SENATE COMMITTEE ON ARMED SERVICES

STATEMENT OF

GENERAL C. R. KEHLER

COMMANDER

UNITED STATES STRATEGIC COMMAND

BEFORE THE

SENATE COMMITTEE ON ARMED SERVICES

27 MARCH 2012

SENATE COMMITTEE ON ARMED SERVICES

Chairman Levin, Senator McCain, and distinguished members of the committee, thank you for the opportunity to testify today. I'm very pleased to be here alongside General Keith Alexander, Commander of U.S. Cyber Command—an essential component of U.S. Strategic Command's (USSTRATCOM) global capabilities.

Since I assumed command a little more than a year ago, we have been challenged by new fiscal constraints at home and complex national security events abroad. I am very proud of how our men and women in uniform and Defense civilians are meeting these financial and operational challenges with professionalism, dedication, and a keen mission focus. I know our team members very much appreciate your support, and I look forward to working with you as we maintain the world's finest military, avoid a hollow force, and make strategy-based capability decisions, all the while keeping faith with our all-volunteer force.

***Introduction.*** Today, I am pleased to report to you that America's Strategic Command is strong, resilient, and ready. At USSTRATCOM, we continue to improve our capabilities and synchronize our multiple mission responsibilities—individually and with our partners in the other Combatant Commands (CCMDs)—to deter strategic attacks, to enhance the combat capability of the joint force, and to assure access and use of the critical domains of space and cyberspace. I look forward to discussing the global strategic environment, the new Defense Strategic Guidance, and how USSTRATCOM's strategic deterrence and assurance efforts support the *National Security Strategy*.

| Commander USSTRATCOM Priorities |
| --- |
| • Deter nuclear attack with a safe, secure, and effective nuclear deterrent force. |
| • Partner with the other combatant commands to win today |
| • Respond to the new challenges in space |
| • Build cyberspace capability and capacity |
| • Prepare for uncertainty |

**STRATEGIC CONTEXT**

Without question, we face a very challenging global security environment. The coming years are likely to be characterized by constant change, enormous complexity, and profound uncertainty. Since my last appearance before the committee, we have witnessed our fair share of change. The Budget Control Act of 2011 realigned national fiscal priorities. U.S. forces withdrew from Iraq, and they partnered with our allies to support the Libyan people. The Arab Spring brought dramatic change to an unsettled region, and tensions grew inside Syria and between Iran and the world. In North Korea, Kim Jong Il's death made way for a new generation in power. And, violent extremists suffered several setbacks—most notably Osama bin Laden's death.

Some of these events were positive; some were not. For some, the outcome remains uncertain. In a few cases we were surprised and, looking forward, surprise is one of the greatest dangers we will face. Indeed, violent extremism, popular revolutions, persistent conflict, financial stress, competition for natural resources, and the transition and redistribution of power among global actors will continue to bring uncertainty to our national security landscape.

***Hybrid Conflict.*** Conflict remains a fundamentally human enterprise conducted for political purposes. Yet, technology and ideology are pushing its means and methods in new and evolutionary directions at an ever-increasing pace. At USSTRATCOM, we believe we can glimpse the future of conflict if we look carefully today, so that we can prepare.

First, conflict will encompass all domains—including air, sea, land, space, and cyberspace—all tied together through the electromagnetic spectrum. Second, it will cross traditional geographic boundaries—particularly with the emergence of new cyber weapons, the increased use of space, and the proliferation of familiar weapons like ballistic missiles. Third, it

will involve multiple participants. A wider range of actors has access to advanced capabilities with lower entry costs, seeking to challenge us from the shadows. Finally, conflict will be hybrid—not neatly categorized as "regular" or "irregular" warfare. More actors, leveraging combinations of capabilities, strategies, and tactics—potentially including weapons of mass destruction (WMD)—will seek to achieve their goals by denying or disrupting our nation's ability to project power and maintain global awareness across all domains.

These are sobering challenges. Hybrid, technologically advanced, and cross-domain threats can reach our doorstep in seconds, threatening vital capabilities and critical infrastructure. The same networks that enable global commerce, navigation, and communication also present tremendous potential for disruption. In particular, cyber tools combined with phenomenal increases in computing power may have surpassed the threat posed by more traditional means of espionage, presenting particularly problematic economic and national security challenges.

The time honored military concepts surrounding speed and distance have also changed, increasing the speed at which initiative can shift, compressing our decision space, and stressing our strategies, plans, operations, and command relationships. Centuries ago, it could take months to influence an adversary by moving an army. However, navies, then airpower, and now space and cyberspace capabilities dramatically compressed the time and distance required to create effects. Adversaries today need not occupy any territory to create disruptive and potentially decisive strategic effects across domain and geographic boundaries. We should not expect adversaries to leave our homeland completely undisturbed while we operate globally.

***New Strategic Approach.*** In such a complex and profoundly uncertain world, sustaining the strategic stability that enables security at home, global commerce for our nation, and freedom of action within the global commons requires great resilience and deep integration. The threats

we face are not divisible by geography or domain. We must meet them with a similarly indivisible joint force—the strength of which lies not in its parts, but in their sum.

