NOT FOR DISTRIBUTION UNTIL RELEASED BY THE

SENATE COMMITTEE ON ARMED SERVICES

STATEMENT OF

GENERAL KEVIN P. CHILTON

COMMANDER

UNITED STATES STRATEGIC COMMAND

BEFORE THE

SENATE COMMITTEE ON ARMED SERVICES

24 MARCH 2010

NOT FOR DISTRIBUTION UNTIL RELEASED BY THE

SENATE COMMITTEE ON ARMED SERVICES

Chairman Levin, Ranking Member McCain, distinguished members of the Committee on Armed Services, thank you for the opportunity to testify today, representing the extraordinary men and women of United States Strategic Command (USSTRATCOM). I'm privileged to showcase this joint team's achievements, discuss our requirements, and highlight future national security challenges across our mission areas. USSTRATCOM's active duty and reserve military members, civilians, and contractors form a superb joint team, whose dedicated planning, advocacy, and operational execution efforts advance our warfighting priorities. We continue to strengthen and sharpen our focus on deterrence while at the same time preserving our freedom of action in space and cyberspace. Before continuing, I must say that we appreciate your support, because legislative investments across our mission areas are essential to our providing global security for America.

Admiral Mullen's memorandum CJCS Guidance for 2009-2010 detailed the Joint Force's strategic objectives through 2010. These objectives include defending our national interests in the broader Middle East and South Central Asia, considering ways and means to improve the force's health, and balancing global strategic risks through deterrence. The uninformed observer might expect USSTRATCOM to aid the Joint Force only with deterrence, but this globally operational command does much more. In fact, the Quadrennial Defense Review (QDR) identified six key missions for the Department of Defense (DoD),[1] and USSTRATCOM plays a role in each of these missions, whether by conducting operations, supporting and advocating for global warfighter needs, closing gaps in geographic seams, or building relationships across a growing range of partners.

[1] The six mission areas are: (1) defend the United States and support civil authorities at home, (2) succeed in counterinsurgency, stability, and counterterrorism operations, (3) build the security capacity of partner states, (4) deter and defeat aggression in anti-access environments, (5) prevent proliferation and counter weapons of mass destruction, and (6) operate effectively in cyberspace.

USSTRATCOM continues to support actively the DoD work on the Quadrennial Defense Review (QDR), Space Posture Review (SPR), Nuclear Posture Review (NPR), Ballistic Missile Defense Review (BMDR), and the new Strategic Arms Reduction Treaty (START) negotiations. These reviews and START will shape the role of our strategic capabilities and define the investments necessary to recapitalize and sustain them, while highlighting USSTRATCOM's place at the nexus of today's primary national security challenges. We are now helping to translate these reports into the strategy and plans that our components and the joint force need. This year we will continue to focus on further developing our workforce, sustaining the highest possible standards in the nuclear enterprise, and integrating our global capabilities to support national and theater objectives. These efforts will require investing in the deterrent enterprise, identifying mechanisms to better integrate operations, plans, requirements, and activities among our components, standing up U.S. Cyber Command (USCYBERCOM) to better execute our cyber mission, and sustaining the critical national security capabilities provided by on-orbit satellite constellations.

U.S. STRATEGIC COMMAND

As we address today's challenges, USSTRATCOM has already devoted significant effort to align our priorities, plans, and investments across our components while simultaneously executing deterrence, space, and cyberspace operations. We have initiated and sustained several successful engagement efforts. USSTRATCOM's reinvigorated military-to-military outreach programs, which included senior-leader discussions with key friends and allies, including the United Kingdom, France, Japan, South Korea, Australia, and Israel on such topics as deterrence, space, cyberspace, and missile defense. USSTRATCOM was honored to host the United Kingdom's First Sea Lord, Admiral Sir Mark Stanhope; Australia's Vice Chief of Defence Force, Lieutenant General David Hurley; France's Chief of the Defense Staff, General Jean-

Louis Georgelin; and China's Vice Chairman of the Central Military Commission, Gen Xu Caihou. Gen Xu's request to visit USSTRATCOM during his U.S. tour highlighted China's recognition of USSTRATCOM's global role, and our very positive exchange showcased the tremendous potential of military-to-military relationships to build confidence and understanding between our countries. These dialogues are important and must continue.

Over the past year, we welcomed the stand-up of Air Force Global Strike Command and our components' increased focus on the deterrence mission. In addition to maturing the adjustments we made in our headquarters staff, USSTRATCOM's GLOBAL THUNDER 2009 deterrence exercise constituted the most extensive nuclear command, control, and communications (NC3) field exercise in over a decade. It demonstrated the full range of nuclear deterrence capabilities by integrating submarine strategic deterrent patrols, more than 90 aircraft sorties, an ICBM test launch, and five days of continuous airborne command-and-control operations. GLOBAL THUNDER's success demonstrated the readiness of America's strategic forces. Continued support for the joint training requirements and the established Combatant Commander Exercise Engagement (CE2) Defense-wide account is essential to ensuring future USSTRATCOM mission readiness.

