that our NC3 systems interoperate as the core of a broader, national command and control system. We are working to shift from point-to-point hardwired systems to a networked IP-based national C3 architecture that will balance survivability and endurability against a diverse range of threats, deliver relevant capabilities across the range of interdependent national missions, and ultimately enhance Presidential decision time and space. Specific programs now in work include the Family of Beyond-line-of-sight Terminals (FAB-T), Presidential National Voice Conferencing (PNVC), the Multi-Role Tactical Common Data Link (MR-TCDL), Phoenix Air-to-Ground Communications Network (PAGCN), the E-4B Low Frequency communications upgrade, the B-2 Common Very Low Frequency Receiver communications upgrade, and the E-6B service life extension program.

Nuclear Triad. Per the 2010 NPR, "retaining all three Triad legs will best maintain strategic stability at reasonable cost, while hedging against potential technical problems or

vulnerabilities." The commitment to the triad was reinforced in the U.S. Nuclear Weapons Employment Planning guidance the President issued in June 2013. USSTRATCOM executes strategic deterrence and assurance operations with Intercontinental Ballistic Missiles, Ballistic Missile Submarines, and nuclear capable heavy bombers. Each element of the nuclear triad provides unique and complimentary attributes of strategic deterrence, and the whole is greater than the sum of its parts.

Intercontinental Ballistic Missiles (ICBMs). Our ICBM force promotes deterrence and stability by fielding a responsive and resilient capability that imposes costs and denies benefits to those who would threaten our security. Though fielded in 1970, the Minuteman III ICBM is sustainable through 2030 with smart modernization and recapitalization investments. USSTRATCOM continues to work with the Air Force on initiatives to modernize safety and security capabilities and to address age-related ground support system concerns such as Transporter-Erector vehicles and re-entry system test equipment. The Ground Based Strategic Deterrent Analysis of Alternatives (AoA) is studying a full range of ICBM concepts which will shape our land-based deterrent force well beyond 2030.

Ballistic Missile Submarines (SSBNs). Recapitalizing our sea-based strategic deterrent force is my top modernization priority and I am committed to working closely with the Navy on this program. The Navy's SSBNs and Trident II D5 ballistic missiles constitute the Triad's most survivable leg and the assured response they provide underpins our nuclear deterrent. This stealthy and highly capable force is composed of two major elements, the missile and the delivery system. Both are undergoing needed modernization. With respect to the missile, we are extending the life of the D5 missile to be capable until after 2040. With respect to the submarine that delivers these missiles, the OHIO class submarine has already been extended from 30 to 42

years of service—no further extension is possible and these submarines will start leaving service in 2027. As such, the Ohio Replacement Program (ORP) must stay on schedule. No further delay is possible. Continued and stable funding for the Ohio Replacement SSBN also supports our commitment to the United Kingdom to provide a Common Missile Compartment design and will ensure both their and our new SSBNs achieve operational capability on schedule.

Heavy Bombers. While the nation relies on the long-range conventional strike capability of our heavy bombers, the nuclear capability of B-52 and B-2 bombers continues to provide us with flexibility, visibility and a rapid hedge against technical challenges in other legs of the Triad. Last March, for example, the U.S. carried out training flights of B-52 and B-2 bombers over the Korean Peninsula to assure partners and allies and underscore our security commitment to extended deterrence in the Asia-Pacific region. Maintaining an effective air-delivered standoff capability is vital to meet our strategic and extended deterrence commitments and to effectively conduct global strike operations in anti-access and area-denial (A2AD) environments. Planned sustainment and modernization activities, to include associated NC3, will ensure a credible nuclear bomber capability through 2040.

Looking forward, a new highly survivable penetrating bomber is required to credibly sustain our broad range of deterrence and strike options beyond the lifespan of today's platforms. The Long Range Standoff AoA was completed in 2012 and concluded that a follow-on nuclear cruise missile was necessary to replace the aging Air Launched Cruise Missile (ALCM).

Weapons and Infrastructure. Nuclear weapons and their supporting infrastructure underpin our nuclear triad. All warheads today are on average nearly 30 years old. Surveillance activities are essential to monitoring the health of our nuclear warheads. Life Extension Programs (LEPs) are key to sustaining our nuclear arsenal into the future, mitigating age-related

effects and incorporating improved safety and security features. Our robust science-based Stockpile Stewardship provides us confidence in sustaining our nuclear forces without a return to nuclear testing, which the United States halted in 1992.

The DOD and the Department of Energy (DOE) have worked together to develop a synchronized, multi-decade plan for a modern, safe, secure and effective nuclear stockpile. The Nuclear Weapons Council (NWC) approved what has been referred to as the "3+2" plan—so named because the long term result is three ballistic missile and two air-delivered warheads. This framework sustains a nuclear force that addresses both near term technical needs and future triad capability requirements. The W76-1 LEP is in progress to support the submarine leg of the triad. This is particularly important as the W76-1 represents the majority of our survivable deterrent force. The Air Force and the National Nuclear Security Administration (NNSA) continue to make progress on a full life extension for the B61 gravity bomb that includes both nuclear and non-nuclear components, critical to our strategic capabilities and extended deterrent commitments. Both LEPs are necessary to maintain confidence in the reliability, safety and intrinsic security of our nuclear weapons. Looking to the future, we continue to work with NNSA on the feasibility of an interoperable nuclear package for our ballistic missile warheads and options for sustaining our air-delivered standoff capabilities.

