The Institute for Foreign Policy Analysis, Inc. (IFPA), now in its thirty-fifth year, develops innovative strategies for new security challenges. IFPA conducts studies, workshops, and conferences on national security and foreign policy issues and produces innovative reports, briefings, and publications. IFPA’s products and services help government policymakers, military and industry leaders, and the broader public policy communities make informed decisions in a complex and dynamic global environment. With offices in Cambridge, Massachusetts, and Washington, D.C., the Institute maintains a global network of research advisors and consultants.

The International Security Studies Program (ISSP) is dedicated to teaching and research across the international security spectrum. As one of the largest fields of study within the multidisciplinary curriculum of The Fletcher School, Tufts University, the ISSP offers a full schedule of graduate-level courses and seminars. The ISSP sponsors a diverse range of “outside the classroom” educational activities, including annual conferences devoted to critical defense-related issues, a simulation exercise, a lecture series, field trips, and publications.

The Air Force Chief of Staff’s Strategic Studies Group (CSAF SSG) provides the CSAF with strategic assessments, options, and recommendations concerning military and national security strategy, and supports the CSAF in his role as a member of the Joint Chiefs of Staff. It conducts independent analyses of proposed policies, strategies, and Air Force concepts. In performing these tasks, the CSAF SSG undertakes studies informed by leading-edge information, perspectives, and judgments from across the USAF and allied air forces, think tanks, academia, and the interagency and joint community. Advisory in nature, the CSAF SSG does not make policy, management, or acquisition decisions.

The Defense Threat Reduction Agency (DTRA) safeguards America and its friends from weapons of mass destruction (chemical, biological, radiological, nuclear, and high explosives) by reducing the present threat and preparing for future threats. Under DTRA, Department of Defense resources, expertise and capabilities are combined to ensure the United States remains ready and able to address the present and future WMD threat environment.
38th IFPA-Fletcher Conference on National Security Strategy and Policy

Air, Space, & Cyberspace Power in the 21st-Century

January 20–21, 2010
Ronald Reagan Building and International Trade Center

FINAL REPORT

From a conference organized by

The Institute for Foreign Policy Analysis
International Security Studies Program of
The Fletcher School, Tufts University

Co-sponsored by

The Air Force Chief of Staff’s Strategic Studies Group

With the support of

The Defense Threat Reduction Agency
# Contents

**Foreword** ..................................................................................................................... vii

**Executive Summary** .................................................................................................... x

  Interrelated Conclusions ...................................................................................... xiii

  Closing Conference Thoughts .............................................................................. xvii

**Introduction** .................................................................................................................. 1

  The United States as an Aerospace Nation: .............................................. 2

  Challenges and Opportunities

**The 21st Century Security Setting: Implications** .............................................. 6

  for USAF and Joint Planning

    Technology Diffusion ......................................................................................... 7

    Proliferation Trends .......................................................................................... 7

    Anti-access/Access Denial Technologies ....................................................... 11

    Challenges to U.S Space Dominance ............................................................. 12

    Cyber Warfare .................................................................................................... 13

    Critical Infrastructure Protection and EMP Threats .................................. 15

    China: Adversary or Partner? .......................................................................... 17

    Unconventional Warfare Challenges and Terrorist Threats .................. 19

    The Second Nuclear Age and Post-Cold War ........................................... 21

    and Post 9/11 Deterrence

**Deterrence in a Multi-nuclear World** .......................................................... 21

  and Allied/Partner Reassurance

    Rebuilding and Investing in the Nuclear Enterprise: ........................... 26

    Global Strike Command

    Non-nuclear Strategic Strike ............................................................................. 27

    Nuclear Weapons, Dual-Capable Aircraft, .................................................. 28

    and NATO Deterrence

    Non- and Counter-proliferation and ................................................................. 28

    Cooperative Threat Reduction

**Airpower from Service and** .......................................................... 32

  Combatant Command Perspectives

    North American Aerospace Defense ............................................................. 32

    and U.S. Northern Command

    U.S. Transportation Command .................................................................. 34

    U.S. Special Operations Command ............................................................... 36
U.S. Joint Forces Command .......................................................37
Airpower and the U.S. Navy .........................................................39
Airpower and the U.S. Marine Corps ..........................................41

International Perspectives: Developing Global Partnerships .. 43
  Leveraging NATO Capacities for USAF Planning ....................44
  Allied Country Perspectives .......................................................48

Identifying Future Force Structure Needs ..................................57
  Winning Today’s Wars and Preventing Tomorrow’s ..................57
  Confronting High-end and Asymmetric Threats ..............59
  Balancing Future Capability Requirements .................................60

Devising an Acquisition Strategy to Develop, Build, and Maintain USAF Force Structure
  Reconciling Budget Constraints with .........................................68
  Modernization Needs
  Restoring and Developing Critical Technical Expertise ..........70
  Sustaining the Defense Industrial Base and ......................72
  Leveraging the Private Sector

Strategic Surprise and Wildcard Considerations ..........................74

Aligning the Air Force Vision with the Future Security Setting ..........................77

Interrelated Conclusions ..........................................................79

Closing Conference Thoughts .....................................................85

Glossary of Terms and Acronyms ..............................................87
On January 20–21, 2010, the Institute for Foreign Policy Analysis (IFPA), in association with the International Security Studies Program (ISSP) of The Fletcher School, Tufts University, convened the 38th IFPA-Fletcher Conference on National Security Strategy and Policy. This conference, entitled *Air, Space, and Cyberspace Power in the Twenty-first Century*, was co-sponsored by the Air Force Chief of Staff’s Strategic Studies Group (CSAF SSG) with the support of the Defense Threat Reduction Agency (DTRA). As with previous conferences in the IFPA-Fletcher series, this meeting was designed to provoke frank and in-depth discussions about key and emerging national security issues. Its focus was air, space, and cyber power. Conference sessions addressed such topics as deterrence, dissuasion, and war prevention; forward basing, alliances, and international security cooperation; emerging global security trends; homeland defense; and humanitarian and disaster relief.

It is obvious that no vision of twenty-first-century U.S. national security can be complete without air and space as well as cyberspace. The surface of the globe consists entirely of land and the seas. Before the advent of airpower, all armed conflicts were fought on land or at sea. Since the Earth in its entirety – land and sea – is surrounded by airspace, only air and space afford the fullest and most rapid mobility with truly global range – capable of operating above any part of the Earth’s surface – land or sea – unconstrained by the barriers of the
Air, Space, and Cyberspace Power in the Twenty-First Century

seas or land, by narrow straits or high mountains. Only airpower can move unfettered by geography.

It was only with the coming of manned flight and then the space age that such global reach and rapid mobility became fully possible. No nation has succeeded more fully than the United States in incorporating such a vision, together with a supporting aerospace strategy, into its military capabilities. Airpower led us out of the Cold War and into the success of Desert Storm. Airpower proved indispensable in Kosovo and again in Iraq and now in Afghanistan. Airpower stands guard as we meet today’s homeland security challenges. Airpower is vital to humanitarian operations.

As Alexander P. de Seversky, one of the great strategists of airpower in its formative years, pointed out in a seminal article in the August 1955 issue of *Air Force Magazine*: “Airpower is the ability of a nation to assert its will via the air medium. Freedom of air navigation when maintained by one side through successful, sustained combat is known as air superiority.” It is this basic principle that has informed our vision of airpower for more than half a century. How this fundamental tenet is adapted to twenty-first-century challenges was the focus of the conference on which this report is based.

With this focus in mind, we designed the conference to provide first an overview of the twenty-first-century security setting with the broad spectrum of threats against which aerospace power must be developed extending from the high to the low end, from peer competitors to irregular warfare. We then addressed dissuasion and deterrence requirements, which differ dramatically today from the Cold War era, encompassing nuclear and conventional components as well as states and non-state actors. Next we examined operational-level issues such as force structure and modernization priorities across the spectrum of contingencies. Then we considered the challenges of balancing capabilities with modernization priorities and devising a necessary acquisition strategy in light of such challenges as maintaining critical skills and addressing budgetary shortfalls and operating within a shrinking R&D community and technological/industrial base.

We then turned our attention to international perspectives and the role of U.S. allies and coalition partners as we and they work to leverage our respective capabilities and to maximize resulting synergisms. We benefited from regional and combatant command perspectives. Throughout the conference, as reflected in this report, there was a focus on cyberspace. Together with international space, international waters, and space, cyberspace constitutes one of the four global commons.
This conference presented an unusual opportunity to break free of intellectual blinders, isolation, and possible groupthink to explore new ideas and to connect the dots outside the box. For each of the sessions we brought together a broad range of expertise – from the civilian and military communities, from the government and private sector, from the United States and abroad. In the audience we also had a vast array of expertise, knowledge, and experience from which the conference and this report benefited. This report is published to give broader dissemination to the topics and issues addressed at the conference. Building on the various presentations and discussions, this report is designed as a contribution to the ongoing effort, within and outside the United States Air Force, to understand and integrate aerospace and cyberspace as fully as possible into national security strategy and policy. Because this report was prepared in the months following the conference, it includes references to subsequent events and additional information.

Further conference data, including speaker transcripts, PowerPoint presentations, and the agenda, can be found online at http://www.ifpafletcherconference.com/.

Robert L. Pfaltzgraff, Jr.
President, Institute for Foreign Policy Analysis
and Shelby Cullom Davis Professor of International Security Studies
The Fletcher School, Tufts University
On January 20–21, 2010, the Institute for Foreign Policy Analysis (IFPA), in association with the International Security Studies Program (ISSP) of The Fletcher School, Tufts University, convened the 38th IFPA-Fletcher Conference on National Security Strategy and Policy. Entitled Air, Space, and Cyberspace Power in the Twenty-first Century, this conference was co-sponsored by the Air Force Chief of Staff’s Strategic Studies Group (CSAF SSG) with the support of the Defense Threat Reduction Agency (DTRA). The spectrum of contingencies for which U.S. airpower plays an indispensable role extends from the high end to low end, encompassing near-peer competitors as well as armed non-state actors. The United States must prepare for regular and irregular warfare, and for hybrid warfare, which includes regular and irregular elements.

Several key themes emerged from conference discussions:

- The United States Air Force (USAF) must be prepared to fight wars simultaneously across the spectrum of conflict, as irregular warfare, hybrid warfare, and major conventional operations are all likely to take place in the emerging global security environment.

- Air Force capabilities are increasingly vulnerable to attack. The USAF needs to address issues of protection, including defense of installations, redundancy of capabilities, and survivability of assets.

- The air, sea, space, and cyber domains will be increasingly contested as additional states and non-state actors acquire advanced technologies.

- The USAF needs to work jointly with the other services, especially the Navy, and with allies to leverage capabilities; increase flexibility, interoperability, and sustainability; and preserve America’s ability to project air and naval power into potentially contested regions – such as the Western Pacific,
the Persian Gulf, and the Arctic – vital to U.S. national security.

- States and other actors are increasingly empowered to wage asymmetric warfare against the United States, encompassing potential kinetic and non-kinetic attacks such as cyber war, jamming, anti-satellite (ASAT), and electromagnetic pulse (EMP).
- Improving joint service integration, planning, and interoperability is increasingly important, as is building partnerships with allies, non-governmental organizations (NGOs), and the whole of the U.S. government.

These key themes were based on several basic trends and issues, all of which will have important implications for the Air Force:

- Technology proliferation in general, made possible by easily accessible computing power and enabling or contributing to the following:
  - Diffusion of ballistic and cruise missile technology and the proliferation of precision munitions
  - Proliferation of weapons of mass destruction (WMD)
  - Development of anti-access/area-denial (A2/AD) technologies
  - Challenges to U.S. space dominance, including ASAT capabilities and EMP threats
  - Cyber warfare
  - Unconventional warfare challenges and terrorist threats
- The future of nuclear and non-nuclear strategic deterrence
- Joint Strike Fighter (JSF) procurement and modernization of dual-capable aircraft (DCA)
- The potential for strategic surprise

Conference participants identified several areas that must be addressed to hedge against strategic surprise, including the need to:

- Examine new command-and-control (C2) network concepts to find ways to address bandwidth constraints facing U.S. forces today. In the cyber arena, the USAF should consider next-generation computer network operations, firewalls, and internet protocols for assured access to government networks.
- Retain the U.S. edge in stealth technologies in the face of increasingly sophisticated enemy integrated air defense environments and near-peer competitor deployment of fifth-generation fighter aircraft. For this purpose continuing cutting-edge electronic warfare, a key enabling capability across the conflict spectrum, is essential.
• Continue development of unmanned technologies for a range of missions. Crucial to twenty-first-century warfare, unmanned vehicles should focus on increased loiter time and enhanced capacities to deal with emerging threats. The exploration of next-generation target discrimination technologies is important especially where the risk of collateral damage is high.

• Develop new sensing technologies to find, fix, and track mobile and high-value targets. If WMD are used, the military services will be tasked with a range of consequence management missions. Preparations to meet WMD emergencies can be gauged through simulations and interagency exercises, including regeneration of the Top Officials (TOPOFF) series supported by U.S. Joint Forces Command (JFCOM).

• Develop forensics capabilities to attribute WMD and cyber attacks accurately and quickly. This will require better cooperation both across U.S. government agencies as well as with U.S. allies and partners.

• Prepare for catastrophic failure of communications systems in the event of an ASAT, EMP, or cyber attack. Pursuit of next-generation protection for space systems is crucial, as is the exploration of alternative and complementary capabilities for space-based networks assets.

• Develop programs to foster cultural awareness and language proficiency for Air Force personnel. The USAF should support and further promote a culture in which educational opportunities are considered essential to career advancement. Greater investment in graduate school programs and USAF officer participation in fellows programs will enhance the Air Force’s capacity to operate in multinational and interagency environments, contribute to USAF security cooperation, and support U.S. national security goals.

• Develop alternative energy sources for aircraft propulsion and other ways to reduce energy costs. The present U.S. dependency on petroleum, especially by the USAF, which consumes more petroleum products than any other government entity, makes it vulnerable to the threat of another oil shock or energy-price increases. The need for alternative energy sources should be a research and development (R&D) priority for the Air Force and DoD.
INTERRELATED CONCLUSIONS
Several interrelated conclusions emerged from the conference and focused on the following: deterrence strategy, the nuclear enterprise, the U.S. basing infrastructure, the A2/AD threat, asymmetric challenges, space dominance, cyber security, organizational change and joint force operations, combatant command (CO-COM) support, engagement and international security cooperation, acquisition reform and affordability, and support to civil authorities.

Deterrence Strategy
In stark contrast to the bipolar Cold War nuclear setting, today’s security environment includes multiple, independent nuclear actors. Some of these independent nuclear weapons states are potential adversaries, some are rivals, and some are friends, but the initial decision for action by any one of them may lie beyond U.S. control. The United States may need to influence, signal, and restrain enemies, and it may need to continue to provide security guarantees to non-nuclear friends and allies. America may also face catalytic warfare, where, for example, a U.S. ally such as Israel or a third party such as China could initiate action that might escalate to a nuclear exchange. Although the United States would not be a party to the nuclear escalation decision process, it could be drawn into the conflict. Compared to a bipolar world, very little is known about strategic nuclear interaction and escalation in a multipolar world. The U.S. nuclear deterrent must restrain a wider variety of actors today than during the Cold War. This requires a range of capabilities and the capacity to address specific challenges. The deterrent must provide security guarantees and assurance sufficient to prevent the initiation of catalytic warfare by an ally, while deterring an adversary from resorting to nuclear escalation. America may also need simultaneously to deter more than one nuclear state.

Deterrence requirements include four critical elements: early warning, C², delivery systems, and weapons. The Air Force plays an indispensable role in furnishing the U.S. early warning system in its entirety through satellites and radar networks. In command and control, infrastructure is provided by the Air Force, including Milstar satellites and, in the future, advanced extremely high frequency (AEHF) satellites. In the area of delivery systems and weapons, two-thirds of the strategic triad – intercontinental ballistic missiles (ICBMs) and bombers – is furnished by the Air Force and its Global Strike Command.
U.S. Overseas Basing and the Anti-Access/Area-Denial Threat

The increased availability of anti-access/area-denial assets coupled with growing threats to the sea, air, space, and cyberspace commons are challenging the power projection capabilities of the United States. These threats, in the form of aircraft and long-range missiles carrying conventional or nuclear munitions, present problems for our overseas bases. States such as North Korea, China, and Iran jeopardize the notion that forward-deployed U.S. forces and bases will be safe from enemy attack. Consequently, the United States must create a more flexible basing structure encompassing a passive and active defense posture that includes these features: dispersal, hardening, increased warning time of attack, and air defenses. Simultaneously, the United States must continue to develop long-range, offensive systems such as low-observable manned and remotely piloted strike aircraft, precision missiles, and intelligence, surveillance, and reconnaissance (ISR) platforms to penetrate heavily defended A2/AD environments. This approach will increase the survivability of U.S. forward-deployed assets and power projection capabilities and thus bolster deterrence and U.S. guarantees to America’s allies and friends.

Asymmetric Challenges

The increasing number of actors gaining access to advanced and dual-use technologies augments the potential for asymmetric attacks against the United States and its allies by those who are unable to match U.S. military capabilities. Those actors pose increasing challenges to the ability of the United States to project power through the global commons. Such attacks could target specific U.S. vulnerabilities, ranging from space assets to the financial, transportation, communications, and/or energy infrastructures, and to the food and water supply, to mention only the most obvious. Asymmetric attacks denying access to critical networks and capabilities may be the most cost-effective approach to circumventing traditional U.S. force advantages. The USAF and DoD must develop systems and technologies that can offset and defend against asymmetric capabilities. This will require a robust R&D program and enhanced USAF cooperation with its sister services and international partners and allies.

Space Dominance

Space is increasingly a contested domain where U.S. dominance is no longer assured given the growing number of actors in space and the potential for kinetic and non-kinetic attacks, including
ASAT weapons, EMP, and jamming. As a result, the United States must protect vital space-based platforms and networks by reducing their vulnerability to attack or disruption and increasing the country’s resilience if an attack does occur. Required steps include hardening and incorporating stealth into next generation space systems and developing rapid replenishment capacity (including micro-satellite technologies and systems and new launch capabilities). At the same time, America must reduce its dependence on space capabilities with air-based substitutes such as high altitude, long endurance, and penetrating ISR platforms. Increased cooperation among the services and with U.S. allies to develop such capabilities will also be paramount.

**Cyber Security**

Cyber operations are vital to conducting USAF and joint land, sea, air, and space missions. Given the significance of the cyber threat (private, public, and DoD cyber and information networks are routinely under attack), the United States is attempting to construct a layered and robust capability to detect and mitigate cyber intrusions and attacks. The USAF’s cyber operations must be capable of operating in a contested cyber domain to support vital land, sea, air, and space missions. USAF cyberspace priorities include developing capabilities to protect essential military cyber systems and to speed their recovery if an attack does occur; enhancing the Air Force’s capacity to provide USAF personnel with the resolution of technical questions; and training/recruitment of personnel with cyber skills. In addition, the USAF and DoD need to develop technologies that quickly and precisely attribute attacks in cyberspace. Cyber attacks can spread quickly among networks, making it extremely difficult to attribute their perpetrator, and therefore to develop a deterrence strategy based on retaliation. In addition, some cyber issues are in the legal arena, including questions about civil liberties. It is likely that the trend of increased military support to civil authorities (for example, in disaster relief operations) will develop in the cyber arena as well. These efforts will entail greater service, interagency, international, and private-sector collaboration.

**Organizational Change and Joint Force Operations**

To address growing national security challenges and increasing fiscal constraints, and to become more effective, the joint force needs to adapt its organizations and processes to the exigencies of the information age and the security setting of the second decade of the twenty-first century. This entails developing a strategy
that places increased emphasis on joint operations in which each service acts in greater concert with the others, leverages capacities across the services (two land services, three naval services, and five air services) without duplicating efforts, and encourages interoperability. This would provide combatant commanders (CCDRs) with a greater range of capabilities, allowing heightened flexibility to use force. A good example of this approach is the Air-Sea Battle concept being developed jointly by the Air Force and Navy, which envisions heightened cooperation between the two services and potentially with allies and coalition partners.

**Intelligence, Surveillance, and Reconnaissance Capabilities**

There is an increasing demand for ISR capabilities able to access and persist in contested airspace in order to track a range of high-value mobile and hard-to-find targets, such as missile launchers and underground bunkers. This increases the need for stealthy, survivable systems and the development of next-generation unmanned platforms. The USAF must continue to emphasize precision targeting, both for strike and close-air-support missions. High-fidelity target identification and discrimination enabled by advanced radars and directed-energy systems, including the ability to find, track, and target individuals within a crowd, will provide battlefield commanders with improved options and new opportunities for leveraging joint assets.

**Engagement and International Security Cooperation**

Allies and coalition partners bring important capabilities from which the USAF and other services have long benefited. For example, allies and coalition partners can provide enhanced situational awareness and early warning of impending crises as well as assist in understanding the interests, motivations, traditions, and cultures of potential adversaries and prospective coalition partners. Moreover, foreign partner engagement and outreach are an avenue to influence partner and adversary perspectives, thus shaping the environment in ways favorable to U.S. national security interests. Engagement also may be a key to realizing another Air Force and joint priority: to sustain or gain access to forward operating bases and logistical infrastructure. This is particularly important given the growing availability of A2/AD assets and their ability to impede U.S. power projection capabilities.
Procurement Choices and Affordability

The USAF needs to field capabilities to support current operations and pressing missions while at the same time pursuing promising technologies to build the force of the future. Affordability, effectiveness, time urgency, and industrial base issues inevitably shape procurement choices and reform. The Air Force must maintain today’s critical assets while also allocating resources to meet future needs. Given the long lifespan anticipated for many weapon systems, planners need to make the most reliable cost estimates and identify problems at the outset of a weapons system’s development phase so that they can be corrected as early and cost-effectively as possible.

Support to Civil Authorities

As evidenced in the aftermath of the 2010 earthquakes in Haiti and Chile (the Chile earthquake hit after this conference), the USAF has a vital role to play in the U.S. response to international relief operations and support to civil authorities. In Haiti, the USAF reopened the airport and deployed contingency response elements, while also providing ISR support for the joint forces in the theater. In Chile, USAF satellite communication capabilities were critical to the recovery and relief efforts. USAF civil support roles are likely to grow to include greater use of the Reserve Components. Consequently, USAF planners should reassess the active and reserve component mix of forces and capabilities to identify potential mobilization and requirement shortfalls.

CLOSING CONFERENCE THOUGHTS

A recurring conference theme was the need for the USAF to continue to examine specific issues of opportunity and vulnerability more closely. For example, a future initiative could include focused working groups that would examine such questions and issues as:

- How can air, space, and cyberspace capabilities best support deterrence, preserve U.S. freedom of action, and support national objectives?
- How should the USAF leadership reconceptualize its vision, institutional identity, and force posture to align as closely as possible with the future national security setting?
- What is the appropriate balance between high-end and low-end air and space capabilities that will maximize military options for national decision makers, given emerging threats and fiscal constraints?
• What are the opportunities, options, and tradeoffs for investment and divestment in science and technology, infrastructure, and programmed capabilities?

• What are additional interdependent concepts, similar to Air-Sea Battle, that leverage cross-service investments to identify and foster the development of new joint capabilities?

• What are alternative approaches to officer accessions and development to support shifting and emerging Air Force missions, operations, and force structure, including cyber warfare?

• How can the USAF best interact with Congress to help preserve or refocus the defense-industrial base as well as to minimize mandates and restrictions that weigh on future Air Force investments?

Finally, the USAF must continue to be an organization that views debate, as the Chief of Staff of the Air Force put it in his opening conference address, “...as the whetstone upon which we sharpen our strategic thinking.” This debate must also be used in pursuit of political support and to ensure that the USAF maintains and develops critical capabilities to support U.S. national security priorities. The 38th IFPA-Fletcher Conference on National Security Strategy and Policy was conceived as a contribution to that debate.
Almost a century has passed since the advent of airpower and Billy Mitchell’s demonstration of its operational potential with the sinking of the Ostfriesland on July 21, 1921. For most of that time, the United States has benefitted from the rapid development of air and space power projection capabilities, and, as a result, it has prevailed in successive conflicts, contributed to war deterrence and crisis management, and provided essential humanitarian relief to allies and friends around the world. As we move into the second decade of the twenty-first century, the U.S. Air Force (USAF), like its service counterparts, is re-assessing strategies, operational concepts, and force structure. Across the conflict spectrum, security challenges are evolving, and potential adversaries–state and non-state actors–are developing anti-access and other asymmetric capabilities, and irregular warfare challenges are becoming more prevalent. The potential exists for “hybrid” warfare in which state adversaries and/or non-state actors use a mix of conventional and unconventional capabilities against the United States, a possibility made more feasible by the diffusion of such capabilities to a larger number of actors. Furthermore, twenty-first-century security challenges and threats may emanate from highly adaptive adversaries who ignore the Geneva Conventions of war and use military and/or civilian technologies to offset our military superiority.

