THE REVOLUTION IN WAR

Michael G. Vickers

Robert C. Martinage

Thinking Smarter About Defense

Center for Strategic and Budgetary Assessments

CSBA

www.csbaonline.org

The Revolution in War

by

Michael G. Vickers

Robert C. Martinage

Center for Strategic and Budgetary Assessments

December 2004

ABOUT THE CENTER FOR STRATEGIC AND BUDGETARY ASSESSMENTS

The Center for Strategic and Budgetary Assessments (CSBA) is an independent, policy research institute established to promote innovative thinking about defense planning and investment strategies for the 21st Century. The Center is directed by Dr. Andrew Krepinevich and funded by foundations, corporations, government, and individual grants and contributions.

This report is one in a series of CSBA analyses on future warfare and transformation strategy. The authors would like to thank Steven Kosiak, Andrew Krepinevich, Barry Watts, and Robert Work.

The analysis and findings presented here are solely the responsibility of the Center for Strategic and Budgetary Assessments and the authors.

1730 Rhode Island Ave., NW
Suite 912
Washington, DC 20036
(202) 331-7990

CONTENTS

Executive Summary

A revolution in war has been underway for nearly three decades. Beginning in the mid–1970s, in an effort to compensate for the numerical superiority of Warsaw Pact forces, the US military sought to exploit a number of asymmetric technological advantages. Despite the demise of the threat for which these "offset" capabilities were created, they have continued to be developed, and have been leveraged to great effect in wars ranging from Desert Storm to Operation Iraqi Freedom. To date, the revolution in war has been principally characterized by:

- The emergence of all-weather precision war;
- The advent of stealth;
- The rise of unmanned systems;
- The tactical and operational exploitation of space; and
- The emergence of early forms of network-based warfare and joint-force integration.

Thus far, the US military has enjoyed a monopoly on the revolution in war. Within the next two decades, however, the revolution could shift from a purely opportunity-based one for the United States to one that portends significant threats, as well as opportunities. If there is competition within the revolution in war, it is likely to be highly asymmetric. It is entirely conceivable, moreover,

that a competitor could "leapfrog" the United States in some areas of future competition.

Major advances in the core military capabilities that are underwriting the revolution in war—awareness, connectivity, range, endurance, precision, miniaturization, speed, stealth, automation, and simulation—are likely over the next one or two decades, and significant discontinuities in the conduct of war could lie ahead. The future course of the revolution in war could range from a continuation of current trends and the existing warfare regime, to a "revolution within the revolution" due to asymmetric exploitation of disruptive capabilities (e.g., robust, "anti–access/area denial" networks, offensive information warfare and space warfare capabilities) by strategic competitors, to a successor revolution that would involve a much greater break with the ongoing revolution in war (e.g., the emergence of an unmanned warfare–dominant regime). While the emergence of a revolution within the revolution or a successor revolution is still highly uncertain, we believe that the outcome of six warfare competitions will be determinative of the character of the future warfare regime:

- Evolving anti-access and area-denial capabilities versus current and new forms of power projection;
- Increased capabilities for preemption versus increased denial capabilities;
- Hiders versus finders;
- Space access versus space control;
- Missile attack versus missile defense, information warfare (IW) attack versus IW defense, and biological warfare (BW) attack versus BW defense; and
- Increased capabilities for political–military coercion versus capabilities for counter–coercion.

As these key warfare competitions unfold, discontinuous change could occur within and across the primary warfare dimensions of air, land and sea. New forms of war could emerge in several other dimensions: space, information, and the biological. Air warfare could be transformed from a regime dominated by manned, theater-range, air superiority aircraft to one dominated by extended-range,

unmanned, and stealthy platforms. The conduct of land warfare could shift from a regime dominated by mobile, combined-arms, armored forces to one that is dominated by much lighter, stealthier and information-intensive forces that make heavy use of robotics. War at sea could be transformed by the emergence of "anti-navy" capabilities that allow nations to assert a degree of surface control over adjacent maritime areas out to several hundred miles. This development would likely lead to new forms of naval power projection, including increased reliance on undersea warfare and relatively small, stealthy, networked surface vessels. Increased commercial and military use of space could lead to the emergence of a wide range of offensive and defensive space control capabilities. Computer network attack (CNA) tools and radio-frequency (RF) weapons could be widely used to attack information infrastructures and information-intensive forces. Designer BW and the emergence of biological operations could also figure prominently in an advanced revolution in military affairs (RMA) regime.

At the "lower end" of the conflict spectrum (e.g., the war on terrorism, intra-state conflict, and stability operations), non-state actors could become far more virulent and insurgency-induced state failures could become far more prevalent. At the highest-end, the strategic scope of the revolution in war (including a prospective revolution within the revolution and potential successor revolutions) will likely be truncated by the continued "overhang" of nuclear weapons, though new forms of strategic warfare will likely also emerge.

Although it has grown increasingly dominant in the ongoing revolution in war, the US military is by no means adequately hedged at present for the prospect of discontinuous change within or across military regimes (a revolution within the revolution or a successor revolution). Failure to adequately hedge represents significant future challenges risk.

I. Introduction

A revolution in war has been underway since the late 1970s.[1] Although its future path is yet to be determined, we are likely only in the early phase of this revolutionary change. Subsequent change could be even more discontinuous and profound, with potentially serious consequences for the currently dominant position of the United States.[2] This monograph examines the fundamental changes in the conduct of warfare that have occurred over the past three decades, and provides a framework for thinking about additional changes that may still lie ahead.

[1] The term "revolution in war" should be considered synonymous with "military revolution," "revolution in military affairs" (RMA) and "military-technical revolution" (MTR).

[2] For earlier writings on this revolution, see Michael G. Vickers, *Warfare in 2020: A Primer* (Washington, DC: Center for Strategic and Budgetary Assessments (CSBA), 1996); and Michael G. Vickers, "The Revolution in Military Affairs and Military Capabilities," in *War in the Information Age: New Challenges for U.S. Security* ed. Robert Pfaltzgraff and Richard Shultz (Washington, DC: Brassey's, 1997), pp. 29-47.

THE STRUCTURE OF MILITARY REVOLUTIONS

Military revolutions are periods of discontinuous change that render obsolete or subordinate existing means for conducting war. They are often, though by no means always, linked with broader political, social, economic, and scientific transformations, and are brought about by changes in militarily relevant technologies, concepts of operation, methods of organization, and/or available resources.[3] The development of a military revolution may be rapid, or it may evolve more gradually before a revolutionary threshold is reached. The fundamental discontinuity represented by revolutionary change in war arises from change that is profound, but also rapid and destabilizing in its impact. Revolutions shatter existing military regimes and rapidly establish new ones in their wake.[4]

Revolutionary change in aggregate military capabilities is a function of developments in five core areas: firepower; mobility; protection; sustainment; and command, control, communications, and intelligence (C3I). It can result from an order-of-magnitude or greater increase in one of these functional areas (as was the case with the atomic bomb) or, more typically, from synergistic interactions between two or more of these areas. For change in military capabilities to reach

[3] Historically, political, social, economic, scientific and technological revolutions have contributed directly and powerfully to revolutionary change in war, but their impact is dependent on their ability to lead directly to the development of regime-shattering military capabilities. Several military revolutions have occurred independently of societal revolutions; the latter are thus neither necessary nor sufficient for revolution in war. New technologies, warfighting concepts, organizations, and resources effect change within and across core capabilities, but their relative importance varies substantially across military revolutions. See Michael Vickers, *The Structure of Military Revolutions* (Washington, DC: Unpublished CSBA report submitted to the Office of the Secretary of Defense—Office of Net Assessment, 2003), p. 28.

[4] A "military regime," as defined here, encompasses the weapons, strategies, tactics, and forms of organization that comprise aggregate military capabilities during a period, and the amount of military power that can potentially be generated from them. Put more simply, it is the way war is generally conducted over a strategically coherent period of time. A change of military regimes can occur through evolutionary change in military capabilities or revolutionary change. Military regimes may encompass both forms of change.

a revolutionary threshold, it must increase capabilities at the strategic and operational levels of war to such an extent that, in their aggregate effect, they are able to render subordinate or obsolete fundamental aspects of the existing military regime.[5] Military revolutions have historically advantaged the strategic/operational offense, and have thus provided a powerful impetus for major changes in strategic balances.

Military revolutions are most frequently realized by a "defining battle," in which the revolutionary force or forces waging it demonstrate the dominance of the new way of war. A form of strategic surprise, "regime surprise," is endemic to periods of revolutionary change in warfare. A military revolution, along with the new military regime it ushers in, is consolidated when competitors are compelled to adapt to it, usually through direct emulation, but through other means as well.

The historical record provides evidence of more than a dozen cases of revolutionary change in the conduct of war. The modern period in general, and the past two centuries in particular, has witnessed the greatest rate of change. Since the early fifteenth century, the conduct of war has been radically altered ten times. Seven of these transformations have occurred within the past two hundred years, making the nineteenth and twentieth centuries, in effect, an Age of Military Revolutions.[6]

---

[5] Vickers, *The Structure of Military Revolutions*, p. 28.

[6] Cases of revolutionary change in war include: the advent of chariot warfare in the seventeenth century B.C.; the eruption of massed infantry in the early twelfth century B.C.; the development of the New Model Macedonian Army in the fourth century B.C.; the artillery revolution in the fifteenth century A.D.; the guns and sails, and gunpowder-infantry revolutions during the early sixteenth century A.D.; the Napoleonic revolution during the late eighteenth and early nineteenth century A.D.; the railroad, rifle and telegraph revolution during the mid-nineteenth century A.D.; the battleship-battlecruiser-submarine revolution during the early twentieth century; the revolutions in armored warfare and air superiority and in naval air power during the interwar years; and the atomic and thermonuclear/ballistic missile revolutions during the 1940s and 1950s. (See Vickers, *The Structure of Military Revolutions*, pp. 24-25.) The modern cases of revolutionary change in war have several potentially important implications for the ongoing RMA. The military revolutions in early modern Europe were central developments

ORIGINS, SCOPE AND METHODOLOGY OF THIS STUDY

This study traces its origins to research conducted over a decade ago in the Office of Net Assessment/Office of the Secretary of Defense. It substantially extends upon this and other earlier work, examining in much greater depth where the RMA has been and where it might be headed.[7] To cope with the considerable uncertainty involved in speculating about revolutionary developments in warfare that may occur over the next two-to-three decades, this study adopts a "core competitions" framework. It identifies six core strategic and technological competitions whose outcome will likely determine the basic character of future warfare.