Today's strategic mission requirements also demand the finest in command, control, and communications capabilities. Our 1950s-era headquarters falls short of providing the capabilities we need. We appreciate Congressional support for the planning and design funds appropriated in Fiscal Years 2009 and 2010 and requested for 2011. These investments move us closer to a 21st century headquarters and command center for deterrence, space, and cyberspace operations.

In the cyber domain, the Secretary of Defense directed USSTRATCOM to establish United States Cyber Command (USCYBERCOM) as a sub-unified command. This effort continued the reorganization of cyber forces that began with the Secretary's direction in October

2008 to place USSTRATCOM's Joint Task Force for Global Network Operations (JTF GNO) under the operational control of Joint Functional Component Command for Network Warfare (JFCC NW). From their inception, JFCC NW and JTF GNO had segregated offensive and defensive military cyber operations. This segregation detracts from natural synergies and ignores our experience in organizing to operate in the air, land, sea, and space domains. The establishment of USCYBERCOM will remedy this problem in the cyber domain and create a robust sub-unified command to address the growing importance of the cyber domain to national security. We have already begun consolidating JTF GNO and JFCC NW in preparation for the formal establishment of USCYBERCOM, which awaits confirmation of the nominated commander. We look forward to continuing to work with Congress and our Agency partners as we move forward to establish USCYBERCOM.

The Services are also reorganizing their cyber forces in order to present trained and equipped cyber operators to the Joint Force. Over the past year, each Service reshaped the alignment of its cyber forces into a more unified organization, and we welcome the stand-up of Army Forces Cyber Command, Marine Corps Forces Cyberspace Command, Fleet Cyber Command, and the 24th Air Force. These forces will enhance our ability to operate and defend DoD information networks and provide the President with response options in cyberspace.

To enhance the level of global strategic dialogue and USSTRATCOM's support to other Combatant Commands, we are more broadly engaging our military and non-military partners. In 2009, USSTRATCOM launched new or renewed annual symposia for each of our three lines of operation. More than 5,000 attendees, representing multiple commands, universities, industry, and at least ten other countries (including His Excellency Sergey Kislyak, Ambassador of the Russian Federation to the United States) held substantive discussions on challenges facing our deterrence, space, and cyberspace professionals. USSTRATCOM teams also deployed across

the globe to provide in-theater subject-matter expertise. Our teams facilitated more effective employment of our capabilities in intelligence, surveillance, and reconnaissance (ISR), space, operational security, electronic warfare (EW), and cyber. These accomplishments, along with development of integrated missile defense (IMD) capabilities and increases in space situational awareness (SSA), represent just a small part of USSTRATCOM's accomplishments.

STRATEGIC CONTEXT

Last spring, President Obama stated that as the world "has become more interconnected…we've seen events move faster than our ability to control them." Global economic and political turmoil, rapidly evolving information technology, nontraditional threats, continuing overseas contingency operations, and terrorism represent just some of the factors influencing global and regional security challenges. Moreover, state and non-state actors pursue traditional and asymmetric means to challenge the U.S. and our allies. With the exception of the U.S., all nuclear weapon states continue to modernize their nuclear weapon stockpiles and in some cases grow them further. Although the U.S. and Russia are reducing their strategic arsenals, North Korea and Iran remain on a dangerous nuclear path. Additionally, we find increasing threats to our freedom of action in the global commons of space and cyberspace, even as the importance of these domains to our national security continues to grow. For example, Iran's successful February 2009 satellite launch and North Korea's attempt a few months later illustrate the spread of space launch technology. However, successful space-launch vehicles can also represent progress toward an effective intercontinental ballistic missile capability. If perfected, such long-range ballistic missiles would place a larger area of the world at risk.

Cyber networks weave through every facet of our lives and enable extraordinary communication, intelligence, and command and control capabilities. However, an adversary acting in cyberspace can steal critical information, thwart vital data transmissions, or create

devastating effects beyond the cyber domain. Governments, militaries, corporations, universities, and the individual computer user must guard against vulnerabilities that are open to criminals, organized hacktivists, state actors, and insider threats. Addressing these challenges while capitalizing on the dramatic enabling capabilities of cyberspace requires an unwavering watchfulness, a dynamic defense-in-depth construct, a workforce that is carefully recruited, trained, and properly retained, strong partnerships, an infrastructure that supports global employment of DoD forces, and a realization that DoD's cyber culture, conduct, and capabilities must change.