As it develops strategy and force structure in this global setting, the Air Force confronts constraints that will have important implications for budget and procurement programs, basic research and development (R&D), and the maintenance of critical skills, as well as recruitment, education, training, and retention. Given the dynamic nature of the security setting and looming defense budget constraints, questions of where to assume risk will demand bold, innovative, and decisive leadership. The imperative for joint
operations and U.S. military-civilian partnerships is clear, underscoring the need for a whole-of-government and whole-of-society approach that encompasses international and non-governmental organizations (NGOs).

THE UNITED STATES AS AN AEROSPACE NATION: CHALLENGES AND OPPORTUNITIES

In his address opening the conference, General Norton A. Schwartz, Chief of Staff of the Air Force (CSAF), pointed out how, with its inherent characteristics of speed, range, and flexibility, air-power has forever changed warfare. Its advent rendered land and maritime forces vulnerable from the air, thus adding an important new dimension to warfare. Control of the air has become indispensable to national security because it allows the United States and friendly forces to maneuver and operate free from enemy air attack. With control of the air the United States can leverage the advantages of air and space as well as cyberspace. In these interdependent domains the Air Force possesses unique capabilities for ensuring global mobility, long-range strike, and intelligence, surveillance, and reconnaissance (ISR). The benefits of airpower extend beyond the air domain, and operations among the air, land, maritime, space, and cyber domains are increasingly interdependent.

General Schwartz stated that the Air Force’s challenge is to succeed in a protracted struggle against elements of violent extremism and irreconcilable actors while confronting peer and near-peer rivals. The Air Force must be able to operate with great precision and lethality across a broad spectrum of conflict that has high and low ends but that defies an orderly taxonomy. Warfare in the twenty-first century takes on a hybrid complexity, with regular and irregular elements using myriad tools and tactics. Technology can be an enabler but can also create weaknesses: adversaries with increased access to space and cyberspace can use emerging technologies against the United States and/or its allies. In addition, the
United States faces the prospect of the proliferation of precision weapons, including ballistic and cruise missiles as well as increasingly accurate mortars, rockets, and artillery, which will put U.S. and allied/coalition forces at risk. In response to mounting irregular warfare challenges American leaders have to adopt innovative and creative strategies. For its part, the USAF must develop airmen who have the creativity to anticipate and plan for this challenging environment. Leadership, intellectual creativity, capacity, and ingenuity, together with innovative technology, will be crucial to addressing these challenges in a constrained fiscal environment.

System Versatility
In meeting the broad range of contingencies – high, low, regular, irregular, and hybrid – the Air Force must maintain and develop systems that are versatile, both functionally (including strike or ISR) and in terms of various employment modes, such as manned versus remotely piloted, and penetrating versus stand-off systems. General Schwartz emphasized the need to be able to operate in conflict settings where there will be demands for persistent ISR systems able to gain access to, and then loiter in, contested or denied airspace. The targets to be identified and tracked may be mobile or deeply buried, of high value, and difficult to locate without penetrating systems. General Schwartz also called attention to the need for what he described as a “family of systems” that could be deployed in multiple ways with maximum versatility depending on requirements. Few systems will remain inherently single purpose. Indeed, he emphasized that the Air Force must purposefully design versatility into its new systems, with the majority of future systems being able to operate in various threat environments. As part of this effort further joint integration and inter-service cooperation to achieve greater air-land and air-sea interoperability will continue to be a strategic necessity.

Space Access and Control
Space access, control, and situational awareness remain essential to U.S. national security. As potential rivals develop their own space programs, the United States faces challenges to its unrestricted access to space. Ensuring continuing access to the four global commons – maritime, air, space, and cyberspace – will be a major challenge in which the USAF has a key role. The Air Force has long recognized the importance of space and is endeavoring to make certain that U.S. requirements in and for space are met and anticipated. Space situational awareness is vital to America’s ability to help evaluate and attribute attacks. Attribution, of course, is
essential to deterrence. The USAF is exploring options to reduce U.S. dependence on the Global Positioning System (GPS), which could become vulnerable to jamming. Promising new technologies, such as “cold atoms,” pseudolites, and imaging inertial navigation systems that use laser radar are being investigated as means to reduce our vulnerability.

Cyber Capabilities
The USAF continues to develop cyber capabilities to address opportunities and challenges. Cyber threats present challenges to homeland security and other national security interests. Key civilian and military networks are vulnerable to cyber attacks. Preparing for cyber warfare and refining critical infrastructure protection and consequence management will require new capabilities, focused training, and greater interagency, international, and private sector collaboration.

Challenges for the Air Force
General Schwartz set forth a series of challenges for the Air Force, which he urged conference participants to address. They included:

- How can the Air Force better address the growing demand for real-time ISR from remotely piloted systems, which are providing unprecedented and unmatched situational awareness?
- How can the USAF better guarantee the credibility and viability of the nation’s nuclear forces for the complex and uncertain security environment of this century?
- What is the way ahead for the next generation of long-range strike and ISR platforms? What trade-offs, especially between manned and unmanned platforms, should the USAF consider? How can the USAF improve acquisition of such systems? How can the USAF better exploit the advantage of low-observables?
- How can the Air Force better prepare itself to operate in an opposed network environment in which communications and data links will be challenged, including how to assure command and control (C2) in bandwidth-constrained environments?
- In counter-land operations, how can the USAF achieve improved target discrimination in high collateral damage situations?
- How should the USAF posture its overseas forces to ensure access? What basing structure, logistical considerations, and
protection measures are required to mitigate emerging anti-access threats?

- How can the Air Force reduce its reliance on GPS to ensure operations in a GPS-denied environment?
- How can the USAF lessen its vulnerability to petroleum shortages, rising energy prices, and resulting logistical and operational challenges?
- How can the Air Force enhance partnerships with its sister services and the interagency community? How can it better collaborate with allies and coalition partners to improve support of national security interests?

These issues were addressed in subsequent conference sessions.
The opening session focused on the multidimensional and dynamic security setting in which the Air Force will operate in the years ahead. The session included a discussion of the need to prioritize necessary capabilities and to gauge “acceptable risks.” Previous Quadrennial Defense Reviews (QDRs) rested on the basic assumption that the United States would be able to support operations simultaneously or nearly simultaneously in two major regional contingencies, with the additional capacity to respond to smaller disaster-relief and/or stability operations missions. However, while the 2010 QDR maintains the need for U.S. forces to operate in two nearly simultaneous major wars, it places far greater emphasis on the need to address irregular warfare challenges. Its focus is maintaining and rebalancing U.S. force structure to fight the wars in which the United States is engaged today while looking ahead to the emerging security setting. The QDR further seeks to develop flexible and tailored capabilities to confront an array of smaller-scale contingencies, including natural disasters, perhaps simultaneously, as was the case with the war in Afghanistan, stability operations in Iraq, and the Haiti relief effort.

The 2010 QDR highlights important trends in the global security environment, especially unconventional threats and asymmetric challenges. It suggests that a conflict with a near-peer competitor such as China, or a conflict with Iran, would involve a mix, or hybrid, of capabilities that would test U.S. forces in very different ways. Although predicting the future security setting is a very difficult if not an impossible exercise, the 2010 QDR outlines major challeng-
es for the United States and its allies, including technology proliferation and diffusion; anti-access threats and the shrinking global basing infrastructure; the possibility of weapons of mass destruction (WMD) use against the U.S. homeland and/or against U.S. forces abroad; critical infrastructure protection and the massed effects of a cyber or space attack; unconventional warfare and irregular challenges; and the emergence of new issue areas such as Arctic security, U.S. energy dependence, demographic shifts and urbanization, the potential for resource wars (particularly over access to water), and the erosion or collapse of governance in weak or failing states.

TECHNOLOGY DIFFUSION
Technology proliferation is accelerating. Compounding the problem is the reality that existing multilateral and/or international export regimes and controls have not kept pace with technology, and efforts to constrain access are complicated by dual-use technologies and chemical/biological agents. The battlefields of the future are likely to be more lethal as combatants take advantage of commercially based navigation aids for precision guidance and advanced weapons systems and as global and theater boundaries disappear with longer-range missile systems becoming more common in enemy arsenals. Non-state entities such as Hezbollah have already used more advanced missile systems to target state adversaries. The proliferation of precision technologies and longer-range delivery platforms puts the United States and its partners increasingly at risk. This proliferation also is likely to affect U.S. operations from forward operating locations, placing additional constraints on American force deployments within the territories of allies. Moreover, as longer-range ballistic and cruise missiles become more widespread, U.S. forces will find it increasingly difficult to operate in conflicts ranging from irregular warfare to high-intensity combat. As highlighted throughout the conference, this will require that the United States develop and field new-generation low-observable penetration assets and related capabilities to operate in non-permissive environments.

PROLIFERATION TRENDS
The twenty-first-century security setting features several proliferation trends that were discussed in the opening session. These trends, six of which were outlined by Dr. Robert L. Pfaltzgraff, Jr., President of the Institute for Foreign Policy Analysis, and Shelby Cullom Davis Professor of International Security Studies, The Fletcher School, Tufts University, framed subsequent discussions.
First, the number of actors—states and armed non-state groups—is growing, together with strategies and capabilities based on more widely available technologies, including WMD and conventional weapons. This is leading to a blurring of categories of warfare that may include state and non-state actors and encompass intra-state, trans-state, and interstate armed conflict as well as hybrid threats.

Second, some of these actors subscribe to ideologies and goals that welcome martyrdom. This raises many questions about dissuasion and deterrence and the need to think of twenty-first-century deterrence based on offensive and defensive strategies and capabilities.

Third, given the sheer numbers of actors capable of challenging the United States and their unprecedented capabilities, the opportunity for asymmetric operations against the United States and its allies will grow. The United States will need to work to reduce key areas of vulnerability, including its financial systems, transportation, communications, and energy infrastructures, its food and water supply, and its space assets.

Fourth, the twenty-first-century world contains flashpoints for state-to-state conflict. This includes North Korea, which possesses nuclear weapons, and Iran, which is developing them. In addition, China is developing an impressive array of weaponry which, as the Commander of U.S. Pacific Command stated in congressional testimony, appears “designed to challenge U.S. freedom of action in the region and, if necessary, enforce China’s influence over its neighbors – including our regional allies and partners’ weaponry.”

These threats include ballistic missiles, aircraft, naval forces, cyber capabilities, anti-satellite (ASAT) weapons, and other power-projection capabilities. The global paradigm of the twenty-first century is further complicated by state actors who may supply advanced arms to non-state actors and terrorist organizations.

---

Fifth, the potential for irregular warfare is rising dramatically with the growth of armed non-state actors. The proliferation of more lethal capabilities, including WMD, to armed non-state actors is a logical projection of present trends. Substantial numbers of fractured, unstable, and ungoverned states serve as breeding grounds of armed non-state actors who will resort to various forms of violence and coercion based on irregular tactics and formations and who will increasingly have the capabilities to do so.

Sixth, the twenty-first-century security setting contains yet another obvious dimension: the permeability of the frontiers of the nation state, rendering domestic populations highly vulnerable to destruction not only by states that can launch missiles but also by terrorists and other transnational groups. As we have seen in recent years, these entities can attack U.S. information systems, creating the possibility of a digital Pearl Harbor.

Taken together, these trends show an unprecedented proliferation of actors and advanced capabilities confronting the United States; the resulting need to prepare for high-end and low-end conflict; and the requirement to think of a seamless web of threats and other security challenges extending from overseas to domestic locales.

Another way to think about the twenty-first-century security setting, Dr. Pfaltzgraff pointed out, is to develop scenarios such as the following, which are more illustrative than comprehensive:

- A nuclear Iran that engages in or supports terrorist operations in a more assertive foreign policy
- An unstable Pakistan that loses control of its nuclear weapons, which fall into the hands of extremists
- A Taiwan Straits crisis that escalates to war
- A nuclear North Korea that escalates tensions on the Korean peninsula

What all of these have in common is the indispensable role that airpower would play in U.S. strategy and crisis management.

Speakers in the opening session discussed a range of proliferation trends, each of which poses unique challenges for the United States and its allies:

- Horizontal proliferation: States that are hostile to the United States acquire nuclear weapons
- Vertical proliferation: States such as China and Russia expand their nuclear forces with new-generation technologies and modernization programs
- Cascading proliferation: States that are allies of the United States move toward nuclear weapons if they conclude that the extended U.S. nuclear guarantee is no longer credible
• Efforts by non-state actors to acquire nuclear weapons: such actors emerge in increasing numbers, posing unprecedented threats to the United States and its allies.

Russia and Proliferation
Crisis stability may be challenged by ongoing nuclear modernization programs in Russia. Russian military doctrine emphasizes nuclear weapons, and Russia is heavily reliant on tactical nuclear weapons for the defense of its vast frontiers. In exercises simulating a Russia-NATO contingency, Russia’s large arsenal of non-strategic nuclear forces (NSNF) has been used in response to a hypothetical invasion that is the result of a crisis. In fact, Russia views a substantial (and modernized) nuclear weapons arsenal as an important source of global prestige.

China and Proliferation
Among the nuclear weapons states recognized by the Non-Proliferation Treaty (NPT), China is unique. While others have reduced their nuclear postures, China is moving in the opposite direction. This encompasses new strategic nuclear systems as well as tactical weapons, including enhanced radiation capabilities and nuclear artillery. Where China will stop in its build-up has yet to be determined. To date, China has sought a minimal deterrent posture rather than one of nuclear parity with the United States. Today, with its increasing economic strength, China is better able to afford larger nuclear forces, and if the United States reduces its nuclear forces to very low levels, Beijing may conclude that parity is both affordable and desirable.

In addition to nuclear weapons and ballistic missile modernization efforts, China is also developing ASAT and EMP capabilities that will challenge U.S. space, network, and strategic superiority, and strengthen the perception of China as a growing Asia-Pacific military power.

North Korea, Iran and Proliferation
Nuclear North Korea and aspirant nuclear Iran present several major challenges for the United States. According to Dr. Robert Joseph, Senior Scholar at the National Institute for Public Policy and former U.S. Under Secretary of State for Arms Control and International Security, these challenges include the need for the United States to consider both offensive and defensive capabilities to prepare for contingencies such as the transfer of nuclear technologies from North Korea to third parties or the need to protect America and its allies in the event of an Israeli attack on Iran’s nuclear in-
frastructure. It was suggested that a more proactive posture is necessary that builds on and employs U.S. and multilateral counter-proliferation capacities, including the Proliferation Security Initiative (PSI) and other efforts to detect, halt, and defeat WMD programs and the transfer of such capabilities.

ANTI-ACCESS/ACCESS DENIAL TECHNOLOGIES

A major conference theme was the likelihood that the United States will face increasing challenges as a result of the wider availability of anti-access technologies to other actors. China, Russia, and Iran are each pursuing anti-access/access-denial (A2/AD) technologies to confront the United States and its allies with unacceptable risks and hence deter or defeat U.S. forces. However, A2/AD capabilities are also becoming available to non-state actors such as Hezbollah, which employed C-802 missiles (made by China and allegedly provided by Iran) to target an Israeli warship during the 2006 Lebanon war.

The sheer number of actors gaining access to advanced and dual-use technologies increases the potential for asymmetric attacks against the United States and its allies by those who are unable to match U.S. military capabilities. They pose increasing challenges to the ability of the United States to project power through narrow seas (for example, the Taiwan Straits) and in the space and cybersecurity domains. Denial of access to critical networks and capabilities may be the most cost-effective means of offsetting U.S. conventional force advantages. By definition such attacks target specific U.S. vulnerabilities, ranging from space assets to transportation nodes and communications infrastructure. A2/AD tactics might entail the use of small-boat “swarm” formations, as the Iranians are developing, or ASAT technologies. Another anti-access option is EMP, brought about by detonating a nuclear weapon at an altitude to cause catastrophic damage to infrastructure such as U.S. space-based networks, ISR, and navigation systems. A2/AD tactics may also include cruise or ballistic missile attacks against U.S. expeditionary strike groups or U.S. forward bases and allied territories, either of which might cause a coalition partner to impose constraints on U.S. op-
erations from its territories out of fear that it would suffer collateral damage.

**CHALLENGES TO U.S SPACE DOMINANCE**

As discussed throughout the conference, space is an increasingly important domain for both military and commercial operations. As airpower has been followed by space power and now cyber-space power, new threats emerge with ever increasing rapidity and profound implications for the character and speed of warfare. As the nation most invested in space-based technologies, assets, and communications networks, the United States has a vital national interest in assuring that it has continuing access to space. However, the number of states with space programs, together with the growth of a commercial sector in space and the sophistication of technology and weaponry, has increased rapidly. Entry into the space domain today can begin with a credit card; any individual or armed group can purchase a satellite phone and a GPS receiver. An adversary seeking to inflict widespread disruption or damage on the United States would have an incentive to attack U.S. space-based assets. Thus, innovative thinking about space is an increasingly important U.S. security imperative as more actors exploit space for their own military or commercial ends.

If the increased availability of technologies for space-related capabilities is enabling a broader range of state and non-state actor threats, it is also posing new challenges to U.S. access to space, including such critical functions as enhanced early warning; ISR; communications; and navigation. In the past, USAF and joint planners focused almost exclusively on the protection of systems and networks performing these tasks. However, conference participants suggested that it will be necessary to refocus U.S. space priorities from domain protection to mission assurance. According to General Robert Kehler, Commander, U.S. Air Force Space Command, mission assurance of U.S. space-based and space-oriented systems requires an ability to protect critically important space assets; the continuing development of Air Force relationships with the com-

![General Robert C. Kehler, USAF Commander, U.S. Space Command](image)
batant commands that facilitate use of USAF capabilities as part of the joint team; and the development of the talent and expertise to meet future requirements. The issues discussed included the need for redundant networks; a strategy to augment and replenish degraded or destroyed assets; and a space-oriented R&D program that anticipates necessary capabilities and leverages existing and on-the-horizon technology solutions. The survivability and resilience of U.S. space networks are imperative. The need to assure that the United States can operate in contested environments suggests that alternative architectures should be considered, including systems or platforms that might reduce USAF and joint reliance on satellites.

**CYBER WARFARE**

Cyber warfare has become a major security challenge. U.S. networks are susceptible to exploitation and attack with potentially serious national security consequences. Cyber attacks on military networks have shown that critical systems are vulnerable. Time and distance become essentially irrelevant because cyber war can be conducted across global distances in milliseconds. Such attacks can also spread quickly among networks, making it extremely difficult to attribute their source and perpetrator and to take retaliatory action, and therefore to develop a deterrence strategy. As Deputy Secretary of Defense William Lynn noted, even if the originator of an attack could be identified, unless it is a state, cyber attackers may not have assets that can be the object of potential retaliation. The cyber events of recent years reveal a lag between their discovery and implementation of defensive measures. The sophistication and number of attacks are increasing, leaving U.S. networks continuously under threat. This vulnerability is magnified by the increased accessibility and proliferation of low-cost computing devices. In the cyber domain, adversaries do not need to invest in expensive next-generation systems in order to pose a threat to U.S. national security. The threat is multi-dimensional and can come from states and non-state actors alike. U.S. financial networks and other critical infrastructure are at risk from cyber attacks; these
include botnet attacks, attacks on supervisory control and data acquisition (SCADA) systems, and Trojan horses (software designed to infiltrate cyber networks without being detected and then extract information), an approach the Chinese are said to be perfecting.

Moreover, cyber operations can be carried out without a highly visible military crisis taking place, as a way to influence political decision making in other countries or to restrict information and to control populations, as China demonstrated against Google. Assistant Secretary of Defense for Global Strategic Affairs Michael Nacht noted that, according to a study completed by the U.S. Cyber Consequence Unit, the 2008 cyber attacks against Georgian targets were carried out by civilians with little or no direction from the Russian military. However, according to the study, the organizers of the attacks had advance notice of Russian military operations and were tipped off that these military operations were about to be carried out; the orchestrated cyber operation against Georgia preceded Russia’s military action. Another conclusion was that the cyber attacks were aided and abetted by Russian organized-crime elements. Russia also appears to have employed such attacks against Estonia in 2007 to signal political discontent with that country’s pro-Western policies. More recently, Iran has used information warfare to stifle democratic movement, employing computer network operations as part of a strategy to disseminate disinformation and to compromise internet use. In each of these examples, assumptions were made about the origin of the attacks, but attribution remains a chal-

lenge, which complicates efforts to develop options for retaliation and for protecting civilian and military networks from cyber attacks.

The idea of using government assets and cyber expertise to protect private networks has challenges, some of which are legal, including questions about civil liberties. However, in the twenty-first-century, military support to civil authorities is growing (for example in disaster relief operations), and this trend is likely to develop in the cyber arena as well. With this in mind, one participant suggested the need to find ways to deal with privacy and other potential concerns. In short, cyber security issues are driving a reevaluation of traditional security concepts and strategies, including organizational structure. It may become necessary to reconfigure C2 to ensure an unbroken, flat chain of command that is more resilient and dependable in an increasingly degraded environment resulting from cyber attacks. Clearly, the United States must develop contingency plans for a range of cyber scenarios in which U.S. civilian and military networks could be compromised. As with consequence management operations, the military will likely be tasked to provide capabilities to help deal with a large-scale cyber attack even though much of the knowledge base and infrastructure for such an attack lie primarily in the private sector.

CRITICAL INFRASTRUCTURE PROTECTION AND EMP THREATS

EMP effects pose a renewed threat to the United States and its critical infrastructure that could seriously impede net-centric warfare operations. EMP, created by the detonation of a nuclear weapon above or within the atmosphere, could cause simultaneous and broadly distributed damage and disruption to electronics, resulting in the loss of critical services. For example, an EMP burst could directly affect the some three thousand commercial flights (as well as military flights) airborne over the United States at any given time, causing them to crash and thus resulting in thousands of fatalities and enormous physical damage.

During the Cold War, U.S. planners assessed EMP largely from the perspective of U.S.-Soviet deterrence: EMP was regarded as a tool that could be used to degrade or destroy U.S. early-warning systems and/or communications networks, thereby eliminating America’s ability to carry out a nuclear strike against the Soviet Union. An EMP attack was generally viewed as a precursor to a nuclear attack, largely precluding concerns about civilian infrastructure which would have been destroyed in the ensuing nuclear strike. Today an EMP attack could be mounted against civilian
and military infrastructure. Given the nation’s extensive vulnerability, EMP should be regarded as the ultimate example of an asymmetric threat. According to Dr. Robert Hermann, a member of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, and Senior Partner, Global Technology Partners, LLC, EMP constitutes one of the small number of existential threats to the United States. It could cause such devastation to infrastructure, including the U.S. strategic nuclear capability, that America would face catastrophic economic, societal, political, and military conditions.

The nation’s principal vulnerability, however, is the electric-power grid, which is extremely fragile because of its size and interconnectivity. The loss of electricity would have cascading effects on other systems, including water supply, telecommunications, transportation, food distribution, and health care. This threat calls for efforts on a scale not present during the Cold War for such a contingency. For one thing, U.S. National Guard assets would likely be tasked by state governors to mitigate the consequences of an EMP event that compromised civilian infrastructure, particularly if essential services such as power generation and water supply were damaged or destroyed.

Today, countries such as China and Iran are believed to have active EMP programs. Reducing the vulnerability of U.S. civilian infrastructure to EMP (see figure 2) should be regarded as a key U.S. priority, according to Dr. Hermann. Survival in an EMP environment is a necessity for U.S. military forces and in particular for the nation’s strategic nuclear deterrence systems. Because the consequences of an EMP attack can be mitigated by technologies for protection, detection, and recovery, the USAF was urged to identify priorities for hardening against EMP effects.

China is another crucially important player on the global security landscape, given its emerging international role and national security strategy. There was general conference agreement that the Sino-American relationship is complex, interdependent, and competitive. Beijing views the United States as its principal future strategic adversary. This is a fact that the United States needs to keep in mind as it seeks to build its relationship with China and, in doing so, to minimize the likelihood of miscalculation. China is build-
ing asymmetric capabilities to exploit U.S. vulnerabilities mainly in space and cyberspace.