The next chapter focuses upon the origins and central characteristics of the revolution in war to date. It describes the changes in core capabilities underwriting this revolution, and how they could lead to further discontinuous change (a "revolution within the revolution"), as well as to the emergence of war in space, the information spectrum, and the advanced biological realm. In the third

---

underwriting the West's rise to global dominance. The Napoleonic revolution during the last decades of the eighteenth century and the first decade of the nineteenth and the railroad, rifle, and telegraph revolution of the mid-nineteenth century were brought about in large measure by developments outside the military sphere. The battleship-battlecruiser-submarine revolution at the turn of the twentieth century illuminates the problems of technological flux, self-obsolescence, and non-hierarchical changes in power relationships (e.g., the emergence of the submarine as a "capital" ship killer). The interwar revolutions in armored warfare, air superiority, and naval air power underscore how differences in concepts of operation and methods of organization can result in large disparities in military capability among similarly equipped adversaries. Finally, the bifurcation of warfare into nuclear and conventional regimes induced by the atomic and thermonuclear/ballistic missile revolutions could significantly limit the strategic scope of the current RMA.

[7] The original (unpublished) paper was Michael G. Vickers, "A Concept for Theater Warfare in 2020," Office of Net Assessment/Office of the Secretary of Defense, November 1993. See also Vickers, *Warfare in 2020: A Primer*; Vickers, "The Revolution in Military Affairs and Military Capabilities" in *War in the Information Age: New Challenges for U.S. Security;* and Michael Vickers and Robert Martinage, *The Military Revolution and Intrastate Conflict (*Washington, DC: CSBA, 1996).

chapter, we describe and analyze six strategic and technological competitions that we believe will shape the future course of this revolution. In the fourth chapter, we describe how asymmetric resolution of these competitions could affect high-end conventional warfare across each dimension of the future battlespace, as well as at the upper and lower ends of the conflict spectrum. We conclude with a few brief comments on where the US military stands in terms of hedging against the dangers and realizing the full potential of the ongoing revolution in war.

II. The Ongoing Revolution in War

The revolution in war grew out of developments in the last decade and a half of the Cold War. It has five central attributes at present: the ability to strike with great accuracy independent of range; the ability, through the use of stealth, to penetrate defenses with impunity; the emergence of unmanned warfare; the tactical and operational exploitation of space; and the ability to move information rapidly and widely across a joint battle network and exploit the effects of increased joint force integration. To date, the US military has enjoyed a monopoly on these revolutionary changes in military capabilities. Over time, however, the revolution in war could shift from an opportunity-based revolution for the US military to one that portends significant threats, as well as opportunities. This chapter focuses primarily on the origins and development of the revolution in war. It also sets the stage for a more detailed discussion of a potential advanced phase (covered at length in the subsequent chapters) by explaining how the combined effect of advances in ten capability areas—awareness, connectivity, range, endurance, precision, miniaturization, speed, stealth, automation, and simulation—could lead to a revolution within the revolution.

ORIGINS AND DEVELOPMENT OF THE REVOLUTION IN WAR

Soviet military theorists began writing in the mid-1970s, initially in classified documents, about the prospect of a "military-technical revolution (MTR)" based on the integration of advanced sensor systems, communication and battle management systems, and advanced conventional weapons into what was termed a "reconnaissance-strike complex." These discussions were apparently triggered, at least in part, by the US development of new sensor systems to "look deep" and extended-range, precision-strike weapons to "shoot deep" into the territory of Warsaw Pact nations.[8] After several promising technical developments in this area and a strong endorsement of the deep-strike concept by a 1976 Defense Science Board (DSB) summer study, Under Secretary of Defense William Perry testified to Congress in 1978:

> Precision guided weapons, I believe, have the potential of revolutionizing warfare. More importantly, if we effectively exploit the lead we have in this field, we can greatly enhance our ability to deter war without having to compete tank for tank, missile for missile with the Soviet Union. We will effectively shift the competition to a technological area where we have a fundamental long-term advantage....The objective of our precision guided weapon systems is to give us the following capabilities: to be able to see all high value targets on the battlefield at any time; to be able to make a direct

[8] Ear9ly research on deep-strike capabilities, including moving-target-indication (MTI) radar, stand-off missiles, and terminally guided submunitions, began in the mid-1970s under DARPA's Integrated Target Acquisition and Strike System (ITASS) program. See Richard H. Van Atta et al, *Transformation and Transition: DARPA's Role in Fostering an Emerging Revolution in Military Affairs, Volume 1—Overall Assessment* (Alexandria, VA: Institute for Defense Analyses, 2003), pp. 17-18.

> hit on any target we can see, and to be able to destroy any target we can hit.[9]

The pursuit of this deep-strike capability was part of a broader "offset strategy" espoused by Secretary of Defense Harold Brown that sought to counter the quantitative superiority of Warsaw Pact forces in Europe by using selected technological advantages as force multipliers.[10] In assessing the US-Soviet military balance, Secretary of Defense Brown asserted, "If the United States looks for comparative advantages against a potential Soviet adversary with superior numbers of forces, one of the most obvious is the relatively lower cost of incorporating high technology into US military equipment."[11] Although many of the technologies underwriting this strategy were actually conceived of and developed during the 1970s, most of them did not reach operational maturity until the mid-to-late 1980s, and in some cases, the early 1990s. High-priority R&D initiatives during this period focused on the rapid fielding of:

- New battle management and tactical reconnaissance systems, including Airborne Warning and Control System (AWACS) and Joint Surveillance and Target Attack Radar System (JSTARS) aircraft;

---

[9] William Perry, Testimony to the US Senate Armed Services Committee, Hearing on Department of Defense Appropriations for FY1977, Part 8: Research and Development, February 28, March 7, 9, 14, 16, and 21, 1978, p. 5598.

[10] The pursuit of this deep-strike capability ultimately provided the basis for what became known as the Air-Land Battle doctrine or, in NATO parlance, Follow-on Forces Attack (FOFA). Officially adopted in 1982, the basic concept was to leverage the reconnaissance-strike capabilities of the US military and its NATO allies to destroy second-echelon Soviet forces at the outset of hostilities, while they were still deep within enemy territory. This capability was also seen as a more credible alternative to nuclear retaliation for deterring limited Soviet aggression in Europe. See William J. Perry, "Desert Storm and Deterrence," *Foreign Affairs*, 70, No. 4, Fall 1995, p. 68; William J. Perry (Under Secretary of Defense, Research and Engineering), *The FY 1981 Department of Defense Program for Research, Development, and Acquisition* (Washington, DC: DoD, 1980), p. II-1.

[11] Harold Brown, Thinking about National Security—Defense and Foreign Policy in a Dangerous World (Boulder, CO: Westview Press, 1983), pp. 229-230.

- Enhanced guidance and navigation systems made possible by the advent of the global positioning system (GPS);

- A wide variety of air-, sea-, and ground-launched, precision-guided munitions (PGMs); and

- Radar-evading stealth aircraft, such as the F-117 Nighthawk.

In 1978, several disparate R&D efforts in these areas were organized into a technology demonstration program run by DARPA called "Assault Breaker."[12] This effort was expanded in 1985 under the "Smart Weapons Program" to include the development of "autonomous air vehicles" that could autonomously search large areas of terrain for mobile targets and "intelligent munitions" that could both find and hit targets with high accuracy.[13]

Troubled by the clear US lead in key enabling technologies, especially microelectronics, the Soviets began to conduct exercises in 1979 that explored alternative concepts for fighting an opponent equipped with a reconnaissance-strike complex.[14] By the early 1980s, Soviet discussions about the emerging MTR began to appear more widely in professional military journals.[15] Soviet military theorists

---

[12] The Assault Breaker program brought together ongoing R&D programs in infrared sensors; stand-off, airborne, synthetic aperture radar with MTI capability (i.e., JSTARS); long-range tactical missiles (including what later become the Army Tactical Missile System); precision-guide munitions; terminally guided submunitions; and heterogeneous sensor fusion. For a short history of the Assault Breaker program, see Richard H. Van Atta et al, *Transformation and Transition: DARPA's Role in Fostering an Emerging Revolution in Military Affairs,* pp. 19-22.

[13] Ibid., p. 23.

[14] William E. Odom, *The Collapse of the Soviet Military* (New Haven, CT: Yale University Press, 1998), p. 76.

[15] See Mary C. FitzGerald, "The Impact of New Technologies on Soviet Military Thought," in Roy Allison, ed., *Radical Reform in Soviet Defence Policy: Selected Papers from the Fourth World Congress for Soviet and East European Studies* (New York, NY: St. Martin's Press, 1992), pp. 98-100; Mary C. FitzGerald, *Impact of the RMA on Russian Military Affairs* (Washington, DC: Hudson Institute, Spring 1998); Notra Trulock et al., *Soviet Military Thought in Transition: Implications for the Long-Term Competition* (Arlington, VA: Pacific-Sierra Research Corporation, 1988); Mary C.

wrote about the prospect that information technologies could enable conventional, long-range, precision-strike systems to gain an effectiveness approaching that of tactical or even strategic nuclear weapons.[16] In 1984, the Chief of the Soviet General Staff, Marshal N.V. Ogarkov asserted that:

> Highly accurate, terminally guided weapons systems, unmanned aircraft, and....new electronic control systems...make it possible to increase sharply (by at least an order of magnitude) the destructive power of conventional weapons, bringing them closer...to weapons of mass destruction in terms of effectiveness.[17]

Aside from the many operational benefits that could be derived from the fielding of advanced reconnaissance-strike capabilities, senior DoD officials concluded at the time that expanded US investment in these areas seemed strategically useful simply because it was clearly discomforting to the Soviets.[18] In 1988, *The Commission on Integrated Long-Term Strategy*, co-chaired by Fred Iklé and Albert Wohlstetter, established a working group tasked with projecting the likely contours of the future security environment (FSE). The working group surmised that the rapid pace of change in reconnaissance-strike capabilities and other military technologies was likely to be a central feature of the FSE. The Commission summarized

---

FitzGerald, *Marshal Ogarkov On Modern War: 1977-1985* (Alexandria, VA: Center for Naval Analyses, 1986), pp. 25-59.