Our challenges demand strategic thinking, unity of action, joint interdependence, commander focus, flexibility, decentralized execution, and innovation. They also require a robust, strategic imagination that allows us to anticipate the unexpected and to react to surprise in stride when—not if—it occurs. As a result, at USSTRATCOM we are emphasizing that every plan and operation must be well integrated with other combatant commands. We must work together, across other CCMDs and interagency partners, to shape the environment away from conflict, to assure our allies, to expand our leaders' decision space, and to protect our nation's global access and freedom of action.

As the U.S. transitions from a decade of conflict abroad and acts to sustain its leadership in the world, we are guided by a new strategic approach entitled *Priorities for 21st Century Defense*. We understand that we will face the future with a joint force that is smaller, but also more agile, flexible, ready, and technologically advanced. We will have a global presence, emphasizing the Asia Pacific region and the Middle East, while preserving key commitments elsewhere and our ability to conduct primary missions to protect our core national interests.

The new defense strategic guidance establishes priorities and delineates ten primary missions of the U.S. Armed Forces—most of which have particular relevance to USSTRATCOM. For **Counterterrorism and Irregular Warfare**, USSTRATCOM provides space, ISR, precision strike, and cyber support. As we fulfill our responsibility to **Deter and Defeat Aggression**, we are developing tailored, 21st century deterrence options to address a wider range of adversaries across the spectrum of conflict. USSTRATCOM's global capabilities also enhance the ability of the joint force to **Project Power Despite Anti-Access and Area-**

**Denial Challenges**, perhaps our greatest military advantage. This supports deterrence at all levels. USSTRATCOM plays a key role in DOD efforts to **Counter Weapons of Mass Destruction**, synchronizing planning, advocating for capabilities, and delivering expertise to other commands. In closely linked, technologically advanced national security areas we ensure America's ability to **Operate Effectively in Cyberspace and Space** each and every day. Here we face real threats to our systems and networks—threats that are growing and require continued vigilance, improvement, and resilience. As we work to **Maintain a Safe, Secure, and Effective Nuclear Deterrent,** the strategy says "we will field nuclear forces that can under any circumstances confront an adversary with the prospect of unacceptable damage both to deter potential adversaries and to assure U.S. allies and other security partners that they can count on America's security commitments." The professionals in USSTRATCOM perform the nuclear deterrence mission every day. Finally, and while principally the role of geographic CCMDs, we supports a wide range of efforts to **Defend the Homeland and Provide Support to Civil Authorities**, including our cybersecurity assistance to the Department of Homeland Security and missile defense programs.

These are not the only primary missions mentioned in the new strategy. As a supporting command, USSTRATCOM also regularly contributes to CCMD efforts to provide a stabilizing presence; to conduct stability and

**Primary Missions of the U.S. Armed Forces**

- **Counterterrorism and Irregular Warfare**
- **Deter and Defeat Aggression**
- **Project Power Despite Anti-Access/Area-Denial Challenges**
- **Counter Weapons of Mass Destruction**
- **Operate Effectively in Cyberspace and Space**
- **Maintain a Safe, Secure, and Effective Nuclear Deterrent**
- **Defend the Homeland and Provide Support to Civil Authorities**
- Provide a Stabilizing Presence
- Conduct Stability and Counterinsurgency Operations
- Conduct Humanitarian, Disaster Relief, and Other Operations

counterinsurgency operations; and to conduct humanitarian, disaster relief, and other operations.

In sum, the new strategy calls for a strategic approach that promotes agile, decentralized action from fully integrated—I would say fully interdependent—and resilient commands and joint forces. And, over the last decade, our joint force has made great strides integrating unique Service and interagency capabilities. Our joint forces have become more integrated, and our joint commands have become more interdependent—producing greater unity of effort. Since the threats we face are not necessarily divisible by geography or domain, integration that advances cross-domain synergy[1] is imperative.

Achieving effective joint force synergy was a key principle in the strategy that shaped Fiscal Year 2013 budget requirements. Implementing the new strategy in a period of fiscal constraints is a substantial challenge, but I am confident that we can recalibrate our capabilities and make selective additional investments to succeed in these mission areas, based on priorities outlined in the strategy. This is the right approach.

**U S. STRATEGIC COMMAND TODAY**

Over the last decade, USSTRATCOM's responsibilities have grown in size and scope, responding to evolving national security needs. Ten years ago this fall, DOD disestablished both U.S. Space Command[2] and the first U.S. Strategic Command[3]—merging them and beginning the development of USSTRATCOM with its broad, functional responsibilities. Within just the past year, the Secretary of Defense added to our duties by reassigning the Joint Warfare Analysis

[1] Cross domain synergy: "The complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others—to establish superiority in some combination of domains that will provide the freedom of action required by the mission." *Joint Operational Access Concept*, Foreword.

[2] A unified combatant command responsible for military space activities and (at the time) the relatively new computer network operations mission.

[3] A unified combatant command activated in 1992, solely focused on the nuclear deterrence and associated command and control missions.

Center[4] to USSTRATCOM. We also returned several "information operations" responsibilities to the Joint Staff, such as planning, coordinating, and executing cross-AOR and national-level operations, supporting other combatant commands' planning efforts, and advocating for military deception and operations security capabilities. This realignment of responsibilities allows us to better focus on the enduring joint electronic warfare and electromagnetic spectrum mission.