A considerable portion of conference discussion was devoted to China’s rising power. China’s military buildup includes A2/AD strategy and cyber warfare capabilities. Differences between the United States and China on issues related to Taiwan, Iran, and Tibet have hampered U.S. government efforts to collaborate with China. The modernization of China’s military power includes fifth-generation fighter aircraft; a new generation of ballistic missiles capable of reaching Taiwan, Japan, and U.S. forces in the Asia-Pacific area; and rapidly maturing counter- and cyber-warfare capabilities.

According to Timothy Thomas, Senior Analyst at the Foreign Military Studies Office, Fort Leavenworth, Kansas, Chinese thinking about cyberspace, particularly the inevitability of a future internet war, differs significantly from that of the United States. For China the importance of cyberspace is derived from its concept of strategy. Chinese strategy is based on the idea of comprehensive national power. Whereas the United States focuses on the operational environment, the Chinese take a holistic, big picture, strategic approach that brings into sharp focus the various factors that are believed to shape or provide the defining characteristics of the objective world. The essence of Chinese strategy is the manipulation of factors to China’s advantage that shape the objective world. For example, they include the level of U.S. science and technology, the numbers and deployment locations of U.S. military forces, and the percentage of GDP spent on defense. The Chinese ask themselves how such factors can be altered to China’s advantage and which part of China’s governing apparatus can be tasked with the implementation of Beijing’s strategy.

Contrasted to the U.S. emphasis, the Chinese approach is broader and focused on the longer term, while the U.S. approach is segmented with a shorter-term focus. For example, China’s leadership views cyberspace first as a means to “make noise in the West and to attack in the East” – in other words, as a diversionary tactic to bring about change in the strategic environment. In China’s view, cyber war makes possible the exploitation of U.S. vulnerabilities. Moreover, the Chinese
see cyberspace as a tool that can strategically manipulate an adversary, including the adversary’s troop deployments and defense spending. Therefore cyber capabilities represent a key element of China’s national power much like diplomacy and economic capabilities. In contrast to U.S. thinking about space and cyber issues, China seems to be less concerned about short-term strategic dominance and more interested in increasing strategic influence over time in the cyber domain and utilizing this dimension of warfare to alter the objective world to Beijing’s advantage.

As described by Timothy Thomas, Chinese internet strategy has four major elements to change the objective world. The first is preemption or sabotage through the development of network technology and systems. The other three elements are electronic long-range reconnaissance; exfiltration or the acquisition of information and knowledge to be utilized to strengthen China’s national security capabilities; and the development of electronic shi. Reconnaissance allows China to identify more accurately an adversary’s vulnerabilities while collecting (exfiltrating) technical information that can be used to strengthen China’s technology base. Shi, according to Chinese philosophy, is one of the three requisites for governance and is established by identifying an adversary’s vulnerabilities and then assigning the appropriate tools to target and exploit those vulnerabilities.

From the Chinese perspective, both offensive and defensive capabilities are necessary to make most effective use of the cyber domain. For this reason the People’s Liberation Army (PLA) is experimenting with numerous concepts and capacities to enhance computer network operations and exercise control over internet access and information operations. Chinese military thinking is based on the assumption that a victorious army wins by first successfully preparing for victory and then seeking battle. In contrast, an army is already defeated if it enters battle without having prepared the ground for victory. China’s leaders see cyber war as an essential part of their effort to shape the objective world in order to assure that China will be victorious.

**UNCONVENTIONAL WARFARE CHALLENGES AND TERRORIST THREATS**

As has been illustrated by the conflicts in Iraq and Afghanistan and as discussed by Dr. Richard Shultz, Professor of International Politics and Director of the International Security Studies Program, The Fletcher School, Tufts University, irregular warfare requires a new paradigm and different capabilities from those necessary to con-
front peer or near-peer states. A major premise underlying the 2010 QDR is that irregular warfare challenges are increasing as the number of weak or failing states grows and more armed groups emerge. These groups undermine stability within such states. Failed or failing states cannot control their territory. They may be weakened by widespread corruption. Some armed groups are inspired by a radical Islamist jihadist theology or ideology that strives to incite wars and conflicts between those extremist groups and the West. In other cases, armed groups of criminal elements band together, sometimes across borders, for financial gain and/or to support common objectives. Consequently, the security environment where U.S. forces operate will likely include a complex array of these types of actors. They may be difficult to target because they often choose to take refuge among local populations. Some may have state sponsorship and thus will have sanctuaries and complex logistical and training organizations within national borders. In some instances, the United States will be forced to target these groups in countries that may even be friends or allies. U.S. operations may take place in difficult and austere terrains, or in urban areas with the need to minimize collateral damage and implement programs and strategies to build trust and confidence in local populations.

Addressing irregular warfare challenges necessitates, as noted earlier, a whole-of-government approach within the United States, together with greater interdependence among U.S. joint and allied military forces. For the U.S. Air Force, this means continuing attention to special operations forces (SOF) and capacities as well as intra-theater mobility. Recent experience in Afghanistan also illustrates how far “joint” has really come, even including cross training between Air Force units and ground forces in the areas of close air support, combat search-and-rescue operations (personnel recovery), medical evacuations on the battlefield, and heightened coordination in U.S. Navy and Air Force operations. It also underscores the need to develop a cadre of personnel with critical cultural and language skills who also have advanced training in human terrain mapping, international relations, and conflict prevention.
Deterrence was discussed extensively at the conference, including but extending beyond nuclear deterrence. In his 2009 Prague speech President Obama outlined a vision of “global zero” with respect to nuclear weapons. The 2010 Nuclear Posture Review (NPR) calls for reduced U.S. emphasis on nuclear weapons, which nevertheless remain vital to U.S. security as long as other nations continue to possess such weapons. The NPR retains the triad of strategic nuclear forces. The Air Force has command responsibilities for two of the three legs, ICBMs and bombers. With respect to NATO deterrence strategy, the issue of non-strategic nuclear forces (NSNF) has come to the fore again.

For the USAF, important force structure and modernization issues are bound up with the nuclear debate. Apart from the future of the manned bomber platform and missile defense, three issues are of particular importance to the USAF: 1) the future of non-nuclear strategic deterrence; 2) Joint Strike Fighter (JSF) procurement and allied thinking on the modernization of dual-capable aircraft (DCA); and 3) the need to sustain the Air Force’s nuclear enterprise. Each has broad importance for twenty-first-century deterrence, as discussed later in this report.

THE SECOND NUCLEAR AGE AND POST-COLD WAR AND POST 9/11 DETERRENCE

We have entered what Dr. Paul Bracken, Professor of Management and Professor of Political Science, Yale University, called the “second nuclear age.” He pointed out that a growing number of states are acquiring nuclear weapons. This constitutes a new phenomenon that must be factored into deterrence planning. It is particularly important because the literature on deterrence has been heavily based on a bipolar paradigm. To some extent, this was an oversimplification because more than the two superpowers possessed nuclear arsenals during much of the Cold War. Additional states became nuclear weapons possessors: first the United Kingdom, followed by France, and later by China. One nuclear crisis took place between parties other than the United States: the China-
Russia standoff in 1969. At the time, Chinese nuclear forces were placed on alert against the possibility of a Soviet surgical strike to disable China’s emerging nuclear capability. Nevertheless, the bipolar strategic nuclear paradigm remained a central feature of the Cold War because the United States and the Soviet Union each had a vast nuclear arsenal, and there was, in practice, great centralization of nuclear decision making respectively in Moscow and Washington. As a result, nuclear deterrence was viewed mainly through a bipolar lens in which the superpowers, by and large, did not have to factor in the perspectives and motivations of other nuclear actors in their security decision making. Each had the other as the primary focus of nuclear deterrence.

In marked contrast, the second nuclear age is characterized by multiple, independent nuclear decision-making centers. Some of these independent nuclear weapons states are potential adversaries, some are rivals, and some are friends, all of whom Washington will seek to influence, signal, and restrain. In addition, the United States may need to continue to provide security guarantees to non-nuclear friends and allies. It may face the possibility of catalytic warfare where, for example, an American ally such as Israel, or a third party such as China could initiate action that might escalate to include the United States.\(^5\) In such a scenario, the United States would not have been directly a party to the decision chain to initiate such escalation, even though it could be drawn into the escalating conflict.

By the same token, there is likely to be a learning curve between nuclear weapons acquisition and the determination of how, when, and what strategies should be employed. The United States may face the possibility of cataclysmic conflict between two major powers, or between a major and a minor power or two minor powers, or even a conflict between a major power and a non-state actor.

---

\(^5\) Catalytic warfare is a term coined by Dr. Herman Kahn in the early 1960s to refer to the “notion that some third party or nation might for its own reasons deliberately start a war between two major powers.” According to Kahn, “the widespread diffusion of nuclear weapons would make many nations able, and in some cases also create the pressure, to aggravate an ongoing crisis, or even touch off a war between two other powers for purposes of their own.” See Herman Kahn, *Thinking the Unthinkable*, (New York: Horizon Press, 1962), 57, 217.
or whether the weapons will be used. What is the learning curve, for example, for a nuclear North Korea or a nuclear Iran? Will either or both be prepared actually to use nuclear weapons? In the absence of a definitive answer to such questions, the U.S. nuclear deterrent must restrain a wider variety of actors today than it did during the Cold War. Deterrence functions by denying benefits, imposing costs, and encouraging restraint. An effective deterrence posture requires a range of capabilities and the capacity to orient forces to address specific challenges. The deterrent must provide security guarantees and assurances sufficient to prevent the initiation of catalytic warfare by an ally, while deterring an adversary from resorting to nuclear escalation. As Dr. Bracken pointed out, compared to the extensive literature on deterrence, there has been little recent attention devoted to the dynamics of escalation in a multi-nuclear world. For example, how does one measure escalation? What are the different escalation frameworks? Is escalation the intensification of the use of force? Is it about crossing thresholds? What is counter-escalation when one party escalates against another? In short, there is abundant need for developing and understanding the strategic interactions and therefore escalation in a multinuclear world.

In light of the complexities of today’s security environment, General Kevin Chilton, Commander, U.S. Strategic Command (STRATCOM), described his efforts to develop a broader, whole-of-government approach to deterrence. This combines military, economic, diplomatic, political, and information resources to dissuade or deter potential adversaries from making decisions that put America’s vital national interests at risk. General Chilton spoke about the need not only to define vital interests as clearly as possible, but also to understand which actors have the capabilities or might be developing the means to hold these interests at risk, understanding the key decision makers and their processes as well as what they value the most and, just as important, what they fear.

Elaborating on deterrence requirements, General Chilton emphasized the importance of four critical elements: early warning, command and control, delivery systems, and weapons. In each, the Air Force plays an indispens-
able role. In the early warning area, the United States relies on the Air Force through satellites and radar network. In command and control, key elements are provided by the Air Force, including Milstar satellites and, in the future, advanced extremely high frequency (AEHF) satellites. In the area of delivery systems, as noted earlier, two legs of the strategic triad, ICBMs and bombers, are furnished by the Air Force. For nuclear weapons, the Air Force has crucially important responsibilities to ensure the safety and security of the current stockpile. General Chilton outlined the continuing need for a comprehensive stockpile management program that ensures that warheads have built into them the requisite safety and security measures while ensuring their continued reliability.

The discussion of nuclear weapons and deterrence included a detailed consideration of extended deterrence in a multinuclear world. As Dr. Clark A. Murdock, Senior Adviser, International Security Program, Center for Strategic and International Studies, suggested, the United States faces a three-dimensional problem: how to reduce its reliance on nuclear deterrence while assuring allies that extended deterrence can be trusted, and maintaining a safe, secure, and effective nuclear arsenal. America will need both to deter potential adversaries while it assures allies of the reliability of an extended security guarantee. The United States also faces the need to deter use of biological or chemical weapons. The United States has demonstrated in the post-Cold War era (in Iraq for example) that it is not deterred by the prospect that its adversaries may have biological or chemical weapons. However, America has sought to prevent nuclear acquisition by potential adversaries out of fear that it might be deterred if they possess nuclear weapons.

As long as nuclear weapons exist, extended deterrence and assurance must remain serious U.S. commitments. This means sustaining a robust nuclear weapons capability. The logic set forth by Dr. Murdock included the assumption that global reductions in nuclear inventories can only be achieved if nations lessen their reliance on nuclear weapons. Yet we have nations seeking nuclear weapons not necessarily to use them in war but instead to prevent or even threaten their use. Nuclear weapons may be acquired not only for defensive or deterrent purposes but also for offensive uses, including nuclear deterrence.
blackmail. If in the second nuclear age there are increasing numbers of nuclear weapons states, this means that such states are becoming more dependent on nuclear weapons. Therefore, striking the proper balance between reducing U.S. reliance on nuclear weapons and maintaining credible extended deterrence and assurance becomes an imperative for U.S. security policy.

Building on the theme of sharp differentiation between the bipolar Cold War era and the emerging multinuclear world, Dr. Camille Grand, Director, Fondation pour la Recherche Stratégique in France, underscored the fact that nuclear proliferation is accelerating and could cease to be manageable. The quickening pace of nuclear proliferation is evident in the fact that in the first fifty years of the nuclear age we had on average one new nuclear power per decade. In the last twelve years alone four additional nuclear players have emerged, in this case from regions where international tensions are great, namely East Asia, South Asia, and the Middle East. In addition to the problem of a growing number of nuclear-weapon states is the proliferation of missiles and other WMD.

The discussion of nuclear deterrence, according to Dr. Grand, is complicated by the nuclear abolitionist debate, which has attracted widespread attention. This contrasts sharply with the paucity of thinking about the future of deterrence. The need to rethink deterrence may have been inhibited by the abolition debate. The issues are intertwined, especially if we retain nuclear weapons but rely less on such capabilities. Dr. Grand suggested that we cannot disconnect the various aspects of the nuclear debate, missile defense, space policy, and conventional strike capabilities. Added to this mix is a global civilian nuclear energy renaissance that is likely to lead additional countries to acquire expertise that could evolve toward nuclear weapons if they choose to take that path.

Among the effects of such trends will be the weakening of the nonproliferation regime. Dr. Grand observed that the NPT will not survive the withdrawal of a second country (in addition to North Korea) that cheats within the treaty and subsequently withdraws.
Contrary to the wishes of nuclear abolitionists, we may see the re-nuclearization of international relations, with increased risk of use. Dr. Grand warned that delegitimizing nuclear weapons would lead to the de-legitimization of deterrence, which would create the very instability that is contrary to the goals of the abolitionists. He pointed to the need to think about and define the key features of an interim world order that will remain stable and safe even as we hold out the long-term vision of a nuclear-weapons-free world.

**REBUILDING AND INVESTING IN THE NUCLEAR ENTERPRISE: GLOBAL STRIKE COMMAND**

As a visible commitment to the nuclear enterprise, the Air Force stood up the Global Strike Command (AFGSC) on August 7, 2009. As described by its Commander, Lt. General Frank G. Klotz, the AFGSC’s mission is to prepare combat-ready forces for nuclear deterrence and global strike operations. Its purpose is to align the ICBM and nuclear-capable long-range bomber force under a single chain of command. The command was founded on the premise that, however important other defense priorities may be, none is greater than the responsibility for operating, maintaining, securing, and supporting nuclear weapons. With the formal activation of AFGSC a response task force and a crisis action team were established, trained, and equipped to deal with serious incidents, including weapons system accidents and natural disasters. The AFGSC has developed a rigorous inspection process to instill uncompromising adherence to standards.

The first transfer of operational forces took place on December 1, 2009, when the AFGSC assumed responsibility for ICBM missions. On February 1, 2010, the transfer of forces to AFGSC was completed with the assignment of the long-range nuclear-capable bomber mission from the Air Combat Command, together with the Eighth Air Force. The B-52 and B-2 are critical parts of the bomber component because of their great flexibility and versatility. The two different bombers provide mutually reinforcing and complementary capabilities. As General Klotz suggested, the B-52 has unique unmatched stand-off capabilities, while the B-2 stealth bomber is able to attack heavily defended targets.
The stand-up of AFGSC sends the message that nuclear deterrence and global strike forces remain vitally important to the United States.

**NON-NUCLEAR STRATEGIC STRIKE**

Credibility is essential to deterrence. In order to enhance credibility, the United States is exploring deterrence modernization options based on non-nuclear strategic systems such as ICBMs armed with conventional warheads, and conventional hypersonic missiles. According to Dr Grand, non-nuclear strategic systems, such as conventional ICBMs, have the potential to dilute, or weaken, nuclear deterrence, while a British participant suggested they could be “escalatory,” if their use would elicit a nuclear response from an adversary who might not be able to discriminate between a conventional strike and a nuclear strategic strike. Proponents of non-nuclear strategic deterrence options suggest that such systems have greater capacity to provide escalation management in a way that nuclear weapons cannot.

Clearly, non-nuclear strategic deterrence presents controversial issues that need to be addressed. Most basic is the question of whether, and to what extent, nuclear weapons confer a unique deterrence quality because of their very nature. Nuclear weapons have been widely viewed as the ultimate means of deterring adversaries, and there is probably no equivalent conventional substitute. In assessing the substitutability of conventional weapons for deterrence, not only must such differences be taken into account, but so must the views of enemies and allies as well. Specifically, American decision makers must develop an understanding of what adversaries value most and what they fear most and the implications for deterrence requirements.

In deterring terrorists, including nuclear-armed terrorists who embrace an ideology or religion that affirms martyrdom, the possibility that a deterrence concept based on retaliation may be more an invitation than a deterrent raises questions about the need to separate terrorists from their enablers. This is based on the presumption that while terrorists may be prepared for martyrdom, enablers seek their own survival. If states form a key part of the enabling network, the ability to establish attribution (tracing the terrorist operation back to a state sponsor) provides yet another basis for deterrence. Therefore, tools for quickly establishing attribution, together with military capabilities for retaliation, in which the USAF is likely to have an important, if not defining, role, should be developed. These may include nuclear and non-nuclear response capabilities.
against such sponsors. As addressed elsewhere in this report and at the conference, twenty-first-century deterrence requires a mix of capabilities for retaliation, denial, and defense.

**NUCLEAR WEAPONS, DUAL-CAPABLE AIRCRAFT, AND NATO DETERRENCE**

With the end of the Cold War the United States reduced its emphasis on nuclear weapons without eliminating such capabilities from its defense posture in Europe. As long as such weapons are retained, the issue of delivery systems, and in particular dual-capable-aircraft (DCA), remains important. With the signing of New START and its reductions in delivery systems and nuclear warheads, what has yet to be addressed is the large numbers (about two thousand) of Russian non-strategic, tactical nuclear warheads, estimated to be at least ten times the size of the U.S. stockpile of such systems located at several sites in Europe. There are rising pressures from a number of NATO-European members, including Germany, to withdraw remaining tactical nuclear weapons from Europe. Some see NSNF, in the words of NATO Secretary General Anders Fogh Rasmussen, as “an essential part of a credible deterrent.”6 Others in Europe view them as a Cold War relic.

The United States and several other NATO countries view such weapons as necessary as long as Russia retains its vast NSNF capability. Unilateral NATO withdrawal would exacerbate the Russian preponderance in such weapons. Whatever the outcome of this ongoing debate, the process by which the NSNF are withdrawn is likely to be lengthy. Therefore, the need for delivery systems, notably DCA, will remain a USAF responsibility. For NATO this means a renewed commitment to conduct training exercises to enhance the certification process of nuclear forces in nations deploying DCA, and most importantly to ensure the security and safety of nuclear storage sites in NATO Europe. This may also mean making the JSF a dual-capable platform in order to maintain the U.S. deterrence guarantee to the alliance.

**NON- AND COUNTER-PROLIFERATION AND COOPERATIVE THREAT REDUCTION**

In addition to maintaining a credible and reliable nuclear deterrent posture, the Obama administration has elevated the importance of

---

arms control and counter-proliferation. Therefore, threat reduction initiatives in the nuclear, chemical, and biological weapons areas are assuming greater significance, particularly if nuclear weapons will have heightened appeal to some state and non-state actors even as they assume a lesser role in U.S. deterrence. It is conceivable that actors seeking to inflict catastrophic damage on the United States and its allies will not share the Western aversion to nuclear weapons. Here, “loose nuke” scenarios need to be considered, with greater focus on mission areas (for example, render-safe and consequence management activities).

Against the challenges posed by the proliferation of chemical, biological, radiological, and nuclear (CBRN) materials and questions of stockpile safety, threat reduction is an important U.S. initiative. Building on the successes of the Nunn-Lugar Cooperative Threat Reduction (CTR) initiative, the United States is seeking to develop the Nunn-Lugar Global Cooperation program. This initiative promotes the idea that the ongoing effort to secure and dismantle nuclear, chemical, and biological weapons, and delivery vehicles in the former Soviet Union (FSU) remains important. However, as Andrew C. Weber, Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs, suggested, new threat reduction priorities have emerged outside the FSU that need to be addressed. The next era of the Nunn-Lugar program is global rather than FSU-focused, calling for a global early warning system for biological attacks as well as for nuclear weapons. The program includes building partner capability to counter WMD with the goal of preventing a terrorist group from acquiring such a capability. Assistant Secretary Weber presented a strategy based on a two-pronged approach that includes reversing the neglect of the U.S. nuclear de-

7 Senator Richard Lugar and former Senator Sam Nunn authored the Nunn-Lugar Act in 1991 establishing the Cooperative Threat Reduction Program. The program seeks to help the states of the former Soviet Union safeguard and dismantle their stockpiles of nuclear, chemical, and biological weapons, related materials, and delivery systems. The Defense Threat Reduction Agency (DTRA) executes the program for the Department of Defense and works in coordination with partner governments and other U.S. government agencies that administer related projects.
Andrew Weber described his office’s efforts to counter the full range of nuclear, biological, and chemical threats and to prevent both terrorists and rogue states from acquiring the technical assistance and materials to develop such weapons. In addition to the potential for nuclear terrorism, he emphasized the threat of biological weapons. This is a strategic threat that includes, for example, the devastating consequences of ten grams of anthrax released in an American or allied city or the detonation of a ten-kiloton improvised nuclear device. The United States’ emerging priorities include Pakistan, whose nuclear weapons security remains a concern; ungoverned territories where al-Qaeda is operating, in states such as Somalia; and regions including the Persian Gulf and parts of Asia plagued by illicit trafficking and where the potential exists for rejuvenation of the A.Q. Khan or a successor nuclear proliferation network.8

This likely means increased emphasis on the Proliferation Security Initiative with the need for greater sea-based and air-based interdiction. It may also require enhanced security cooperation to build partner capacities for combating illicit trafficking and/or support to civil authorities in developing consequence management capacities. Moreover, it could include Air Force efforts to train and equip partner states in these areas, as well as USAF personnel who can operate critical aerial ports of embarkation and debarkation (APOE/Ds) in WMD environments, together with intra-theater lift in support of U.S. or coalition forces operating in irregular warfare settings such as Afghanistan. This underscores the need for rapid movement of personnel and supplies across terrain that is often rugged and inhospitable, and/or the presence of hostile forces that makes ground-based movement dangerous and slow.

---

8 Dr. Abdul Qadeer Khan is widely credited with being the father of Pakistan’s atomic bomb. However, in acquiring the technologies and skills to implement Pakistan’s nuclear weapons program, he also set up a highly successful nuclear black market and contributed to nuclear weapons development in a handful of other countries, including North Korea, Libya, and Iran.
The global nature of proliferation has led the United States to move beyond its earlier post-Soviet Union CTR focus to a broader emphasis. Several models have been set forth, the first of which is essentially the Nunn-Lugar model based on the FSU. This model will continue to require USAF participation, especially with weapons dismantlement and exploitation of sensor technologies to meet new verification and monitoring needs, for example, those associated with New START. The second model applies to specific non-FSU countries and will require tailored USAF programs, many of which already exist, as well as its unique partner-building capacities. The Office of the Secretary of Defense (OSD) is currently focusing on countries such as Pakistan, Afghanistan, Georgia, and Kenya. Many of the activities being discussed include Air Force equities and should emerge as aspects of component command security cooperation. The third model is a regional approach in which countries collaborate on the development and deployment of security networks for surveillance, air policing, or intelligence fusion. This is an approach that should be considered by the USAF and regional component commands, in the form of both exercise development and building partner capacities.
Although each of the combatant commands (COCOMs) has specific functional or geographical responsibilities, extensive discussion took place throughout the conference about the areas of synergy, overlap, and interdependence among the commands. As noted by IFPA Vice President and Director of Studies Dr. Charles M. Perry, the combatant commanders (CCDRs) are chartered by law to be the hubs for strategy and military execution in their areas of responsibility (AORs). In terms of airpower operations, the CCDRs rely on the assets and expertise of their service component commands, each of which brings to the COCOMs a broad range of capabilities for long-range strike, surveillance, air- and space-domain control, and global mobility, among other critical mission areas.