[16] The Soviets also emphasized the prospective contribution of weapons based on new physical principles to the MTR, including kinetic-energy weapons, particle-beam weapons, laser weapons, and electromagnetic pulse weapons.

[17] Several of Ogarkov's colleagues held similar views. Many Soviet strategists in the early 1980s asserted that advanced conventional weapons could potentially achieve many of the objectives of a general nuclear war such as destroying the opposing side's nuclear potential, armed forces, command and control systems, and major political and economic centers. See Mary C. FitzGerald, "The Impact of New Technologies on Soviet Military Thought," pp. 103-109.

[18] Statement by Andrew W. Marshall at a CSBA roundtable session on future warfare, March 19, 2002.

the working group's findings, which partially echoed earlier Soviet assessments on the MTR, as follows:

> Dramatic developments in military technology appear feasible over the next twenty years. They will be driven primarily by the further exploitation of microelectronics, in particular sensors and information processing, and the development of directed energy. . .The U.S. leads in developing many of the relevant technologies, which may be a source of concern to the Soviets....The much greater precision, range, and destructiveness of weapons could extend war across a much wider geographic area, make war much more rapid and intense, and require entirely new modes of operation....The precision associated with the new technologies will enable us to use conventional weapons for many of the missions once assigned to nuclear weapons.[19]

Building upon the work of the Iklé-Wohlstetter Commission, the Office of Net Assessment within the Office of the Secretary of Defense embarked upon a more detailed assessment of the MTR in 1989. According to Mr. Andrew Marshall, the director of the Office of Net Assessment since its creation in 1973, the assessment had two related goals: first, to determine if Soviet analysts were correct about the prospect and likely implications of an information technology-based MTR; and second, if a military revolution was indeed on the horizon, to identify critical issues for defense management to consider.[20] Work on that preliminary assessment was completed three years later in 1992.[21]

---

[19] Fred C. Iklé and Albert Wohlstetter (co-chairmen), *Discriminate Deterrence—Report of the Commission on Integrated Long-Term Strategy* (Washington, DC: DoD, January 1988), p. 8.

[20] Statement by Andrew W. Marshall at a CSBA roundtable session on future warfare, March 19, 2002.

[21] An unclassified version of this assessment was released by CSBA in 2002. See Andrew Krepinevich, *The Military-Technical Revolution: A Preliminary Assessment* (Washington, DC: CSBA, September 2002).

Despite the demise of the threat for which "Assault Breaker" and related reconnaissance-strike capabilities were originally designed, they continued to be developed and were leveraged to great effect by the US military over the past decade. Many defense analysts assert that the lop-sided victory of the US-led coalition in Operation Desert Storm marked the full realization of a new RMA. Soviet observers, for example, concluded soon after the war that "the integration of control, communications, reconnaissance, electronic combat, and delivery of conventional fires into a single whole" had been realized "for the first time."[22]

While many pieces of a nascent reconnaissance-strike complex were demonstrated during Desert Storm, coalition forces did not in fact integrate them on a large scale.[23] For example, communications between the US armed services, as well as between coalition partners, were hampered by incompatible equipment and datalink standards. The air tasking order (ATO), which listed details about most coalition fixed-wing sorties each day, typically took up to 72 hours to compile and was frequently out of date by the time it was disseminated. The size of the ATO so overwhelmed old transmission equipment and computer terminals that units in the field sometimes consumed more than five hours attempting to download and print out their portion.[24] Since the Navy did not have the hardware required to receive the ATO electronically, it had to be flown out and delivered by hand from ship-to-ship each day. Finally, despite important strides made in assembling elements of a reconnaissance-strike complex, including the first operational use of JSTARS, the coalition had a very difficult time finding, tracking, and targeting high-value mobile targets. Hunting down Scud ballistic missile transporter-erector-launcher (TEL)

---

[22] Some Soviet assessments characterized Operation Desert Storm as more of a transitional war bridging the old and new military regimes. See "Soviet Analysis of Operation Desert Storm and Operation Desert Shield," Doc. 006-91, translated by Defense Intelligence Agency (DIA), October 28, 1991, p. 32. See also Mary C. FitzGerald, *The Soviet Image of Future War: Through the Prism of the Persian Gulf* (Alexandria, VA: The Hudson Institute, May 1991).

[23] Thomas Keaney and Eliot Cohen, *Revolution in Warfare: Air Power in the Persian Gulf* (Annapolis, MD: Naval Institute Press, 1995), p. 199.

[24] Thomas Keaney and Eliot Cohen, *Gulf War Air Power Survey Summary Report* (Washington, DC: US Government Printing Office (GPO), 1993), pp. 148-149.

vehicles, for example, proved particularly problematic. Although coalition air forces flew some 2,400 sorties attempting to find and attack Scud TELs, none were successfully destroyed.[25]

For these and many other reasons, the Gulf War is probably better understood as a "precursor war" that offered a glimpse of the revolutionary potential of the various "offset" capabilities mentioned earlier. Nearly a decade later, Operation Allied Force in 1999 reinforced the value of those same capabilities and provided an indication of the roles that unmanned systems, submerged power projection platforms, and offensive IW might play in future wars. Operations in Afghanistan and Iraq in 2001 and 2003 provided additional evidence that a revolution in war is well underway.

The Emergence of All-Weather, Precision War

PGMs and standoff cruise missiles have risen dramatically in prominence over the last decade. PGMs comprised about seven percent of the conventional munitions employed in bombing attacks during the Gulf War. According to the *Gulf War Air Power Survey* conducted after the war, those aircraft employing PGMs were typically an order of magnitude more effective in terms of target/sortie ratios than aircraft employing "dumb" conventional bombs.[26] In total, over 17,000 PGMs, 288 Tomahawk Land Attack Missiles (TLAMs) and 35 Conventional Air-Launched Cruise Missiles (CALCMs) were used to attack Iraqi targets.[27] Although the use of PGMs in the Gulf War was

[25] Christopher Bowie, "Destroying Mobile Ground Targets in an Anti-Access Environment," *Northrop Grumman Analysis Center Paper*, December 2001, p. 3.

[26] Keaney and Cohen, *Gulf War Air Power Survey – Summary Report*, p. 243. The ratio was derived by examining 12 representative sorties of F-117 and F-111F aircraft carrying PGMs with 12 sorties flown by aircraft delivering unguided bombs. The former covered 26 targets employing a total of 28 PGMs, while the latter covered two targets, expending 168 bombs.

[27] Of the roughly 17,000 PGMs expended, 9,342 were laser guided bombs, 5,448 were air-to-surface missiles (e.g., Mavericks), and 2,039 were high-speed, anti-radiation missiles (HARMs). See Keaney and Cohen, *Revolution in Warfare: Air Power in the Persian Gulf*, pp. 191-193.

nothing new (several thousand were dropped on North Vietnam between 1972 and 1973), the intensity of the precision-strike campaign was unprecedented. In six weeks, Coalition forces dropped more than twice the number of laser-guided bombs (LGBs) released over North Vietnam in nine months.[28]

Since the Gulf War, the percentage of PGMs used in US power projection operations has increased by roughly an order of magnitude. In six of the last seven US military operations, PGMs accounted for sixty percent or more of the total ordnance used against enemy targets (see Table 1).

Long-range, precision-strike weapons (i.e., air- and sea-launched cruise missiles) were the *only* weapons used in both Operation Desert Strike, conducted against Iraq in 1996, and Operation Infinite Reach, involving deep strikes against targets in Sudan and Afghanistan in 1998. In Operation Allied Force in Kosovo, the ratio of PGMs relative to dumb bombs was about 30 percent, or more than four times greater than it was during Operation Desert Storm.[29] GPS-guided TLAMs were used to attack nearly half of all government, military and police headquarters, air defense systems, and electric power grids that were hit throughout the war. Twenty-six TLAMs, including 10 with submunitions, were also used against 18 mobile and relocatable targets (primarily SAM radars and launchers) during the conflict.[30]

---

[28] Ibid., p. 203.

[29] Benjamin S. Lambeth, *NATO's Air War for Kosovo* (Santa Monica, CA: RAND, 2001), p. 88.

[30] Bryan Bender, "Tomahawk Achieves New Effects in Kosovo," *Jane's Defence Weekly*, July 19, 2000, p. 3. Approximately 181 of the 218 TLAMs hit their intended target.

Table 1: US Conventional Precision-Strike Trends Since the Gulf War

Operation	TLAMs Expended	CALCMs Expended	Short Stand-Off / Gravity PGMs Expended	Unguided Munitions Dropped	Conventional Precision Strike as % of Total
Deliberate Force–Bosnia, 1995	13	33	662	318	69
Desert Strike–Iraq, 1996	31	13	0	0	100
Desert Fox –Iraq, 1998	330	90	230	250	72
Infinite Reach–Sudan/ Afghanistan, 1998	79	0	0	0	100
Allied Force –Kosovo, 1999	218	111	~6,700	~16,000	~30
Enduring Freedom–Afghanistan, 2001-2	~75-85	0	~13,000	~9,000	~60
Iraqi Freedom–Iraq, 2003	~750	153	~18,300	~9,130	~68

The war in Kosovo also occasioned the first combat employment of the all-weather, GPS-aided, Joint Direct Attack Munition (JDAM).[31]

[31] The JDAM is essentially a tail kit that can be attached to existing 500-, 1,000- and 2,000-pound gravity bombs. By using the data provided by a GPS-aided inertial guidance system, the tail kit can guide a previously dumb bomb to within meters of its intended target. It can strike targets about 13 kilometers away from its point of release when dropped from an altitude of 20,000 feet. B-2 stealth bombers were the only aircraft configured to drop JDAMs during Operation Allied Force. Owing to the small size of the JDAM stockpile at the time, only about 650 were dropped over the course of the air campaign. See Bill Sweetman, "The Falling Price of Precision," *Jane's International Defense Review*, April 2002, p. 47.

The JDAM's development was spurred by LGB shortcomings encountered in the first Persian Gulf War, when strikes were periodically foiled by sandstorms and smoke from oil drum fires set by Iraqi forces. The combination of a low-cost inertial navigation system and GPS not only enables the JDAM to strike precisely through obscurants, but also allows pilots to release them from much higher altitudes than other PGMs without sacrificing accuracy, enhancing aircraft and pilot survivability.