Sustaining and modernizing the nuclear enterprise's infrastructure is crucial to our long term strategy. A new uranium facility at Y-12 in Oak Ridge, Tennessee will address deteriorating conditions in our Manhattan Project era facilities, while our interim plutonium strategy will meet stockpile requirements over the next decade as we explore long term production alternatives. Continued investment in the nuclear enterprise infrastructure is needed to provide critical capabilities that meet our stockpile requirements.

In the wake of recent unfortunate personnel incidents within the ICBM force involving integrity issues, I fully support the Secretary's initiative to assemble key stakeholders within the DOD to fully digest the implications and to seek long-term systemic solutions that will maintain trust and confidence in the nuclear enterprise. This has my utmost attention.

New START Implementation. USSTRATCOM continues to work with the Office of the Secretary of Defense (OSD), the Joint Chiefs of Staff (JCS) and the Services to effectively and efficiently implement the reductions called for in New START. Now more than three years old, New START has continued to contribute to the U.S.' insight into Russia's nuclear forces and has contributed to increased transparency and predictability between our two nations. Since the treaty's entry into force in 2011, the U.S. and Russia have each conducted over 54 inspections and have exchanged over 5,500 New START message notifications. To date, the U.S. has eliminated 39 B-52Gs and 50 Peacekeeper ICBM silos, thus removing them from accountability under New START. The U.S. also made substantial progress toward de-MIRVing MM III ICBMs on alert, thereby reducing the number of warheads in a deployed status. This year, we will finalize our preferred New START force structure and we are on track to achieve New START's limits of 1,550 deployed warheads, 700 deployed delivery systems, and 800 deployed and non-deployed delivery systems by February 2018.

Space Operations

Our national space capabilities provide us with the ability to globally navigate, communicate and observe natural and man-made events in areas where non-space sensors are either not available or not feasible. Space capabilities are also a key component of strategic deterrence. Our space sensors, command and control systems, and space situational awareness

capabilities are critical in supporting both our deployed nuclear forces and our national decision making processes.

As highlighted in the President's 2010 National Space Policy, these capabilities "allow people and governments around the world to see with clarity, communicate with certainty, navigate with accuracy and operate with assurance." Determined adversaries who understand the military and economic advantages provided by space, along with an expanding debris population on orbit, increase the challenges of operating in this critical domain. Space continues to be increasingly congested, contested and competitive. The National Security Space Strategy offers a set of approaches to mitigating those characteristics: partnering with responsible nations, international organizations and commercial firms to promote responsible, peaceful and safe use of space; maximizing the advantages provided by improved space capabilities while reducing vulnerabilities; and preventing, deterring, defeating and operating through attacks on our space capabilities.

Key to all of these efforts is sufficient Space Situational Awareness (SSA)—the data that allows us to understand what is on orbit, where it is, and how it is being used. Our goal is to ensure space remains an open domain for all legitimate users. Sharing SSA information with other nations and commercial firms promotes safe and responsible space operations, reduces the potential for debris-making collisions, builds international confidence in U.S. space systems, fosters U.S. space leadership, and improves our own SSA through knowledge of other owner/operator satellite positional data.

For all its advantages, there is concern that SSA data sharing might aid potential adversaries, therefore we are taking positive steps to ensure that does not occur. In accordance with U.S. law, USSTRATCOM has negotiated SSA Sharing Agreements with 41 commercial

entities and five nations (France, Italy, Japan, Australia, and Canada) and is in the process of negotiating agreements with five additional nations (Germany, Great Britain, Israel, South Korea, and Brazil). Through these sharing agreements, USSTRATCOM assists partners with activities such as launch support; maneuver planning; support for on-orbit anomaly resolution, electromagnetic interference reporting and investigation; support for launch anomalies and de-commissioning activities; and on-orbit conjunction assessments.

USSTRATCOM's Joint Functional Component Command for Space (JFCC-Space), located at Vandenberg Air Force Base in California, leads the efforts to ensure continuous and integrated space operations and routinely track tens of thousands of space objects in orbit around the Earth. This includes over 1,100 active satellites owned and operated by approximately 74 nations and government consortia, plus hundreds of small commercial and academic satellites.

We must sustain judicious and stable investments to preserve the advantages we hold in this dynamic and increasingly complex environment while continuing to seek out innovative and cooperative solutions with allies and partners to ensure the products and services we derive from operating from space remain available, even when threatened by natural events or the actions of a determined adversary. These include both active and passive protection measures for individual systems and constellations and a critical examination of the architectural path we will follow to ensure resilience and affordability in space. We are exploring options such as disaggregation as a method to achieve affordable resilience but additional analysis is necessary in this area.

Cyberspace Operations

Today, we conduct our UCP assigned cyberspace missions through our assigned sub-unified command, US Cyber Command (USCYBERCOM) located at Ft. Meade, Maryland. I have delegated the authority to USCYBERCOM to conduct the day-to-day business of directing

DOD information network operations and defense, planning against cyber threats, coordinating with other combatant commands and appropriate U.S. government agencies, providing military representation for cyber matters, planning and executing operational preparation of the environment, and executing cyber operations as directed. USSTRATCOM retains authority for oversight of advocacy and theater security cooperation.