STRATEGIC DETERRENCE

In an environment of such rapid economic, political, military, and technological changes, many wonder if "deterrence" is still possible. Today's multi-polar and increasingly complex strategic environment, which includes threats posed by proliferation and terrorism, requires that we increase our focus on deterrence because effectively deterring threats to our nation and our allies is not only possible, it is essential.

Since the end of the Cold War, however, the serious study of deterrence theory and strategy has been inadequate. Much like our changing global context, modern deterrence challenges necessitate more complex approaches. The modern era of smart power requires a commitment to a whole-of-government deterrence effort that capitalizes on the full range of diplomatic, information, military, and economic activities. Despite this complex environment, we have skipped an entire generation of future policy makers, strategists, academics, and military professionals in terms of training and developing them in the field of deterrence. Preliminary work on the NPR and new START treaty revealed this shortage of human capital. USSTRATCOM's first annual Deterrence Symposium, held this past summer in Omaha, was our initial public effort to revitalize attention to deterrence theory, thought, and practice.

Speaking in Prague last year, President Obama articulated his goal of moving toward a world without nuclear weapons, including a desire to reduce global nuclear dangers and the role of nuclear weapons in our national security strategy, while urging other nations to do the same. The President also asserted that "as long as these weapons exist, the United States will maintain a safe, secure, and effective arsenal to deter any adversary, and guarantee that defense to our allies." Just days before the President's remarks, the Strategic Posture Commission concluded that "nuclear weapons are both the greatest potential threat to our way of life and important guarantors of U.S. security." The commissioners agreed on two parallel paths forward: "one path which reduces nuclear dangers by maintaining our deterrence, and the other which reduces nuclear dangers through arms control and international programs to prevent proliferation." As the command uniquely responsible for our nuclear deterrent and for synchronizing DoD combating weapons of mass destruction (CWMD) planning, STRATCOM finds itself actively engaged in all of these endeavors.

Throughout the 65-year history of nuclear weapons, no nuclear power has been conquered or even put at risk of conquest, nor has the world witnessed the globe-consuming conflicts of earlier history. More than 180 state parties to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) have either foresworn the pursuit of nuclear weapons (in many cases because of the promise of America's extended deterrent umbrella) or pledged in good faith to move toward eventual disarmament. The U.S. and Russia have made steep reductions in their nuclear arsenals since the end of the Cold War (a seldom recognized but important demonstration of U.S. commitment) while joining together to pursue the goals of the Cooperative Threat Reduction Program. We have invested considerable intellectual effort toward a stable world order, where nuclear weapons seem at once dangerous, undesirable,

expensive, a tempting source of power and prestige, and yet also essential to continued peace and stability.

Today, our nuclear weapons and triad of delivery systems remain essential to our national security. Nonetheless, in light of the global security environment, we should continually consider to what degree nuclear weapons remain relevant, whether ours measurably encourage or discourage proliferation, and to what extent reductions and/or force size and posture changes enhance peace and strategic stability. At the end of the day, all of our actions must enhance the security of the United States, our most solemn responsibility.

The role of our nation's nuclear weapons in maintaining peace and stability, and therefore the security of the United States, is deterrence. Our deterrence strategy is predicated on the effectiveness of six distinct facets that in the aggregate make our strategy credible. These six facets are weapons, delivery systems, threat warning, nuclear command and control (NC2), weapon production, and industrial base. I will briefly discuss each of these.

Weapons

Nuclear weapons remain fundamental to our deterrent capability. Increasing the safety, security, and long-term confidence in the U.S. nuclear arsenal remains a top priority. However, the weapons we rely on today for deterrence were designed for short operating lives in a different era with different safety and security requirements. While individual components may last for years, combining the components in a radioactive environment has effects that we cannot fully predict. As recently noted in government review of the stockpile assessment, our current approaches to delivery system sustainment are not tenable over the long term and, for the weapons themselves, they are also not tenable if we desire to implement improvements to safety and security features.

As we ramp up to full-rate W76-1 production, we must also address promptly the B61 warhead life extension. By doing the B61 nuclear life extension now along with the funded non-nuclear life extension, we have an opportunity to save cost by avoiding a second life extension in the 2020s while increasing confidence in the safety, security, and effectiveness of the stockpile consistent with the President's vision. We must act now to fit the life extension within the narrow window of opportunity in the production complex.