During Operation Enduring Freedom, the proportion of PGMs to dumb bombs rose to approximately 60 percent—an increase of almost an order-of-magnitude relative to the Gulf War.[32] More than half of the PGMs expended in Afghanistan could be delivered in adverse weather conditions or through obscurants (e.g., smoke and sand clouds), which was a five-fold increase relative to Allied Force.[33] The majority of these all-weather PGMs were low-cost JDAMs.[34] On one

[32] The percentage fluctuated from less than 60 percent to more than 70 percent over the course of the war. See William Arkin, "Weapons Total from Afghanistan Includes Large Amount of Cannon Fire," *Defense Daily*, March 5, 2002, p. 12; Sweetman, "The Falling Price of Precision," p. 46; and Eric Schmitt, "Improved U.S. Accuracy Claimed in Afghan Air War," *New York Times*, April 29, 2002, p. A16.

[33] Of the 13,000 PGMs dropped during Operation Enduring Freedom, approximately 7,000 were equipped with all-weather, GPS-aided guidance. In comparison, only 10 percent of the PGMs dropped in Operation Allied Force were similarly equipped. If HARMs and WCMDs are included in the calculation, then just under 90 percent of the weapons expended in Afghanistan were all-weather capable, as compared to roughly 25 percent of the PGMs expended in Allied Force. See Christopher Bowie, Robert Haffa, and Robert Mullins, *Future War: What Trends in America's Post-Cold War Military Conflicts Tell Us About Early 21st Century Warfare* (Northrop Grumman Analysis Center, January 2003), pp. 47-48.

[34] To replenish stocks after the war, DoD requested Boeing to nearly double the JDAM's production rate from 1,500 to 2,800 units per month and boosted the planned buy from 88,000 to 236,000 units through FY 2008. Plans are also in place to make the JDAM more resistant to jamming or spoofing of GPS signals and to increase its accuracy by reducing its circular error probable (CEP) from 13 meters to three meters. See Arkin, "Weapons Total for Afghanistan includes Large Amount of Cannon Fire," p. 12; Schmitt, "Improved U.S. Accuracy Claimed in Afghan Air War," *New York Times*, April 29, 2002; Michael Sirak, "U.S. Air Force Boosts Proposed JDAM Buy," *Jane's Defence Weekly*, April 17, 2002; and Christopher Castelli, "Afghanistan Ops

occasion 100 JDAMs were delivered within 20 minutes—an average of five bombs every minute—to shatter dug-in, front-line Al Qaeda and Taliban forces.

During Operation Iraqi Freedom, PGMs enabled both manned and unmanned aircraft to strike Iraqi ground forces throughout the depth of the theater, military-related infrastructure (e.g., fuel and supply depots, airfields, and garrisons), distributed Iraqi air defenses, and a range of strategic targets (e.g., C3 facilities and leadership targets) with a minimum of collateral damage. Every weapon dropped or fired into Baghdad was precision guided.[35] The average miss distance of the more than 6,500 JDAMs dropped against Iraqi targets was 10-12 feet, or about the length of the bomb.[36] Navy surface combatants and submarines in the Persian Gulf, Red Sea, and eastern Mediterranean Sea fired some 750 TLAMs, or an average of more than 35 missiles per day, as compared to 288 fired over the course of Operation Desert Storm. In total, PGMs accounted for about seven out of every ten bombs dropped during the war.[37] The intensity of the

---

Highlight Needs for Smaller, Precision-Guided Bombs," *Inside the Navy*, April 22, 2002, p. 1.

[35] Lt Gen Michael Moseley, Combined Forces Air Component Commander, Pentagon-Saudi Arabia Two-Way Briefing, April 5, 2003.

[36] Ibid. See also: John A. Tirpak, "Precision: The Next Generation," *Air Force Magazine*, November 23, 2003, p. 46.

[37] Lieutenant General T. Michael Moseley, *Operation Iraqi Freedom – By the Numbers* (Prince Sultan Air Base, Saudi Arabia: U.S. Central Air Forces (USCENTAF), 2003), p. 11. See also: Defense Official, Air Force News – Quick Facts, April 15, 2003, Available at http://www.af.mil/news/Apr2003/4170367. shtml; Adam Herbert, "The Road to Victory," *Air Force Magazine*, May 2003, p. 17. As of April 8, 2003, DoD reported that PGMs accounted for "about 70-80 percent" of total munitions dropped. See General Richard Myers, Chairman, Joint Chiefs of Staff, *DoD News Briefing*, April 7, 2003; Major General Stanley McChrystal, Vice Director for Operations (J-3), Joint Staff, *DoD News Briefing*, April 8, 2003; and John H. Cushman Jr. and Thom Shanker, "War in Iraq Provides Model of New Way of Doing Battle," *New York Times*, April 10, 2003.

Includes 562 Hellfire rockets (AGM-114); 253 Joint Stand-Off Weapons (JSOWs); 918 Maverick missiles (AGM-65); 408 HARMs (AGM-88); 908 Wind-Corrected Munitions Dispensers (WCMDs), including 88 Sensor Fused Weapons (SFW); 98 EGBU-27s; 8,618 LGBs (all types), and 6,542 JDAMs (all

precision-strike campaign was unprecedented. In comparison to the first Gulf War, an equivalent number of PGMs were dropped in roughly half the time.

All-weather, precision air strikes were responsible for much, if not most, of the destruction of Iraqi Republican Guard divisions. Within less than two weeks, two reinforced divisions defending Baghdad were attrited to substantially less than 50 percent of their original combat strength.[38] The Medina Division, located southwest of Baghdad, was reportedly reduced to below 20 percent.[39] A significant portion of this attrition took place during a severe, three-day sandstorm that reduced the effectiveness of laser- and electro-optically guided weapons.

This trend toward increased reliance on all-weather, precision-strike capabilities seems certain to continue and will likely accelerate over the course of the next decade. The US military is already in the process of developing, fielding and refining several promising systems, including:

- Extended-range, jam-resistant JDAMs that can strike targets up to 40 kilometers away from their point of release;[40]

- Compact, 250-lb, highly accurate small diameter bombs (SDBs) that will enable bombers, strike aircraft, and eventually, UCAVs to target many more aimpoints per sortie than is currently possible;[41]

---

types). Ibid. See also: John A. Tirpak, "Precision: The Next Generation," *Air Force Magazine*, November 2003, pp. 50-51.

[38] General Richard Myers, DoD News Briefing, April 1, 2003. See also: Bradley Graham, "U.S. Air Attacks Turn More Aggressive," *Washington Post*, April 2, 2003, p. 24; and John Diamond and Dave Moniz, "Air Campaign Shifts Aim to Guard," *USA Today*, April 2, 2003, p. 4.

[39] Rick Atkinson, Peter Baker, and Thomas E. Ricks, "Confused Start, Swift Conclusion," *Washington Post*, April 13, 2003, p. 1.

[40] By using a compressed-wing kit, the JDAM-ER will reportedly have a range of about 40 kilometers. Bryan Bender, "JDAM's Range Trebled," *Jane's Defence Weekly*, May 3, 2000.

[41] The Small Diameter Bomb (SDB), which weighs approximately 285 pounds, was previously called the Small Smart Bomb. It may be produced in both

- Stealthy Joint Air-to-Surface Stand-off Missiles (JASSMs) with a range of over 350 kilometers, accuracy on the order of three meters, and a 1000-lb, multipurpose warhead;[42] and

- Tactical Tomahawks (TacToms) that will be capable of loitering above the target area for up to three hours while searching for

---

winged and non-winged variants. The SDB system is expected to meet the "R-95" standard for accuracy, meaning that 95 percent of the bombs dropped should fall within a three-meter radius of the aimpoint. With the aerodynamic lift generated from fold-out wings, it should be able to glide to targets 75 kilometers downrange or over 50 kilometers to either side of the aircraft. Low-rate initial production of the baseline SDB is scheduled to begin in mid-2005, leading to a limited operational capability in 2007. Although development of a follow-on weapon, referred to as SDB Phase II, could begin as early as FY 2006, it is unlikely to be fielded until the 2010 timeframe. The SDB Phase II weapon is expected to have a terminal seeker, an automated target recognition capability for attacking mobile and relocatable targets, and a two-way datalink for in-flight retargeting and BDA. The Air Force plans on acquiring over 24,000 SDBs over the next 15 years. See Michael Sirak, "Small Diameter Bomb May Get Seeker, Datalink," *Jane's Defence Weekly*, January 14, 2004, p. 10; Gail Kaufman, "Boeing Wins USAF's Small Diameter Bomb Competition," *DefenseNews.com*, August 28, 2003; Ron Laurenzo, "Smaller Bombs Could Make Air Power Even More Effective," *Defense Week*, December 3, 2001, p. 1; Elaine Grossman, "Quickly Fielded Small Diameter Bomb Among Top USAF Weapon Priorities," *Inside the Pentagon*, March 29, 2001, p. 1; and Adam Hebert, "Smaller Bombs for Stealthy Aircraft," *Air Force Magazine*, July 2001, pp. 42-44.