NORTH AMERICAN AEROSPACE DEFENSE AND U.S. NORTHERN COMMAND

North American Aerospace Defense Command (NORAD) and U.S. Northern Command (NORTHCOM) are responsible for providing air defense and early warning for Canada and the continental United States as well as preparing for homeland defense and civil-support missions stretching from the Arctic to the Gulf of Mexico and parts of the Caribbean. NORTHCOM’s area of responsibility (AOR) also includes Mexico. Each of the military services has unique capacities that contribute to NORAD’s and NORTHCOM’s missions; the Air Force’s
contribution is to provide air defense over the homeland and monitor air traffic both within and outside U.S. borders. The USAF also has assumed responsibility for establishing a layered defense in the maritime domain, partnering with the U.S. Navy, the Coast Guard (USCG), government agencies, and allies to provide maritime homeland defense. Adversaries’ continued pursuit of advanced missile and weapons technologies has increased the USAF’s role in missile defense, as well as in early warning, space-based ISR, and contingency plans for strike and preventive options.

NORTHCOM’s collaboration with Mexico is growing as the increasing number and reach of armed and criminal groups threaten that country’s stability and the border region. It is essential to stem illicit trafficking across the Mexican/U.S. border. One of NORTHCOM’s most important initiatives is information sharing with Mexico, which is dependent on USAF air and space assets to heighten situational awareness. NORTHCOM collaboration with U.S. Southern Command (SOUTHCOM) is widely recognized as essential to combating illicit traffic from South America and the Caribbean into Central America and Mexico.

NORTHCOM has also assumed new responsibilities in the Arctic, which holds increasing strategic importance. Arctic security will require greater interaction with U.S. European Command (EUCOM), as nations of northern Europe lay claim to Arctic territories, sea routes, and resources. Russia also has an interest in the Arctic, and this could impose a greater role on the USAF, especially in the area of security cooperation, capacity building for partners, and the development of “rules of the road,” including protocols for civil air patrols and search and rescue missions. The opening of the Northwest Passage has created new opportunities and challenges for homeland defense that will include U.S.-Canadian collaboration on the air defense of the Arctic. As characterized by Senator Mark Begich of Alaska, the Arctic is “aerospace’s new frontier,” and, as a result, the USAF must anticipate likely challenges and opportunities associated with Arctic security issues. This may re-
quire the Air Force, which already operates throughout Alaska, to retrofit some of its assets for operations in the Arctic climate. According to General Victor E. Renuart, Jr., Commander, NORAD and NORTHCOM, the United States has not yet fully developed its ability to operate in the Arctic. This will become necessary with the increasing importance of the Arctic both as a security environment and because of growing U.S. economic interest there. Another arena of importance to which General Renuart referred was cyberspace. In light of the emphasis being placed on cyber war by other countries, U.S. vulnerabilities must be addressed as a homeland defense issue. America will need growing numbers of people trained to operate in cyberspace and must develop young cyber warriors possessing great agility and adaptability in the dynamic new security setting.

Last but not least, General Renuart discussed the January 2010 earthquake in Haiti. Because SOUTHCOM was not configured as a command to respond to large-scale disasters, NORTHCOM was called upon to provide assistance. Together with the Air Force, NORTHCOM responded to the call with disaster response expertise, based on what it is trained to do if a similar disaster occurred in the United States. As General Renuart put it, NORTHCOM essentially gutted its headquarters, sending some sixty members to SOUTHCOM. This illustrates the close cooperation that has developed among commands.

U.S. TRANSPORTATION COMMAND

The U.S. Transportation Command (TRANSCOM) is tasked with meeting the mobility and logistical needs of the COCOMs in a timely manner. To do this, General Duncan J. McNabb, TRANSCOM Commander, pointed out that the command works with the Joint Staff on its Global Employment Force (GEF) plans and maintains relationships with allies, coalition partners, and civilian agencies and companies, which can be activated to meet emerging needs. TRANSCOM is tasked with the creation of effective distribution
networks and transportation routes to facilitate the delivery of food, humanitarian aid, and equipment to meet military needs and to support counter-insurgency strategy. Timely delivery of food, fuel, and other supplies makes the difference between the success and failure of an operation. In Afghanistan, where much of the distribution network depends on extremely vulnerable routes, force protection and the development of alternative modes of access into the theater are vitally important elements of TRANSCOM plans.

Designing an efficient distribution process requires innovative use of available assets. Afghanistan, for example, is a landlocked country with a difficult terrain that poses serious challenges for TRANSCOM. Although new transit routes are being sought in negotiations with Afghanistan’s neighbors, Pakistan occupies a place of immense strategic importance in the transit of U.S. supplies to Afghanistan. The Northern Distribution Network was the result of a successful joint effort between TRANSCOM and the U.S. Central Command (CENTCOM) to invite Afghanistan’s northern neighbors to participate in a commercial transportation network to provide an alternative to the extremely vulnerable Pakistani routes. Over sixty-five hundred containers have come through the Northern Distribution Network, diversifying the number of access routes available for supplying U.S. troops. All of the sensitive and lethal materials (such as live munitions) are delivered by air because of Afghanistan’s geostrategic location and the vulnerability of land routes into and within the country.

Other constraints affect the supply chain into Afghanistan, notably restrictions on the use of airpower from Central Asia bases and/or excessive financial costs imposed by countries seeking to benefit from this U.S.-NATO necessity. If necessary, TRANSCOM has a contingency plan to deliver all essential U.S. supplies into Afghanistan with Air Force assets. Although this would require a large-scale effort, the Air Force has the means to deliver essential supplies in hostile environments. Clearly, airpower plays an indispensable role in moving personnel and supplies within Afghanistan. Air transport is often the most efficient means of reaching remote locations and sometimes the only way to do so. Therefore, intra-theater airlift is vital in Afghanistan and in other conflict set-
tings where rapidity of movement of personnel and supplies within hostile environments is indispensable to mission success.

U.S. SPECIAL OPERATIONS COMMAND

The mission of U.S. Special Operations Command (SOCOM) is to “provide fully capable Special Operations Forces (SOF) to defend the United States and its interests” and to “synchronize planning of global operations against terrorist networks.” This has led SOCOM to learn about such networks, including money laundering that supports terrorist operations. In 2005 SOCOM was also tasked with planning and synchronizing the war on terror. This assignment specified that SOCOM would coordinate joint efforts to achieve a unity of effort across commands for counter-terrorist operations. SOCOM, as General David P. Fridovich, Director, Center for Special Operations, SOCOM, explained, provides a strategic headquarters that looks for global gaps in the seams among the regional commands that must be filled in the war on terror. SOCOM is a unique command in that it also supports other commands with needed forces. SOCOM functions at a broad strategic level as well as at the operational and tactical levels. In Afghanistan, for example, SOCOM works in support of CENTCOM while in special circumstances as a supported command itself.

Over the past several years, and particularly since the change in strategy in Afghanistan, the need to integrate air operations with ground force campaigns more seamlessly has become evident. Close air support and precision targeting are problematic issues in Afghanistan, especially when USAF strikes are called in to support the NATO-led International Security Assistance Force (ISAF). As a result, enhanced joint tactical air control training with the other services and with allies and partners has become an important operational requirement. So has the need to deliver the analysis of ISR data quickly to the tactical-level users in the form of actionable intelligence. NATO’s establishment of the NATO SOF Coordination Centre (NSCC), which transitioned on March 1, 2010 to

---

9 See http://www.socom.mil/SOCOMHome/Pages/About.aspx
NATO Special Operations Headquarters (NSHQ), the headquarters element of a NATO SOF component, opens the door for the USAF to play a significant role in shaping development of a NATO SOF aviation component.

General Fridovich echoed others at the conference in emphasizing the complexity of today’s security setting based on several key assumptions: 1) the irregular warfare environment will remain important; 2) although the nation state is not going away, it will be increasingly challenged; 3) crime, criminality, terrorism, and migration exist especially in places where there is poor governance; and 4) terrorists and criminal organizations feed on each other in cooperative efforts to achieve their various goals (terrorists to get financial support and criminal organizations to realize economic gain). SOCOM can bring together and synchronize quickly the resources needed to combat such threats. This includes strategic-level planning as well as special operations support teams that work closely with the other military commands and civilian agencies and with each of the military services.

U.S. JOINT FORCES COMMAND

U.S. Joint Forces Command (JFCOM) is tasked with supporting combatant commanders with timely and mission-ready joint capabilities, based on the command’s development of new operational concepts, experimentation in doctrine and force posture, and joint and combined training in new concepts and/or force transformation. Major General David M. Edgington, Chief of Staff, JFCOM, explained that JFCOM leaders work closely with the geographic CCDRs to identify and exploit new opportunities among allies, and with the other functional COCOMs to ensure that force requirements to meet new challenges are identified and implemented. Much of JFCOM’s current effort is focused on irregular and hybrid warfare challenges. Indeed, in the 2009 Capstone Concept for Joint Operations (CCJO) that JFCOM published in 2009, the command presented its perspective on the emerging threat environment and delineat-
ed transformation priorities, including weapons acquisition and new and anticipated defense requirements, particularly counter-WMD requirements.  

In general, the CCJO highlights five national security missions for the joint force from 2016 to 2028. First and foremost, of course, is winning wars. The second priority is protecting U.S. territory, population, and critical infrastructure. The third is deterring potential adversaries and countering threats to vital U.S. interests. The fourth is developing cooperative security through comprehensive policies that integrate and synchronize the spectrum of capabilities and interests of the United States and its partners. The fifth priority is responding to foreign and domestic crises, including natural disasters and terrorist acts in order to alleviate human suffering and restore civil order. In each of these areas JFCOM embraces a whole-of-government approach, attempting to develop concepts of operations with the combatant commands and others with whom JFCOM will work. Such interagency partners are asked to send to exercises personnel who would actually be deployed in a real-world situation, including those who would be empowered to make decisions so that working relationships can be built as training proceeds enabling JFCOM to deploy forces for particular missions.

The CCJO describes three major ideas that should drive joint force operational thinking for these missions. First, future joint force commanders must tailor their approaches to address the unique requirements of each new operational environment, guided by political and strategic realities rather than being constrained by pre-existing templates. Second, operations are likely to be conducted using a combination of kinetic and non-kinetic capabilities. Security force assistance and building partner capacity are essential elements of projecting U.S. power. Finally, on a dynamic, complex, and fast-paced battlefield, U.S. forces must be able to recalibrate their operations through access to quick-reaction and robust assessment capabilities. This may require a more decentralized C² structure to allow lower-echelon forces to operate more independently, while ensuring that ISR information is efficiently collected, analyzed, and disseminated.

JFCOM is developing a new joint C² architecture and doctrine in an effort to create a single system within which all the services can operate. In response to the complexity of future threats, C² must be decentralized to enable execution of the commander’s in-

---

10 In 2010, JFCOM produced an assessment of the future operating environment called the Joint Operating Environment (JOE), http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf. This document outlines a vision of future planning and the threat environments likely to confront U.S. operating forces.
tent from the strategic level down to the tactical. This system must also be sufficiently robust and resilient to overcome growing A2/AD capabilities with which adversaries will attempt to remove the commander’s command and control ability.

Building and improving partner capacity is another area to which JFCOM can make unique contributions, and coalition operations must be included as fully as possible in JFCOM planning even though the United States must not exclude the possibility that it might operate alone. JFCOM engages in education and training across the services and with allies. Effective modeling and simulation, using live and virtual exercises, are a key part of its educational and training programs. The USAF in particular has been incorporating JFCOM ideas to improve its own educational and training efforts.

AIRPOWER AND THE U.S. NAVY

In the 1970s and 1980s the Air Force and the U.S. Army together created the AirLand Battle doctrine to meet the threat then posed by the conventionally superior Soviet/Warsaw Pact forces in Europe. Later, in Operation Desert Storm and more recently in Operation Enduring Freedom and Operation Iraqi Freedom, USAF capabilities were central to CENTCOM’s strategy. In light of this experience, the USAF and the Navy initiated discussions in 2009 regarding an Air-Sea Battle concept, a logical and necessary extension and enlargement of Navy-USAF cooperation. The maritime services – the Navy and the Marines – and the USAF are already partners in JSF development, missile defense operations, electronic warfare development, and tactical air operations. They partner in deterrence, information operations, and counter-WMD, and counter-terrorism missions in joint commands like STRATCOM.

The Navy faces the need to combat anti-satellite threats, anti-ship ballistic missiles, advanced surface-to-surface missiles, small boats employing swarm tactics, and new-generation ballistic and cruise missiles. Each of these challenges underscores the need to work with the USAF. Thus, the basis exists for common operations across a broad threat spectrum. Specifically, the Air-Sea Battle concept is a joint response to a strategic environment characterized by increasingly interconnected threats and a growing number of adversaries who possess technologies capable of threatening U.S.

---

freedom of action and freedom of movement across all domains. Military power-projection operations have long been an essential element of U.S. national security strategy. However, countries such as China, Iran, and North Korea are developing sophisticated A2/AD capabilities that could threaten U.S. power projection in places such as the Western Pacific and Persian Gulf. These systems are likely to challenge the U.S. ability to deploy and sustain military forces in the Western Pacific and Persian Gulf in the years ahead.

How Air-Sea Battle will function is still being determined. The USN-USAF development of Air-Sea Battle is focused on enabling the “marriage of stealths,” for power projection that includes air, sub-surface, and SOF capacities; manned and unmanned ISR; assured communications; and new-generation strike capabilities. In the ISR arena, emphasis is being given to remotely piloted aircraft (RPA) development and acquisition, especially the Global Hawk and Broad Area Maritime Surveillance (BAMS) systems. In the strike arena, the USN and USAF have identified robust long-range strike capabilities as essential to deterrence and for providing a spectrum of response options for the president. This could translate into establishment of an integrated strike force, leveraging the capabilities of next-generation bombers, missiles, and RPA. In particular, a joint stealth task force synthesizing use of Air Force long-range aircraft such as the B-52 and B-2, tactical aircraft like the F-22 and F-35, and Navy surface ships and submarines would increase U.S. power projection capabilities in denied environments.

In order to continue operating in an anti-access environment both the USN and USAF will require more resilient and robust C² structures. Air-Sea Battle discussions at the conference included electronic warfare, particularly the need to field systems capable of surviving electronic jamming, together with the future role of RPA.

Among the issues discussed by Admiral Jonathan Greenert, Vice Chief of Naval Operations, were two emerging missions: cyberspace and ballistic missile defense. In January 2010, the Navy established its fleet cyber command as a component of the new U.S. Cyber Command (USCYBERCOM) that is described elsewhere in this report. This new Navy command builds on the service’s net-
work warfare command that was created in 2002. The Navy merged some twenty-three disparate organizations to create a new focus on cyberspace.

Like cyberspace, ballistic missile defense (BMD) cuts across the combatant commands and the military services. The Navy’s interest in ballistic missile defense was heightened after the North Korean Taepodong II tests in the late 1990s. The Navy’s ballistic missile defense platforms have proven capabilities to defeat ballistic missiles and support the needs of all of the COCOMs. The Aegis systems afloat will be supplemented by Aegis Ashore. Admiral Greenert underscored the C2 challenges for ballistic missile defense and the need to work with the other services to ensure that the right joint architecture is in place. By 2015 the Navy will develop a partnership in which Maritime Operations Centers (MOCs) will be linked to Air Operations Centers (AOCs) for command and control. There will also be substantial increases in the number of Aegis cruisers and destroyers that are BMD capable.

AIRPOWER AND THE U.S. MARINE CORPS

Lieutenant General George J. Trautman III, Deputy Commandant for Aviation, U.S. Marine Corps, explained that the Marine Corps is an expeditionary service that operates from the sea, in amphibious environments, and forward in key regional theaters, often in harsh conditions and frequently dependent on its own air assets to meet mission objectives. However, in Iraq and now in Afghanistan, USMC ground forces are working closely with USAF and USN air assets. Air traffic control issues continue to affect operations, although USAF-USMC and Navy collaboration is improving in this arena, and most of the unresolved issues have to do with U.S. al-

12 Aegis Ashore essentially consists of land-based versions of the launchers, SM-3 interceptors, and related equipment found on U.S. Navy Aegis ballistic missile defense-capable ships to defend against attacking ballistic missiles. It is being developed for deployment abroad. See the testimony of Lieutenant General Patrick J. O’Reilly, USA, Director, Missile Defense Agency, before the House Armed Services Committee, Strategic Forces Subcommittee on April 15, 2010, (particularly pages 5-6), http://www.mda.mil/news/public_statements.html.
lies and partnerships. Marine task forces also rely on seamless integration among the elements of the Marine Air Ground Task Force (MAGTF) to minimize risk to troops.13 While each Marine expeditionary unit (MEU) has its own indigenous aviation combat element, the Corps has had to rely on USAF and USN rotary lift and other capabilities to meet its ground force objectives, especially in challenging theaters such as Afghanistan.14

Despite the trend toward greater interdependence among the forces, the Marine Corps continues to emphasize its own air capability, preferring to rely on USMC forces for close air support and strike operations. However, with the Goldwater-Nichols Act of 1986, which streamlined U.S. military commands and mandated the further development of joint force planning and capabilities, the Marines and the Navy improved their collaboration on airpower strategies and procurements, culminating in the deployment of USMC aircraft aboard Navy carriers in integrated USMC/USN air wings. As defense procurement budgets decline, it is likely that multipurpose aircraft and unmanned vehicles may replace some components of the Marines’ aviation element. For the Marines, it will be important to sustain capabilities for forcible-entry operations and for closer USAF-USMC collaboration on air-ground operations and close air support.

The Marine Corps leadership is considering replacing the EA-6B Prowler with a JSF platform optimized for electronic warfare missions.15 To achieve this capability, it will be necessary to incorporate stealthy jammer pods on the JSF, increasing its value as a multipurpose platform capable of operating in permissive as well as denied environments. Apart from the JSF, the Marine Corps is also working with the USAF on the KC-130J to replace its aging KC-130F tanker fleet. The new KC-130J will provide increased speed, range, an improved air-to-air refueling system, night systems, and survivability enhancements.

13 The Marine Air-Ground Task Force is a USMC term to describe the principal organization for missions across the range of military operations. A MAGTF is a balanced air-ground, combined arms task organization of Marine Corps forces under a single commander structured to accomplish a specific mission.
14 The Marine Corps has seven MEUs, three on the West Coast, three on the East Coast and one in Japan. At the time of the conference in January 2010 two MEUs were deployed to Haiti in the aftermath of the earthquake.
15 The Marine Corps variant of the USAF JSF multi-role fighter is a short take-off/vertical landing aircraft that will take the place of the F-18, AV-8B, and, eventually, the EA-6B Prowler; the USAF version will replace F-16s, while the USN JSF will replace early versions of the F-18.
 Allies have been an essential part of U.S. national security strategy even though the capabilities gap in favor of the United States has widened in recent decades. Nevertheless, both the United States and its allies are likely to face growing constraints on defense spending in the years to come. As a result, the need for global partnerships will grow in order to take maximum advantage of combined capabilities of allies who share common interests.

In Iraq, the United States has operated with allies and coalition partners. In Afghanistan, the United States is working with NATO and other countries, notably Australia, Japan, and the Republic of Korea (ROK). As Dr. Jacquelyn K. Davis, IFPA Executive Vice President, pointed out, the history of alliances contains numerous examples of friction and disputes among allies and coalition partners. Such arrangements change as interests change; the issue shapes the coalition. As Lord Palmerston once famously quipped, “Nations have no permanent friends or allies, they only have permanent interests.” Winston Churchill’s dictum is equally pertinent to the effect that the only thing worse than fighting with allies is fighting without allies in wartime. To be sure, NATO, which celebrated its sixtieth anniversary in 2009, and the U.S.-Japan security relationship, which marked its fiftieth year in 2009, are testimony to the fact that the United States and other countries are capable of working together over a sustained period for the common good, while promoting their own interests. Nevertheless, there have been questions about the relevance of NATO in the post-Cold War world. Some in Europe seek to build European se-
security institutions as a supplement or alternative to NATO. Some in the United States cite problems with NATO in Afghanistan, including restrictive rules of engagement that may hamper the effective use of available forces, and the reluctance of allies to commit forces of sufficient size for sustained periods. Others believe that the Alliance remains important to balance Russia’s possible geostrategic resurgence and thus provides reassurance to those newer NATO members.

NATO has been developing a new strategic concept based on the role of the Alliance in today’s security setting. It has also been engaged in an ongoing transformation that includes headquarters realignments and new thinking about forces rationalization, basing, and manning concepts. For the USAF, these include such mission areas as air defense, ballistic missile defense, early warning and surveillance, cyber security, counter-terrorism and combating WMD, and strategic deterrence, all of which were discussed at the conference, as noted in this report.

LEVERAGING NATO CAPACITIES FOR USAF PLANNING

General Stéphane Abrial, Supreme Allied Commander Transformation, and former Chief of Staff of the French Air Force

General Stéphane Abrial, Supreme Allied Commander Transformation (SAC-T) and former Chief of Staff of the French Air Force, pointed out that airpower has always been central to NATO, which is the premier international partnership for airpower. One of the most concrete testimonies to the collective defense set forth in Article 5 of the North Atlantic Treaty is common air policing, in which Alliance members collectively preserve the integrity of NATO air
This integration goes far and deep. For example, as General Abrial pointed out, the NATO E-3 Airborne Warning and Control System (AWACs) component is not only the Alliance’s largest deployable unit, it is the world’s only integrated multinational flying unit. Another example is the role that NATO air forces have played in policing Baltic airspace since 2004, when Estonia, Latvia, and Lithuania became members. However, the Alliance today faces strategic challenges to its ability to synchronize operational planning. Differing threat perspectives, defense spending cuts, program priorities, and restrictions on the use of force for out-of-area contingencies have all hampered NATO operations in Afghanistan and limited their utility. The United States has emphasized the transformation of NATO capabilities and organization to contribute to out-of-area operations and to build broader global partnerships. This process has been hindered because of the unwillingness or inability of some members to modernize their forces to meet post-Cold War security needs.

The war in Afghanistan has brought to light other problems, including rules of engagement and other constraints placed by some members on the use of their forces and the length of time such forces are made available. For example, in early 2010, the governing coalition in the Netherlands fell as a result of differences over extending the Dutch deployment in Afghanistan. Because of the Afghanistan experience it may be many years before NATO again commits itself to an out-of-area operation. Consequently, some conference participants suggested, the United States cannot assume that NATO forces will be available for such contingencies. Nevertheless, the United States is likely to work with specific allies who share common interests, thus creating coalitions of the willing with these countries. Therefore, NATO – and U.S. forces assigned to EUCOM – must be prepared for a variety of threats, including cyber activities, Iran’s nuclear and missile programs, piracy, illicit trafficking, and the growth of extremism. Thus, NATO’s air commons will remain a core mission and the basis for continuing cooperation among NATO member air forces.

16 Article 5 of the 1949 North Atlantic Treaty states that “The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.”
General Abrial observed that space is another crucial domain that calls for a more active NATO role in fostering partnership. ISAF operations in Afghanistan would be seriously degraded and perhaps rendered impossible if military forces were deprived of space assets. This includes operations ranging from time-sensitive targeting to communications and ISR. However, the current NATO space framework relies on the use of national assets that may no longer be adequate. The problem arises from barriers to more fully sharing nationally collected intelligence. Increased Alliance partnerships with cost sharing to develop common space programs such as ISR systems would minimize or even eliminate many such problems. General Abrial suggested that with the rising cost of satellites and current budgetary constraints, greater cost sharing among NATO members is both beneficial to enhanced intelligence sharing and welcome for economic reasons. As a result, NATO should invest in a space policy that embraces the cooperative development of space assets.

The cyber domain presents another area of growing concern and interest for NATO, particularly because in the highly networked information age the weakness of one ally increases the vulnerability of all. In May 2008, NATO established the Cyber Defense Center of Excellence in Tallinn, Estonia, which is supported by the NATO Network Enabled Capability (NNEC) program. It is designed to bring together various capabilities, including military (strategic to tactical) and civilian, through an information infrastructure. It is intended to create a culture of information sharing and communications to reinforce situational awareness and decision making. Although cyber security will undoubtedly remain a national responsibility, it also needs to be addressed cooperatively by NATO. For example, cyber security has important implications for Article 5 of the North Atlantic Treaty, namely whether and when cyber attacks form the basis for invoking an Article 5 collective defense response. There is not yet a common understanding of the distinction between cyber vandalism and a cyber attack that would trigger Article 5. Any NATO-wide approach to cyberspace requires reconciling an array of national perspectives and threat perceptions related to the cyber domain and national sovereignty issues.