We must also begin exploring sustainment options for the W78 ICBM and W88 SLBM warheads. The Strategic Posture Commission noted that any options would require some combination of refurbishment, reuse, and replacement, with decisions best made on a case-by-case basis. The Nuclear Posture Review is examining the appropriate policy guidance for considering future choices between refurbishment, reuse, and replacement. A recent study by the JASON Defense Advisory Group concluded that only reuse or replacement options allow for the inclusion of intrinsic surety features that would be the last line of defense against unauthorized use. I urge you to support life extension studies requested this year to best inform the Administration and Congress for future decisions.

The Fiscal Year 2010 National Defense Authorization Act created the Stockpile Management Program to increase safety, security, and long-term effectiveness of the U.S. stockpile without nuclear testing. I believe we can meet the goals of this program without seeking new military capabilities or resorting to nuclear testing. Reductions in the number of warhead types and in the size of the hedge stockpile are also possible.

Delivery Systems

The triad of diverse and complementary strategic delivery systems has supported our national security objectives in the past and will continue to do so well into the future. USSTRATCOM is actively working with the Services to validate proposals to recapitalize and

modernize our forces. Our intercontinental ballistic missile (ICBM) force celebrated its 50th birthday in 2009 and remains the most responsive and cost-effective leg of the triad. The Air Force is concluding a decade-long modernization effort to sustain the Minuteman III through 2020 and is continuing the necessary steps to meet the Congressional mandate to sustain the system through 2030. USSTRATCOM actively supports current life-extension programs and is working closely with the Air Force to determine the requirements of our next land-based strategic deterrent system. The Navy's SLBMs constitute the triad's most survivable and assured response element. A stealthy delivery platform and a highly reliable weapon system have proven an effective strategic deterrent combination, and USSTRATCOM supports the Navy's efforts to design a replacement for the Ohio-class ballistic missile submarine and sustain the Trident II D5 ballistic missile to meet future deterrent requirements. Finally, our nation will continue to require a nuclear-capable bomber's inherent flexibility to address a variety of possible adversaries and contingencies. USSTRATCOM supports the Air Force's efforts to sustain and modernize mission-critical B-2 and B-52 systems. We are also working with the Air Force to identify requirements for the next manned, nuclear-capable, long-range strike platform and air-delivered standoff weapon.

Threat Warning

Another key element of credible deterrence is threat warning that provides attribution. For decades, the Defense Support Program (DSP) and our early warning radars have provided the essential data necessary to ensure timely and informed decisions. They provide prompt and accurate data to the President and combatant commanders for detection, identification, and predicted impact point of ballistic missiles. Sustainment of our early warning radars and fielding of the Space Based Infrared Satellite (SBIRS) geosynchronous constellation are essential to maintaining timely threat warning and attribution. However, though SBIRS was originally

programmed to launch in 2002 as a replacement for DSP, we have not yet launched a single SBIRS satellite, and current schedules forecast that the first will not be ready before December 2010. I encourage your continued support to ensure the successful deployment of this system.

NC2

For deterrence to be effective, potential adversaries must know that the President can direct our nuclear forces under all circumstances. This requires a reliable and secure NC2 architecture. Our NC2 systems deliver warning and attribution information, provide for positive control of nuclear forces, and ensure our ability to employ nuclear weapons per Presidential direction. To remain effective in the most hostile nuclear environment, our NC2 relies on resilient satellite communication constellations (MILSTAR and its replacement, the Advanced Extremely High Frequency (AEHF)), cryptographic protection, and hardening. Many of our current NC2 systems were built during the Cold War and therefore require new investment for upgrades or replacement. Additionally, continued delays in procurement of AEHF-related equipment are a concern. The vital task of fielding modern and survivable NC2 systems is worthy of your full support.

Weapons Production

The Strategic Posture Commission and JASON noted that regardless of which life-extension options we choose for existing warheads, success relies on maintaining and renewing expertise and capabilities in science, technology, engineering, and production techniques unique to the nuclear weapons program. The National Nuclear Security Administration's (NNSA) aging infrastructure limits its sustainment capacity, forcing all life extension activities into a tight, sequential, and delicately balanced timeline that incurs undue risk. Moreover, our nuclear weapons design and manufacturing workforce is both aging and shrinking due to a lack of meaningful work, unstable funding, and the perception that nuclear weapons work is not

important. The custodians of America's nuclear deterrent—NNSA and its National Laboratories—have long labored in deteriorating plutonium and uranium facilities that date to the Manhattan Project and that the Strategic Posture Commission termed "decrepit." Decrepit is unacceptable. We owe our people at NNSA and the National Laboratories better. We owe our nation better.

To sustain the nuclear deterrent and successfully execute the Stockpile Management and Stewardship Programs, we must invest in new plutonium and uranium facilities, strengthen the science, technology, and engineering base needed to sustain and certify the stockpile, and seek out and develop our very best scientists and engineers. The President's 13% increase in requested NNSA funding represents a long-overdue investment in the nuclear complex and its people. I strongly urge you to support this request.