[42] The JASSM is designed to attack several classes of fixed and moving targets. DoD currently plans to acquire over 4,900 JASSMs, including 1,400 copies of an extended-range variant that is expected to have a range of around 800 kilometers, or more than two-and-a-half times the range of the baseline model. Each JASSM costs about $400,000, which is about one-third the cost of a TLAM. See John A. Tirpak, "Precision: The Next Generation," *Air Force Magazine*, November 2003, pp. 50-51; Tony Capaccio, "Lockheed Martin Cruise Missile Declared Combat-Ready By U.S.," *Bloomberg.com*, October 20, 2003; Michael Sirak, "US Air Force Plans Substantial Increase in Cruise Missile Buy," *Jane's Defence Weekly*, September 17, 2003, p. 7; Lorenzo Cortes, "Roche Doesn't See JASSM Use in Iraqi Freedom," *Defense Daily*, April 2, 2003, p. 1; David Fulghum, "Stealthy JASSM Approved for Low-Rate Production," *Aviation Week & Space Technology*, January 7, 2002, p. 25; and Michael Sirak, "US DoD Approves JASSM Production," *Jane's Defence Weekly*, January 2, 2002, p. 6.

mobile, time-critical targets and receiving in-flight retargeting instructions.[43]

PGMs are also becoming "smarter" and more lethal. The newly fielded Sensor Fused Weapon (SFW), for example, consists of ten submunitions that each contain four "skeet" anti-armor warheads equipped with passive infrared and active laser sensors. Once dropped from an aircraft, the SFW's submunitions descend by parachute, and as they near the ground, they propel their skeet warheads outward in a radial pattern. Each skeet warhead can independently scan the ground beneath them for a target and then fire an explosively formed penetrator slug downward through the top of a detected vehicle. The 40 skeets contained within a single SFW can search for and engage stationary and mobile ground combat vehicles within a 30-acre area.[44] With a payload of over 30 SFW weapons, a single bomber could saturate a battlefield with over 1,200 anti-vehicle skeet warheads in one sortie. SFWs released from a Wind-Corrected Munitions Dispenser (WCMD) were used for the first time in combat on April 2, 2003 when B-52s dropped six of them on Iraqi vehicles moving south

[43] TacToms include a UHF satellite datalink for receiving in-flight targeting updates. In addition to the standard unitary warhead, it will also be able to carry a kinetic-energy penetrator for striking hardened or deeply buried targets, as well as a variety of submunitions such as combined-effects bomblets, brilliant anti-armor (BAT), and sensor fused weapon (SFW). In the first of four operational flight tests, on April 5, 2003, a TacTom was successfully launched by the USS *Stetham* from within the Navy's sea test range off the coast of southern California. (Stephen Trimble, "Tactical Tomahawk Achieves First Operational Test," *Aerospace Daily*, April 8, 2003.) During Operation Iraqi Freedom, the Navy expended more than one-third of their inventory of TLAMs. The Navy plans to accelerate procurement of the TacTom from 456 to 600 missiles per year, as well as to boost the planned buy by 671 missiles for a new total of 2,396 in order to replenish its inventory. The TacTom achieved IOC in May 2004 and has entered full-scale production. (Tony Capaccio, "Raytheon Tomahawks Miss Few Iraqi Targets, Navy Says," *Bloomberg.com*, April 12, 2003; Anne Marie Squeo, "Navy's Tomahawk Arsenal Dwindles," *Wall Street Journal*, April 3, 2003; and Peter Pae, "Raytheon's Task: More Missiles, On the Double," *Los Angeles Times*, April 3, 2003.)

[44] See the Textron Systems Corporation's website at www.systems.textron.com/sfw.htm. See also Glenn Goodman, "Tank Eradicators," *Armed Forces Journal International*, August 2000, pp. 38-39.

out of Baghdad.[45] The effect was devastating—the Iraqi column was destroyed. In total, almost 90 SFWs were expended over the course of the war.

Within the next five years, the Air Force plans to begin fielding an even more capable mobile-target killer based upon the Low-Cost Autonomous Attack System (LOCAAS).[46] A successful live-warhead test of a prototype LOCAAS was conducted in March 2003.[47] This 36-inch long, 100-pound, turbine-powered, winged weapon can loiter over the battlefield for up to 30 minutes and use its laser-radar (LADAR) sensor and rapid ATR capability to identify and track multiple dispersed targets, including tanks, infantry fighting vehicles, missile launchers, and other combat vehicles on the move.[48] Cruising at an altitude of around 750 feet and a speed of 200 knots, the search footprint on the ground of each LOCAAS is over 80 square kilometers.[49] After identifying multiple targets within its engagement envelope, it can decide which one is the highest priority, based on pre-programmed instructions, and attack it with a multi-mission warhead

---

[45] Stephen Trimble, "Pentagon Eyes Larger Role for Battle-Tested Sensor Fuzed Weapon," *Aerospace Daily*, April 9, 2003; "WCMD-Equipped Sensor Fuzed Weapons Dropped on Iraqi Vehicle Column," *Defense Daily*, April 3, 2003, p. 1.

[46] Within the Air Force, the LOCAAS will compete for production funds with alternative next-generation PGM designs under the Autonomous Wide-Area Search Munition (AWASM) program, which was formerly referred to as the Wide Area Search Autonomous Attack Miniature Munition (WASAAMM) initiative.

[47] Michael Sirak, "USAF Looks to Speed Work on "Smart" Weapon," *Jane's Defence Weekly*, April 2, 2003.

[48] LOCAAS is expected to have a fly-out range of over 150 kilometers. General Lester Lyles (Commander, US Air Force Material Command) and Major General Paul Nielsen (Commander, US Air Force Research Laboratory), Testimony before the Tactical Air and Land Forces Subcommittee, US House Armed Services Committee, Hearing on "Air Force Science and Technology Programs," July 19, 2003. See also Clifford Beal, "Brave New World," *Jane's Defence Weekly*, February 9, 2000, pp. 25–26; and Clifford Beal, "Redesign for LOCAAS Air Weapon," *Jane's Defence Weekly*, June 16, 1999, p. 8.

[49] Lockheed Martin (Missiles and Fire Control), LOCAAS Factsheet, 2002. See also: Sandra Erwin, "Air Force Wants Missiles Redirected in Flight," *National Defense*, May 2003, p. 29; and Glenn Goodman, "Tank Eradicators," *Armed Forces Journal International*, August 2000, pp. 40-41.

that can be shaped as a penetrating rod for piercing armor, as an aerodynamically stable slug for standoff kills, or as a fragmentation warhead for softer targets. A single F/A-22 Raptor or F-35 Joint Strike Fighter (JSF) will be able to carry up to 16 LOCAAS weapons and the B-2 will be able to carry 192 of them. The LOCAAS could also be carried by UCAVs, dispensed from missiles fired from ground-based Multiple Launch Rocket System (MLRS) and Army Tactical Missile System (ATACMS) batteries, or released from cruise missiles launched from future unmanned underwater vehicles (UUVs), submarines, or surface ships.[50] Individual LOCAAS weapons will be able to communicate with each other to prevent multiple engagements of the same target and to facilitate bomb damage assessment (BDA).

The effectiveness of PGMs is also being enhanced by the development of new ISR capabilities. During the past two decades, for example, the fielding of more capable reconnaissance satellites (e.g., short-latency, electro-optical imaging and day-night, all-weather, high-resolution radar imaging), UAVs, and airborne, multi-mode radar platforms such as the JSTARS has made it easier to locate, identify and track enemy ground vehicles, especially in open terrain. New intelligence analysis and battle management tools have dramatically reduced the time needed to identify targets, generate mensurated coordinates, and plan an attack.

As demonstrated repeatedly over the last decade, fixed installations (e.g., ports, airfields, hangers, supply depots, and C3 nodes) can be quickly and effectively destroyed by modern PGMs. In light of the above-mentioned trends, it is probable that high-signature

[50] Lockheed Martin, for example, has already proposed building a Vertical Launch Autonomous Attack System (VLAAS) that comprises a vertically launched rocket (a modified anti-submarine rocket) equipped with a tactical munitions dispenser containing four LOCAAS submunitions. According to Lockheed Martin, the four LOCAAS submunitions could search an area about 25 square kilometers in size for fast patrol craft/missile boats or ground-based time critical targets. A standard VLS cell could accommodate up to six VLAAS missiles. See Mark Hewish, "US Services Considered Naval and UAV-launched LOCAAS," *Jane's International Defense Review*, March 2002, p. 15; Michael Sirak, "Lockheed Martin Offers Naval Strike Weapon," *Jane's Defence Weekly*, April 18, 2001, p. 10; and Michael Sirak, "Inexpensive Ship-Launched Weapons for Long-Range Engagements," *Jane's International Defense Review*, June 2001, p. 21.

mobile targets (e.g., large mechanized units and surface ships) will become increasingly vulnerable to detection and attack over the coming decade.[51] This is not to suggest, however, that the battlespace is, or will soon become completely transparent. Competitors have already reacted to US advances in ISR by placing more emphasis on operating in "cluttered" battlespace, as well as by exploiting mobility; dispersion; and increasingly sophisticated cover, camouflage, concealment, deception, and denial (C3D2) techniques. As will be discussed in Chapter III, the increasing lethality of PGMs is closely linked with the competition between hiders and finders.

The Advent of Stealth

Development of modern stealth technologies and their application to combat aircraft began in earnest in the mid-1970s.[52] The impetus for

---

[51] The growing ability of the US military to exploit sensor networks to find heavy mechanized forces and then target them with increasingly smart PGMs might be construed as an RMA by itself. Although a one-sided revolution, it could meet the test of rendering obsolete an existing means of warfare, in this case, high-signature, mechanized ground combat. A critical question, however, is whether asymmetric responses by prospective adversaries will be able to negate this US capability. For example, if adversaries are able to field robust anti-access capabilities that prevent the US military from deploying the requisite array of sensor systems and tank-busting strike platforms into a given theater of operations, then armored warfare could remain practicable. An additional RMA threshold will be crossed when competitors are able to field reconnaissance-strike networks that allow them to find and destroy US mechanized forces and other high-signature mobile targets (e.g., ships operating in littoral waters). See David Ochmanek, Edward Harshberger, David Thaler and Glenn Kent, "Find, Hit, Win," *Air Force Magazine*, April 1999, p. 51. See also Ochmanek, Harshberger, Thaler, and Kent, *To Find and Not to Yield – How Advances in Information and Firepower Can Transform Theater Warfare* (Santa Monica, CA: RAND, 1998) and *Winning the Halt Phase of Future Theater Conflicts: Exploiting Advances in Firepower* (Santa Monica, CA: RAND, 1997).

[52] DARPA proposed the stealth fighter concept to the Director of Defense Research and Engineering (DDR&E) in 1974 and let conceptual development contracts to Lockheed and Northrop in 1975. Lockheed was selected to develop a quarter-scale, proof-of-concept aircraft, dubbed HAVE BLUE, in 1976, which was successfully flight tested in 1977. The research effort then transitioned to a "black" Air Force procurement program called SENIOR TREND. See Van Atta et al, *Transformation and Transition: DARPA's Role in Fostering an*

R&D efforts to reduce the radar cross section (RCS) of aircraft was the fielding of increasingly capable surface-to-air missiles (SAMs) by the Soviet Union such as the mobile SA-6, many of which were exported to its client-states throughout the world. The potential significance of this technology was clearly illustrated during the 1973 Yom Kippur War. Over the course of 18 days, well-trained Israeli pilots flying the same planes as their American counterparts and employing the same evasive maneuvering techniques, lost some 80 planes to Syrian and Egyptian SAMs and radar-guided antiaircraft batteries.[53] By extrapolating the Israeli loss ratio to a war between US and Warsaw Pact forces in Europe equipped with similar capabilities, it appeared that the US Air Force would be "decimated" in only a few weeks.[54]

Lockheed's Skunk Works began preliminary R&D on the application of stealth to strike aircraft in 1975.[55] The first test flight of the stealthy F-117 Nighthawk attack aircraft took place six years later in 1981. Only two years later, the Nighthawk covertly entered into service, but its existence was not officially acknowledged until 1988. It first saw action in December 1989 in Operation Just Cause in Panama.