The long series of changes begun in 2002 might appear random, but it was not. Moving missions of global significance and trans-regional impact to a single combatant command allows one organization to apply a global, strategic perspective to unique problem sets and to gain synergy from a range of strategic capabilities. USSTRATCOM is now able to provide our national leaders with a range of strategic, operational, and tactical options and capabilities that contribute to deterrence and enhance the effectiveness of the joint force.

Today, USSTRATCOM exists to perform two fundamental missions: 1) to deter attack and assure our allies with a combination of capabilities that goes far beyond the nuclear force; and, 2) along with the other CCMDs, to employ force as directed to achieve national security objectives. The complementary (not merely additive) nature of USSTRATCOM's unique, strategic responsibilities allows us to wield formidable global capabilities every day, usually as a supporting command (and usually supporting multiple commands simultaneously), supporting global and regional deterrence and assurance activities.

| USSTRATCOM Mission |
| --- |
| USSTRATCOM conducts global operations in coordination with other combatant commands, Services, and U.S. government agencies to deter and detect strategic attacks against the U.S. and its allies, and is prepared to defend the nation as directed. |

For example, USSTRATCOM provided several of America's unique B-2 bombers to U.S. Africa Command to support last year's Operation ODYSSEY DAWN—quickly providing an essential capability not otherwise available in that command. After the tragic events in Japan,

[4] Formerly assigned to U.S. Joint Forces Command, JWAC is headquartered at Naval Support Facility Dahlgren, VA.

USSTRATCOM also delivered substantial modeling and communications support to U.S. Pacific Command's (USPACOM) Operation TOMODACHI recovery efforts. Finally, later this year and in recognition of emerging Asia-Pacific challenges, we will co-host a major exercise with USPACOM to test and demonstrate joint capability and command interdependence, as we continue to explore and refine opportunities for greater collaboration.

These and many other scenarios highlight how the interdependent combination of capabilities and synchronization of activities within USSTRATCOM and with the other CCMDs facilitates a more flexible and effective joint force effort. To that end, our staff is developing and implementing a more comprehensive and deliberate deterrence and assurance campaign to sustain our capabilities, synchronize our efforts, and position us to act as needed.

**DETERRENCE AND ASSURANCE**

Deterrence and assurance have been part of the national lexicon for well over half a century, and although different today, they remain important and highly relevant concepts. The Cold War ended 20 years ago. Today, deterrence and assurance are not solely about Cold War deterrence objectives, they are about our nation's unique security needs—in a world that still has nuclear weapons. Deterrence is fundamentally about influencing an actor's decisions. The deterrence decision calculus still revolves around familiar concepts like imposing costs and denying benefits; however, in today's world we also strive to highlight the consequences of restraint (benefits of the status quo).

Deterrence is about communicating our capabilities and intentions, and it is about more than just one weapon system. It is about what the U.S. and our allies as a whole can bring to bear, tailored to specific actors and threats. Its practice encompasses both the nuclear and a strong conventional offensive force, missile defenses where appropriate, unfettered access and

use of space and cyberspace, and, in all warfare areas, modern capabilities that are resilient and sustained. Our challenge is to apply deterrence and assurance concepts to today's complex global security environment. Deterring, detecting, and preventing attacks against the U.S. is the responsibility of every combatant commander, and although strategic deterrence is USSTRATCOM's particular responsibility, it is a global charge we carry out in close coordination with other CCMDs and elements of government.

For decades, "strategic deterrence" focused solely on leveraging U.S. nuclear capabilities to deter our adversaries, but that day—the era of "one size fits all" deterrence and assurance—has passed. Strategic deterrence today requires combinations of tailored options and capabilities, wielded across multiple commands as an integrated whole, based on a robust understanding of the adversary's decision calculus and our mission context. It requires faster output from our intelligence, strategy, and planning experts. This is not easy. We must shape deterrence approaches that communicate expectations, strength, and resilience well in advance of adversary decisions, taking every opportunity to better understand each actor's expectations and perceptions—particularly in space and cyberspace.

***Combating Weapons of Mass Destruction (CWMD)***. The threat posed by WMD in the hands of violent extremists transcends all of USSTRATCOM's priorities and encompasses every geographic area of responsibility (AOR). The *2010 National Security Strategy* states that "there is no greater threat to the American people than weapons of mass destruction, particularly the danger posed by the pursuit of nuclear weapons by violent extremists and their proliferation to additional states."[5] Published shortly thereafter, the 2010 *Nuclear Posture Review* (NPR) noted that 21st century nuclear dangers are "grave and growing threats." Nuclear weapons foster a

[5] *National Security Strategy of the United States*, pp. 4.

sense of strategic stability between some actors, but WMD in general remain dangerously alluring capabilities to rogue and non-state actors.

The NPR elevated the prevention of nuclear proliferation and nuclear terrorism to the top of the policy agenda as it outlined five objectives to guide the U.S. in reducing global nuclear dangers. USSTRATCOM plays a principal role in efforts to reduce nuclear dangers by deterring WMD usage, dissuading their acquisition, and supporting efforts to eliminate potential WMD threats. This is a great challenge, and we are working to ensure our sense of urgency and pace of preparation match the threat.