Industrial Base

Industrial base challenges complicate the sustainment of current and the development of future delivery systems. An inability to produce items such as solid rocket motors and advanced navigation and control systems would threaten our ability to maintain strategic platforms. Perishable skills and technologies are required to sustain current systems beyond their expected life span and to develop the systems required for the future. The FY2010 NDAA requirement to develop a SRM industrial base plan is an important step toward ensuring essential skills and capabilities in that portion of the deterrent industrial base, and we look forward to the results of the OSD led task force chartered to fulfill this direction. Sufficient funding to sustain a responsive industrial base is a critical element of maintaining the credibility of deterrence, and we ask for continued Congressional support.

GLOBAL STRIKE

A limited, credible conventional prompt global strike capability would provide the President a broader range of non-nuclear options to address emerging threats rapidly. However, we continue to lack the ability to promptly deliver conventional effects against targets in denied or geographically isolated areas. As we continue to make progress through Research, Development, Test, and Evaluation (RDT&E) subprojects, I ask for your continued support for a PGS capability that will be carefully sized to avoid perturbing our strategic relationships with Russia and China.

SPACE

Operations in the space domain continue to enable an increasing number of capabilities that are essential to military operations, as well as the U.S. and global economy. At the same time, events during the past few years have reminded the world that space is no longer a pristine or unchallenged domain, but one that is subject to consequential mishaps, whether malicious or unintended. This was apparent in the aftermath of last year's Iridium/Cosmos satellite collision, which removed any uncertainty about the destructive threat of space objects. We need sustained investment to provide comprehensive SSA, actionable collision avoidance (conjunction) analysis, robust on-orbit space constellations, and modeling and simulation capabilities.

The importance of SSA to effective and sustained space operations grows each day. Trackable space debris grows each time existing debris collides or breaks apart, new objects enter orbit, or our sensors improve to reveal increasingly smaller objects. Despite significant SSA investments and advances to ensure our freedom of action in space, debris growth (4,600 objects in 1980; more than 21,000 today) continues to outpace SSA upgrades. This places a new urgency on improving SSA sensors and the technical and human capital resources performing collision avoidance analysis. In addition to maintaining critical legacy capabilities, new investments must focus on sensors, data fusion, network linkages, and our human capital base.

Most of today's sensors reside on legacy missile-warning platforms in the northern hemisphere. This coverage remains important but is inadequate for today. We must continue to work with international partners to expand the few sensors that make up our current capability. Further, we must provide space operators the same situational awareness we expect in every other domain, along with the tools and information to operate and protect national assets. The next generation of SSA sensors will provide coverage from space itself—a new vantage point. The Space Based Surveillance System (SBSS) will provide such coverage, and we continue to support this important step forward.

A noteworthy SSA advancement began when Congress authorized the Air Force's pilot program on the desirability and feasibility of providing collision avoidance data to commercial and non-U.S. government partners. After the successful development of the Commercial and Foreign Entities (CFE) program, DoD transitioned operational responsibility for CFE from the Air Force to USSTRATCOM's Joint Functional Component Command for Space (JFCC Space) in 2009. JFCC Space's Joint Space Operations Center (JSpOC) at Vandenberg Air Force Base now provides important data to prevent collisions between satellites, manned space craft, and debris. In this effort, cooperative relationships between DoD and owner-operators are essential to developing behavioral norms for responsible space-faring nations. USSTRATCOM will continue to refine collision-avoidance measures, sponsor agreements with space-faring nations and commercial entities, and foster greater mutual support through allied and partner engagements.

Another consequential area of space interest lies in how we manage the sustainment of our current constellations. The past decade's strong focus on improving efficiency and cost effectiveness now threatens the uninterrupted delivery of several essential capabilities, as requirements for increasingly complex and efficient systems push delivery timelines to the

future, exhaust our stock of replacement vehicles, increase costs, and leave capabilities at risk. We worked closely in the last year with a variety of independent commissions, studies mandated by Congress, and DoD examinations that revealed shortfalls in capacity and capabilities in the next five to seven years. Program schedule delays, cost overruns, dwindling inventories, and over confidence derived from our highly successful launch record could create the circumstance where just a single launch failure creates a capability gap.

Lastly, effective 21st century space operations will depend on our ability to accurately model the environment and employ simulators for training our operators. Modeling and simulation capabilities provide operators the ability to experiment, fail, adjust, and try again with a mere fraction of the resources. Once a robust simulation capability exists, new and increasingly complex exercises can demonstrate successes and vulnerabilities, facilitate new tactics, techniques, and procedures, and dramatically expand our understanding of, and ability to operate within, the space domain. The ability to experiment with new platforms and capabilities will enhance U.S. freedom of action and further improve U.S. space operations in a way that further aligns space and space-based capability requirements with those in every other domain.