This alignment allows USSTRATCOM to manage the integration of all our capabilities to deter or defeat attacks in multiple scenarios while taking full account of the interdependencies and interactions among combatant commands and across the air, sea, land, and space domains, and in cyberspace—all tied together through the electromagnetic spectrum.

USSTRATCOM, through USCYBERCOM, is working with Joint Staff and the DOD Chief Information Officer (DOD CIO) to implement the Joint Information Environment framework (JIE). The JIE provides a foundational framework to enable improvements in our ability to see and defend the DoD Information Network. Furthermore, the JIE framework is intended to enable timely and secure information sharing in the joint environment, improving warfighters ability to access critical data and information for mission command. Alignment of the JIE with the equivalent IC information technology enterprise is a key component required to achieve this goal.

Our primary obstacles to cyberspace operations within DOD are issues of capacity and capability. None of these activities can occur without a right-sized and well-trained cadre of cyber professionals. The Cyber Mission Force (CMF) construct will address the significant challenges of recruiting, training, and retaining the people, facilities and equipment necessary to generate the human capital required for successful cyberspace operations. Our plans call for the creation of 133 cyber mission teams manned by over 6,000 highly trained personnel by the end

of FY16. To date, 17 of those teams are fielded and engaged in a variety of missions. The majority of these teams will support the combatant commands with the remainder supporting national missions. Budget stability is the key to achieving this vision, as every training day we lose to fiscal constraints will cause further delays in fielding the CMF.

Missile Defense

I believe that effective missile defense is an essential element of the U.S. commitment to strengthen strategic and regional deterrence against states of concern—continued investments in this area are essential to national defense. Today, 30 operational Ground Based Interceptors (GBIs) protect the U.S. against a limited ICBM attack from potential regional threats such as North Korea. In March of 2013, Secretary Hagel announced the decision to add 14 GBIs in Alaska and a second Army/Navy Transportable Radar Surveillance-2 (AN/TPY-2) radar in Japan, study a potential third CONUS GBI site, and restructure the SM-3 IIB interceptor into an advanced kill vehicle technology program. These decisions will hedge against a growing North Korean threat, add additional sensor capability to improve coverage, introduce needed Exo-atmosphere Kill Vehicle (EKV) improvements, and will facilitate quickly adding a third CONUS GBI site if needed. We continue to examine new threats and consider alternative ways and means for a future architecture to improve sensors and discrimination for greater Ballistic Missile Defense System (BMDS) effectiveness.

USSTRATCOM's Joint Functional Component Command for Integrated Missile Defense (JFCC-IMD) is located in Colorado Springs, Colorado and continues to conduct a variety of activities aimed at maturing our missile defense capabilities. First, they are working to operationalize developmental missile defense capabilities in coordination with other combatant commands and the Missile Defense Agency (MDA). These efforts serve to integrate sensors across mission domains and geographical areas, synchronize and manage the availability of

missile defense assets, and hedge against the possibility of threats developing faster than originally anticipated. Second, they are working to develop and implement joint training to enable integration and synchronization with other combatant commands, and host and orchestrate international missile defense wargaming scenarios. These efforts identify and recommend sourcing solutions to ensure appropriate forces are employed; synchronize global missile defense planning at all levels to ensure unity of effort across our geographically distributed network of sensors and shooters, across multiple organizations, and across multiple domains; and collaborate with key allies and partners. Finally, they are integrating warfighters into missile defense testing and evaluation.

The European Phased Adapted Approach (EPAA) protecting our NATO allies is on schedule with Phase I becoming operational in Dec 2011 using a forward based radar and Aegis Ballistic Missile Defense (BMD) ships. Phase II is on track for completion in 2015 and will add an Aegis Ashore system in Romania, SM-3 IB interceptors, and additional Aegis BMD ships. Phase III planned for 2018 will add an Aegis Ashore in Poland and a more capable SM-3 IIA interceptor both on land and at sea. Steady progress was made in 2013 as we continued development and testing of Aegis BMD software, construction of Aegis Ashore test and operational facilities, SM-3 Block IIA system design, and successful SM-3 operational and developmental flight tests.

The Cobra Dane radar located at Eareckson AFS, Alaska is critical to homeland defense and must be sustained. This unique asset provides unmatched coverage against long range threats from northeast Asia as well as helping to catalogue many thousands of space objects. Cobra Dane is an aging system and requires continued investment. Additionally, the deployment

of an operational THAAD missile defense system to Guam provides vital protection against North Korean provocations toward one of our key Territories.

Global Strike

USSTRATCOM's Joint Functional Component Command for Global Strike (JFCC-GS) operates from Offutt AFB, Nebraska with headquarters at Barksdale AFB, Louisiana. JFCC-GS provides a unique ability to command and control our global strike capabilities and build plans that rapidly integrate into theater operations. This includes integration of combat capability including those associated with kinetic and non-kinetic effects. The following key capabilities are integral to supporting my Global Strike mission.