**2010 Nuclear Posture Review Objectives**

- Preventing nuclear proliferation and nuclear terrorism
- Reducing the role of nuclear weapons in U.S. national security strategy
- Maintaining strategic deterrence and stability at reduced nuclear force levels
- Strengthening regional deterrence and reassuring U.S. allies and partners
- Sustaining a safe, secure, and effective nuclear arsenal

We have unique CWMD responsibilities at USSTRATCOM. We synchronize global CWMD planning efforts across the CCMDs, work to improve interagency relationships, and synchronize advocacy for essential CWMD capabilities. Our semi-annual global CWMD synchronization conferences have highlighted the need to improve coordination and to expand foundational intelligence and information sharing to deter and address emerging threats. This includes accelerating the speed with which we develop and field capabilities like stand-off detection for nuclear materials, better nuclear forensics, and improved global situational awareness.

One important CWMD development in the past year was the activation of USSTRATCOM's Standing Joint Force Headquarters for Elimination (SJFHQ-E). SJFHQ-E

stood up officially on 3 February 2012[6] and is commanded by the two-star officer who is also deputy director of the USSTRATCOM Center for Combating WMD (SCC WMD)[7]. When fully operational next year, SJFHQ-E will be a full-time, trained, deployable, joint command and control element able to quickly integrate into an operational HQ, conduct both deliberate and crisis planning, and maintain awareness of the WMD environment. This small standing headquarters will be augmented when needed and will operate in close coordination with the Defense Threat Reduction Agency and the U.S. Army's 20th Support Command.

***Nuclear Deterrence.*** Ensuring a safe, secure, and effective nuclear deterrent force remains a core responsibility of USSTRATCOM and is my #1 priority. As stated in the NPR, nuclear weapons retain an important role in our country's defense. They represent a unique, relevant, and powerful deterrent capability even as their role changes. Nuclear deterrence remains a tremendously important component of strategic deterrence as we seek to influence adversary decision makers by communicating a credible capability.

We have witnessed an impressive, 65-year period with neither nuclear use nor great-power war, during which we regularly adjusted our nuclear capabilities to match the global environment. Since the end of the Cold War, we significantly altered our own nuclear force structure and posture. We reduced the total number of ballistic missile submarines (SSBNs), converted four Ohio-class SSBNs to carry conventional cruise missiles, affirmed the B-1 bomber's non-nuclear role, removed all dual-capable heavy bombers from nuclear alert, eliminated the Peacekeeper Intercontinental Ballistic Missile (ICBM), substantially reduced the Minuteman ICBM force, withdrew numerous weapons abroad, and dramatically reduced our nuclear stockpile. In total, our stockpile is down over 75% from the day the Berlin Wall fell.

[6] Our goal is for SJFHQ-E to reach full operational capability by the end of 2013.
[7] Located at Ft. Belvoir, VA, SCC WMD is co-located with the Defense Threat Reduction Agency (DTRA). Mr. Ken Myers serves as the SCC WMD Director, as well as the DTRA Director.

These are significant changes. At each decision point along the way, the U.S. carefully accounted for potential impacts on deterrence capability and strategic stability. The end result is a substantially smaller force but one in which confidence remains to deter adversaries, assure allies, and maintain strategic stability in a crisis.

USSTRATCOM operates the nuclear deterrent force and is responsible for nuclear weapon employment planning. I can assure you that today's weapons and Triad of delivery platforms are safe, secure, and effective. The Triad—SSBNs, ICBMs, and nuclear-capable heavy bombers, with their associated tankers—continues to serve us well by providing unique and important attributes (survivability, promptness, and flexibility) that create insurmountable problems for any would-be adversary. Moving forward, and to sustain our strong nuclear deterrent force, we fully support the continued modernization and sustainment of delivery systems, weapon life extension programs, stockpile surveillance activities, nuclear complex infrastructure recapitalization, naval reactor design activities, and upgrades for nuclear command, control, and communications (NC3) capabilities. We are also working across DOD to finalize and synchronize New Strategic Arms Reduction Treaty (New START) implementation decisions routine operations and maintenance to minimize impacts on the operational force. We are on track to fully implement the central limits of New START by February 5, 2018.

As we consider possible future changes, I remain committed to the principle that a well-defined strategy must ultimately drive nuclear force structure and posture. USSTRATCOM is a full participant in the analysis of future deterrence requirements called for in the NPR, and we are providing military operational advice regarding implications of alternative approaches. Let me briefly review today's nuclear force.

***Weapons***. Over the past few years, a national consensus emerged around the need to modernize our weapons, delivery platforms, and the programs and facilities that sustain them. Since assuming command, I visited each of the nation's nuclear laboratories[8] and key industrial facilities. Seeing the condition of our nation's nuclear facilities and meeting the dedicated people who are the actual stewards of our nuclear weapons stockpile provided me a unique and irreplaceable appreciation for their needs.

As our weapons continue to age and we face the continued erosion of the nuclear enterprise's physical and intellectual capital, we must protect important investments for stockpile certification, warhead life extension, and infrastructure recapitalization. These investments are central to the new *Priorities for 21st Century Defense*, and without them, maintaining the long-term credibility and viability of the nation's nuclear deterrent will not be possible. Of all the elements of the nuclear enterprise, I am most concerned with the potential for declining or inadequate investment in the nuclear weapons enterprise that would result in our inability to sustain the deterrent force.