CYBERSPACE

Interest in the cyber domain grows daily. Most of this is positive, as technology connects the world and enables commerce, communication, transit, and research in ways never before imagined. The practical reality of Moore's Law[2] is a world where many technological platforms seem obsolete just as they are widely fielded. Unfortunately, as Secretary of State Clinton noted in January, "these technologies are not an unmitigated blessing." We can anticipate that adversarial actors will make cyberspace a battle front in future warfare. Even today, intrusions

[2] Moore's Law, named for Intel co-founder Gordon E. Moore, is the observation that processing speed and memory capacity for commercially available computers tend to double about every two years.

and espionage into our networks, as well as cyber incidents abroad, highlight the unprecedented and diverse challenges we face in the battle for information.

In May of 2009, the Administration finished a detailed Cyberspace Policy Review. It concluded that "the architecture of the Nation's digital infrastructure…is not secure or resilient" and "without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself." Both the White House's Cyberspace Policy Review and the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency concluded that national cyber security requires dramatically enhanced policy and operational coordination. These reports highlighted the need for a uniform, rapid, dynamic, and machine-speed approach. Such an approach demands a culture of responsibility and an "always-on" enterprise infrastructure to support global employment of our military forces.

USSTRATCOM is responsible for operating DoD information networks, planning against cyber threats, advocating for new capabilities, and coordinating with other commands and Agencies. I noted last year that cyberspace is our least mature line of operation, and it is likely to remain so for some time, as cyberspace presents new and unique challenges and opportunities. Cyber operations revolutionize the way we move information, conduct commerce, and fight wars. We have had technological revolutions before, most notably a century ago when people first took to the skies. Some wondered why we would ever need to fly, but no one today can imagine life without air travel or national security without air forces. In the 1970s, few people felt they would ever need a personal computer, but a network outage today is a serious concern for the largest corporations, the smallest businesses, and most American households. Just as the U.S. mastered the air domain, we will continue to strive to preserve our freedom of action in cyberspace.

Significant change seldom comes without a seminal event. In the strategic and space arenas, we have experienced nuclear procedure issues, the Iridium-Cosmos satellite collision, and China's Anti-Satellite (ASAT) weapon tests. Last year, the cyberspace domain had just such an event as DoD information networks experienced a serious intrusion, resulting in a ban on removable media and other corrective actions. The event identified best practices and shortcomings in network security procedures and hardware accountability, causing us to ask not just what we knew about network health but how we knew it—and whether that information was reliable. Our forces developed new network monitoring and evaluation systems and grappled with the security needs of sprawling networks where low cost and efficiency have often taken priority over security. Cyberspace weaves through our lives in ways that make network problems a concern for everyone. Each and every individual user is a critical element of cyber defense.

Our national defense capabilities are now underpinned by the assured availability of the enterprise IT infrastructure and our command–and-control and information-sharing systems. These constitute the DoD information networks. USSTRATCOM must continue to defend while actively improving DoD information networks—interdependent imperatives—with new and expanded cyber capabilities. The networks requires improved defense-in-depth measures from the perimeter down to individual users, like the Host-Based Security System (HBSS), and a shareable, common operating picture that allows for the free flow of information among the combatant commanders, Services, and Agencies.

Additionally, we require continued Congressional support for critical DoD programs and initiatives through which we build, operate, harden, and assure robust and resilient command-and-control and information-sharing systems. These programs and initiatives include globally

diverse terrestrial and satellite communications networks, emerging commercial satellite communication capabilities, and the globally available enterprise IT services that reside on them.

GLOBAL SYNERGY – Joint Enabling Missions

INTEGRATED MISSILE DEFENSE

Many rogue actors consider terror, blackmail, and weapons of mass destruction to be increasingly attractive capabilities. The recently completed BMDR notes the growing threat of ballistic missiles as they become more flexible, mobile, survivable, reliable, and accurate from greater ranges. Countering the growing desire among many states for such cost-effective weapons and symbols of national power requires sustained and carefully designed missile defense investments.

As the lead combatant command for missile-defense advocacy, USSTRATCOM continues to work closely with the Services, Missile Defense Agency, and the Missile Defense Executive Board (MDEB) to shape investments. Improvements in sensor and shooter platforms, including upgrades to the Aegis weapon system and Standard Missile-3 (SM-3), production of the Terminal High Altitude Area Defense (THAAD) system, and fielding of the AN/TPY-2 forward-based X-band radar provide more effective capabilities for our geographic combatant commanders. However, these advances have required an increased focus at USSTRATCOM and within the MDEB and Global Force Management processes on how best to satisfy the requirements of multiple geographic combatant commanders while appropriately balancing theater and homeland defense efforts. Strong Congressional support is enabling the rapid fielding of regional systems.