USSTRATCOM's Joint Warfare and Analysis Center (JWAC) in Dahlgren, Virginia enhances our Strategic Deterrence and Global Strike missions by providing unique and valuable insight into selected adversary networks. JWAC's ability to solve complex challenges for our nation's warfighters—using a combination of social and physical science techniques and engineering expertise—is invaluable to protecting the nation and helping the Joint Force accomplish its missions.

Our Mission Planning and Analysis System (MPAS) is the nation's only comprehensive planning system for developing nuclear options. MPAS supports my responsibilities for Strategic Deterrence and Global Strike through the development of nuclear options for the President, as well as holding time-sensitive targets at risk through crisis action planning. Continued modernization of MPAS is essential to our ability to conduct global strike operations.

Conventional prompt strike (CPS) capability offers the opportunity to rapidly engage high-value targets without resorting to nuclear options. CPS could provide precision and responsiveness in A2AD environments while simultaneously minimizing unintended military,

political, environmental, economic or cultural consequences. I support continuing research and development of these important capabilities.

Combating Weapons of Mass Destruction (CWMD)

A WMD-armed terrorist is one of the greatest potential threats we face today, and no region of the world is immune from potential chemical, biological, radiological or nuclear risks. USSTRATCOM is DOD's global synchronizer for CWMD planning efforts, leveraging the expertise resident in our Center for Combating Weapons of Mass Destruction (SCC-WMD) and our partners at the Defense Threat Reduction Agency (DTRA)—both located at Ft. Belvoir, Virginia. Together, our organizations conduct real-world and exercise CWMD activities with the other combatant commands to identify, prioritize, and mitigate WMD risks posed by proliferation of WMD technology and expertise to nation states and non-state actors. We have been successful so far, but given the magnitude of the WMD threat, we can ill afford to short-change these efforts.

The Standing Joint Force Headquarters for Elimination (SJFHQ-E) was certified for initial operating capability in September 2012. SJFHQ-E provides a full time, trained joint command and control element that can quickly integrate into strategic- to operational-level headquarters to provide WMD elimination planning, intelligence, and operational expertise for a Joint Force Commander. Additionally, the SJFHQ-E recently completed its relocation from Aberdeen Proving Grounds, MD to Ft Belvoir, VA to better leverage DTRA's expertise and manpower.

USSTRATCOM has and continues to support United States Central Command (USCENTCOM), United States European Command (USEUCOM) and DTRA as part of the international effort to eliminate Syria's chemical weapons program. Our personnel are providing

direct support to USEUCOM in preparation for the removal and destruction of chemical materials from Syria and will remain engaged until elimination of Syria's program is complete.

Intelligence, Surveillance, & Reconnaissance (ISR)

The demand for ISR will always outpace our ability to fully satisfy all requirements. At the same time, we are focused on the goal of reducing the "cost of doing business" as articulated in *Sustaining U. S. Global Leadership Priorities for 21st Century Defense.* Located at Bolling AFB, Maryland, USSTRATCOM's Joint Functional Component Command for ISR (JFCC-ISR) is working with our headquarters, the Joint Staff, the Services, the combatant commands and the IC to improve the management of the DOD's existing ISR capabilities. I fully support this initiative which focuses on maximizing effectiveness of the capabilities we have, while minimizing duplication of effort between DOD and the IC.

Joint Electronic Warfare

Given the importance and need of Joint Electronic Warfare, USSTRATCOM, in collaboration with the Joint Staff and the Office of the Secretary of Defense, continues to drive the development of comprehensive Joint Electromagnetic Spectrum Operations (JEMSO) policy and doctrine that consolidates the activities of Electronic Warfare (EW) and Spectrum Management. The National Military Strategic Plan for EW (NMSP-EW) was approved in late 2013, providing a framework for EW operations, articulating threats and vulnerabilities, and clarifying risks and strategic imperatives for electromagnetic spectrum (EMS) control. The joint architecture plan for Electromagnetic Battle Management (EMBM) is currently under development—the preliminary work done so far will identify applicable architectures in order to better refine requirements.

USSTRATCOM assesses systems to determine vulnerabilities to jamming, orchestrates events to evaluate the ability to detect jamming and operate in such an environment, coordinates

with the combatant commands to determine impacts to plan execution, and sponsors initiatives to combat jamming and generate requirements. These assessments and initiatives greatly improve the DOD's understanding and mitigation of JEMSO capability gaps and vulnerabilities.

We seek to use the EMS more efficiently by investing in time and technology sharing and fully investigating spectrum re-use opportunities. There are a number of ongoing spectrum reallocation efforts with potential adverse impacts to DOD operations. We will continue to work closely with DOD CIO, Joint Staff, and National Telecommunications and Information Administration (NTIA) to ensure warfighter requirements are adequately considered prior to any decision.

Command and Control (C2) Facility

In 2012, the U.S. Army Corps of Engineers (USACE) broke ground on a C2 Facility for USSTRATCOM. This project will replace a C2 Facility that is over 57 years old, plagued with numerous heating, cooling, and power infrastructure deficiencies and will provide the necessary information technology infrastructure to support USSTRATCOM in the digital age. The construction team is working hard to keep the project on schedule, to ensure that we are optimizing resources, and to create an infrastructure that has a lower cost of ownership than our current facility. When complete, the new C2 Facility will play an effective and integral part of our strategic deterrent as well as USSTRATCOM's other assigned missions for decades to come. I appreciate the steadfast support that Congress continues to provide for this effort.