Emerging Revolution in Military Affairs, pp. 12-15. For a narrative history of the development of stealth aircraft by Lockheed's Skunk Works, see: Ben R. Rich and Leo Janos, *Skunk Works* (New York: Little, Brown & Company, 1994), p. 17.

[53] The Israeli Air Force lost 109 aircraft during the 1973 war. Approximately 46 aircraft were shot down by SAMs and 31 by anti-aircraft artillery. While the cause of the remaining aircraft losses is unknown, a portion of them were almost certainly downed by SAMs. See Anthony H. Cordesman and Abraham R. Wagner, *The Lessons of War – Volume I, The Arab-Israeli Conflicts, 1973-1989* (Boulder, CO: Westview Press, 1990), pp. 89-93.

[54] Ben R. Rich and Leo Janos, *Skunk Works*, p. 17.

[55] During the 1960s, the Skunk Works gained important experience in reducing an aircraft's RCS by designing and building the SR-71 Blackbird reconnaissance aircraft. The RCS of the SR-71 was reduced with shaping techniques and by applying radar-absorbing materials (RAM) to the wings, tail and fuselage. The stealth shaping techniques explored in the later part of the 1970s, however, promised to reduce the RCS of contemporary low-observable designs by three or more orders-of-magnitude. Ibid., pp. 23-27.

During the Gulf War in 1991, targets in heavily defended central Baghdad were assigned almost exclusively to the F-117.[56] Despite the relative sophistication of Iraq's air defense network, not a single F-117 was shot down or damaged over the course of some 1,300 sorties. Although it flew less than two percent of the total attack sorties against Iraq, the F-117 struck nearly 40 percent of the strategic targets and "remained the centerpiece of the strategic air campaign for the entire war."[57] The F-117s low-signature made it possible to conduct strike sorties with substantially fewer supporting aircraft in comparison to non-stealthy force packages.[58] In their seminal work on role of air power during the Gulf War, Tom Keaney and Eliot Cohen concluded:

> Stealthy, low observable platforms were the keystones of Coalition attacks against the Iraqi air defense system, leadership, and communications targets early on the first day of the war, even in heavily defended areas. Throughout the war, they attacked with complete surprise and were nearly impervious to Iraqi air defenses. These platforms needed minimal support from other aircraft but were able to provide stealth to a much larger force by disabling the enemy air defense system, thus making all Coalition aircraft harder to detect and attack. Stealth thus not only restored a

[56] See Conduct of the Persian Gulf War – Final Report to Congress (Washington, DC: DoD, April 1992), pp. 88-174.

[57] Thomas Keaney and Eliot Cohen, Gulf War Air Power Survey – Summary Report, p. 224. See also Keaney and Cohen, Revolution in Warfare: Air Power in the Persian Gulf, p. 190.

[58] In their 1995 study on the *Future Bomber Force*, the Commission on Role and Missions (CORM) included a comparison of a non-stealth attack during the Gulf War with a stealth attack that took place at about the same time. The non-stealth force package consisted of 38 fighter/attack aircraft, but only eight were assigned to bomb the three aimpoints targeted in the mission. The remaining 30 aircraft were required for electronic jamming, suppression of enemy air defenses, and protection against potential airborne threats. In contrast, the stealth attack package comprising 20 F-117s attacked 37 aimpoints in areas with an equal or higher air defense threat – which is roughly "an over 1,200 percent increase in target coverage using 47 percent fewer aircraft." See CORM, Future Bomber Study (Arlington, VA: Aerospace Education Foundation, 1995), pp. 2-3. See also Colonel Gary Crowder, "Effects Based Operations," Air Combat Command Briefing, Spring 2003, p. 5.

> measure of surprise to air warfare, it also provided air forces some freedom of action that otherwise would not have been attainable.[59]

Echoing that view, General Charles Horner, the commander of Coalition air forces during Desert Storm, testified to Congress that:

> The F-117 allowed us to do things that we could have only dreamed about in past conflicts. Stealth enabled us to gain surprise each and every day of the war. For example, on the first night of the air campaign the F-117s delivered the first bombs of the war against a wide array of targets, paralyzing the Iraqi air defense network.[60]

Similarly, during the first 58 days of Operation Allied Force, only the stealthy B-2 bomber and F-117 Nighthawk were used to strike targets in heavily defended Belgrade.[61] Flying some 49 sorties from Whiteman Air Force Base in Missouri, B-2s delivered an average of nearly 15 weapons per sortie and over 80 percent of their targets were hit on the first pass.[62] Although they flew less than one-half of one percent of the strike sorties, B-2s dropped 11 percent of the bombs

---

[59] See Keaney and Cohen, Revolution in Warfare: Air Power in the Persian Gulf, p. 190.

[60] Lt. Gen. Charles Horner, *Prepared Statement*, hearing on DoD Appropriations, April 30, 1991.

[61] Bill Sweetman, "B-2 Is Maturing into a Fine Spirit," *Jane's International Defense Review*, May 2000.

[62] During this phase of the war, B-2s flew only three percent of the strike sorties, but struck one-third of the targets. Christopher Bowie, Robert Haffa, and Robert E. Mullins, *Future War: What Trends in America's Post-Cold War Military Conflicts Tell Us About Early 21st Century Warfare* (Northrop Grumman Analysis Center, January 2003), p. 48). Part of the explanation for the B-2's high degree of accuracy is that its GPS-aided targeting system halved the circular error probable (CEP) of the JDAM. Barry Watts, "The B-2: Kosovo and Beyond," Northrop Grumman Analysis Center Briefing, May 2000, p. 4; and Frank Wolfe, "Pentagon Report Lauds B-2; Notes Shortfalls," *Defense Daily*, February 16, 2000, p. 6.

delivered against fixed targets in Serbia and Kosovo.[63] They also required much less jamming and fighter escort support than non-stealthy strike packages. In fact, on a few occasions, they flew night bombing missions without any escort at all. During Operation Iraqi Freedom in 2003, F-117s and B-2s, now forward-based in deployable shelters, were used to strike the most heavily defended Iraqi targets.

The value of stealth for penetrating enemy air defense systems, at least those that employ radar and infrared sensors for surveillance, tracking and targeting, is manifest. In addition to enhanced survivability in high-threat environments, stealth confers other advantages such as the ability to gain operational-strategic surprise by striking with little or no warning. Accordingly, DoD has put considerable effort into pushing the state-of-the-art in stealth over the last decade, as illustrated by the development of the F/A-22 Raptor and F-35 JSF, which incorporate signature reduction technologies that are substantially more advanced than those first demonstrated by the F-117 Nighthawk more than two decades ago. Future platforms may incorporate a new generation of stealth technologies such as active signature nullification; visual signature control using photochromic, thermochromic, and electrochromic materials;[64] next-generation stealth coatings, films, and radar absorbent material (RAM); and adaptive "smart skins" that leverage advances in micro-electromechanical systems (MEMS) and biomimetic materials.[65] Signature reduction techniques are also being applied to a broader range of platforms. During Operation Iraqi Freedom, a stealthy, high-altitude UAV prototype reportedly made its operational debut in the skies over Baghdad.[66] Similarly, the US military's first built-for-

---

[63] Benjamin Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Assessment* (Santa Monica, CA: RAND, 2001), p. 91.

[64] The goal would be to reduce the solar glint, visual contrast, and optical cross section of aircraft. See Bill Sweetman, "How Low Can You Go?" *Jane's International Defense Review*, January 2002, p. 23.

[65] USAF Scientific Advisory Board (SAB), *New World Vistas – Air and Space Power for the 21st Century*, Materials Volume, pp. 57-70, 128-136; Board on Army Science & Technology, *STAR 21: Strategic Technologies for the Army of the Twenty-First Century*, pp. 68-71, 80-81, 389-449.

[66] David Fulghum, "Stealth UAV Goes to War," *Aviation Week & Space Technology*, July 7, 2003, p. 20.

purpose unmanned combat air vehicle (UCAV), called the X-45, incorporates a variety of stealth features.[67] Conceptual studies for stealthy aerial refuelers and transports have been undertaken by US defense industry.[68]

Stealth is being applied to naval and ground vehicles as well. Sweden, Norway, and France, for example, already have comparatively stealthy surface ships as sea.[69] Sweden's 600-ton *Visby* class corvette exploits a variety of techniques, including carbon-fiber reinforced plastic construction, to minimize RCS, infrared, acoustic, magnetic, hydrodynamic pressure, visual, and electronic signatures.[70] Similarly, to minimize their signature, the next-generation of US surface combatants (i.e., the Littoral Combat Ship (LCS), future destroyer (DD-X), and future guided-missile cruiser (CG-X)) are expected to incorporate a low-clutter topside design, electric-drive, embedded

---

[67] Tom Goldman (Director, Boeing, J-UCAS Business Development, "Joint Unmanned Combat Air System—Overview and Update," briefing at CSBA, August 2003. A stealthy, carrier-based UCAV is also under development. See: Office of the Secretary of Defense, *Unmanned Aerial Vehicle Road Map 2002-2027* (Washington, DC: DoD, December 2002), p. 12; and David Fulghum, "First Flight for Pegasus," *Aviation Week & Space Technology*, March 3, 2003, p. 34.

[68] The US Air Force and Air Force Special Operations Command are in the process of validating requirements for a future stealthy transport (M-X), next-generation gunship (AC-X), a stealthy penetrating tanker (K-X), and a low-observable cargo aircraft (C-X). The plan is to develop a common, modular airframe that could be modified to meet unique mission requirements in each area. The goal is to be able to field these aircraft in the 2020 timeframe. Andrew Koch, "US Wants Next-Generation Stealth Aircraft," *Jane's Defence Weekly*, October 29, 2003.

[69] The *Visby* is in sea trials but will not officially enter into service until 2005. See Richard Scott, "Visby to Sail by Year's End," *Jane's Defence Weekly*, September 5, 2001, p. 29; and David Foxwell and Joris Janssen Lok, "Approaching the Vanishing Point: The Emergence of Stealth Ships," *Jane's International Defense Review*, September 1998, pp. 43-48.