***Ballistic Missile Submarines (SSBNs)***. The Navy's SSBNs and sea-launched Trident D-5 ballistic missiles constitute the Triad's most survivable leg. This stealthy and highly-capable force requires modernization to replace aging and hull life-limited Ohio-class ballistic missile submarines. Although the Ohio-class replacement program will now be delayed by two years, the risk will be manageable. We must continue necessary preparatory activities and work to develop and field the Common Missile Compartment for both the Ohio-class replacement and the United Kingdom's Vanguard follow-on

[8] Los Alamos National Laboratory (NM), Sandia National Laboratory (NM), and Lawrence Livermore National Laboratory (CA).

submarines. With your support, I am confident that today's approach described in the FY 2013 budget request will continue the sea-based leg's strong deterrent capability.

***Intercontinental Ballistic Missiles (ICBMs)***. The Air Force's widely dispersed Minuteman III ICBMs comprise the Triad's most responsive platform leg, and the Air Force is successfully concluding efforts to sustain the Minuteman III force through 2020 and to enhance safety and security for the foreseeable future. USSTRATCOM is working with the Air Force to support life-extension programs to sustain the force through 2030. We are also participating in the Ground Based Strategic Deterrent Analysis of Alternatives to study the full range of concepts to eventually inform a decision to recapitalize the land-based Triad leg.

***Heavy Bombers***. While the nation relies on the long-range conventional strike capability of our heavy bombers, their nuclear capability continues to provide us with critical flexibility and visibility, as well as a rapid hedge response against technical challenges in other legs of the Triad. Planned sustainment and modernization activities will ensure a credible nuclear bomber capability through 2035. Looking forward, a new, penetrating bomber is required to credibly sustain our broad range of deterrence and strike options beyond the lifespan of today's platforms. The budget supports this effort, and USSTRATCOM is working with the Air Force to develop requirements for the next dual-capable (nuclear and conventional) long-range strike platform and associated Long Range Stand-off missile. The Air Force is also replacing the aging KC-135 tanker fleet with the KC-46A, ensuring an enduring air refueling capability essential to long-range bomber operations and airborne nuclear command and control platform endurance.

***Nuclear Command, Control, and Communications (NC3)***. In many ways, the NC3 component of the nuclear deterrent force is the most problematic. Ensuring continuously available and reliable communication from the President to the nuclear force is fundamental to our deterrence credibility. As with many systems and capabilities across our force structure, various NC3 components require modernization. Through smart investment and programming decisions, leveraging existing and emerging technologies, and in partnership across the department and interagency, we can achieve a robust and resilient 21st century NC3 architecture that both ensures this critical communication chain remains protected and is capable of addressing a broader range of threats and operational requirements. Within this context, I want to convey my appreciation for Congress' focus on NC3, and specifically Fiscal Year 2012 support for the new USSTRATCOM Headquarters Command and Control Complex at Offutt Air Force Base.

As we pursue deterrence and assurance concepts in today's complex global security environment, we recognize that a broad range of capabilities must contribute to tailored options. We believe the full range of capabilities assigned to USSTRATCOM comprise our deterrence "tool kit." Each of these also contributes to daily operations and activities that enhance the combat capability of the joint force. Let me briefly describe the status of other capability areas:

***Intelligence, Surveillance, and Reconnaissance (ISR)***. In a global environment characterized by complexity, asymmetric threats, and uncertainty, detecting and understanding adversary plans, intentions, and warning indicators has never been more important. As ISR technologies and platforms have improved in both the quality and quantity of data collected, we have seen a steadily increasing demand for ISR collection to meet routine and crisis

requirements. Through our Joint Functional Component Command for ISR (JFCC ISR),[9] USSTRATCOM's leadership in managing DOD's ISR capabilities and in assessing ISR performance has been pivotal to meeting today's intelligence challenges.

As our global knowledge demands expand, orchestrating our ISR operations to gain greater effectiveness and efficiency is increasingly necessary and challenging. First, preventing strategic surprise requires unparalleled battlespace awareness. Second, the demand for ISR collection continues to outpace our ability to fully resource that demand. Therefore, we must refine our ISR global force management processes and hone our collection strategies to improve our agility and effectiveness, making our ISR capabilities even more responsive combat multipliers.

Our ability to process and analyze data from increasingly capable ISR platforms is also a growing challenge. Not only are analysts dealing with more data, but also with an increased operations tempo that imposes ever greater demands on the timeliness of their analyses and reporting. Conservative estimates predict a one hundred percent increase in analysts is necessary to meet our combatant commanders' requirements. This level of growth would be unrealistic in almost any environment, let alone a fiscally constrained one, driving us to seek further efficiencies and concepts to get more from our existing analytic enterprise.

A key to doing this will be to improve data management, increase computing power and capability to help the analysts, and manage ISR processing, exploitation, and dissemination (PED) more effectively. Our intent is to manage resources globally while maintaining regional and local focus. This will ensure we can move faster to our highest priorities during and between emerging crises and contingencies, guaranteeing knowledge dominance for our commanders.

[9] Located at Joint Base Anacostia-Bolling (JBAB), DC. LTG Burgess is the Director of DIA and is dual-hatted as CDR JFCC ISR.

JFCC-ISR has been pursuing these goals, and their efforts paid dividends during the recent simultaneous intelligence demands imposed by Libyan operations, the Japanese reactor crisis, and the Afghanistan surge. While our vectors are in the right direction, we must continue to build our ISR concepts and processes to be even more agile and effective in the future.