OUR PEOPLE

People remain our most precious resource and deserve our most robust support. The critical bonds of trust, teamwork and professionalism unite the USSTRATCOM family. Last year we created a Resilience Coordination Office, an effort that has been noted as a potential

benchmark program for the DOD. Resilience coordinators provide training, information, resources and other tools to present healthy behavior options in response to life stressors. Sexual assault, workplace violence, breaches of integrity, alcohol abuse and associated behaviors have my strongest personal condemnation, and my entire staff understands my expectation to report and denounce inappropriate behavior whenever and wherever it occurs.

My travels to a number of USSTRATCOM and partner locations since I took command in November 2013 confirm my belief that we have an outstanding team in place across all our mission areas. I am proud to serve alongside the men and women of USSTRATCOM and have the utmost respect for their professionalism, dedication to our missions and sustained operational excellence even through difficult times. These great Americans will do all they can for their nation, but are rightly concerned about their futures given last year's furloughs and planned manpower reductions over the next several years. These reductions are not inconsequential—we believe we can achieve the Department's goals but not without a commensurate loss of organizational agility and responsiveness.

CONCLUSION

We are experiencing dynamic changes within the DOD as we transition toward a different force posture and a reduced defense budget. In spite of this environment, our UCP missions remain unchanged as we partner with our fellow combatant commands to deter adversaries, assure allies, protect critical infrastructure, preserve freedom of movement, and respond to crises.

In today's uncertain times, I am proud to lead such a focused, innovative and professional group dedicated to delivering critical warfighting capabilities to the nation. We are building our future on a strong and successful past, and your support, together with the hard work of the

outstanding men and women of the United States Strategic Command, will ensure that we remain ready, agile and effective in deterring strategic attack, assuring our allies, and defeating current and future threats.

STATEMENT OF

GENERAL KEITH B. ALEXANDER

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

SENATE COMMITTEE ON ARMED SERVICES

27 FEBRUARY 2014

Chairman Levin, Senator Inhofe, distinguished members of the Committee, thank you for the opportunity to speak to you today on behalf of the men and women of the United States Cyber Command (USCYBERCOM). As you know, this will be the last time I have the honor of talking about our Command's fine and dedicated Service members and civilian personnel before this Committee. It always gives me great pleasure to tell you about their accomplishments, and I am both grateful for and humbled by the opportunity I have been given to lead them in the groundbreaking work they have done in defense of our nation.

USCYBERCOM is a subunified command of U.S. Strategic Command in Omaha, Nebraska though based at Fort Meade, Maryland. It has approximately 1,100 people (military, civilians, and contractors) assigned with a Congressionally-appropriated budget for Fiscal Year 2014 of approximately $562 million in Operations and Maintenance (O&M), Research, Development, Test and Evaluation (RDT&E), and military construction (MILCON). USCYBERCOM also has key Service cyber components: Army Cyber Command/Second Army, Marine Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, and Air Forces Cyber/24th Air Force. Together they are responsible for directing the defense ensuring the operation of the Department of Defense's information networks, and helping to ensure freedom of action for the United States military and its allies—and, when directed, for defending the nation against attacks in cyberspace. On a daily basis, they are keeping U.S. military networks secure, supporting the protection of our nation's critical infrastructure from cyber attacks, assisting our combatant commanders, and working with other U.S. Government agencies tasked with defending our nation's interests in cyberspace.

USCYBERCOM resides with some key mission partners. Foremost is the National Security Agency and its affiliated Central Security Service (NSA/CSS). The President's recent decision to maintain the "dual-hat" arrangement under which the Commander of USCYBERCOM also serves as the Director of NSA/Chief, CSS means the co-location of USCYBERCOM and NSA/CSS will continue to benefit our nation. NSA/CSS has unparalleled capabilities for detecting threats in foreign cyberspace, attributing cyber actions and malware, and guarding national security information systems. At USCYBERCOM, we understand that re-creating a mirror capability for the military would not make operational or fiscal sense. The best, and only, way to meet our nation's needs today, to bring the military cyber force to life, and to exercise good stewardship of our nation's resources is to leverage the capabilities (both human and technological) that have been painstakingly built up at Fort Meade. Our nation has neither the resources nor the time to redevelop from scratch the capability that we gain now by working with our co-located NSA partners. Let me also

mention our other key mission partner and neighbor at Fort Meade, the Defense Information Systems Agency (DISA). DISA is vital to the communications and the efficiency of the entire Department, and its people operate in conjunction with us at USCYBERCOM on a constant basis. We all work in conjunction with the extensive efforts of several federal government mission partners, particularly the Department of Homeland Security (DHS), the Department of Justice and its Federal Bureau of Investigation (FBI), and other departments and agencies. We also work with private industry and allies in the overall mission of securing our networks, identifying threat actors and intentions, building resiliency for federal and critical infrastructure systems, and supporting law enforcement in investigating the theft and manipulation of data.