[70] The *Visby* incorporates signature-reduction techniques. See Richard Scott, "Visby to Sail by Year's End," p. 29; and Joris Janssen Lok, "Visby Heralds Big Changes for Sweden's Hit and Run Navy," *Jane's International Defense Review*, August 2000, p. 28.

multi-function apertures for antennas and electronic systems, and use of composite materials and RAM in their construction.[71]

Several states (e.g., Sweden and France) have fielded prototype main battle tanks with a significantly smaller RCS, as well as reduced thermal and acoustic signatures, as compared to traditional designs.[72] The Army hopes to make the 20-ton Future Combat System, which is slated for initial fielding in 2012, as stealthy as possible through the use of a low-profile design and composite material, as well as by incorporating an electric-drive system. While the latter could significantly reduce the vehicle's acoustic and thermal signature, its realization will depend upon breakthroughs in high-density energy storage systems (e.g., efficient hybrid-electric systems and fuel cells) over the course of the next decade.

The Rise of Unmanned Systems

Historically, the single greatest impediment to robotic development has been limited data-processing capability. Fortunately, computational power has increased by about six orders-of-magnitude over the last 35 years and the current technological forecast is for Moore's Law to hold for at least another decade.[73] As a direct

[71] Electric-drive propulsion could reduce a surface ship's signature in a variety of ways. Most significantly, it promises to be much quieter acoustically than mechanical drive. Second, new propulsor configurations made possible by electric drive (e.g., podded propulsor) could reduce a ship's wake, making it more difficult to detect by overhead sensors or to attack with wake-homing torpedoes. Third, the internal design flexibility afforded by electric drive could permit a reduction in the volume of space devoted to exhaust ducts, which could in turn reduce the ship's infrared signature. See Ronald O'Rourke, "Electric-Drive Propulsion for U.S. Navy Ships: Background Issues for Congress," *CRS Report to Congress*, Document Code RL 30622, July 31, 2000, pp. 17-19.

[72] Examples included the Swedish SAT/MARK and the French AMX 30 B-2 technology demonstrators. See R.M. Ogorkiewicz, "The Quiet Approach," *Jane's International Defense Review*, September 2002, pp. 32-35.

[73] In 1965, when Gordon Moore, then research director of Fairchild Semiconductor and later co-founder of the Intel Corporation, made his now famous prediction that the number of transistors on a silicon microchip would

beneficiary of these advances in data processing power, machine intelligence has improved enormously over the last few decades and will continue to do so over the next. Technological advances in high-density energy storage, miniaturization, sensors, and machine perception and learning algorithms have also contributed to the rise of more capable unmanned systems. As will be discussed below, while unmanned aircraft have arguably matured the most over the last few decades, promising new unmanned undersea vehicles (UUVs), unmanned ground vehicles (UGVs), and unmanned surface vehicles (USVs) have also been developed and, in a few instances, operationally deployed.

Unmanned Aircraft from Vietnam to Operation Iraqi Freedom

Over the past three decades, unmanned aircraft have matured from relatively unreliable platforms with niche roles in ISR and "baiting" enemy air defense systems to multipurpose combat systems with tremendous operational utility.[74] In Afghanistan in 2001 and this past year in Iraq, for example, UAVs equipped with mix of infrared, electro-optical (EO), and SAR sensors have proven invaluable in providing persistence surveillance over the battlefield.

During the war in Vietnam, variants of the remotely controlled, low-flying Firebee drone (e.g., the Lightning Bug) flew thousands of missions over North Vietnam, snapping still pictures with a high-resolution, wet-film camera, baiting enemy SAM batteries, and collecting electronic intelligence data. Owing to poor navigation and rudimentary flight controls, however, many missed their targets or

---

double every year, the state of the art was 64 transistors per chip. Intel's Pentium IV chip released in 2000, in comparison, contains 42 *million* transistors. The cost of computing power has dropped by about six orders of magnitude over the last fifty years. See Rodney A. Brooks, Director of MIT Artificial Intelligence Lab, *Briefing to SAIC Robotics Workshop*, March 1997, p. 1.

[74] For a thorough history of US development of UAVs over the last half century, see Thomas Ehrhard, *A Comparative Study of Weapon Systems Innovation: Unmanned Aerial Vehicles in the United States Armed Services* (Washington, DC: John Hopkins University, PhD dissertation, 2000).

crashed. During the 1970s, the United States developed, built, and tested—but never operationally deployed—dozens of high-altitude, long endurance UAVs as part of the ambitious Compass Arrow and Compass Cope programs.[75] The programs were eventually terminated because the cost-versus-performance tradeoff was unattractive in comparison to manned reconnaissance aircraft like the U-2.

With the decreasing cost and increasing performance of microprocessors, DARPA launched a series of "black" UAV R&D initiatives in the 1980s, including the Amber and Condor programs. The former successfully demonstrated an air vehicle with a flight duration approaching 40 hours at an altitude of 25,000 feet, while the Condor flew for over 60 hours, reaching an altitude of over 67,000 feet. Although neither of these prototype systems was fielded, they pushed the state-of-the art in composite construction, inertial navigation, fly-by-wire flight control, and most importantly, automated flight control systems.[76]

The Advanced Airborne Reconnaissance System (AARS) program, code-named "Quartz," was also launched in the mid-1980s. Intended as a means for finding and tracking mobile launchers for Soviet IRBMs and ICBMs, the AARS was envisioned as an extremely stealthy UAV equipped with an array of high-resolution sensors and high-capacity satellite communications capabilities.[77] After spending

---

[75] The Compass Arrow UAV, 28 of which were built, could fly at an altitude of over 80,000 feet for about four hours. The Compass Cope UAV could pilot itself to a series of preprogrammed waypoints and had an endurance of over 24 hours. See Rebecca Grant, "Eyes Wide Open," *Air Force Magazine*, November 2003, p. 39.

[76] Ehrhard, *A Comparative Study of Weapon System Innovation: Unmanned Aerial Vehicles in the United States Armed Services*, pp. 169-178.

[77] With a wingspan of some 250 feet, it would have been able to fly at an altitude of about 80,000 feet for several days at a time. For an excellent overview of this program, see Ehrhard, *A Comparative Study of Weapon System Innovation: Unmanned Aerial Vehicles in the United States Armed Services*, pp. 136-158. See also: John Boatman, "USA Planned Stealthy UAV to Replace SR-71," *Jane's Defence Weekly*, December 17, 1994, p. 1; David A. Fulghum, "Stealthy UAV Is a Flying Wing," *Aviation Week & Space Technology*, July 11, 1994, p. 21; and Michael Dornheim, "Mission of Tier 3

about $1 billion on its development, the AARS program was terminated in 1992 just as it was about to enter full-scale development.[78] With the collapse of the Soviet Union, its high unit cost of close to $500 million dollars could no longer be justified. Its low-observable, "flying clam shell" design and other key technologies (e.g., sensors and flight controls), however, were incorporated into subsequent systems, including a stealthy UAV that reportedly flew in the skies above Iraq in 2003.[79]

During the first Gulf War, UAVs performed a wide variety of relatively short-range, tactical ISR missions. Pioneer UAVs, for example, flew over 200 sorties, most of which were dedicated to identifying targets and performing BDA. The combination of both manned and unmanned ISR platforms, however, was insufficient to provide persistent, wide-area surveillance over Iraq. After the war, geographic and temporal gaps in ISR coverage were identified as one of the principal causes of the coalition's unsuccessful "hunt" for Scud missile TELs. In 1993, a Defense Science Board summer study recommended that these gaps be filled with longer endurance, higher flying UAVs that could not only exploit breathtaking advances in microelectronics and miniaturization, but also the availability of GPS for precision navigation. This finding was echoed in DoD's Bottom-Up

---

Reflected in Design," *Aviation Week & Space Technology*, June 19, 1995, p. 54.

[78] A scaled-down version of the AARS with a 150-foot wingspan and reduced sensor payload was subsequently introduced as the only serious candidate for the Tier III UAV requirement that was generated during the Bottom-Up Review (BUR) in 1993. However, with an estimated production cost of $150 to $400 million per copy, the Tier-III version of the AARS had few champions within Congress and the Services. Ehrhard, *A Comparative Study of Weapon System Innovation: Unmanned Aerial Vehicles in the United States Armed Services*, pp. 144, 152. See also: See David A. Fulghum, "Secret Flying Wing Slated for Rollout," *Aviation Week & Space Technology*, September 19, 1994, p. 24; and David A. Fulghum, "UAV Contractors Plot Stealthy Redesigns," *Aviation Week & Space Technology*, August 15, 1994, p. 60.

[79] Although details are unavailable, several sources report that a stealthy UAV was used operationally over Iraq during Operation Iraqi Freedom. See David Fulghum, "Unafraid and More Than Alone," *Aviation Week & Space Technology*, December 15, 2003, p. 60.

Review of the same year, which led to an expansion in UAV-related R&D and a restructuring of UAV programs into three capability groupings: Tier I (UAVs that could be quickly fielded), Tier II (medium-altitude, long-endurance), Tier II-plus (high-altitude, long-endurance), Tier III (stealthy, high-altitude, long-endurance), and Tier-III-minus (stealthy, medium-altitude/endurance).

The Tier I program led to the fielding of the Gnat-750, an offshoot of the Amber program, which has an endurance of more than 40 hours and an altitude ceiling of over 20,000 feet. Several Gnat-750s saw action in the Balkans, monitoring air bases, entrenchments, supply caches and troop movements.[80] While the Tier-III programs were eventually abandoned, primarily for cost reasons, the Tier II R&D effort yielded the now familiar Predator and Global Hawk UAV systems that have performed admirably in recent US military operations. As an interim measure, the Predator was armed with Hellfire missiles, giving it a limited ground-attack capability, which proved extremely useful during combat operations in Afghanistan and Iraq. Building upon this success, the US military not only accelerated the development of more capable, armed variants of the Predator, but also built-for-purpose UCAVs.