***Global Strike***. USSTRATCOM is responsible for planning, coordinating, and executing global strike activities (kinetic nuclear, kinetic conventional, and non-kinetic) and advocating for required capabilities. Global strike capabilities allow DOD to expand the range of integrated deterrent options available to the President and enable combatant commanders' access to capabilities not otherwise available in their particular AOR. USSTRATCOM's unique strategic capabilities enable us to rapidly support national and theater global strike missions in a number of ways.

In addition, USSTRATCOM continues to support and advocate for a rapid conventional strike capability. This would enhance strategic deterrence with the ability to promptly deliver a non-nuclear effect against a limited subset of highest value targets at substantial ranges. The Air Force, Defense Advanced Research Projects Agency (DARPA), and the Army have made important progress developing non-ballistic, boost-glide technologies applicable to a Conventional Prompt Global Strike (CPGS) mission, as highlighted by the Army's successful flight test of the Advanced Hypersonic Weapon concept this past November. I ask for your continued support of research, development, test, and evaluation funding as we explore various conventional global strike system concepts and basing alternatives.

***Integrated Missile Defense (IMD)***. Ballistic missiles remain a significant threat to the U.S. homeland and a growing threat to our allies and our forces deployed abroad. As a means of terror, or to deter U.S. or allied regional intervention, or as a trans-regional means to employ

WMD, ballistic missiles continue to become more accurate, lethal, and capable—attractive attributes to any number of current or potential adversaries.

In response, U.S. and allied capabilities to deter, detect, and defeat these weapons are also growing, and decades of research and development continue to pay dividends in terms of capability and credibility. And, as we consider a more integrated joint force, missile defense is an area that particularly highlights the importance of considering the full range of integrated strategic capabilities—since ballistic missile threats can rapidly transit areas of responsibility and may perhaps best be deterred or defeated via space, cyberspace, or global strike capabilities long before their launch requires action from regionally-based interceptors.

Ballistic missile threats are likely to grow at least as rapidly as our defensive assets, and we have little margin for error in acquisition and force management decisions. USSTRATCOM plays important roles coordinating operational support and synchronizing missile defense planning, operating concepts, and capability advocacy. Our Joint Functional Component Command for Integrated Missile Defense (JFCC IMD)[10] leads an annual global ballistic missile defense assessment to look across all areas of responsibility, consider individual combatant commanders' assessments of risk, find common threads, and make recommendations to reduce global risk. USSTRATCOM also coordinates the Air and Missile Defense Prioritized Capabilities List (PCL) across other CCMDs, improving the Services' and the Missile Defense Agency's (MDA) understanding of prioritized joint warfighter capability needs. This enhances efforts to provide persistent detection; expand data sharing among the U.S., allies, and partners; field effective defensive systems; and provide appropriately robust joint training. As the Joint Functional Manager for missile defense capabilities, JFCC IMD recommends the global

[10] Located at Schriever AFB, CO. LTG Formica serves as CDR JFCC IMD, as well as Commanding General U.S. Army-Strategic (ARSTRAT) and Army Space and Missile Defense Command (SMDC).

allocation of low-density, high-demand assets, including force rotations, and force sufficiency—thus making the best use of limited resources.

Over the past year, these efforts substantially improved our overall missile defenses. We upgraded and integrated early warning radars in Greenland and England, improving battle-management software for data integration. We increased the number of Aegis BMD-equipped ships. And, we fielded and integrated additional elements of the European Phased Adaptive Approach (EPAA), an effort that improves missile defenses through the acquisition and integration of more advanced capabilities and the expansion of key partnerships.

In specific cases, such as limited threats against the U.S. and/or regional contingencies, our growing missile defenses play important deterrence and assurance roles. The application of future Phased Adaptive Approaches to other regions is an integral part of theater defenses, and we must continue to strengthen regional partnerships to meet emerging ballistic missile threats. I am confident that planned and budgeted missile defense investments will continue to support deterrence and assurance goals by significantly improving the protection of our homeland, our forward-based forces, and our allies. USSTRATCOM is committed to future capability development efforts that leverage past successes, address the most pressing and most likely threats, and produce field-tested, reliable assets in a cost-effective manner.

***Electromagnetic Spectrum (EMS) and Electronic Warfare***. The EMS is the connective tissue for literally every aspect of civil, commercial, and military activity. For example, signals flowing through the spectrum connect airborne ISR aircraft to the ground troops they support, to the fleet offshore, and to commanders anywhere in the world. We are all linked, in an increasing number of ways, to modern technological necessities whose very design assumes unfettered

access across the spectrum. Yet, this access is something we assume with increasing risk, particularly for the closely linked national security areas of space and cyberspace.

Today, there are three general concerns regarding the EMS. First, increased demand for interconnectivity and a growing base of EMS "users" is creating pressure to make greater segments available for public use. Second, growing use is creating "crowding" in the EMS—a problem that can result in inadvertent interference of civil, commercial, and military activities alike. EMS use priorities must be carefully managed to ensure access for force training, readiness, and operations. Finally, our growing civil, commercial, and military reliance on the electromagnetic spectrum presents adversaries an opportunity. We must assume adversaries will seek disruptive or destructive EMS capabilities to obtain their own asymmetric edge. At a time when no single discipline or command can address any conflict alone, efforts to strengthen integration, ensure persistent spectrum access where and when we need it, and deter adversary disruption or exploitation are important deterrence and assurance objectives.