The NATO Special Operations Forces (SOF) Headquarters Element

The NATO SOF Coordination Centre (NSCC) was established at NATO’s 2006 Riga Summit as the central feature of the NATO SOF Transformation Initiative (NSTI). According to Brigadier Lance Mans, Deputy Director, NSCC, its purpose is to provide a frame-
work for enhancing the capacity of NATO SOF to work together on the battlefield by establishing common training and education programs and by fostering intelligence sharing and communications connectivity in operational contingencies.

In 2009, the NATO Military Committee designated the NSCC as the core of the NATO SOF Headquarters (NSHQ) element. The NATO SOF Headquarters was established on March 1, 2010 to provide a focal point for all NATO SOF activities as well as guidance for national SOF development. Since its inception, the NSCC – now the NSHQ – has grown rapidly to become an enabler for NATO operations, including in Afghanistan, where NATO SOF forces operate under ISAF authority. The NSHQ was formed to support NATO operations in addition to those in Afghanistan, as depicted in figure 4. With the creation of a deployable command element the NSHQ can support counter-piracy, counter-WMD missions, and other operations for which the NATO Response Force (NRF) was created. The NRF has been unable to carry out these operations, however, because member states have not signed up to lead its rotations or to

![Image](image-url)

**FIGURE 4**

SOF in the Spectrum of Conflict

- Peace support operations
- Conventional entry
- Combat operations
- Stability operations
- Peace engagement

Adapted from Brigadier Lance Mans’ conference presentation, “NATO SOF Coordination Centre (NSCC).”
meet Supreme Headquarters Allied Powers Europe (SHAPE) force-generation goals for the response force.

SOF initiatives related to NATO member air forces have been limited, in part because of inadequate NATO aviation assets such as vertical lift, but also because of budget shortfalls in member countries. Nevertheless, a large pool of air resources is available among NATO countries on which SOF can draw. Several organizations are addressing this problem, the first being Air-Ground Surveillance, which may acquire unmanned aircraft to be owned by NATO. The C-17 Consortium, made up of both NATO and non-NATO members, offers three C-17s on a pay-by-the-hour basis. Air mobility and ISR are key enablers for SOF operations and the creation of a dedicated SOF air wing may benefit NATO’s SOF concept. The C-17 Consortium could serve as the model for a NATO SOF air wing.

ALLIED COUNTRY PERSPECTIVES

The conference furnished an unique opportunity for allies to share their perspectives on the major issues of air, space, and cyberspace. Cooperative arrangements were also discussed in depth. Although the USAF has many international partnerships, the focus here was on the United Kingdom (UK), Japan, and Australia.

United Kingdom

As they move forward with the latest Strategic Defence Review (SDR), British defense planners are making an overarching assumption that the UK will maintain a capacity to respond to the unexpected, while charting a course in which there is a direct relationship between alliance strategy and defense capabilities. It is a fundamental premise that in most instances the UK will not employ forces on its own, but instead join with the United States, NATO, or as a part of another European force. British Air Vice Marshal Stephen J. Hillier pointed out that the UK faces three general defense constraints: 1) the budget; 2) a growing societal aversion to the use of force and high casualties; 3) budget and other non-NATO multinational missions. The costs of operating the C-17s are based on the number of hours each consortium member uses the aircraft.

17 In September 2008, ten NATO members, together with Partnership for Peace nations Sweden and Finland, signed a memorandum of understanding to acquire three C-17 Globemaster long-range transport aircraft (two purchased from Boeing, a third provided by the U.S. Air Force), which are assigned to NATO’s Heavy Airlift Wing and jointly operated from Pápa Air Base, Hungary, allowing a shared, pooled fleet. The C-17 Consortium allows each participating nation (Bulgaria, Estonia, Finland, Hungary, Lithuania, the Netherlands, Norway, Poland, Romania, Slovenia, Sweden and the United States) to support NATO strategic airlift operations in Afghanistan and elsewhere, as well as individual nations’ sovereign airlift needs and other non-NATO multinational missions. The costs of operating the C-17s are based on the number of hours each consortium member uses the aircraft.
and 3) the degree to which political leaders in NATO countries and elsewhere will be willing or able to make tough political choices, given the constraints of coalition governments and/or the nature of the domestic political debates in some countries. The UK will need to deliver defense more efficiently and more effectively. It faces the challenge of continuing to meet defense requirements against direct threats to the UK and its overseas territories. Instead of determining defense requirements from scenario-based assessments, the SDR is likely to be driven principally by budget considerations. The result will be a force structure substantially different from one based on prospective threats and risks derived from scenarios and analyses of the emerging security setting.

The SDR will address the question of whether the UK should maintain forces only sufficient for multiple small-scale interventions, or whether it should sustain a capacity for high-end conflict, as well as lesser contingencies. Proponents of the former approach argue the need for forces specifically for such operations such as counter-terrorism, CBRN, noncombatant evacuation operations (NEO), and post-conflict stabilization.

Defense planners have also been discussing potential asymmetric challenges such as cyber attacks from peer competitors such as China and Russia and from non-state actors such as Hezbollah, Hamas, and al-Qaeda. Determining if and when a cyber attack should trigger a NATO Article 5 response is important but difficult. Locating the source of a cyber attack is itself a formidable obstacle to a NATO Article 5 response. However, with the establishment of the UK Office for Cyber Security, there is every expectation that the SDR will result in greater investment in cyber security capabilities.

British thinking about future force requirements is focused on several issues. They include readiness levels; the size and character of the Army; the frontline-territorial Army mix; globalization of the defense industrial base and delineation of the core British defense-industrial capabilities that will need to be maintained; the
future of strike aircraft and unmanned systems; *Trident* modernization and deterrence; and UK forward deployments and access. These issues are similar to those being examined in the United States. How they are resolved will reflect British willingness to take risks about the future security setting by jettisoning, modifying, or delaying specific capabilities, acquisitions, and concept development. Currently, UK defense thinking is based on the capability to conduct one medium-scale operation and as many as two smaller contingencies. The preferred framework appears to be a force that can engage in multiple small-scale contingencies at the same time that an operation on the scale of the present conflict in Afghanistan is sustained.

In recent years the future of aircraft carriers in the Royal Navy has been discussed. Plans were made for the construction of two new carriers that were scheduled to enter service by the middle of the next decade. The carrier debate now appears to be over; the second carrier will likely be delayed, and the number of JSF aircraft it will carry is still undecided. The UK seeks to go to a dyad of JSF and Eurofighter platforms for the Royal Air Force (RAF) and the Royal Navy. However, the manned-versus-unmanned debate is influencing thinking about future strike systems, and, given the likely contingencies in which strike aircraft would be used, new questions have arisen about the acquisition of JSF. Moreover, cost overruns and changes in the number of JSF to be purchased by the United States could further complicate the British decision. Nevertheless, it is likely that the RAF will continue to participate in the JSF program, although perhaps in tandem with procurement of new-technology strike options. Given that affordability is an issue for all UK forces, British defense planners hope that international programs may be one means of establishing a viable budget strategy for “big ticket” procurements.

Several enduring issues outlined in the 1998 UK defense review are likely to resurface in the next SDR. These include basing rights and future access to overseas facilities as part of a comprehensive approach to defense. Airpower is crucial for military operations not only in Afghanistan, but across the conflict spectrum, where its flexibility, speed of response, and reach that it affords will remain highly valued. Individual airpower capabilities, Air Vice-Marshal Hillier pointed out, such as ISR, mobility, and lift have an obvious and enduring utility in support of joint and combined operations in what the UK terms the comprehensive approach – ensuring that all levels of government are successfully coordinated to enable coherent, consistent operations. Nevertheless, there are specific challenges for airpower, he concluded, as a result of in-
creasing constraints on defense budgets. Airpower must be shown to be not only necessary, but also affordable. Because airpower can look expensive, Hillier added, the Air Force must not price itself out of the market. In this respect, he suggested, the RAF must to do more with its international partners.

Air Vice-Marshal Hillier made several other observations of direct relevance to airpower and its twenty-first-century role. Cost, he asserted, is relative. In the some eleven years that the UK contributed combat aircraft, tankers, and surveillance aircraft to enforcement of no-fly zones over Iraq, the expense of the aircraft and individual flying hours looked quite high. However, exercising containment with relatively little political or military risk for over a decade, using mostly airpower, was a remarkably cost-effective way to achieve strategic objectives. Air Vice-Marshal Hillier underscored the importance of control of the air and the continuing need to remind other nations that the strength of their air force keeps them from being attacked from the air. He added that air forces also need to mitigate some of airpower’s traditional limitations, such as constrained persistence.

Finally, Air Vice-Marshal Hillier highlighted themes that were evident in other conference sessions, including the need to consider the balance between 1) kinetic and non-kinetic activity and effect, with the assumption that there will be considerably greater willingness to pursue non-kinetic rather than kinetic options; 2) the most likely types of conflict versus the most dangerous – and therefore the balance between high-end and low-end capabilities including the cyber dimension; and 3) manned and unmanned airpower, especially as a cost-effective response to the demand for persistent ISR for operations in Afghanistan. He stressed that the RAF needs to consider platform development, including survivability across the spectrum of conflict and maximum synchronization with enabling capabilities. It will also be necessary to take into account legal and moral issues, as well as media perceptions of future operations such as the use armed UAVs.

Japan

The Japan Self-Defense Forces (JSDF) have engaged in many international peace cooperation activities with U.S. forces. As General Kenichiro Hokazono, Chief of Staff of the Japan Air Self-Defense Force (JASDF), pointed out, since 1992 Japan has participated in peacekeeping operations in Cambodia, Mozambique, the Golan Heights, and East Timor. Japan has also sent units to Iraq and in support of missions in Afghanistan. The JASDF fields F-15 aircraft, and the Japanese are interested in purchasing F-22 and/or F-35
aircraft for air defense. In addition, U.S. security policy in the Pacific relies on forward bases and logistical infrastructure in Japan.

During the Cold War, Japanese security was focused on the Soviet threat, including the air defense of Japan. The Soviet Union’s occupation of four Japanese islands – the Northern Territories – at the end of World War II enhanced the sense of a Soviet threat and complicated U.S. efforts to persuade successive Japanese governments to assume a broader role in regional and multilateral security. However, Japan became a full ally of the United States in 1958, and in the 1980s and into the 1990s Japanese forces, mainly air units, participated in several humanitarian aid and disaster relief missions. The humanitarian reconstruction support operation in Iraq was the first long-term overseas deployment for the JASDF. Constitutional restrictions have limited JASDF contributions for Iraqi reconstruction to airlift. The success of this mission was due in part to the close cooperation of the JASDF with other air forces, particularly

18 Article 9 of Japan’s post-war constitution, which was adopted in 1947, renounces war and “the threat or use of force as a means of settling international disputes.” Over the years, Japanese politicians have debated amending Article 9, but this has never attracted significant support. Moreover, while successive Japanese governments have supported the broadening of missions for Japan’s Self-Defense Forces, these missions have been limited to disaster relief and peace support operations, or they have taken place in the context of U.S.-Japan security cooperation. In 1997 U.S.-Japan security cooperation yielded new defense planning guidelines that included the possibility of Japanese participation in regional contingencies, but within circumscribed rules of engagement that needed to be spelled out in special legislation. After the al-Qaeda attacks on September 11, 2001, the Japanese government approved the Anti-Terrorism Special Measures Law, which allows Japan’s participation in UN-sanctioned operations, but limits that participation to non-combat activities, logistics support, and humanitarian roles. At present, Japan has no forces engaged in Iraq, and its support to operations in Afghanistan was limited to a maritime refueling mission, which expired in January 2010. In February 2010, following the earthquake in Haiti, the Japanese government authorized C-130 flights out of Florida to provide engineering support and aid to Haiti under the 1992 International Peace Cooperation Law to allow for the longer duration of this effort and to provide a basis to renew the mission if necessary.
the USAF and the Republic of Korea Air Force. The JASDF learned important lessons about the current operating environment from these deployments and gained critical skills through its overseas contributions and international partnering. In addition to acquiring a broader understanding of real-world operations, including threat environments featuring surface-to-air missile (SAM) use, the JASDF grappled with maintenance and redeployment issues, including mental health care for deployed airmen and support to their families in Japan.

To meet the challenges and fulfill the diverse missions of the future security environment, Japan recognizes that it must continue close defense cooperation with the United States and with international partners under United Nations auspices. Faced with diversifying threats, the JASDF will be required to play a wider range of roles. As a consequence, the U.S.-Japan alliance, particularly JASDF and USAF cooperation, will assume greater importance for the JASDF. While national defense will remain the primary mission for Japan’s military forces, JASDF leadership is seeking to identify prospective missions, including conflict prevention, reconstruction and stabilization, operations in contested domains, and space and cyberspace roles.

Although the main responsibility for Japanese space activities resides in the Ministry of Education, Culture, Sports, Science, and Technology, in 2007 Japan approved a law allowing the use of space for national defense, empowering the JASDF to identify requirements for an enhanced Japanese role in space. General Hokazono suggested that space communication and space surveillance are two areas on which the JASDF is focusing for development. According to General Hokazono, Japan is considering sending personnel to the United States for basic space education in order to gain greater knowledge about space activities. Emphasizing the continuing importance of the U.S.-Japan security partnership, General Hokazono referred to space and cyberspace as new domains in which Japan and the United States could usefully cooperate. However, he did not discuss cyber security and the conditions under which a cyber attack would constitute an act of war. This issue needs to be considered more fully not only within NATO but also in the Japan-U.S. security relationship.

Australia

Australia is a key U.S. partner in the Asia-Pacific area. Air Commodore David Steele, Air Attaché, Australian Embassy in the United States, pointed out that Australia has military forces in Afghanistan working closely with the United States and the ISAF.
ed States and Australia also cooperate on space and cyberspace. The Joint Defense Facility at Pine Gap, Australia, is a core element in U.S.-Australian defense collaboration, particularly in intelligence surveillance, shared early warning, and verification and compliance of arms control agreements. In addition to its geostrategic location, Australia also possesses unique capacities for dealing with regional emergencies. In 1999, Australia was the lead element of a United Nations peacekeeping force that deployed to East Timor to restore order after a majority of the population rebelled against Indonesian rule.

In addition to its strong participation in peace support and stabilization missions, including in Iraq and in Afghanistan, the Australian government has been active in regional efforts to train and equip South Pacific armies as well as in efforts of the Association of Southeast Asian Nations (ASEAN) to engage China in a constructive security dialogue. The Australian 2009 defense white paper, *Defending Australia in the Asia Pacific Century: Force 2030*, acknowledges the importance of the U.S.-Australian security relationship, while recognizing the growing power and influence of China in the Asia-Pacific area. The white paper, which encompasses the 2030 timeframe, speculates that China’s rise comes at a time when the United States is preoccupied in other areas of the world. It also reiterates that the Korean peninsula could once again become a flashpoint for conflict. Thus the white paper implies that U.S. power is waning at a time when the potential for conflict in the Asia-Pacific area is growing. At the same time, the Middle East, which is currently the U.S. focus, will remain a source of instability in the period out to 2030, particularly if Iran’s nuclear ambitions are realized. Climate change and resource scarcities are also noted in the white paper. New concepts for propulsion and energy-efficient systems are discussed as imperatives for Australia’s military forces.

The defense white paper sets forth Australia’s strategic interests in geographical terms: the security of Australia itself, its immediate Asia-Pacific neighborhood, and the wider world where such considerations as democratization and the rule of law play a major role in shaping Australian security perspectives. Australia identifies its ANZUS partners (New Zealand and the United States) as its principal allies.\(^\text{19}\) In 2008, Australia signed a memorandum of defense

\(^{19}\) ANZUS is supplemented by the Five Power Defense Arrangements. Signed in 1971, these are a series of agreements between the United Kingdom, Australia, New Zealand, Malaysia, and Singapore pledging the five states to consult with each other in the event of external aggression or threat of attack against Malaysia or Singapore. These agreements were formulated after the UK’s 1967 decision to withdraw its forces from positions east of the Suez and after the termination of British defense guarantees to defend Malaysia and Singapore from external attack.
cooperation with Japan. Moreover, the Australian government has sought to engage China in regional security talks. However, even though China is not identified as an adversary, Australia focuses on the development of capabilities to counter China’s upgraded missile and naval power projection capabilities.

Australia’s defense policy is based on three overarching requirements. The first is to develop or acquire autonomous self-defense capabilities. In other words, to the greatest extent possible, Australia seeks to provide for its own defense. The second premise is based on the recognition that Australia is nevertheless limited in what it can do by itself to defend a country of continental size. Therefore, Australia must have allies and coalition partners. Australian defense forces must be capable of operating with the United States and other partner forces such as the United Kingdom and New Zealand in contingencies where shared interests are at stake. The third premise is related to the second in that it seeks to increase Australian capacity for leading coalitions of the willing and operating with partners, preferably under the auspices of the United Nations. For the Royal Australian Air Force (RAAF) this means the development of expeditionary capabilities and force structures, as well as enhanced collaboration with USAF and UK forces.

**FIGURE 5**

RAAF Transition

<table>
<thead>
<tr>
<th>now</th>
<th>mid-transition</th>
<th>future</th>
</tr>
</thead>
<tbody>
<tr>
<td>F111</td>
<td>Super Hornet</td>
<td></td>
</tr>
<tr>
<td>FA18 A/B</td>
<td>JSF</td>
<td></td>
</tr>
<tr>
<td>Hawk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KC30A MRTT</td>
<td>Wedgetail AEWC</td>
<td></td>
</tr>
<tr>
<td>C130J</td>
<td>C130J +2</td>
<td></td>
</tr>
<tr>
<td>C130H</td>
<td>BFLD ALFT</td>
<td></td>
</tr>
<tr>
<td>CC08</td>
<td>B350</td>
<td></td>
</tr>
<tr>
<td>C17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP-3C</td>
<td></td>
<td>MUAS</td>
</tr>
<tr>
<td>PC9</td>
<td></td>
<td>new trainer</td>
</tr>
</tbody>
</table>

Reprinted from Air Commodore David Steele’s conference presentation, “International Perspectives: Developing Global Partnerships.”
To deal with emerging challenges, the RAAF has a specific plan for platform and organizational restructuring, including ongoing work on C² systems and network development. The RAAF has outlined a purchase plan for platform upgrades and a hedging strategy to bridge the expected gap between platform retirement and the deployment of new capabilities. For example, because the F-111 will be retired at the end of 2010, the RAAF is purchasing twenty-four F-18 *Super Hornets* to ensure its air combat capability until it acquires the JSF. Other plans include fielding a high-altitude, long-endurance RPA similar to *Global Hawk* which, among its missions, could help monitor the growing number of illegal immigrants coming into Australia. The RAAF’s acquisition priorities are presented in figure 5.

The future environment will demand that the international community and Australia continue to innovate, particularly with regard to global partnerships. As Air Commodore Steele stated, airmen must be prepared to engage at the tactical, operational, strategic, and intellectual levels. In particular, maximizing the use of spare capacity, especially training platforms and simulators will be essential. For platforms such as the C-17 that are common to more than one air force, training simulators often lie unused. If such systems were shared among nations deploying the same airframes, greater force efficiencies and reduced costs could be achieved.

Continuing this theme, Air Commodore Steele also observed that space and cyberspace are areas particularly ripe for international collaboration because of their increased importance to national security and allied/coalition operations and where situational awareness is fundamental to mission success. In the space domain, the RAAF has a requirement to improve and modernize communications networks and is investing in a wideband global satellite to provide *ultra high frequency satellite communications* (UHF SATCOM) over the Indian Ocean.
The face of warfare will continue to change with regular, irregular, and hybrid threats. In this security setting, it was broadly agreed at the conference, the United States and the USAF must develop forces that embrace multifunction and modular capabilities with agility, precision, speed, and stealth as essential attributes for conflict extending from high-end to low-end threats.

WINNING TODAY’S WARS AND PREVENTING TOMORROW’S

According to David A. Ochmanek, Deputy Assistant Secretary of Defense for Force Development, current U.S. forces are well suited to deal with the middle of today’s conflict spectrum, where the United States can defeat a hostile state’s military forces. This leaves challenges and gaps for the USAF at the high and low ends of the spectrum, with a special challenge being posed by adversaries using a combination of regular and irregular warfare. Non-state adversaries at the lower end (in the organization of their forces, not lower in level of lethality) of the conflict spectrum are challenging the United States with insurgent tactics that are extremely difficult to detect and counter. In addition, as noted by several conference speakers and discussed in greater detail below, state adversaries are developing anti-access capabilities to suppress or deny the operations of U.S. forces and to intimidate allies and partners into denying these forces access to their air space, facilities, and territory. In short, insurgency and terrorism will remain key characteristics of the security environment, and lethal technologies will become increasingly widespread and therefore will pose heightened security threats.

David A. Ochmanek, Deputy Assistant Secretary of Defense for Force Development
For the USAF, this places a premium on capabilities such as long-dwell precision fire support assets, robust communications networks, and ISR capabilities, including RPA, as well as the personnel to process, exploit, and disseminate information down to the tactical level. In order for troops to operate for prolonged periods in austere environments, greater force protection, logistics, and intra-theater lift are needed.

Like several other speakers, Major General Darren W. McDew, Vice-Director of Strategic Plans and Policy, the Joint Staff, pointed out that such challenges demand persistent engagement by the joint force, together with international partnerships that include efforts to strengthen indigenous forces and governments in order to establish security. The rising threat of piracy in the Gulf of Aden and the Indian Ocean, for example, must be dealt with on land as well as at sea, because it is rooted in an enabling network that operates from Somalia and its large areas of territory where governance is contested. According to Major General McDew, the key to meeting such challenges lies in a strategy that builds greater partner capacity, including strengthening local authorities, security force assistance, and stability operations. Such a concerted effort must be based on whole-of-government and whole-of-society approaches that encompass defense, diplomacy, and development. It includes interagency cooperation within the government and collaboration with the NGO community, as shown in figure 6.

**FIGURE 6**

Inter-Agency Collaboration

- whole of government
- defense
- diplomacy
- development
- whole of society

- Building Partnership Capacity
- Authorities
- Security Force Assistance
- Stability Operations

Reprinted from Major General Darren McDew’s conference presentation, “Finding the Appropriate Mix: Balancing Capabilities with Priorities.”
Mr. Ochmanek pointed out that this strategy has been applied successfully in the Philippines. The U.S. military worked behind the scenes with and through the Philippine armed forces to help them provide security to their own people. This strategy is being promoted by the 2010 QDR as a type of “preventive partnership” to avert conflicts before they erupt, and as an indirect counter-insurgency tool to win the hearts and minds of the local population.

Both Major General McDew and Mr. Ochmanek emphasized that building partnerships is not only a military priority, but also one that must include other interagency partners and U.S. allies. The Joint Interagency Task Force and Combined/Joint Interagency Task Force (CJIATF) concepts are likely to increase in importance in U.S. operations, particularly for humanitarian/disaster relief and counter-insurgency missions. Building partnership capacity and security force assistance also calls for unique and specific personnel expertise and specialized capabilities that can be mobilized on short notice. In order to maximize the likelihood of mission success, the USAF identifies and fields “partner-appropriate” platforms and equipment in coalition operations that are as interoperable as possible among allies.

Finally, the services have a pressing need to recruit and retain personnel with critical language skills and a capacity to operate in foreign cultures. To attract and keep such people, the USAF and its sister services will have to ensure viable career paths and progression in the chain of command that reward and encourage such career paths.

CONFRONTING HIGH-END AND ASYMMETRIC THREATS

The Secretary of Defense and the QDR include, but do not limit their focus to irregular warfare, non-state actors, and the conflicts in Afghanistan and Iraq. As Mr. Ochmanek pointed out, state adversaries such as China, a nuclear-armed North Korea, and potentially a nuclear-armed Iran pose significant threats to the United States, particularly as they develop enhanced anti-access capabilities. As a result, access to forward-deployed bases and over-flight rights are likely to become more difficult and expensive. Moreover, the assumption that forward-deployed U.S. forces and American bases would be a sanctuary from enemy attack is no longer valid. Both U.S. bases and logistics lines are increasingly at risk from ballistic and cruise missiles, submarines, enemy aircraft, and other threats.