Allow me to review the highlights since our last posture hearing before the Committee a year ago. The main point I want to leave with you is that we in US Cyber Command, with the Services and other partners, are doing something that our military has never done before. We are putting in place foundational systems and processes for organizing, training, equipping, and operating our military cyber capabilities to meet cyber threats. USCYBERCOM and the Services are building a world class, professional, and highly capable force in readiness to conduct full spectrum cyberspace operations. Seventeen out of one hundred thirty-three projected teams have achieved full or "initial" operational capability, and those teams are already engaged in operations and accomplishing high-value missions. The Cyber Mission Force is no longer an idea on a set of briefing slides; its personnel are flesh-and-blood Soldiers, Marines, Sailors, Airmen, and Coast Guardsmen, arranged in military units that are on point in cyberspace right now. We are transforming potential capability into a reliable source of options for our decision makers to employ in defending our nation. Future progress in doing so, of course, will depend on our ability to field sufficient trained, certified, and ready forces with the right tools and networks to fulfill the growing cyber requirements of national leaders and joint military commanders. That is where we need your continued support.

The Threat Picture

The Department of Defense along with the Department of Homeland Security, the Department of Justice, and the Federal Bureau of Investigation have primary responsibilities to defend the United States in cyberspace and to operate in a global and rapidly evolving field. Our economy, society, government, and military all depend on assured security and reliability in this man-made space, not only for communications and data storage, but also for the vital synchronization of actions and functions that underpins our defenses and our very way of life. USCYBERCOM concentrates its efforts on defending

military networks and watching those actors who possess the capability to harm our nation's interests in cyberspace or who intend to prepare cyber means that could inflict harm on us in other ways.

Unfortunately, the roster of actors who concern us is long, as is the sophistication of the ways they can affect our operations and security. We have described some of these in previous hearings, and I know the Director of National Intelligence recently opened his annual World Wide Threat Assessment for Congress with several pages on cyber threats, so I'll be brief here.

I can summarize what is happening by saying that the level and variety of challenges to our nation's security in cyberspace differs somewhat from what we saw and expected when I arrived at Fort Meade in 2005. At that time many people, in my opinion, regarded cyber operations as the virtual equivalents of either nuclear exchanges or commando raids. What we did not wholly envision were the sort of cyber campaigns we have seen in recent years. Intruders today seek persistent presences on military, government, and private networks (for the purposes of exploitation and disruption). These intruders have to be located, blocked, and extracted over days, weeks, or even months. Our notion of cyber forces in 2005 did not expect this continuous, persistent engagement, and we have since learned the extent of the resources required to wage such campaigns, the planning and intelligence that are essential to their success, and the degree of collaboration and synchronization required across the government and with our allies and international partners. Through concerted efforts, and with a bit of luck, we are creating capabilities that are agile enough to adapt to these uses and others, and I am convinced we have found a force model that will give useful service as we continue to learn and improvise for years to come.

We have some key capability gaps in dealing with these increasingly capable threats. Cyberspace is a medium that seems more hospitable to attackers than defenders, and compared to what real and potential adversaries can do to harm us, our legacy information architecture and some of our weapons systems are not as "cyber robust" as they need to be. Our legacy forces lack the training and the readiness to confront advanced threats in cyberspace. Our commanders do not always know when they are accepting risk from cyber vulnerabilities, and cannot gain reliable situational awareness, neither globally nor in US military systems. In addition, the authorities for those commanders to act have been diffused across our military and the US government, and the operating concepts by which they could act are somewhat undefined and not wholly realistic. Further our communications systems are vulnerable to attacks. We need to rapidly pursue a defense in depth as we envision with the fielding of the Joint Information Environment.

These gaps have left us at risk across all the USCYBERCOM mission areas that I described above.

USCYBERCOM's Priorities

USCYBERCOM is addressing these gaps by building cyber capabilities to be employed by senior decisionmakers and Combatant Commanders. In accordance with the Department of Defense's *Strategy for Operating in Cyberspace*, the people of USCYBERCOM (with their NSA/CSS counterparts) are together assisting the Department in building:

1) A defensible architecture;
2) Trained and ready cyber forces;
3) Global situational awareness and a common operating picture;
4) Authorities that enable action;
5) Concepts for operating in cyberspace;

We are finding that our progress in each of these five areas benefits our efforts in the rest. We are also finding the converse—that a lack of momentum in one area can result in slower progress in others. I shall discuss each of these priorities in turn.

***Defensible Architecture*:** The Department of Defense (DoD) owns seven million networked devices and thousands of enclaves. USCYBERCOM, with its Service cyber components, NSA/CSS, and DISA, monitors the functioning of DoD networks, providing the situational awareness to enable dynamic defenses. Unfortunately, DoD's current architecture in its present state is not fully defensible. That is why the Department is building the DoD Joint Information Environment (JIE), comprising a shared infrastructure, enterprise services, and a single security architecture to improve mission effectiveness, increase security, and realize IT efficiencies. The JIE, together with the cyber protection teams that I shall describe in a moment, will give our leaders the ability to truly defend our data and systems. Senior officers from USCYBERCOM and DISA serve on JIE councils and working groups, and together with leaders from the office of the DoD's Chief Information Officer, Joint Staff J6, and other agencies, are guiding the JIE's implementation (with NSA's support as Security Adviser). JIE has been one of my highest priorities as Commander, USCYBERCOM and Director, NSA/CSS.