To improve joint approaches to the electromagnetic spectrum, USSTRATCOM is focusing its enduring electronic warfare and electromagnetic spectrum responsibilities by establishing the Joint Electromagnetic Spectrum Control Center (JEMSCC). The JEMSCC will expand previous joint electromagnetic spectrum operations efforts, effectively organizing a single warfighter organization to advocate for and support joint electronic warfare capability strategy, doctrine, planning, requirements, resources, test, training, and operational support. The JEMSCC will place a particular focus on the coordination of electromagnetic spectrum-related elements to enhance joint war fighting capabilities across domains and our ability to fight through degraded environments.

***Space***. The *National Security Space Strategy* highlights the importance of U.S. leadership for the global economy, scientific discovery, modern necessities, our national security, and global strategic stability. Though increasingly contested, congested, and competitive, space remains the ultimate high ground, and ensuring access to mission-essential space capabilities through all phases of conflict is essential to maintaining and enhancing the strategic advantages space provides. Mindful of the need to maintain and enhance space's benefits for our national security enterprise, particularly in light of today's dynamic operating environment, the *National Security Space Strategy* identified a set of interrelated strategic approaches designed to sustain not just America's leadership in space but our ability to provide benefits for global navigation, commerce, communication, and research. As the combatant command responsible for military space operations, support, and capability advocacy, USSTRATCOM fully supports these approaches and is actively pursuing capability and cooperative improvements.

| National Security Space Strategy |
| --- |
| • Promote responsible, peaceful, and safe use of space;<br>• Provide improved U.S. space capabilities;<br>• Partner with responsible nations, international organizations, and commercial firms;<br>• Prevent and deter aggression against space infrastructure that supports U.S. national security; and<br>• Prepare to defeat attacks and to operate in a degraded environment |

The space domain physically borders every geographic area of responsibility and shares virtual boundaries with cyberspace. It is vital to monitoring strategic and military developments, responding to natural and man-made disasters, and understanding environmental trends. In short, space systems provide unfettered global access. However, we cannot assume that our space advantages will automatically continue. Today's constellations continue to age and require replacement, and although we still maintain a qualitative edge, technological diffusion and the sheer number of spacefaring nations could place our space advantages at risk. Our assets also

face a range of challenges from both natural or unintentional man-made threats (space weather, accidental collisions, and inadvertent electromagnetic interference) and purposeful jamming, cyber intrusions, interference, anti-satellite weapons, and kinetic attack (on space- or terrestrial-based space assets).

Sustaining U.S. advantages in the space domain requires that we act deliberately to enhance our own military advantage and to reduce strategic risk—both of which require broad collaboration across the U.S. government and with our international partners. We must comprehensively assess the space capabilities we require to sustain our military advantage—focusing on cross-service and cross-organization capabilities to secure the greatest value. This includes working with the Services to refine and communicate clear, well-defined, and realistic requirements for each capability, mindful that the long-term strategy for assured access to space relies on a capable national industrial base. We must also take advantage of opportunities to work with other partners. For example, in January U.S officials announced a 20-year agreement that will add Canada, Denmark, Luxembourg, the Netherlands, and New Zealand to our current partnership with Australia for global military satellite communications. Now shared with these additional partners, the Wideband Global Satellite Communications (WGS) program provides high-capacity communications for many more military users, and this agreement expands the program to secure a planned, ninth satellite.

Reducing risks to space assets begins with situational awareness. Establishing and maintaining situational awareness in this vast, global domain is fundamental. It is also problematic. Each orbital regime presents its own unique challenges, and space is a harsh and technically challenging environment. Over the past several years, the Joint Space Operations Center (JSpOC) under the direction of our Joint Functional Component Command for Space

(JFCC SPACE)[11] has made great progress expanding the number of objects tracked, the number of satellite close-approaches analyzed, and the number of partners involved in the space situational awareness sharing process. We currently track more than 22,000 orbiting objects, and the JSpOC Mission System (JMS) and additional sensors contained in the FY 2013 budget request will further improve our ability to detect smaller objects (increasing the number of objects tracked) and the frequency and fidelity of analyses (further contributing to the safety of space flight). Agreements that allow us to expand space surveillance and communication access points and data sharing hold great promise for improving shared space situational awareness and operational effectiveness. Additional sharing agreements, particularly those that lead to the eventual transition of the JSpOC into a truly international Combined Space Operations Center (CSpOC), have great potential to demonstrate space leadership and expand information available to all users. Finally, clearly communicating expectations and a shared understanding of space norms and responsibilities among space-faring nations will provide an important foundation for deterring undesirable aggression against space capabilities.

***Cyberspace***. Few might ever have imagined how cyberspace would evolve—globally connected and geographically unconstrained—to define modern life for billions of people. Not only have we woven cyberspace into nearly every facet of our personal lives, it has also become essential to the functioning of the global economy and military operations across all domains. In cyberspace we seek to conduct commerce, share information, learn, and entertain. But, through cyberspace others seek to vandalize, steal, disrupt, and, potentially, to destroy. In the military, we rely on many domains or capabilities with the reasonable expectation that we can secure them when required. However, in cyberspace, and across the broader electromagnetic spectrum, we

[11] Located at Vandenberg AFB, CA. Lt Gen Helms serves as CDR JFCC Space as well as Commander, 14th Air Force.

find ourselves almost completely reliant on something we will likely never completely secure. Dealing with that reality is an extraordinary challenge.