20 The JIATF and CJIATF concepts encompass a multiservice, multiagency (and, on occasion, international organizations and agencies) structure designed to address specific requirements or tasks.
U.S. space constellations and cyber networks are also confronting heightened threats. The proliferation of missile and space technology increases the likelihood that U.S. forces will be fighting in non-permissive environments and in domains where the United States may no longer have unchallenged superiority. For example, China has fielded and is developing additional ASAT capabilities. China, Russia, and Iran as well as non-state actors possess or are actively pursuing cyber warfare assets for use against essential U.S. information networks. Given the mounting vulnerability of U.S. space-based assets, Mr. Ochmanek stated that the United States must develop alternatives such as airborne adjuncts for ISR (including the analysis, synthesis, and rapid dissemination of ISR data down to the platoon level), more survivable long-range strike assets, and a mix of stand-off and penetrating platforms to cope with an enemy fielding both offensive and defensive capabilities. The United States also requires credible retaliatory options to threaten an adversary in possession of a limited inventory of nuclear weapons.

BALANCING FUTURE CAPABILITY REQUIREMENTS

Dr. Thomas P. Ehrhard, Special Assistant to the Chief of Staff of the Air Force, stated that balancing capabilities with priorities to find the appropriate force mix is a function of one’s perspective on the future security environment. When the Air Force undertakes this strategic process, it always considers two issues: how can it respond most efficiently to the future it sees approaching, and, possibly most importantly, how can it influence what that future will be? The USAF seeks to shape the future security environment in a manner advantageous to the United States and its allies.

Lieutenant General David Deptula, Air Force Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance, elaborated on the challenge of striking a balance between the requirements of the present security setting and those of the future and how that assessment affects decisions on investment and the force mix. This is a difficult process because the United States is confronted with rising global extremism while traditional threats remain. Moreover,
resource constraints and the global economic downturn call into question how much America’s alliance partners can contribute. At the same time, technology is becoming more readily available to a broader range of potential adversaries. The erosion of the U.S. monopoly on cutting-edge technology further complicates the nation’s security.

According to Lieutenant General Deptula, balancing the challenges of today and tomorrow requires three elements: organizational change, greater service jointness, and increased interdependence. First, the USAF needs to review its organizations and processes so they can be adapted to the demands of the information age. Those currently in place are based primarily on the outdated security architecture of, and challenges addressed by, the 1947 National Security Act. Second, enhanced service jointness entails assembling the appropriate force mix for a contingency. This does not mean that each service will have an equal piece in – or even be part of – an operation. Rather, a joint force commander will select the optimum force from the menu of service capabilities available for a particular operation. Third, interdependence is closely related to the concept of jointness. Because of growing national security challenges and increasing defense resource constraints, each service must act in greater concert with the others. This means minimizing duplication of effort by the services because it creates inefficiencies, promotes redundant concepts of operations, and causes cross-service frictions. Without interdependence, service jointness will not achieve its full potential.

With this in mind, national security strategy must incorporate the above three key elements to ensure the capacity for the systematic application of force across domains. The strategy should place increased emphasis on joint force planning to reach a level of force interdependence that leverages capacities across the services without duplicating efforts. This would provide commanders with a greater range of capabilities, allowing heightened flexibility to apply force. Force interdependence would depend on greater syn-
ergy of operational capacities and require more focused and closer joint service cooperation. For example, an Air Force manned aircraft and a ship-based U.S. Navy Unmanned Combat Air System (UCAS) could be integrated into a joint long-range strike mission.

Discussion addressed the need for partnerships with other services, especially the U.S. Navy, as well as international partnerships. According to Jim Thomas, Vice President for Studies, Center for Strategic and Budgetary Assessment, the Air-Sea Battle concept being developed jointly by the Air Force and Navy should take full account of the growing A2/AD capabilities of regional actors. This calls for greater cooperation not only between the two services but also with allies and coalition partners.

At the international level, Mr. Thomas also suggested development of an airpower equivalent to the “thousand-ship navy,” or Global Maritime Partnership concept set forth when Admiral Michael G. Mullen was Chief of Naval Operations. Several difficult issues would need to be addressed: what would air/ground integration look like in a truly combined international context? How could U.S. partners do more to leverage not only their own airpower, but U.S. airpower as well? The Air Force has several initiatives that provide a basis for greater engagement with allies and coalition partners on this issue, including the Global Air Chiefs Conferences and the Global Community of Airmen.

21 Then-CNO Admiral Michael Mullen’s vision of a “thousand-ship-navy” encompassed nations with a shared stake in international commerce, security, and freedom of the seas willing to participate in global maritime partnerships to improve maritime security and the sharing of information. Membership in this "navy" would be purely voluntary with no legal ties. As explained by Admiral Mullen, the concept is “not actually about having a thousand international ships at sea. It’s more about capabilities: everyone brings what they can, when they can, for as long they can.”

22 The objective of the USAF’s Global Air Chiefs Conferences is to strengthen partnerships with the air chiefs/air force chiefs of staff and their air forces from coalition and allied nations around the globe. The conferences are designed to establish and reinforce air-force-to-air-force relationships, increasing understanding of the operational dynamics faced by airmen, and work toward interoperable solutions to meet common challenges. The first
Rebalancing USAF forces to meet these challenges will result in changes to USAF thinking about missions and their priorities. Mr. Thomas highlighted several growth areas and capabilities requirements for future USAF missions. Reflecting the growing U.S. national security emphasis on WMD elimination and counterproliferation, the USAF may be given new or broader missions to combat WMD, including the targeting of underground facilities, surveillance of suspect activities, preemptive or preventive strikes, and protection of allied/coalition partner assets. This will place a premium on development of flexible longer-range and longer-endurance multi-mission platforms (manned and remotely piloted) capable of conducting strike operations, ISR, and electronic warfare against mobile and hard targets. Related to this is the requirement to ensure that the Air Force possesses the correct weapons in adequate quantities to carry out a protracted high-intensity conventional conflict. Another USAF growth area is security force assistance encompassing training and advising indigenous aviation forces around the world.

Cyber operations and mission assurance comprise an additional area where USAF personnel and capabilities can play a key role. According to Dr. Kamal T. Jabbour, Senior Scientist for Information Assurance, Information Directorate, Air Force Research Laboratory, the United States must develop cyber technologies to enable operations in a contested cyber domain and to assure critical military missions in land, sea, air, and space against threats from cyberspace. This requires persistent situational awareness in all domains, mission and information assurance, and threat avoidance through deterrence and technology. In addition, Mr. Thomas pointed out that the cyber domain is becoming increasingly “of-
fense dominant,” meaning that the advantage frequently goes to the actor who takes the first move in cyber war scenarios. Thus, proactive, offensive cyber activities are likely to be a prominent feature of future operations. Added to this, Air Force space capacities, as has been the case with USAF ISR capabilities, will likely become even more valuable in security assistance, humanitarian relief, and disaster response operations. As a result of the increasing demand for ISR, the USAF will require systems with longer endurance and the capability to operate in non-permissive environments.

David Neyland, Director, Tactical Technology Office (TTO), the Defense Advanced Research Projects Agency (DARPA), outlined his ideas about Air Force priorities. He noted that DARPA has led the way in developing and producing many of the systems that the USAF fields today, including the Pegasus launch vehicle and ISR platforms such as Global Hawk. The TTO focuses on weapons systems, platforms, and space systems. The areas of persistent ISR, logistics, and engagement effects represent overlapping capabilities that the TTO has highlighted for future requirements, as shown in figure 7.

One area of potential interest to the USAF is the development of a long-range anti-ship missile (LRASM) because of its penetration capabilities and because it is not dependent upon GPS or supporting ISR. Another DARPA development is the Hypersonic Flight Demonstration Program (HyFly), a manned aircraft with short-range subsonic weapons. DARPA is also exploring modifications to the Predator to make it capable of vertical takeoff and landing (VTOL) and extended endurance. It is also developing Wasp/

---

23 The three-stage Pegasus is used by commercial, government, and international customers to deploy small satellites weighing up to one thousand pounds into low-Earth orbit. Pegasus is carried aloft by a Stargazer L-1011 aircraft to approximately forty thousand feet over open ocean, where it is released and then free-falls in a horizontal position for five seconds before igniting its first-stage rocket motor. The Global Hawk is a high-altitude, long-endurance unmanned aircraft system with an integrated sensor suite that provides ISR capability worldwide. Global Hawk’s mission is to provide a broad spectrum of ISR collection capability to support joint combatant forces in worldwide peacetime, contingency, and wartime operations.
Shrike micro-air vehicles and an autonomous aerial refueling process between RPA systems, both of which would contribute significantly to persistent ISR.

DARPA is also investigating operational advantages of formation flight through a program that has the potential to significantly reduce the amount of fuel consumed on multi-aircraft missions. Military pilots use formation flight techniques for mutual defense and concentration of firepower, but they also have the effect of reducing fuel consumption. Remedies for pilot fatigue and the ability to maintain the precise formation pattern (the “sweet spot” where the air vortices crossing the wings increase the aircraft’s performance) needed to maximize fuel savings are expected with the automation of the formation flight mode. The goal of DARPA’s formation flight program is to reduce aircraft drag by approximately 10 percent, which would enhance fuel savings and payload capability, and thus extend the range and capability for rapid transport of time-critical payloads. A USAF study found that formation flight involving as few as two aircraft using enhanced autopilot technologies could result in fuel savings up to 14 percent.24

---

Dr. Ashton B. Carter, Under Secretary of Defense for Acquisition, Technology, and Logistics (AT&L), shared his thinking about acquisition reform in the context of the current budget landscape, and about USAF modernization. First, because current operations are the immediate priority, Dr. Carter noted the Air Force’s pivotal role in Afghanistan. The USAF is indispensable in enabling the United States to overcome the challenges of the country’s land-locked position by providing a critically important air bridge and using air drops to reach remote areas as an alternative to the dangers posed by putting convoys on the road. USAF assets also perform vital functions in other theaters, and in addressing these OSD will consider the results of several key ongoing assessments, including the Mobility Capabilities Requirements Study (MCRS), the tanker competition, the administration’s Missile Defense Review and its Space Policy Review, the future of the long-range manned bomber, implementation of the Prompt Global Strike concept, and ongoing assessment of munitions modernization requirements. Considerations such as affordability, effectiveness, time urgency, and industrial-base issues will provide the parameters for decision making, although a key factor will also be the Secretary of Defense’s desire to field additional systems and capabilities for current operations.

For this reason, some programs, notably those for countering improvised explosive devices (IEDs), are of highest priority, and systems relevant to solving this operational challenge, such as the mine-resistant, ambush-protected
Air, Space, and Cyberspace Power in the Twenty-First Century

(MARP) all-terrain vehicle (M-ATV), will be fast-tracked. Although these programs are not specifically related to the Air Force, airpower is critical in transporting such systems into Afghanistan. Without the USAF, it would be extremely difficult to make effective use of such innovative technologies and systems. Promising technologies and systems that can be developed and fielded rapidly to combat WMD, together with other enablers, also should be accelerated, such as low-cost balloon platforms containing sensors to provide greater situational awareness to ground troops seeking, for example, IEDs.

As Dr. Carter observed, a key consideration in developing a defense acquisition strategy is establishing a balance between protecting critical assets and adapting to emerging financial and technological constraints. The Weapons Acquisition Reform Act passed by Congress in 2009 contains important and welcome provisions. These include the need to be more realistic in how cost estimates are formulated so that the DoD does not low-ball itself into something that ends up costing more than anticipated. Another focus of the Weapons Acquisition Reform Act is the need to improve the development phase, including systems engineering. Nevertheless, Dr. Carter acknowledged, there is no silver bullet to acquisition reform. Great attention must be given to the beginning, development phase of a weapons system, but department and service leaders must also anticipate future needs and problems so that they can be identified and corrected as early and cost-effectively as possible. This includes looking at how contracts are structured so that the government gets the best deal for taxpayers. It also includes the issue of fixed-price versus cost-plus contracts. For example, the less planners know about how to develop and produce the technologies, components, and other requirements for an identified future weapons system, the less they know about what it will actually cost. Because of these uncertainties, this situation suggests use of a cost-plus contract. This contrasts with development/production of systems with known technology and easily definable requirements which should be based on a fixed-priced contract. These considerations argue for maximum flexibility and agility in the acquisition and contracting process.

In any event, the shrinking defense industrial base, it was argued by DTRA Deputy Director Major General Randy Manner, USA, poses significant challenges to force de-
velopment overall, particularly as shrinking U.S. defense industrial base, poses challenges to force development, particularly as funds for research and development have been the hardest hit among the Pentagon’s personnel, operating, and procurement budgets. As a result, one participant suggested the United States may be compelled to change the way it thinks about force development; it may no longer have the luxury of fielding a spectrum of niche capabilities. Instead, the path to the future would emphasize modular and multi-function capabilities that could be tailored for specific missions. If possible, a system should be adaptable to a number of circumstances. Not only the USAF, but each of the services and OSD, it was proposed, should explore new options to reconcile budget constraints with modernization needs, retain critical expertise, especially in the systems engineering field, and sustain and reinvigorate industrial-base capacities to meet emerging security requirements and to build constructive partnerships between government and industry.

RECONCILING BUDGET CONSTRAINTS WITH MODERNIZATION NEEDS

Michael J. Bayer, Chairman, Defense Business Board, and President and CEO, Dumbarton Strategies, outlined several pressures and challenges for future defense spending. Although the 2008 U.S. defense budget exceeds the combined national defense investments of China, France, the UK, Russia, Saudi Arabia, Germany, Japan, and Australia for the same year,25 U.S. spending for defense will most likely flatten in the longer term, as figure 8 shows.

---

Pressures on acquisition accounts will increase, resulting in fewer procurements and greater gaps in capabilities, unless remedies can be found. One possible solution is increased joint and interdependent acquisitions; another may lie in the continued appropriation of Overseas Contingency Operations (OCO) funding, though this is by no means assured or necessarily the solution to the nation’s acquisition funding shortfall.26

In the past, steep declines in the defense budget occurred after a conflict, with procurement the first to be reduced. In the last few years, however, significant procurement cuts, including the termination of the combat search-and-rescue (CSAR-X) helicopter and the early cessation of F-22 production, have occurred even when the budget itself was significantly increasing. Today, the defense budget is eroding in several ways. Increases in the cost of only five major defense acquisition programs (MDAP) accounted for $206 billion between 2000 and 2007, or more than 51 percent of the total growth of the MDAP portfolio. In spite of this cost growth for new-generation programs, the biggest cause of pressure on the defense

26 The Department of Defense requested $130 billion in OCS funding for the 2010 fiscal year. These funds primarily support U.S. military operations in Afghanistan, Iraq, and Pakistan.
budget is the rising cost of personnel accounts, including pay raises and healthcare costs. Adding to the pressures on defense spending are the projected massive increases in the national debt and interest payments. This will further erode the availability of federal government funding.

In this environment, the services must come to grips with several hard realities. First and foremost, growing personnel costs will continue to be the heart of the purchasing-power challenge facing the Department of Defense. Together, the service chiefs must go to Congress with ideas for resolving this issue, highlighting the negative implications of fast-growing personnel accounts for force readiness, modernization, and even day-to-day operations. Second, acquisition accounts are the most likely area to be cut in order to meet the requirements of these other growing costs. The service chiefs, together with the Chairman of the Joint Chiefs of Staff and the Secretary of Defense, must educate members of Congress and their staffs about the implications of this trend for future forces. Department and service leaders must adopt a strategy for Congress that lays out the ramifications of shrinking defense budgets and provides options to rectify the situation.

**RESTORING AND DEVELOPING CRITICAL TECHNICAL EXPERTISE**

Dr. Carter noted the importance of sustaining the defense-industrial base and observed that in some key areas – nuclear weapons, for example – critical skills are being lost through retirements and competition with industry for engineering and high-technology expertise. This adverse trend also has serious implications for defense-related R&D. As highlighted by Dr. Werner J. A. Dahm, Chief Scientist of the USAF, the service is facing significant difficulties in attracting personnel with degrees in science, technology, engineering, and math. In part, this trend is tied to shrinking procurement budgets and fewer systems, both in terms of the quantity and variety of systems procured. As a consequence, there are fewer opportunities for the science and engineering workforce to develop the appropriate technical expertise that can be passed on to future generations. There is also less focus on later-stage engineering, which takes place once the early analysis of concepts and alternatives for developing systems and capabilities has been completed. This in turn has consequences for infrastructure and testing: the infrastructure is aging and expensive to maintain, so much of it is being taken out of the inventory without replacement. The R&D community has had to explore ways to perform the role
that physical testing used to play or find ways to modernize infrastructure beyond simple refurbishment. This has been the case, for example, at the Arnold Engineering Development Center, where most of the physical test facilities date back to 1951. Similarly, the bulk of the U.S. space launch range infrastructure is nearing or has passed the end of its intended lifespan. If, as several speakers stressed, space capabilities are increasingly vital aspects of national security, reversing the erosion of the test range facilities must become a priority.

The proliferation of technical expertise in the air, space, missile, and cyber areas has set off another adverse trend for the U.S. R&D community. Twenty years ago, relatively few countries could be considered significant players in advanced aerospace technology development. Today, however, that number has grown dramatically, accelerated by the internet, which provides access to a wide range of technical papers and scientific studies related to defense and dual-use technologies. Some forty-two thousand technical papers are published worldwide every day. This is substantially greater than even a decade ago. While in the past, the time needed to gain access to even a small number of such papers was often protracted, the ability to acquire copies of such papers today has vastly increased, both in the numbers that can be obtained and the speed of access. The result is that in a matter of hours it is possible to become extremely knowledgeable in a given area about what are likely to be the most productive approaches, about what has been tried and what has or has not worked well. In addition, the number of foreign nationals being educated in technical fields in the United States and other Western nations, continues to grow and, contrary to popular belief, foreign students frequently do not remain in the United States but instead return home to build engineering skills and develop militarily significant capabilities and programs in their own nations. Dr. Dahm pointed out that the effects of lowered barriers to entry in the development of military capabilities will not
be fully manifest for several years. Nevertheless, now is the time to assess how this trend may affect USAF and DoD R&D and acquisition strategy in a world of growing and accelerating technology diffusion.

Set against these trends is a fundamental shift in how R&D is conducted not only in the United States, but also in Europe and to some extent in Japan. In the past, most large engineering companies had substantial in-house R&D organizations that conducted everything from basic to applied research to advanced development, and engineering activities interfaced with real systems development. Because of globalization and business streamlining, many of these organizations have shifted resources to produce consumer goods such as personal computers and cell phones, making in-house military R&D less supportable. The subsequent divestiture of commercially based military R&D programs led to the growth of U.S. entrepreneurial companies, which now are responsible for most science- and technology-related industrial activity. Many of these companies are funded through the DoD-sponsored Small Business Innovative Research (SBIR) program. The USAF is the single biggest contributor to SBIR endeavors. In this light, it is worth exploring how best to restructure the SBIR program to support USAF acquisition strategy.

SUSTAINING THE DEFENSE INDUSTRIAL BASE AND LEVERAGING THE PRIVATE SECTOR

Particularly in a constrained budget environment, private sector innovation and resources are essential to help meet emerging security requirements. Jon C. Jones, President of Space and Airborne Systems and Vice President, the Raytheon Company, shared an industry perspective on the future threats faced by the USAF and the role that industry can play in achieving U.S. national security.

† The conference organizers and cosponsors express their condolences on the passing of Jon C. Jones, who died on March 6, 2010.
goals. He focused on three areas in need of innovation: 1) industry’s development and provision of capabilities to U.S. warfighters; 2) the U.S. government’s acquisition and export policies; and 3) the partnership between industry and government to deliver needed capabilities.

The development of a revised acquisition strategy requires innovation and a new partner relationship between government and industry. The Pentagon and industry can innovate by coming up with cost-effective solutions to enhance existing products and improve production to meet or exceed “the speed of need.” For example, the Raytheon Advanced Combat Radar (RACR) program can be retrofitted on F-16s and F-18s to provide a fifth-generation radar capability for fourth-generation platforms. RACR is a Raytheon initiative, financed without government funds. As a result, RACR was developed at a much lower cost than would have been the case had it followed the traditional government procurement process. For applications in space, Raytheon has developed the Responder line of products, a modular, multi-purpose payload with a family of interchangeable mission-specific sensors. It has about 75 percent commonality for a broad range of missions and can be customized for another 25 percent of missions. Mr. Jones said that Responder was developed in approximately eighteen months for a cost of about $15 million.

Another example of how U.S. industry and the government can improve the acquisition process is through export policy reform. A vigorous U.S. export policy will help stabilize the industrial base, promote economies of scale (thus reducing overall procurement costs), and promote interoperability and closer partnership with allies. Export reform needs to include safeguards to protect critical U.S. technologies, which Mr. Jones believes is “a very manageable” issue. Finally, industry, the USAF, and DoD must coordinate R&D efforts more closely to overcome emerging threats and remain competitive in the twenty-first-century security environment.
Strategic Surprise and Wildcard Considerations

The future security setting will undoubtedly be shaped by strategic surprise and wildcard considerations. On September 11, 2001, the United States experienced a strategic surprise, in the form of the al-Qaeda attacks against the World Trade Center and the Pentagon. A previous strategic surprise, of course, was the Japanese attack on Pearl Harbor in 1941. In the future, the United States could be confronted with other strategic surprises that have potentially catastrophic consequences for the U.S. economy and population: an EMP attack leading ultimately to large numbers of deaths as essential services and food supplies vanish, or a biological incident that kills hundreds of thousands of people before consequence management operations can be launched. While Pearl Harbor was an attack on U.S. territory in the Pacific, 9/11 struck at the continental United States. While World War II mobilized the United States to fight in Europe and the Asia-Pacific area, 9/11 brought into sharp focus the nexus between international security and domestic security. Airpower became an essential element of the military’s ability to safeguard civilian airspace over the United States.

Throughout the conference there was discussion of asymmetric strategies and capabilities whose effect would be to circumvent U.S. dominance. If strategic surprise could be predicted with great accuracy, there would be no strategic surprise; but the areas of U.S. vulnerability form a useful basis for focusing efforts to avoid strategic surprise or to mitigate its consequences. Among the asymmetric challenges, those involving EMP, cyber war, and space stand out. It follows that emphasis should be placed first on deterring strategic surprise by protecting assets whose vulnerability would tempt asymmetric action, while reducing the consequences of such asymmetric action. Participants generally agreed that the Air Force, like the other services, will need to sustain basic R&D if strategic surprise is to be avoided or its effects mitigated.
Hedging against Wildcards and Strategic Surprise

Over the course of the conference, participants identified several general areas where attention should be focused in developing hedging strategies against wildcards and strategic surprise. Each has relevance to USAF R&D and acquisition:

- Examining new command-and-control network concepts to find alternative options for the bandwidth constraints facing U.S. forces today. In the cyber arena, the entity that initiates cyber war gains a potentially decisive advantage over the defender. Therefore, countering the cyber threat must be central to USAF and joint planning. Several participants pointed to the doctrinal and legal issues associated with the cyber domain and suggested that many legal questions remain unresolved. For example, does the DoD have a right to watch over and engage with commercial or civilian networks? What are the privacy issues involved?

- Retaining the U.S. edge in stealth technologies in the face of ever more sophisticated enemy integrated air defense environments and peer competitor deployment of fifth-generation fighter aircraft.

- Developing new technologies in electronic warfare, which continues to be a key enabling capability for conflict operations across the warfare spectrum.

- Continuing development of unmanned technologies for missions and programs focused on increased loiter time, aircraft carrier deployments (UCAS, with the Navy, for instance), and enhanced munitions capabilities to deal with new and emerging threats. Moreover, developing next-generation target discrimination technologies is important to operations where the risk of collateral damage is high. This applies not only to RPA but also to manned combat aircraft.

- Developing situational awareness technologies to find, fix, and track mobile and high-value targets and sensors for counter-WMD missions and homeland defense.

- Getting back to basics in understanding the effects of nuclear and biological weapons. If a WMD is used, the U.S. military will be tasked with a range of consequence management missions.

- Enhancing attack attribution capabilities for WMD use. Specifically, this means the further development of nuclear forensics, data-bases, and augmented intelligence among the services, the agencies, and with allies and other U.S. partners.
Hedging against catastrophic systems failure in the event of an enemy breakthrough in ASAT and/or directed-energy warfare (DEW) technologies, or use of an EMP weapon.
In a survey of many of the important areas where the U.S. Air Force is focusing its strategic efforts, Michael B. Donley, Secretary of the U.S. Air Force, spoke about the Air Force’s vision and the challenges of aligning it with future strategic requirements. Although how wars are fought changes and expands into new domains, the enduring characteristics of airpower (speed, range, and flexibility) remain key to providing a wide array of strategic options. According to Secretary Donley, the Air Force sees itself as a partner to be trusted and relied upon in future conflicts whose complex and hybrid nature will pose challenges that require joint applications of power and a whole-of-government approach. Broadening this theme of cooperation, Secretary Donley, like several other speakers, pointed to the importance of coalition partners and allies. America confronts a wide range of strategic challenges such as global terror networks, nations seeking to acquire long-range missiles and nuclear weapons, and suppliers prepared to make such capabilities available to others. Economic and regional powers are emerging whose intentions the United States does not know, failed or failing states continue to present their own distinct challenges, multiple actors are vying to dominate space, and threats from cyberspace are mounting. Planning for uncertainty will be essential in this complex security environment.