***Trained and Ready Forces*:** Over the last year we have made great progress in building out our joint cyber force. When I spoke to you in March 2013 we had just begun to establish the Cyber Mission Forces in the Services to present to USCYBERCOM. This force has three main aspects: 1) Cyber National Mission Teams to help defend the nation against a strategic cyber

attack on our critical infrastructure and key resources; 2) Cyber Combat Mission Teams under the direction of the regional and functional Combatant Commanders to support their objectives; and 3) Cyber Protection Teams to help defend DoD information environment and our key military cyber terrain. On January 17, 2014 we officially activated the Cyber National Mission Force – the U.S. military's first joint tactical command with a dedicated mission focused on cyberspace operations. We have plans to create 133 cyber mission teams by the end of FY 2016, with the majority supporting the Combatant Commands and the remainder going to USCYBERCOM to support national missions. The teams will work together with regional and functional commanders according to a command and control construct that we are actively helping to forge and field.

The training for this force is happening now on two levels. At the team level, each cyber mission team must be trained to adhere to strict joint operating standards. This rigorous and deliberate training process is essential; it ensures the teams can be on-line without jeopardizing vital military, diplomatic, or intelligence interests. Such standards are also crucial to assuring intelligence oversight and to securing the trust of the American public that military operations in cyberspace do not infringe on the privacy and civil liberties of U.S. persons. Our training system is in the midst of certifying thousands of our people to high and joint military-wide standards.

At the individual level, we are using every element of capacity in our Service schools and in NSA to instruct members of the Cyber Mission Force teams. We have compiled a training and readiness manual, a "summer school" for cyber staff officers, and are shaping professional military education to enhance the cyber savvy of the force. To save time and space, furthermore, we have established equivalency standards to give individuals credit for training they have already taken in their Services and at NSA, with a board to adjudicate how much credit to confer for each course. Finally, we have established Job Qualification Records for team work roles to provide joint standards, further reinforcing common baselines of knowledge, skills and abilities across Service-component teams.

As our training system geared up to meet our need for trained operators and certified teams, sequestration-level reductions and furloughs last year seriously impeded our momentum. The uncertain budget situation complicated our training efforts; indeed, we had to send people home in the middle of our first-ever command and staff course last summer. Moreover, every day of training lost had cascading effects for the overall force development schedule, delaying classes, then courses, and then team certifications, to the point we are about six months behind where we had planned to be in training our teams. We are only now catching up to where we should have been months ago in building the Cyber Mission Force.

Increased Operational Awareness: Enhanced intelligence and situational awareness in our networks help us know what is happening in cyberspace. Our goal is to build a common operating picture, not only for the cyber activities of organizations based at Fort Meade but also across the U.S. government. We are moving toward this objective, for instance by coordinating the activities of the USCYBERCOM and NSA operations centers. Achieving it should let all who secure and defend our networks synchronize their activities, as well as see how adversarial and defensive actions can affect one another, which in turn enhances the efforts of planners and the predictability of the effects they seek to attain.

***Capacity to Take Action*:** The last year saw increased collaboration between defenders and operators across the US government and with private and international partners. USCYBERCOM played important roles in several areas. USCYBERCOM, for instance, has been integrated in the government-wide processes for National Event responses. This regularly exercised capability will help ensure that a cyber incident of national significance can elicit a fast and effective response at the right decisionmaking level, to include pre-designated authorities and self-defense actions where necessary and appropriate. In addition, USCYBERCOM participated in whole-of-government actions with partners like the Departments of State, Justice, and Homeland Security in working against nation-state sponsored cyber exploitation and distributed denial-of-service attacks against American companies. Finally, we already benefit from sharing information on cyber threats with the services and agencies of key partners and allies, and are hopeful that cybersecurity legislation will one day make it easier for the U.S. Government and the private sector to share threat data in line with what the Administration has previously requested.

***Operating Concepts*:** To oversee and direct the nation's cyber forces, as previously mentioned, we have established a National Mission Force Headquarters in USCYBERCOM at Fort Meade. This functions in parallel with analogous headquarters units (the four Joint Force Headquarters) for the Service cyber components, which themselves work with the NSA/CSS regional operating centers in Georgia, Texas, and Hawaii.

We can report some good news with respect to the realism of our cyber exercises, which put these operating concepts to the test. USCYBERCOM regularly participates in more than twenty Tier 1 Combatant Command, coalition, and inter-agency exercises. We also run a Cyber Wargame that looks five years into the future and includes industry and academic experts. USCYBERCOM's flagship exercises, CYBER FLAG and CYBER GUARD, are much more sophisticated now and are coupled directly with Joint Doctrine and the Force Model. CYBER FLAG, held each fall at Nellis Air Force Base in

Nevada, includes all the Service cyber components as well as inter-agency and international partners. CYBER FLAG 14 in November 2013 assembled more than 800 participants, included conventional maneuvers and kinetic fires in conjunction with cyber operations, and featured a much more realistic and aggressive adversary in its expanded virtual battlespace. In the past we were tentative about letting the cyber "red teams" loose, for fear they would impair expensive training opportunities for conventional arms. In our recent CYBER FLAG iteration last fall, we figuratively took the gloves off. Our defense consequently got its collective nose bloodied, but the defenders to their credit fought back and prevailed in chasing a determined foe out of our systems. For its part, CYBER GUARD is a whole-of-government event exercising state- and national-level responses to adversary actions against critical infrastructure in a virtual environment. It brings together DHS, FBI, USCYBERCOM, state government officials, Information Sharing and Analysis Centers, and private industry participants at the tactical level to promote shared awareness and coordination to mitigate and recover from an attack while assessing potential federal cyber responses. Finally, we are also building and deploying tools of direct use to "conventional" commanders in kinetic operations, some of which were most recently utilized in the latest Red Flag exercise run to keep our pilots at the highest degree of proficiency.