One of the most significant recent missile defense developments is the Administration's Phased Adaptive Approach (PAA) to missile defense. Given necessary funding and timely fielding, PAA offers an effective and flexible way to address the growing Iranian threat. PAA

also addresses the most urgent threats first with proven, cost-effective platforms as we continue to defend our forward-deployed forces and allies. It also requires that missile defense becomes an increasing part of our international cooperation efforts. The total effect of PAA will provide significantly more capability to counter today's regional threats and improve our ability to defend the United States against any future Iranian ICBM.

A defensive system, however, will be ineffective if not supported by accurate and timely warning and intelligence. Ballistic missiles and space launch vehicles share significant similarities, making launch characterization—the ability to rapidly determine a vehicle's ballistic or orbital trajectory and therefore its intent—essential to recommending appropriate pre-launch postures and post-launch actions. USSTRATCOM's ongoing efforts to refine this capability include sensor and communications upgrades and analytical expansion. As noted above, we face ongoing challenges to sustaining our missile warning constellation's long-term health. The SBIRS geostationary orbit satellite constellation is critical to any missile defense architecture. Additionally, the two Space Tracking and Surveillance System (STSS) demonstrator satellites launched in late 2009 will validate key concepts for a future missile defense satellite constellation. The STSS has the potential to greatly improve our ability to detect, track, and defeat ballistic missiles.

COMBATING WEAPONS OF MASS DESTRUCTION (CWMD)

The specter of weapons of mass destruction (WMD) in the hands of terrorists poses a threat to the United States, our allies, and global security at large. USSTRATCOM is responsible to synchronize DoD-wide planning for counter-WMD (CWMD). Our CWMD campaign plan framework, detailing linkages between military strategic objectives and desired effects, has become the CWMD planning standard for geographic combatant commands.

To further enhance regional combatant commander and interagency planning, USSTRATCOM has developed a Joint Elimination Coordination Element in order to support WMD elimination efforts. This unit will also support DoD efforts to establish a Joint Task Force-Elimination headquarters to provide specialized command and control for WMD elimination operations. Additionally, USSTRATCOM has advanced the development of the Interagency CWMD Database of Responsibilities, Authorities, and Capabilities (INDRAC) system to inform planning, training, advocacy, and other partnerships across the government. Further, we lead semiannual Global Synchronization Conferences to enhance CWMD planning across other commands, the broader whole of government, and our key allies and partners.

To improve the nation's existing capabilities for nuclear forensics and attribution, we are sponsoring a Joint Capabilities Technology Demonstration (JCTD) for National Technical Nuclear Forensics (NTNF). It is designed to improve existing air- and ground-sample collection capabilities. In coordination with U.S. Joint Forces Command, we have conducted a series of experiments to determine the best uses of active interrogation technology to extend the detection ranges of our nuclear and radiological passive detectors. DoD has proposed additional CWMD funding in its Fiscal Year 2011 budget for DoD nonproliferation, counterproliferation, and consequence management programs to accelerate the closure of capability gaps. This additional funding would be applied to nuclear and biological threat reduction; combating nuclear terrorism; nuclear search, detection, and forensics; technical reachback and planning support for the combatant commanders; and integration of CWMD technical, operational, and intelligence expertise for improved WMD threat anticipation and response. We fully support these investments and the efforts of the Defense Threat Reduction Agency (DTRA).

Finally, the USSTRATCOM Center for Combating WMD (SCC WMD) plays a key role in the Proliferation Security Initiative (PSI), a proven counterproliferation architecture. This past

year SCC WMD supported the embedding of PSI activities into a number of combatant commands' exercise programs, developed international PSI training scenarios, and published the first PSI exercise planning handbook. We look forward to accelerating exercise engagements and increasing our focus on potential sources of proliferation.

INFORMATION OPERATIONS

With the exception of psychological operations (PSYOP), USSTRATCOM plans, coordinates, supports, and advocates for information operations (IO) across geographic combatant commands' areas of responsibility. We execute these responsibilities through our joint components: JFCC NW and JTF GNO for cyber operations; and the Joint Information Operations Warfare Center (JIOWC) for electronic warfare (EW), military deception (MILDEC), and operational security (OPSEC).

This year, we will participate in reviews of joint and Service doctrine to evaluate and assess how we conduct warfare in the information environment. Additionally, we are conducting a Strategic Communication Capabilities Based Assessment (CBA), as tasked by the JROC. This CBA will identify requirements and capability gaps among the combatant commands and Joint Staff, including perspectives from the intelligence community, in order to standardize terminology and to resource appropriate DoD strategic communication capabilities.