The United States faces these challenges with finite resources, making it imperative that decision makers know when and where change is occurring so that
limited capabilities can be concentrated where they will have the greatest effect. Continuous engagement with allies and coalition partners provides a key approach to developing informed, shared perspectives on the security environment, together with opportunities to shape the security setting in ways favorable to the United States. Secretary Donley pointed to the importance of such engagement at many levels—from combatant commanders down to the C-17 load masters who are able to speak in the language of their international counterparts. Emphasizing another conference theme, Secretary Donley underscored the emphasis on understanding the culture and language of other countries, including the development of what he termed “coalition-minded warriors.” This is an ongoing Air Force initiative, with nearly 350 political-military and regional affairs specialists now in the Air Force and another 228 presently in the pipeline. As important as this initiative is, Secretary Donley suggested that much remains to be done.

Building on the theme of engagement, Secretary Donley addressed the efforts of the Air Force to help build or rebuild the Iraqi and Afghan air forces to establish safe flight operations, technical schools, and logistical systems. He also described other engagement initiatives, including working with air forces in Europe and elsewhere that have partnerships with the United States to operate advanced weapons systems such as the JSF and space-based assets. Engagement, he suggested, enhances access, with overseas basing constituting the lifeblood of a global U.S. Air Force. Here the continuing challenge is to find the appropriate balance between the forward stationing of U.S. forces in key regions and the need to preserve maximum global flexibility. Understanding the interests, motivations, and sensitivities of potential partners is critically important in helping the U.S. military find that right balance.

Among the other themes stressed by Secretary Donley was the need to accommodate uncertainty by building a balanced force that in essence hedges America’s bets. Flexibility and versatility enhance the ability of U.S. forces to operate across the potential conflict spectrum. However, achieving a more balanced force has an important temporal dimension. Today’s operational needs must be met while making the right investment in tomorrow’s capabilities. In addition to such needs, the USAF must support innovation, including for example, weaponizing RPA and wherever possible “connecting the dots” across the air, space, and cyber domains. Secretary Donley highlighted the need to foster within the Air Force the institutional capacity for innovation with a dynamic approach to strategy.
Several interrelated conclusions emerging from the conference focused on deterrence strategy, the nuclear enterprise, USAF overseas posture and basing infrastructure, anti-access/area-denial threats, asymmetric challenges, space dominance, cyber security, organizational change and joint force operations, combatant command support, engagement and international security cooperation, acquisition reform and affordability, and support to civil authorities.

**Deterrence Strategy**

In contrast to the bipolar Cold War nuclear setting, today’s setting includes multiple, independent nuclear actors. Some of these independent nuclear weapons states are enemies, some are rivals, and some are friends, but the initial decision for action by any one of them may lie beyond U.S. control. The United States will need to influence, signal, and restrain enemies. It will need to deal with nuclear friends and allies and continue to provide security guarantees. America may confront catalytic warfare where an ally or third party could initiate action resulting in a nuclear exchange. Although the United States would not be a party to the nuclear escalation decision, it could be drawn into the escalating conflict. Compared to bipolar escalation, we know very little about strategic nuclear interaction and escalation in a multi-polar, multi-nuclear world. The U.S. nuclear deterrent must restrain a wider variety of actors today than during the Cold War. This requires a range of capabilities and the capacity to address specific challenges. The deterrent must provide security guarantees and assurance sufficient to prevent the initiation of catalytic warfare by an ally, while deterring an adversary from resorting to nuclear escalation. In a multi-polar world the United States may also need simultaneously to deter more than one other nuclear state. Deterrence requires four critical elements: early warning, command and control, delivery systems, and weapons. In each, the Air Force plays an indispens-
able role. Early warning capabilities rely on Air Force satellites and radar networks. Command-and-control infrastructure is provided by the Air Force, including Milstar satellites and, in the future, Advanced Extremely High Frequency (AEHF) satellites.

**The Nuclear Enterprise**

No defense priority is more important than the responsibility for operating, maintaining, securing, and supporting nuclear weapons. The USAF has the responsibility for the bomber and ICBM components. In response to new challenges including nuclear proliferation, the USAF and the joint force will have to look at deterrence and dissuasion through a new conceptual lens, and respond to the perspectives of a broader range of actors and a more diverse set of existential threats. Future actors may not be deterred by traditional means based solely on the threat of retaliation or punishment. As a result, a more extensive set of escalation tools, to include conventional long-range global strike capabilities, will be needed to cope with future crises and conflicts.

**U.S. Overseas Basing and the Anti-Access/Area-Denial Threat**

The increased availability of A2/AD assets coupled with growing threats to the global commons are decreasing the power projection capabilities of the United States. Such threats as cruise-missile-armed aircraft and long-range missiles present challenges for defending America’s overseas bases. Emerging A2/AD capabilities, and their proliferation among potential adversaries, challenge the viability of the notion that forward-deployed U.S. forces and bases will be a sanctuary from enemy attack. Consequently, the United States must create a more flexible basing structure encompassing a passive and active defensive posture that includes speedy dispersal of assets to additional bases; hardening infrastructure/assets to minimize damage if attacked; increased warning time of attack; and air, ballistic, and cruise missile defenses. At the same time, the United States must continue to develop long-range, offensive systems such as low-observable manned and unmanned strike platforms, precision missiles, and ISR assets to penetrate heavily defended A2/AD environments. This approach will increase the survivability of U.S. forward-deployed systems and power projection capabilities and thus bolster deterrence and U.S. guarantees to U.S. allies and friends.
Asymmetric Challenges

The escalating number of actors gaining access to advanced and dual-use technologies increases the potential for asymmetric attacks against the United States and its allies by those who are unable to match U.S. military technology. They pose increasing challenges to the ability of the United States to project power through the global air, maritime space, and cyberspace domains. By definition such attacks target specific U.S. vulnerabilities, ranging from space assets, financial, transportation, communications infrastructure, energy, and food and water supply, to mention only the most obvious. Asymmetric attacks denying access to critical networks and capabilities may be the most cost-effective way to circumvent traditional U.S. force advantages. The USAF and DoD must develop systems and technologies that can offset and defend against asymmetric capabilities. This will require a robust R&D program and enhanced USAF cooperation with its sister services and international partners and allies.

Space Dominance

Space is increasingly a contested domain where U.S. dominance is no longer assured given the growing number of actors in space and kinetic and non-kinetic attack threats, including ASAT weapons, EMP, and jamming. As a result, the United States must protect vital space-based platforms and networks by reducing their vulnerability to attack and/or disruption and increasing their resilience if an attack does occur. Required steps include hardening and incorporating stealth into next-generation space systems; developing rapid-replenishment assets, including micro-satellite technologies and systems and new launch capabilities; and lessening U.S. dependence on space capabilities by supplementing them with air-based assets such as high altitude, long endurance, penetrating, and standoff ISR platforms; and increasing cooperation among the services and with allies to develop such capabilities.

Cyber Security

Given the seriousness of the threat of cyber attacks, DoD has formally recognized cyberspace as a domain. In the cyberspace domain, mission awareness and assurance require an understanding of the dependencies of missions on specific cyber assets, the interdependence of those cyber assets, and the interdependence of those missions. Many USAF functions rely upon cyber assets, making them a prime target for an adversary who cannot or chooses not to confront the United States using conventional methods. Therefore, in addition to developing technology for attributing cy-
ber attacks, the United States must develop contingency plans for a range of cyber scenarios in which U.S. military, as well as civilian and commercial, networks could be compromised or manipulated. Toward this end, the United States is attempting to construct a layered and robust capability to detect and mitigate cyber intrusions and attacks.

However, more needs to be done. For example, the complicated division of responsibility within DoD in the cyber realm illustrates the need to develop a better organizational approach to countering the cyber threat. This is being addressed with the creation of USCYBERCOM, which will operate and defend DoD’s networks and synchronize offensive and defensive cyber capabilities, linking offensive, defensive, and intelligence aspects in a single focus. Each of the services has created a cyber component command tasked with supporting USCYBERCOM as needed. Three priorities for the USAF’s cyber component command were outlined by a conference participant: 1) develop capabilities to protect essential military and civilian cyber systems; 2) enhance the USAF’s capacity to respond to joint warfighter needs in terms of USAF personnel, command participation, and resolution of technical questions; and 3) prioritize training and the recruitment of personnel with the necessary skill sets. These efforts will entail greater service, interagency, international, and private-sector collaboration.

Organizational Change and Joint Force Operations

To address growing national security challenges, increasing defense resource constraints, and to become a more effective and efficient joint fighting force, the U.S. military forces need to adapt their organizations and processes to the exigencies of the information age and security setting of the second decade of the twenty-first century. This requires developing a strategy that places increased emphasis on joint force operations in which each service acts more collaboratively with the others, leverages capacities across the services without duplicating efforts, and encourages the interoperability of systems. This would provide combatant commanders with a greater range of capabilities and allow heightened flexibility to apply force. An excellent example of this approach is the Air-Sea Battle concept being developed jointly by the Air Force and Navy, which envisions heightened cooperation between the two services as well as with allies and coalition partners.
Intelligence, Surveillance, and Reconnaissance Capabilities

ISR capabilities are increasingly in demand to provide access and track a range of high-value and hard-to-find targets in contested airspace, such as mobile missile launchers and underground bunkers. This demand increases the need for survivable and stealthy systems and the development of next-generation unmanned platforms. The USAF must continue to emphasize precision targeting, for both strike and close air support missions. High-fidelity target discrimination enabled by advanced radars and directed-energy systems, including the ability to find, track, and target individuals and individual combatants within a crowd, will provide battlefield commanders with improved options and new opportunities for leveraging joint assets.

Engagement and International Security Cooperation

USAF and service imperatives include augmented allied and coalition partner engagement. Engagement can enhance situational awareness and early warning of impending crises as well as contribute to an understanding of the interests, motivations, traditions, and cultures of potential adversaries and prospective coalition partners. Moreover, foreign partner engagement and outreach provide an avenue to influence partner and adversary perspectives, thus shaping the environment in ways favorable to U.S. national security interests. Engagement also may be the key to realizing another Air Force and joint priority: to sustain or gain access to forward operating bases and logistical infrastructure. This is particularly important given the growing availability of A2/AD assets and their ability to impede U.S. power projection capabilities.

Acquisition Reform and Affordability

The Air Force must field options and capabilities to support current operations and pressing missions while at the same time pursuing promising technologies to build the force of the future. Leadership must strike an appropriate balance between the requirements of the present security setting and those of the future. Affordability, effectiveness, time urgency, and industrial base issues inevitably shape procurement choices and reform. Today’s critical assets must be protected while resources are also allocated to meet future needs. Given the long lifespan anticipated for many weapon systems, planners need to make the most reliable cost estimates and identify problems at the outset of a weapons system’s development phase so that they can be corrected as early and cheaply as possible.
Support to Civil Authorities

As evidenced in the aftermath of the 2010 earthquakes in Haiti and Chile (the Chile earthquake occurred in February 2010, after this conference), the USAF has a vital role to play in international relief operations and support to civil authorities. In Haiti, the USAF re-opened the airport and deployed contingency response elements, while also providing ISR support for the joint forces in the theater. In Chile, USAF satellite communication capabilities were critical to the recovery and relief efforts. USAF civil support roles are likely to grow to include greater use of the reserve components. Consequently, USAF planners should undertake a reassessment of the mix of active and reserve forces and capabilities to identify potential mobilization shortfalls and requirements.
A recurring theme at the conference was the need for the USAF to continue to examine more closely specific issues of opportunity and vulnerability. Such issues could be addressed in focused working groups that would examine such questions as:

- How can air, space, and cyberspace capabilities best support deterrence operations, preserve U.S. freedom of action, and support national objectives?
- How should the USAF leadership re-conceptualize its vision, institutional identity, and force posture to align as closely as possible with the future national security setting?
- What is the appropriate balance between high- and low-end air and space capabilities that will maximize military options for national decision makers, given emerging threats and fiscal constraints?
- What are the opportunities, options, and tradeoffs for investment and divestment in science and technology, infrastructure, and programmed capabilities?
- What are additional interdependent concepts, similar to Air-Sea Battle, that leverage cross-service investments to identify and foster the development of new joint capabilities?
- What are alternative approaches to officer accessions and development to support shifting and emerging Air Force missions, operations, and force structure including cyber warfare and remotely piloted aircraft (RPA)?
- How can the USAF best interact with Capitol Hill to help preserve or refocus the defense-industrial base as well as minimize mandates and restrictions that weigh on future Air Force investments?

The United States Air Force has a long and proud tradition of innovation and leadership during times of great peril for U.S. national security. Neil Sheehan, author of *A Bright Shining Lie*, and *A*
Fiery Peace in a Cold War, a biography of General Bernard Schriever, described for conference participants the creation of what is now the USAF's Ballistic and Systems Division, under the leadership of General Schriever, whose work was crucially important in developing and building the ICBM and related systems. The path to developing this transformative capability was made possible by the technological vision of General Schriever and his determination to face reality and listen to “the bad news” in order to solve rather than ignore problems. When confronted with obstacles, General Schriever brought his case to the attention of Congress and President Eisenhower, thereby garnering the necessary political support to speed the decision-making and acquisition process for what he viewed to be, and what remains, a critical U.S. national security responsibility.

The technological innovations driven by General Schriever have links to many of the capabilities now vital to the USAF in fulfilling its national security missions. The ICBM was also a catalyst for the creation of the aerospace industry, opening space not only to military use, but to civilian and commercial endeavors as well.

In today’s complex security environment, the USAF still needs to be able to harness a technological vision and relate it to a strategic purpose in a way that builds on the Air Force’s indispensable contributions over the years to U.S. national security. To this end, the USAF must continue to be an organization that views debate, as General Schwartz put it in his opening address, “…as the whetstone upon which we sharpen our strategic thinking.” This debate must also be used in pursuit of political support and to ensure that the USAF maintains and develops critical capabilities to support U.S. national security priorities. The 38th IFPA-Fletcher Conference on National Security Strategy and Policy was conceived to serve as a contribution to that debate and discussion.


Glossary of Terms and Acronyms

Note: Sources are referenced in parentheses after the definition. A bibliographic footnote is included the first time a source is used. Definitions without sources are provided by IFPA staff.

A

A2/AD (see anti-access/area-denial).

AC/RC Active component/reserve component. Collaborative efforts between active and reserve components (see reserve component).

actionable intelligence Intelligence with the timeliness, accuracy, and relevance required for a commander to take actions, based on that intelligence, in furtherance of the mission.

active defense The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy.

active defensive posture The preparedness or condition of a force to pursue an active defense.

Advanced Extremely High Frequency (AEHF) satellite A satellite communications system designed to provide secure, survivable communications to U.S. warfighters during all levels of conflict. AEHF is to follow Milstar as the basis for DoD’s military satellite communications architecture. The first flight of the AEHF satellite program, named Pathfinder, will be programmed to operate initially as a Milstar II satellite. The second flight will then be launched as a fully capable AEHF satellite (GlobalSecurity.org).1

Aegis Ashore A land-based Aegis system currently under development.

Aegis Ballistic Missile Defense (BMD) System A U.S. DoD Missile Defense Agency program developed to provide a last line of defense against ballistic missiles. Aegis BMD (also known as Sea-Based Midcourse) is designed to intercept ballistic missiles post-boost phase and prior to reentry. It builds upon the Aegis Weapon System with the AN/SPY-1 radar and Standard missile technologies. Aegis BMD equipped vessels can transmit their target detection information to the Ground-Based Midcourse Defense system, and/or engage potential threats using the SM-3 missile (GlobalSecurity.org).

AEHF (see Advanced Extremely High Frequency satellite).

Aerial port (APORT) An airfield that has been designated for the sustained air movement of personnel and materiel as well as an authorized port for entrance into or departure from the country where located (JP 1-02).²

Aerial port of disembarkation (APOWER) see port of disembarkation.

Aerial port of embarkation (APOEM) see port of embarkation.

AFGSC (see Global Strike Command).

Air defense (AD) All defensive measures designed to destroy attacking enemy aircraft or missiles in the Earth’s envelope of atmosphere, or to nullify or reduce the effectiveness of such attack (JP 1-02).

Air Force Global Strike Command (AFGSC) see Global Strike Command.

Air operations center (AOC) A USAF field headquarters (HQ) for planning air operations.

AirLand Battle doctrine The overall conceptual framework that formed the basis of the U.S. Army’s European warfighting doctrine from 1982 into the late 1990s, emphasizing close coordination between land forces acting as an aggressively maneuvering defense, and air forces attacking rear-echelon forces feeding front line enemy forces (FM 101-5).³

Air-Sea Battle An emerging joint USAF-USN operational concept envisioning heightened cooperation between the two services and potentially with allies and coalition partners to develop power projection that includes air, sub-surface, and SOF capacities, manned and unmanned ISR, assured communications, and new-generation strike capabilities.

Anti-access/area denial (A2/AD), adj. (often used with “threat”, “operations” or “technology”) Designed to hinder the deployment of forces into a combat theater, limit the locations from which those forces can effectively operate, or force them to operate from locations farther from the locus of conflict than they would normally prefer.

Anti-satellite (ASAT), adj. Designed to destroy or disable satellites.

ANZUS Australia-New Zealand-U.S. partnership.

AOC (see air operations center).

AOR (see area of responsibility).


³ Department of the Army, Staff Organization and Operations, FM 101-5, 1993.
Air, Space, and Cyberspace Power in the Twenty-First Century

APOD  Aerial port of disembarkation (see port of disembarkation).

APOE  Aerial port of embarkation (see port of embarkation).

area of responsibility (AOR)  The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations (JP 1-02).

ASAT  (see anti-satellite).

ASEAN  Association of Southeast Asian Nations.

Asymmetry  Dissimilarities in organization, equipment, doctrine, and values between other armed forces (formally organized or not) and U.S. forces. Engagements are symmetric if forces, technologies, and weapons are similar; they are asymmetric if forces, technologies, and weapons are different, or if a resort to terrorism and rejection of more conventional rules of engagement are the norm (FM 1-02).

AT&L  Acquisition, Technology, and Logistics, as in the Under Secretary of Defense for Acquisition, Technology, and Logistics.

Attribute  v. -To establish a party as the originating agent of a particular act.

awareness  Knowledge and understanding of the operational area’s environment, factors, and conditions, to include the status of friendly and adversary forces, neutrals and noncombatants, weather and terrain, that enables timely, relevant, comprehensive, and accurate assessments, in order to successfully apply combat power, protect the force, and/or complete the mission. See operational environment (FM 1-02).

B

B-2  Spirit stealth bomber  A multi-role bomber capable of delivering both conventional and nuclear munitions (GlobalSecurity.org).

B-52  Stratofortress bomber  The primary nuclear-role bomber in the USAF inventory, providing the only air launch cruise missile carriage in the USAF. The B-52H also provides theater commanders with a long range strike capability, carrying nuclear or conventional ordnance with worldwide precision navigation capability (GlobalSecurity.org).

ballistic missile  Any missile that does not rely upon aerodynamic surfaces to produce lift and consequently follows a ballistic trajectory when thrust is terminated (JP 1-02).

BAMS  (see broad area maritime surveillance).

bandwidth  The difference between the limiting frequencies of a continuous frequency band expressed in hertz (cycles per second). The term bandwidth is also loosely used to refer to the rate

4  Department of the Army, Operational Terms and Graphics, FM 1-02, 2010.
at which data can be transmitted over a given communications circuit. In the latter usage, bandwidth is usually expressed in either kilobits per second or megabits per second (*JP 1-02*).

**base** 1. A locality from which operations are projected or supported. 2. An area or locality containing installations which provide logistic or other support. 3. (DOD only) Home airfield or home carrier.

**basing infrastructure** All buildings and permanent installations necessary for support, redeployment, and military forces operations (e.g., barracks, headquarters, airfields, communications, facilities, stores, port installations, and maintenance stations) (*JP 1-02*).

**battlespace awareness** (see awareness).

**broad area maritime surveillance (BAMS)** USN-Raytheon project to develop a USN surveillance UAV (*GlobalSecurity.org*).

**C**

*C-17 Globemaster III* A four engine turbofan aircraft capable of airlifting large payloads over intercontinental ranges without refueling (*GlobalSecurity.org*).

*C-17 Consortium* Group of NATO and Partnership for Peace nations working jointly to acquire the C-17 aircraft, "committed to the belief that by working together, pooling resources and fairly sharing the cost burdens of strategic airlift as one consortium, partner nations will achieve greater efficiencies in defense investment and operational capacity than otherwise possible" (*GlobalSecurity.org*).

**C²** Command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission (*JP 1-02*).

**C³** Command, control, and communications.

**C⁴** Command, control, communications, and computers. Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander’s exercise of command and control across the range of military operations (*JP 1-02*).

**C⁴I** Command, control, communications, computers, and intelligence. See intelligence and C⁴.

**C⁴ISR** Command, control, communications, computers, and intelligence, surveillance, and reconnaissance (see separately intelligence, surveillance, reconnaissance, and C⁴).
C-802 missile  Land attack and anti-ship cruise missile (Western designation Saccade), an improved version of the C-801 which employs a small turbojet engine in place of the original solid rocket engine (GlobalSecurity.org).

Capstone Concept for Joint Operations (CCJO)  The Chairman of the Joint Chiefs of Staff’s (CJCS) vision for how the joint force circa 2016-2028 will operate in response to a wide variety of security challenges, proposing that future joint force commanders will combine and subsequently adapt some combination of four basic categories of military activity combat, security, engagement, and relief and reconstruction in accordance with the unique requirements of each operational situation (cf. full-spectrum operations).

cascading proliferation  A situation in which U.S. allies conclude that the extended U.S. nuclear guarantee is no longer credible and decide to develop nuclear weapons (JP 1-02).

catalytic warfare (sometimes referred to as catalytic attack)  A term coined by Dr. Herman Kahn to refer to the “notion that some third party or nation might for its own reasons deliberately start a war between two major powers.” According to Kahn, “the widespread diffusion of nuclear weapons would make many nations able, and in some cases also create the pressure, to aggravate an on-going crisis, or even touch off a war between two other powers for purposes of their own.” (See Herman Kahn, Thinking the Unthinkable, [New York: Horizon Press, 1962], 57, 217).

CBRN  Chemical, biological, radiological, and nuclear.

CCJO  (see Capstone Concept for Joint Operations).

CENTCOM  (U.S. Central Command).

chemical, biological, radiological, and nuclear (CBRN), adj.  A grouping of threats, each with significant potential to disrupt civil society or destroy civilian property, often associated with weapons of mass destruction.

Civil Air Patrol (CAP)  The official auxiliary of the U.S. Air Force. In addition to providing emergency services, CAP-USAF personnel provide support, liaison and oversight to the more than 57,000 CAP cadets and volunteers (GlobalSecurity.org).

CJIA TF  Combined/Joint Interagency Task Force. A group formed for a specific mission or purpose; may consist of persons and assets from any part of USG.

close air support (CAS)  Air action by fixed- and rotary-wing aircraft against hostile targets that are in close proximity to friendly forces and that require detailed integration of each air mission with the fire and movement of those forces (JP 1-02).

COCOM  (see combatant command).
**cold atoms** A research concept that, along with nanoscale technologies, may result in computer chips for new devices to conduct physics research at a very small scale.

**collateral damage** Unintentional or incidental injury or damage to persons or objects that would not be lawful military targets in the circumstances ruling at the time. Such damage is not unlawful so long as it is not excessive in light of the overall military advantage anticipated from the attack (*JP 3-60*).[^5]

**combat search and rescue (CSAR)** A specific task performed by rescue forces to effect the recovery of distressed personnel during war or military operations other than war (*JP 3-50.2*).[^6]

**combatant command (COCOM)** Nontransferable command authority established by Title 10 (“Armed Forces”), United States Code, Section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority) (*JP 1-02*).

**combatant commander (CCDR)** Commander of a COCOM.

**combat theater** (see theater of operations).

**combined, adj** Comprised of various arms within a single service.

**command and control** (see C^2).

**command, control, communications, and computers** (see C^3).

**conflict spectrum** (see spectrum of conflict).

**contingency** An emergency involving military forces caused by natural disasters, terrorists, subversives, or by required military operations. Because contingencies are by nature unpredictable and uncertain, plans, rapid response, and special procedures must be

in place to ensure the safety and readiness of personnel, installations, and equipment when the unexpected occurs (JP 1-02).