This reliance, like all of our technological advantages, is also clear to potential adversaries who are seeking to use cyberspace as a means to act against U.S. data, forces, or critical infrastructure—particularly shared network infrastructure. Our challenge is to deploy resilient capabilities, sufficient capacity, and effective defenses that preserve access to our technological advantages by securing critical resources and preparing to operate and deliver effects—even when under threat of cyber intrusion.

The *Department of Defense Strategy for Operating in Cyberspace* outlines five strategic initiatives to focus efforts to leverage cyberspace's tremendous opportunities while managing its dynamic nature and vulnerabilities. USSTRATCOM is responsible for operating and defending DOD information networks, planning against designated cyberspace threats, executing cyberspace operations as directed, advocating for cyberspace capabilities, and synchronizing activities with other combatant commands and agencies. In addition to our substantial work maturing the cyber mission, forces, capabilities, and relationships, we are continuing to improve operating concepts to better address cyberspace threats and support combatant commands. While much remains to be done, we have made substantial progress, and

| DOD Strategy for Operating in Cyberspace |
| --- |
| • Treat cyberspace as an operational domain to organize, train, and equip so that DOD can take full advantage of cyberspace's potential<br>• Employ new defense operating concepts to protect DOD networks and systems<br>• Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy<br>• Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity<br>• Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation |

CYBERCOM continues to play an essential role operating and defending DOD's information networks.

Moving forward, we must continue to improve situational awareness and clarify the global roles, responsibilities, expectations, and authorities that contribute to stable and effective deterrence and assurance. Effective defensive and offensive preparation begins with situational awareness. Threats in cyberspace are anything but static, and a useful defensive strategy or capability existing one moment may be ineffective mere seconds later, and improved relationships and technical capabilities allow us to better understand the dynamic cyber environment. Gaining this awareness and then acting quickly and effectively requires improving the complex interagency and international relationships. Cyber security requires the entire government's effort. No single agency or department can effectively address the threats we face in cyberspace; we must constantly evaluate relationships and operational constructs to address constantly evolving threats. The recent Defense Industrial Base (DIB) Pilot program is a great example of the benefits of partnership and the type of activity we look forward to furthering in the future.[12]

Finally, in all of USSTRATCOM's unique functional mission areas, but particularly in cyberspace, I am concerned about sufficient technical capacity and personnel. We must ensure information technology capabilities are fielded with sufficient capacity and in a more resilient, defensible structure that still reaps as many benefits as possible from the open nature of the internet. Furthermore, we need the best trained and educated people to work our cyberspace challenges, and growing tomorrow's cyberspace professionals is fundamentally about education. Ensuring our future security in cyberspace—and really across USSTRATCOM's strategic

[12] The DIB pilot completed transitioning to the Department of Homeland Security this January and is now called the Joint Cybersecurity Pilot (JCSP).

responsibilities—begins with efforts to encourage and improve science, technology, engineering, and math education from an early age. It also includes the recognition that traditional military recruitment and retention programs may not be the best or fastest way to build a stable cyber cadre for the long term.

**OUR PEOPLE**

At USSTRATCOM, we recognize that our people are our greatest and most enduring strength. Shaping the future joint force, professionally and personally, requires diligent attention. As a reflection of our strategy, we must support educational (including lifelong science, technology, engineering, and math ) and other personnel efforts that enable us to recruit, train, exercise, develop, and sustain the unique deterrence, space, and cyber workforce we need.

Indeed, the all-volunteer force is our military's greatest strength, and we must keep the faith with our people and their families. Our Service members, civilians, and their families bear unique sacrifices for our nation, and we especially appreciate their sacrifices over the past decade at war and at home. These sacrifices have come at great cost, and we must continue identifying stresses and providing our troops and their families necessary care. Suicides remain my greatest personnel concern, and I appreciate Service efforts this year to improve the personal resiliency of each member. One suicide is one too many. This is not only every commander's business, but it is the business of every Soldier, Sailor, Airman, Marine, and civilian.

**CONCLUSION**

Mister Chairman, it remains a great honor to lead the men and women of U.S. Strategic Command. This is an interesting time for our nation; and this is more than an interesting time for USSTRATCOM. However, the challenge before us is not just to <u>live</u> in interesting times but to continue to <u>excel</u> in these interesting times. Ultimately, our goal is to anticipate and prevent

strategic attacks, to continue to assure our allies, and to ensure we maintain access to space and cyberspace, which provide the U.S. decisive strategic and operational advantages to achieve our global security objectives. Our success will hinge on the quality of our people and the effectiveness of our response to a new national security reality that continues to test our agility, flexibility, and resolve. Dealing effectively with these challenges and identifying and pursuing opportunities that result will require all the imagination, innovation, and discipline we can muster. Dealing effectively with these challenges will also require us to synchronize, collaborate, and coordinate with the other combatant commands, agencies, and allies to an unprecedented degree.

These are just the sort of interesting times and challenges USSTRATCOM was designed to address. We are equal to the task and determined to continuously improve and stay ahead of the challenge. I appreciate your continued support for USSTRATCOM and all of our Service members and civilians, and I look forward to continuing to work with you over the coming year.