A wide range of military operations depend on unfettered access to the electromagnetic spectrum. For several decades, forces have taken advantage of relatively uncontested access to the electromagnetic spectrum, but spectrum requirements are growing not only for DoD missions but across Federal agencies, state, and local governments and commercial industry. Further, rapidly expanding spectrum usage and technology evolution now threaten to impede our ability to conduct successful military operations. As regions of the spectrum continue to be crowded by commercial and scientific entities and other nations, the warfighter's electromagnetic maneuver

space will become more restricted. Future spectrum policy and use must carefully consider and balance national and economic security interests to enable commercial growth while protecting the equities of DoD and federal agencies.

To address these accessibility concerns and to preserve essential information transfer capabilities, the JROC approved the USSTRATCOM EW CBA. USSTRATCOM also produced a follow-on Initial Capabilities Document (ICD) that identified capability gaps and potential solutions. The ICD also emphasized the need for focused leadership in the EW area and a comprehensive joint investment strategy. In the coming year, and in conjunction with federally funded research and development centers, USSTRATCOM and U.S. Joint Forces Command will study approaches to responding to emerging electromagnetic threats. This review is intended to identify organizational and management approaches that will enable timely, prioritized, and effective EW resourcing decisions.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

Over the past decade, geographic combatant commanders' requirements have increased ISR demand, as highlighted in Iraq and Afghanistan. New and irregular threats reshaped the battlefield and the information required to operate successfully. Today, rapidly increasing capabilities to support the warfighter remain a key geographic combatant commander priority. Determining the appropriate ISR force size is important, given limited resources and dynamic theater needs. USSTRATCOM is leading efforts to develop an ISR force-sizing construct for the Department. This initiative will develop a sound analytical foundation for future ISR allocation and procurement decisions.

To date, DoD has rapidly expanded ISR platform acquisition and fielding, thereby broadening theater access to intelligence. To complement this initiative and as a key facet to meeting the rising demand for ISR products, DoD is also expanding our processing, exploitation,

and dissemination (PED) capabilities. Rapid collection-capability growth challenges our ability to transform raw data into information of intelligence value and to disseminate it to combat forces in a timely fashion. USSTRATCOM continues to advocate for needed PED capabilities with the Services and combat-support agencies and is also developing methods to align ISR allocation with PED capacity to ensure collection effectiveness and to better integrate existing resources. Finally, new assets and new challenges require bases from which to access many regions, such as USAFRICOM's Camp Lemonnier, Djibouti. This important facility deserves sustained support because it provides access to multiple countries and the Horn of Africa while enabling the employment of air and naval assets supporting DoD operations in the region.

As new ISR capabilities come on line, we must transition legacy capabilities to new systems. The Air Force has fielded the first Global Hawk in theater, but challenges remain before it could replace today's U-2 capability. Chief among these is sufficient wideband satellite communications to permit necessary throughput in the Global Hawk communications architecture. USSTRATCOM is working to make sure that a comprehensive communications capability is capable of providing worldwide support prior to the U-2 retirement.

Whether making carefully nuanced deterrence recommendations, evaluating space capabilities, understanding the new and dynamic cyberspace domain, or sustaining our superior strategic capability knowledge base, intelligence provides operational context fundamental to every commander's decision calculus. Since I assumed command of USSTRATCOM in the fall of 2007, my intelligence directorate has done tremendous work using limited resources to support our three lines of operations and our enabling missions. Recently, we received a modest but essential increase in intelligence billet authorizations to establish the USSTRATCOM Joint Intelligence Operations Center (JIOC). This important investment will increase our headquarters capabilities to provide the level of strategic intelligence we require and to distribute appropriate

capabilities to several of our components. We are also working with the Office of the Under Secretary of Defense for Intelligence to establish a second Joint Intelligence Operations Center to support USCYBERCOM. We appreciate continued Congressional support for these initiatives.

CONCLUSION

USSTRATCOM continues to enhance our ability to deliver global security for America each and every day. We have re-emphasized the importance of our nuclear deterrence mission and proven America's long held confidence in our nuclear forces, while also expanding capabilities crucial to operating in the space and cyberspace domain. We enable many space-based and cyberspace capabilities essential to military operations and daily life by sustaining our freedom of action in these domains. USSTRATCOM's uniquely global missions support national objectives, whole-of-government solutions, regional requirements, and enhanced cooperation with our international partners. While many challenges remain in our increasingly interconnected and rapidly changing world, USSTRATCOM is fully engaged to address them. We greatly appreciate the support of the Congress.