**contingency response element** A unit or capability deployed in response to a contingency (see contingency and response force).

**CONUS (continental United States)** United States territory, including the adjacent territorial waters, located within North America between Canada and Mexico (JP 1-02).

**Cooperative Threat Reduction (CTR)** The Nunn-Lugar Act of 1991, an initiative coauthored by Senator Richard Lugar and former Senator Sam Nunn establishing the Cooperative Threat Reduction Program. The program seeks to help the states of the former Soviet Union safeguard and dismantle their stockpiles of nuclear, chemical, and biological weapons, related materials, and delivery systems. The Defense Threat Reduction Agency (DTRA) executes the program for the Department of Defense and works in coordination with partner governments and other U.S. government agencies who administer related projects.

**crisis** An incident or situation involving a threat to the United States, its territories, citizens, military forces, possessions, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, political, or military importance that commitment of U.S. military forces and resources is contemplated in order to achieve national objectives (JP 5-0).^7^

**cruise missile** Guided missile, the major portion of whose flight path to its target is conducted at approximately constant velocity; depends on the dynamic reaction of air for lift and upon propulsion forces to balance drag (JP 1-02).

**CSAF SSG** Chief of Staff of the Air Force’s Strategic Studies Group.

**CSAR** (see combat search and rescue).

**CSAR-X** combat search and rescue replacement helicopter.

**cyber warfare** Hostile or defensive acts performed in or designed to affect an opponent’s use of cyberspace.

**USCYBERCOM** U.S. Cyber Command. A sub-unified command subordinate to U.S. Strategic Command (STRATCOM) charged with addressing vulnerabilities and meeting the array of cyber threats to military systems (GlobalSecurity.org).

**cyberspace** The virtual environment in which digitized information is communicated over computer networks. This includes the entire domain of electronic technology, referring mainly to the computational, communication, and control capabilities this technology derives from the manipulation of electromagnetic energy.

---

DARPA Defense Advanced Research Projects Agency.
DCA (see dual-capable aircraft).
deployed forces Military forces stationed or temporarily sent outside the territorial boundaries of the United States.
deterrence The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction (*JP 1-02*).
DEW (see directed energy weapon).
directed-energy weapon (DEW) A system using directed energy primarily as a direct means to damage or destroy enemy equipment, facilities, and personnel (*JP 1-02*).
dispersal The spreading or separating of troops, materiel, establishments, or activities that are usually concentrated in limited areas to reduce vulnerability.
DoD U.S. Department of Defense, also DOD.
domain protection The protection of specific assets; as opposed to ensuring the carrying out of the functions those assets are designated to perform, whether the assets themselves survive or not (see mission assurance).
DTRA Defense Threat Reduction Agency.
dual-capable aircraft (DCA) Allied and U.S. fighter aircraft tasked and configured to perform either conventional or theater nuclear missions (*JP 1-02*).
dual-use, adj. Having both civilian and military uses.

E
Sentry AWACS (airborne warning and control system)
Aircraft that provides all-weather surveillance, command, control and communications needed by commanders of U.S. and NATO air defense forces (*GlobalSecurity.org*).
EA-6B Prowler A unique national asset that can be deployed from land bases and aircraft carriers to monitor the electromagnetic spectrum and actively deny an adversary the use of radar and communications (*GlobalSecurity.org*).
early warning (EW) Early notification of the launch or approach of unknown weapons or weapons carriers (*JP 1-02*).
electromagnetic pulse (EMP) The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges (*JP 1-02*).
**electronic warfare (EW)** Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (*JP 1-02*).

**EMP** (see electromagnetic pulse).

**environment** (see operational environment).

**EUCOM** U.S. European Command. The command responsible for all U.S. forces in the European theater of operations (TO).

**Eurofighter (Typhoon EF-2000)** A single-seat, twin-engine, agile combat aircraft used in air-to-air, air-to-ground, and tactical reconnaissance roles (*GlobalSecurity.org*).

**EW** (see electronic warfare and early warning).

**exfiltration** In cyber warfare, the collection of technical information from an adversary's cyber assets.

**expeditionary force** An armed force organized to accomplish a specific objective in a foreign country (*JP 1-02*).

---

**F**

**F-111 Aardvark** A multipurpose tactical fighter bomber capable of supersonic speeds (*GlobalSecurity.org*).

**F-16 Fighting Falcon** A compact, multirole fighter aircraft. It is highly maneuverable and has proven itself in air-to-air combat and air-to-surface attack. It provides a relatively low-cost, high-performance weapon system for the United States and allied nations (*GlobalSecurity.org*).

**F-18 Super Hornet** A multi-mission strike fighter providing carrier battle group commanders with a platform that has range, endurance, and ordnance carriage capabilities comparable to the A-6, which has been retired (*GlobalSecurity.org*).

**F-22 Raptor** A USAF air superiority fighter under development to counter emerging worldwide threats. The F-22 Raptor is designed to ensure that America's armed forces retain air dominance (*GlobalSecurity.org*).

**F-35 Joint Strike Fighter (JSF) Lightning II** Project to develop a family of airplanes and attain economies of commonality and scale that drive down the costs of each airplane. The objective is to make the airplanes for about half the cost of today's airplanes (*GlobalSecurity.org*).

**field manual (FM)** A manual published by the Department of the Army explaining official Army doctrine for use by soldiers in the field.

**fix** A position determined from terrestrial, electronic, or astronomical data (*JP 1-02*).

**FM** (see field manual).
force posture  The ability or condition of a force to carry out its mission or some subset thereof.

FSU  Former Soviet Union.

full spectrum operations  The range of Army operations undertaken in the employment of military force, including various combinations of offense, defense, stability, and civil support (FM 3-0).8

fusion  In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of the operational environment and enemy activity (JP 2-0).9

G

GCA  Global Community of Airmen.

GDP  Gross domestic product.

GEF  (see Global Employment Force).

global commons  Locations and resources internationally recognized as belonging to all nations in common.

Global Employment Force (GEF)  Forces belonging to TRANSCOM, which it may selectively activate to meet emerging needs.

Global Hawk  A high-altitude, long-endurance unmanned aerial reconnaissance system designed to provide commanders with real-time imagery of large geographic areas. The Global Hawk can reach an altitude up to sixty-five thousand feet and loiter for more than thirty hours (GlobalSecurity.org).

Global Strike Command or Air Force Global Strike Command (AFG-SC)  USAF command aligning ICBM and nuclear-capable long-range bomber forces under a single command to provide combat-ready forces for nuclear deterrence and global strike operations.

Global Zero  The global campaign to build public and political support for a phased elimination of all nuclear weapons (GlobalSecurity.org).

GPS  Global Positioning System.

H

hardened site  A site, normally constructed under rock or under a concrete cover, designed to protect against the effects of conventional weapons. It may also be equipped to provide protection against the side effects of a nuclear attack and against a chemical or a biological attack (JP 1-02).

8 Department of the Army, Operations, Field Manual 3-0, 2008.
9 Department of Defense, Joint Intelligence, Joint Publication 2-0, 2007.
**high-end conflict** A large-scale, resource-intensive conflict involving regional or multi-regional military action, such as a direct confrontation between two major powers.

**high-value target (HVT)** A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander’s area of interest (*JP 3-09*).\(^\text{10}\)

**horizontal proliferation** The transfer of capabilities (in particular nuclear weapons and other WMD) from one party to another. The parties may be state or non-state actors.

---

**ICBM** Intercontinental ballistic missile (see ballistic missile).

**IED** Improvised explosive device.

**IFPA** Institute for Foreign Policy Analysis, Inc.

**imaging inertial navigation** A positioning system relying on data collected from radar imaging and a craft’s motion instead of on satellites.

**intelligence** 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding (*JP 1-02*).

**Interagency, adj.** Coordinated between organizations from multiple departments within the executive branch of USG; n. (usually “the interagency”) the capacity of various USG organizations to habitually collaborate, or the sum of such efforts in their entirety.

**interoperability** 1. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. 2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases (*JP 1-02*).

**intra-theater mobility** The ability of systems or units to redeploy within a theater of operation.

**irregular warfare** Warfare conducted by armed individuals or groups who are not members of the regular, national armed forces, police, or other internal security forces of a state (*JP 1-02*).

---


ISR  Intelligence, surveillance, and reconnaissance (see each element separately).

ISSP  International Security Studies Program, the Fletcher School, Tufts University.

IT  Information technology.

jamming (also electromagnetic jamming)  The deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy’s effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy’s combat capability (JP 1-02).


JFCOM  U.S. Joint Forces Command. Functional COCOM responsible for providing forces to geographic COCOMs and force transformation.

JIATF  Joint Interagency Task Force (see CJIATF).

joint  Connotes activities, operations, organizations, and so on, in which elements of two or more military departments participate (JP 1). The emphasis is on the cooperative effort.

joint publication (JP)  A DoD publication explaining official DoD doctrine, usually concerning the strategic and operational levels of war.

joint staff (JS)  1. The staff of a commander of a unified or specified command, subordinate unified command, joint task force, or subordinate functional component (when a functional component command will employ forces from more than one Military Department), that includes members from the several Services comprising the force. These members should be assigned in such a manner as to ensure that the commander understands the tactics, techniques, capabilities, needs, and limitations of the component parts of the force. Positions on the staff should be divided so that Service representation and influence generally reflect the Service composition of the force. 2. (usually “the Joint Staff”) The staff under the Chairman of the Joint Chiefs of Staff as provided for in Title 10, United States Code, Section 155 (JP 1).11

joint strike fighter (JSF)  (see F-35 JSF).

JP  (see joint publication).

JSDF (see Japanese Self-Defense Forces).
JSF Joint strike fighter (see F-35 JSF).

K
KC-130F U.S. aerial refueling aircraft (GlobalSecurity.org).
KC-130J Improved aerial refueling platform providing increased speed, range, an improved air-to-air refueling system, night systems, and survivability enhancements over the KC-130F (GlobalSecurity.org).
kinetic adj. Achieving an effect by force of arms; for example, an F-18 firing a rocket at a target is a kinetic attack, while an EA-6B conducting jamming operations is non-kinetic. See non-kinetic.

L
live exercise Training exercise involving actual troops and equipment. If actual munitions are used, it is a live-fire exercise.
load master An Air Force technician qualified to plan loads, to operate auxiliary materials handling equipment, and to supervise loading and unloading of aircraft (JP 3-17).12
loiter To remain within a certain area.
loiter time The length of time an asset is able to loiter.
long-range bomber aircraft A bomber designed for a tactical operating radius of over twenty-five hundred nautical miles at design gross weight and design bomb load (JP 1-02).
low-end conflict A smaller-scale, less resource-intensive conflict usually confined to a single country or region of a country.
low-observable Not easily detected by detection assets.
LRASM Long-range anti-ship missile.

M
Marine air ground task force (MAGTF) Term used by USMC to describe the principal organization for missions across the range of military operations. MAGTFs are a balanced air-ground, combined-arms task organization of Marine Corps forces under a single commander structured to accomplish a specific mission. The term refers to an organization’s functional makeup; MAGTF size may vary.
maritime operations center (MOC) A USN field headquarters (HQ) for planning naval operations.

12 Department of Defense, Air Mobility Operations, Joint Publication 3-17, 2009.
MCRS  *Mobility Capabilities Requirements Study.*

MDAP  Major defense acquisition program.

**medical evacuation**  The movement of personnel who are wounded, injured, or ill between medical facilities when needed.

MEU  Marine expeditionary unit. A Marine air-ground task force (MAGTF) that is constructed around an infantry battalion reinforced, a helicopter squadron reinforced, and a task-organized combat service support element (*JP 1-02*).

*Milstar satellite system*  A satellite system that supports strategic and tactical missions through global communications that are secure, jam resistant, survivable, and with a low probability of intercept (*GlobalSecurity.org*).

**mission assurance**  Ensuring that mission functions are carried out, regardless of whether the assets performing these functions survive or not; as opposed to the protection of specific assets (see domain protection).

**mobility**  A quality or capability of military forces that permits them to move from place to place while retaining the ability to fulfill their primary mission (*JP 1-02*).

MOC  (see maritime operations center).

N

NATO  North Atlantic Treaty Organization.

**NATO Network Enabled Capability (NNEC)**  NATO’s cognitive and technical ability to federate the various components of the operational environment, from the strategic level (including the NATO HQ) down to the tactical levels, through a networking and information infrastructure.

NBC  Nuclear, biological, and chemical. (see CBRN)

**NEO (noncombatant evacuation operations)**  Operations directed by the Department of State or other appropriate authority, in conjunction with the Department of Defense, whereby noncombatants are evacuated from foreign countries when their lives are endangered by war, civil unrest, or natural disaster to safe havens or to the United States (*JP 3-0*).13

**net-centric warfare**  A concept of operations whose foundation is information superiority and the ability to make sense of that information. The idea is to increase combat power by using all assets in the field and at home to link decision makers and shooters electronically. With access to the same information at the same time, they achieve shared awareness, increased speed of com-

---

mand, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization (JP 1-02).

NGO Non-governmental organization.

NNEC (see NATO Network Enabled Capability).

non-kinetic, adj. Achieving an effect without force of arms (see kinetic).

non-permissive environment An operational environment in which host country military and law enforcement agencies have either not established control within national boundaries or else refuse to assist U.S. operations (JP 3-0).

non-strategic nuclear forces (NSNF) Forces armed with relatively low-yield nuclear weapons designed to defeat enemy operations and tactics, not for use as a strategic weapon.

NORAD North American Aerospace Defense Command. A joint organization of Canada and the United States that provides aerospace warning, air sovereignty, and defense for the two countries.

NORTHCOM (U.S. Northern Command) COCOM charged with protecting the United States homeland and support local, state, and federal authorities.

Northern Distribution Network (into Afghanistan) The U.S. line of communication through Central Asian countries to allied forces in Afghanistan.

Northwest Passage The sea lane through Canadian Arctic waters connecting the Atlantic and Pacific Oceans.

NPR Nuclear Posture Review.

NPT Non-Proliferation Treaty.

NRF NATO Response Force (see response force).

NSCC NATO SOF Coordination Centre, re-designated as the NATO Special Operations Headquarters (NSHQ) in March 2010.

NSHQ NATO SOF Headquarters.

NSNF (see non-strategic nuclear forces).

NSTI (NATO SOF Transformation Initiative).

nuclear deterrence (see deterrence).

nuclear parity The state of possessing approximately equal nuclear weapons capabilities.

OCO Overseas contingency operation (see contingency).

OCONUS Outside the continental United States (see CONUS).

OEF (see Operation Enduring Freedom).

OIF (see Operation Iraqi Freedom).

officer accession The system of training and developing civilians and enlisted military members for service as military officers;
more broadly the process of generating officers for service in the armed forces.

**Operation Enduring Freedom (OEF)**  
Overarching term for current U.S.-led multinational mission in Afghanistan.

**Operation Iraqi Freedom (OIF)**  
Overarching term for current U.S.-led multinational mission in Iraq.

**operational level of war**  
The level of war at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas. Activities at this level link tactics and strategy by establishing operational objectives needed to achieve the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events *(JP 3-0)*.

**operational/operating environment**  
A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. See awareness *(JP 3-0)*.

**OSD**  
Office of the Secretary of Defense.

**overwatch**  
A tactical movement technique in which one element is positioned to support the movement of another element with immediate fire. *(FM 3-90)*.\(^\text{14}\)

**P**

**passive defense**  
Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative *(FM 100-12)*.\(^\text{15}\)

**Pegasus**  
An air-launched (via a modified Lockheed L-1011 aircraft), three-stage, all-solid-propellant, three-axis stabilized vehicle. The *Pegasus-XL* vehicle, a “stretched” version of the original *Pegasus* vehicle, can place a four hundred- to one-thousand-pound payload into low-Earth orbit. The original, or standard, version of the *Pegasus* was retired in 2000, and only the *Pegasus XL* is in service today *(GlobalSecurity.org)*.

**penetrating system**  
A system able to penetrate and operate behind enemy lines.

**permissive environment**  
Operational environment in which host country military and law enforcement agencies have established control within national boundaries and have the intent and capability to assist U.S. operations *(JP 3-0)*.

---

People’s Liberation Army (PLA)  The armed forces of the People’s Republic of China.

PGM (see precision-guided munitions).

PLA (see People’s Liberation Army).

platform  A system that carries a certain capability; for example, a bomber may be a platform capable of dropping leaflets.

port of disembarkation (POD)  The geographic point at which cargo or personnel are discharged. This may be a seaport or an aerial port (APOD) (JP 1-02).

port of embarkation (POE)  The geographic point in a routing scheme from which cargo or personnel depart. This may be a seaport or an aerial port (APOE) from which personnel and equipment flow to a port of disembarkation (JP 1-02).

power projection  The ability of a nation to apply all or some of its elements of national power (political, economic, informational, military) to rapidly and effectively deploy and sustain forces in and from multiple dispersed locations to respond to crises, to contribute to deterrence, and to enhance regional stability (JP 3-35).\(^\text{16}\)

precision-guided munitions (PGM, also precision munitions)  A weapon that uses a seeker to detect electromagnetic energy reflected from a target or reference point and, through processing, provides guidance commands to a control system that guides the weapon to the target (JP 3-03).\(^\text{17}\)

Predator (RQ-1 Predator MAE UAV)  A long-dwell unmanned aerial vehicle (UAV) operating in excess of twenty-four hours (equivalent to flying four hundred nautical miles out, loitering for over fourteen hours, and then flying home another four hundred nautical miles). The MQ-1B Armed Predator is a variant of the RQ-1 Predator modified to accomplish a ground attack role as well as reconnaissance (GlobalSecurity.org).

preemptive attack  An attack initiated on the basis of incontrovertible evidence that an enemy attack is imminent (JP 1-02).

programmed capability  Capabilities planned and funded within the DoD acquisitions system.

proliferation  The acquisition or transfer of capabilities (in particular nuclear weapons and other WMD) by state or non-state actors.

pseudolite  A contraction of the term “pseudo-satellite,” used to refer to something that is not a satellite which performs a function commonly in the domain of satellites. Pseudolites are most often small transceivers that are used to create a local, ground-based GPS alternative.


\(^\text{17}\) Department of Defense, Joint Interdiction, Joint Publication 3-03, 2007.
PSI Proliferation Security Initiative.

Q
QDR Quadrennial Defense Review.

R
R&D Research and development.
RAAF Royal Australian Air Force.
RACR Raytheon Advanced Combat Radar.
reconnaissance (recon) A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area (JP 1-02).
redundancy The use of multiple assets for a single purpose to increase the assurance that that purpose will be realized even in the event of the failure of one of those assets.
regular warfare Warfare conducted by members of the regular armed forces, police, or other internal security forces (JP 1-02).
remotely piloted vehicle (RPA) A powered, aerial vehicle that does not carry a human operator. Also known as remotely piloted aircraft (JP 1-02).
reserve component (RC) For the Armed Forces of the United States, RC includes the Army National Guard of the United States, the Army Reserve, the Naval Reserve, the Marine Corps Reserve, the Air National Guard of the United States, the Air Force Reserve, and the Coast Guard Reserve (JP 4-05). 18

Responder A Raytheon space product with modular, multi-purpose payloads and a family of interchangeable mission-specific sensors.
response force A mobile force with appropriate fire support designated, usually by the area commander, to deal with certain threats in the rear area (JP 3-10).
retention The effort to convince qualified service members to renew their military enlistment contract before it expires; more broadly the ability of a military force to maintain its personnel strength in this way.

ROK Republic of Korea, also referred to as South Korea
RPA (see remotely piloted aircraft).

---
sabotage  An act or acts with the intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, including human and natural resources (JP 1-02).

SAC-T  Supreme Allied Commander Transformation.

SAM  surface-to-air missile.

SBIR  Small Business Innovative Research.

SDR  Strategic Defence Review (UK).

second nuclear age  The present age of nuclear weapons, referring to the proliferation of nuclear weapons to numerous powers beyond the United States, the Soviet Union, and their allies.

SHAPE  Supreme Headquarters Allied Powers Europe.

Shrike micro-air vehicle  A new generation of perch-and-stare micro air vehicles based on the Wasp platform capable of: 1) vertical launch; 2) forward flight to a target; 3) transition from forward flight to vertical landing at the target site; 5) secure, stable attachment to its “perch;” 6) sustained perch-and-stare missions, including data collection; and 7) re-launch from the perch to fly home. During perch-and-stare, Shrike will perform surveillance and transmit intelligence via data link to its home base (GlobalSecurity.org).

situational awareness  (see awareness).

SOCOM  U.S. Special Operations Command.

SOF  (see special operations forces).

SOUTHCOM  U.S. Southern Command.

special operations  Operations conducted in hostile, denied, or politically sensitive environments to achieve military, diplomatic, informational, and/or economic objectives employing military capabilities for which there is no broad conventional force requirement (JP 1-02).

special operations forces (SOF)  Those forces within the military services designated by the Secretary of Defense and specifically organized, trained, and equipped to conduct and support special operations (JP 3-05.1).19

spectrum of conflict  (see full-spectrum operations).

stand-off system  A system able to operate without penetrating enemy lines.

START  Strategic Arms Reduction Treaty.

stealth  The ability to escape enemy detection, as from radar.

---

STRATCOM  U.S. Strategic Command. COCOM charged with space operations, information operations, missile defense, global command and control, C4ISR, global strike and strategic deterrence, and combating weapons of mass destruction.

strategic level of war  The level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, and develops and uses national resources to achieve these objectives. Activities at this level establish national and multinational military objectives; sequence initiatives; define limits and assess risks for the use of military and other instruments of national power; develop global plans or theater war plans to achieve those objectives; and provide military forces and other capabilities in accordance with strategic plans (JP 3-0).

strategic triad  The United States’ three primary means of nuclear deterrence: 1) strategic bombers, 2) land-based missiles, and 3) ballistic missile submarines.

strike  An attack to damage or destroy an objective or a capability (JP 3-0).

surveillance  The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means (JP 1-02).

survivability  Concept that includes all aspects of protecting personnel, weapons, and supplies while simultaneously deceiving the enemy. Survivability tactics include building a good defense; employing frequent movement; using concealment, deception, and camouflage; and constructing fighting and protective positions for both individuals and equipment (JP 3-34).

sustainability  The ability to maintain the necessary level and duration of operational activity to achieve military objectives. Sustainability is a function of providing for and maintaining those levels of ready forces, materiel, and consumables necessary to support military effort (JP 1-02).

T
tactical level of war  The level of war at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. Activities at this level focus on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives (JP 3-0).

Taepodong II  North Korean missile believed to be capable of hitting Alaska (GlobalSecurity.org).

target discrimination  The ability of a surveillance or guidance system to identify or engage any one target when multiple targets are present (JP 1-02).

terrorism  The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological (JP 1-02).

theater of operations (TO)  An operational area defined by the geographic combatant commander for the conduct or support of specific military operations. Multiple theaters of operations normally will be geographically separate and focused on different missions. Theaters of operations are usually of significant size, allowing for operations in depth and over extended periods of time (JP 3-0).

TRANSCOM  (U.S. Transportation Command)

Trident II D-5  A three-stage, solid propellant, inertially guided fleet ballistic missile with a range of more than 4,000 nautical miles (4,600 statute miles or 7,360 kilometers).

Trojan horse  Software designed to infiltrate a cyber network without being detected and extract information.

TTO  Tactical Technology Office.

U

U.S. Strategic Command  (see STRATCOM)

UAV  Unmanned aerial vehicle.

UCAS  Unmanned Combat Air System.

UHF SATCOM  Ultra high frequency satellite communications.

UK  United Kingdom.

unconventional warfare  A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted through, with, or by indigenous or surrogate forces that are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes, but is not limited to, guerrilla warfare, subversion, sabotage, intelligence activities, and unconventional assisted recovery (JP 3-05).21

USAF  United States Air Force.

USCG  United States Coast Guard.

USG  United States government.

USMC  United States Marine Corps.

USN  United States Navy.

vertical proliferation The expansion of capabilities (in particular nuclear weapons and other WMD) based on new-generation technologies and modernization programs.

virtual exercise Training exercise involving only leaders in which troops, weapons, and equipment are simulated, usually via computer.

VTOL Vertical takeoff and landing.

Wasp micro-air vehicle (see Shrike micro-air vehicle).

weapons of mass destruction (WMD) Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological (CBRN) weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon (JP 1-02).

whole-of-government approach Concept emphasizing the coordination between organizations from all branches of the U.S. government (cf. interagency).

WMD (see weapons of mass destruction).