Where Are We Going?

Let me share with you my vision for what we at USCYBERCOM are building toward. We all know the US military is a force in transition. We are shifting away from legacy weapons, concepts, and missions, and seeking to focus—in a constrained resource environment—on being ready for challenges from old and new technologies, tensions, and adversaries. We have to fulfill traditional-style missions at the same time that we prepare for emerging ones, with new tools, doctrines, and expectations, both at home and abroad. We are grateful to Congress for lessening the threat of wholesale budget cuts called for by the Budget control Act. That makes it easier for the Department of Defense to maintain its determination to shield our cyberspace capabilities from the resource reductions falling on other areas of the total force. It is fair, and indeed essential, for you to ask how we are utilizing such resources while others are cutting back.

Our answer is that the trained and certified teams of our Cyber Mission Force are already improving our defenses and expanding the operational options for national decision makers, the Department's leadership, and joint force commanders. We are building this force and aligning the missions of the teams with intelligence capabilities and military requirements. Our cyber mission teams will bring even more capability to the "joint fight" and to whole-of-government and international efforts:

- USCYBERCOM is working with the Joint Staff and the combatant commands to capture their cyber requirements and to implement and refine interim guidance on the command and control of cyber forces "in-theater," ensuring our cyber forces provide direct and effective support to commanders' missions while also helping USCYBERCOM in its national-level missions. In addition, we are integrating our efforts and plans with component command operational plans, and we want to ensure that this collaboration continues at all the Commands.

- Our new operating concept to enhance military cyber capabilities is helping to foster a whole-of-government approach to counter our nation's cyber adversaries. Indeed, USCYBERCOM planners, operators, and experts are prized for their ability to bring partners together to conceptualize and execute operations like those that had significant effects over the last year in deterring and denying our adversaries' cyber designs.

Here is my greatest concern as I work to prepare my successor and move toward retirement. Despite our progress at USCYBERCOM, I worry that we might not be ready in time. Threats to our nation in cyberspace are growing. We are working to ensure that we would see any preparations for a devastating cyber attack on our critical infrastructure or economic system, but we also know that warning is never assured and often not timely enough for effective preventive actions. Should an attack get through, or if a provocation were to escalate by accident into a major cyber incident, we at USCYBERCOM expect to be called upon to defend the nation. We plan and train for this every day. My Joint Operations Center team routinely conducts and practices its Emergency Action Procedures to defend the nation through inter-agency emergency cyber procedures. During these conferences, which we have exercised with the participation up to the level of the Deputy Secretary of Defense, we work with our interagency partners to determine if a Cyber Event, Threat or Attack has occurred or will occur through cyberspace against the United States. As Commander, USCYBERCOM, I make an assessment of the likelihood of an attack and recommendations to take, if applicable. We utilize this process in conjunction with the National Military Command Center (NMCC) to determine when and if the conference should transition to a National Event or Threat Conference.

We understand that security is one of the greatest protections for civil liberties, and that liberty can suffer when governments hastily adapt measures after attacks. At USCYBERCOM we do our work in full support and defense of the civil liberties and privacy of Americans. We do not see a tradeoff between security and liberty; we promote both simultaneously, because each enhances

the other. Personnel at USCYBERCOM take this responsibility very seriously. The tools, authorities, and culture of compliance at NSA/CSS give us the ability and the confidence to achieve operational success against some of the toughest national security targets while acting in a manner consistent with civil liberties and rights to privacy. That said, unless Congress moves to enact cybersecurity legislation to enable the private sector to share with the US Government the anomalous cyber threat activity detected on its networks on a real-time basis, we will remain handicapped in our ability to assist the private sector or defend the nation in the event of a real cyber attack. I urge you to consider the now daily reports of hostile cyber activity against our nation's networks and appreciate the very real threat they pose to our nation's economic and national security as well as our citizen's personal information. I am concerned that this appreciation has been lost over the last several months, as has the understanding that—when performed with appropriate safeguards—cyber threat information sharing actually enhances the privacy and civil liberties as well as the security of our citizens.

Conclusion

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to speak, and for all the help that you and this Committee have provided USCYBERCOM over the years. It has been my honor to work in partnership with you for these past 39+ years to build our nation's defenses. Never before has our nation assembled the talent, resources, and authorities that we have now started building into a cyber force. I am excited about the work we have done and the possibilities before us. This is changing our nation's capabilities, and making us stronger and better able to defend ourselves across the board, and not merely in cyberspace. We can all be proud of what our efforts have accomplished in building USCYBERCOM and positioning its men and women, and my successor, for continued progress and success.