The Predator

The Predator, which began as an advanced concept technology demonstration in 1994, can carry a 465-lb. sensor payload (e.g., gimble-stabilized EO/IR and SAR) for up to 24 hours at a mission radius of 500 nautical miles. It typically flies at around 15,000-20,000 feet when conducting ISR missions, but has an altitude ceiling of about 26,000 feet. Although the Predator made its combat debut over Bosnia in 1995 during Operation Deliberate Force, it really came into its own during Operation Allied Force in 1999.[81] Predator UAVs probed Serb air defenses, scouted attack and escape routes, identified targets, performed BDA and allowed NATO to extensively monitor the “ethnic cleansing” of the Albanian population. They also conducted electronic eavesdropping, served as airborne communications relays, and

[80] See: http://www.globalsecurity.org/intell/systems/gnat-750.htm.

[81] By May 1998, Predators had flown more than 600 sorties and logged some 3,800 flying hours over Bosnia.

jammed Yugoslav communications. Had the war lasted a few days longer, the Air Force would have used UAVs equipped with laser designators to pick out Yugoslav military targets.[82] In its post-war analysis of the war, DoD concluded that UAVs were used at "unprecedented levels" and "played an important role in our overall success."[83]

During the war in Afghanistan, in addition to the many long-dwell ISR missions they performed so well in the Balkans, Predators also fed live battlefield video directly to AC-130 gunships.[84] This hunter-killer team was used to attack small groups of Al Qaeda/Taliban fighters and other fleeting targets. In a watershed event for unmanned systems, a handful of Predator UAVs were each armed with two laser-guided, ground-attack Hellfire missiles for directly attacking enemy targets. These CIA-operated UAVs fired 115 missiles at approved Al Qaeda and Taliban targets and laser-designated another 525 targets for destruction by LGBs dropped from manned aircraft.[85] These weaponized Predator UAVs reportedly had a very high success rate.[86] By combining ISR systems and precision-

---

[82] David Fulghum, "Kosovo Conflict Spurred New Airborne Technology Use," *Aviation Week & Space Technology*, August 23, 1999, p. 30.

[83] DoD, *Kosovo/Operation Allied Force After-Action Report–Report to Congress* (Washington, DC: DoD, January 2000), p. 56.

[84] Each gunship was armed with a 105-mm howitzer, a 40-mm cannon, and two 20-mm Gatling guns capable of pouring out 2,500 rounds per minute. See Eric Schmitt and James Dao, "Use of Pinpoint Airpower Comes of Age in New War," *New York Times*, December 24, 2001, p. 1.

[85] Gail Kaufman, "UAVs Shifted Role in Iraq Operations," *Defense News*, December 8, 2003, p. 24. Toward the end of the war over Kosovo (Operation Allied Force), the Air Force had low-flying Predators equipped with stabilized laser-designator turrets so they could pick out Yugoslav military targets for manned fighters flying above the cloud cover, but the war ended before this concept could be tested in combat. See David Fulghum, "Kosovo Conflict Spurred New Airborne Technology Use," *Aviation Week & Space Technology*, August 23, 1999, p. 30.

[86] Kenneth Munson, ed., *Jane's Unmanned Aerial Vehicles and Targets* (London, UK: Jane's Information Group, 2002), p. 240; David Fulghum, "Armed Predator Successful in Wartime Debut," *Aviation Week & Space Technology*, October 22, 2001; and Mark Thompson, "A Killer Drone," *Time*,

strike weapons on the same long-endurance platform, the sensor-to-shooter targeting cycle was effectively reduced to the time required for human operators to authorize a strike. As part of the global war on terrorism, on November 3, 2002, a Predator UAV patrolling over a tribal area in Yemen where the government had negligible control was used to track down and kill an Al Qaeda leader who is believed to have been the mastermind behind the attack on the USS *Cole*, along with five of his associates.[87]

Nine reconnaissance-only (RQ-1) and seven weaponized versions (MQ-1) of the Predator took part in Operation Iraqi Freedom, flying hundreds of ISR missions, firing scores of Hellfire missiles, and designating 146 targets.[88] Predators were used, for example, to strike high-value targets (e.g., SAMs, anti-aircraft artillery, and communication antennas) in and around Baghdad. Because the Predator's Hellfire missile is very accurate and packs only 100 pounds of high explosive, it could effectively strike soft targets in densely populated areas without generating extensive collateral damage. The Air Force has also explored the possibility of arming Predator UAVs

---

November 26, 2001. See also: Neil King Jr. and David S. Cloud, "A Year Before Sept. 11, U.S. Drones Spotted Bin Laden in His Camps, But Couldn't Shoot," *Wall Street Journal,* November 23, 2001, p. 1.

[87] The strike was carried out pursuant to a US presidential finding that authorizes lethal covert action by the CIA against Al Qaeda. See Walter Pincus, "U.S. Strike Kills Six in Al Qaeda," *Washington Post*, November 5, 2002, p. A1, and Walter Pincus, "Missile Strike Carried Out with Yemeni Cooperation," *Washington Post*, November 6, 2002, p. A10.

[88] Although more weaponized Predators were available in Operation Iraqi Freedom than in Enduring Freedom, they fired about half as many Hellfire missiles. Given the large number of available manned strike aircraft in striking range of Iraq, commanders opted to use the still small inventory of Predators to help provide persistent ISR coverage over the battlefield. See Kaufman, "UAVs Shifted Role in Iraq Operations," p. 24; Mosley, *Operation Iraqi Freedom – By the Numbers*, p. 7; and Eric Schmitt, "In the Skies Over Iraq, Silent Observers Become Futuristic Weapons," *New York Times*, April 18, 2003.

with Stinger air-to-air missiles to give them a modest self-defense capability against airborne threats.[89]

The Air Force is in the process of fielding a larger, turboprop-powered version of the Predator that offers a number of capability improvements over the original Predator-A, especially with respect to its potential for conducting precision strikes.[90] Dubbed the MQ-9A Predator B, it will be able to fly 20,000 feet higher, loiter longer, carry an internal sensor payload that is almost 300 pounds heavier, cruise more than twice as fast (200 versus 70 knots), and can carry a much heavier weapons payload (i.e., up to 3,000 pounds). It can also be armed with a wider range of PGMs including the JDAM, TV-guided Maverick, Paveway II LGB, SDB and LOCAAS.[91] Although its range and endurance would be substantially reduced, the MQ-9A has demonstrated the ability to carry up to eight Hellfire missiles, two

[89] A Stinger-armed Predator A was flight tested in 2002 and reportedly flew a mission supporting the U.N. designated no-fly zones in Iraq. Michael Sirak, "USAF Eyes Predator Self-Defence Capability," *Jane's Defence Weekly*, October 23, 2002, p. 7; Amy Butler, "Jumper Says Early Test of Predator with Stinger Missile a Success," *Inside the Air Force*, November 22, 2002, p. 3; Amy Butler, "Senior Sources: Old Predators Used as Decoys to Provoke Iraqi Air Defenses," *InsideDefense.com*, April 8, 2003; Amy Butler, "USAF to Demo Predator against Airborne Targets with Stinger Missile," *InsideDefense.com*, October 2, 2002.

[90] The MQ-9A Predator B UAV has been flying since 2001 and two vehicles have already been delivered to the Air Force. The first of seven "pre-production" air vehicles made its first flight in October 2003. The MQ-9A is expected to begin initial operational test and evaluation in 2007 and enter full-rate production in 2008. Bill Sweetman, "In the Tracks of the Predator: Combat UAV Programs are Gathering Speed," *Jane's International Defense Review*, August 2004, p. 50.

[91] The MQ-9A is expected to have a maximum endurance of 48 hours, but with a typical combat load and mission profile its endurance will likely be closer to 24 hours. A Predator-B successfully attacked a stationary ground target with a 500-lb Paveway II LGB in April 2004. See Michael Sirak, "Predator B Drops Paveway II," *Jane's Defence Weekly*, August 18, 2004, p. 8; and Gail Kaufman, "U.S. Air Force Seeks More Firepower for Predator B," *Defense News*, June 10-16, 2002, p. 20.

JDAMs, and two air-to-air missiles.[92] In addition to a SAR and Multispectral Targeting System, variants of which are also carried by the Predator A, the MQ-9A may also carry a laser-radar (LIDAR) sensor which is claimed to be capable of penetrating moderate cloud cover, smoke, dust, foliage, and camouflage.[93] A stealthier version of the MQ-9A is also under development as is a faster, higher-flying variant powered by a turbofan (jet) engine.[94]

The Global Hawk

The Global Hawk has a ferry range of more than 14,000 nautical miles, a cruising speed of 345 knots, an altitude ceiling of around 65,000 feet, and a total endurance of 36-plus hours.[95] It can taxi, take off, fly to locations more than 3,000 miles away from its base, transmit ISR data back to field commanders over satellite links for up to 24 hours, and then return to base and land—all without intervention by ground-based operators. It can not only fly higher and longer than the Predator, but can also carry a much heavier sensor payload (2,000 versus 450-800 lbs.) Flying at its maximum altitude, the Global Hawk's sensors can cover 3,500 square miles of terrain per hour at resolutions between one and three feet.

The US military rushed two newly developed Global Hawk UAVs to Afghanistan to provide wide-area, persistent surveillance. One carried an EO, IR, and electronic intelligence (ELINT) sensor suite, while the other had a multi-mode SAR system with a MTI capability similar to manned JSTARS aircraft, enabling it to detect, classify, and track moving enemy ground vehicles over a wide area. Global Hawks flew scores of flights, including several in direct support of ongoing

---

[92] Adam Hebert, "New Horizons for Combat UAVs," *Air Force Magazine*, December 2003.

[93] Sweetman, "In the Tracks of the Predator," p. 50.

[94] Nick Cook, "Going Solo?," *Jane's Defence Weekly*, November 19, 2003, p. 22.

[95] Northrop Grumman, "RQ-4A Global Hawk," Fact Sheet. See also: Aeronautical Systems Center, "Global Hawk," U.S. Air Force Fact Sheet. Available on-line at http://www.af.mil/news/factsheets/global.html.

combat operations.[96] One also broke the record for the longest continuous ISR mission by staying aloft for over 26 hours.

During Operation Iraqi Freedom, a single Global Hawk UAV equipped with an integrated sensor suite (i.e., high-resolution EO, SAR/MTI, and IR) captured over 3,600 images and helped to locate and identify more than 300 Iraqi tanks, 50 SAM launchers, 70 SAM transporters, and 300 SAM canisters.[97] By collecting the 24-hour, real-time, all-weather, high resolution imagery needed to identify Iraqi ground vehicles and conduct quick-turn-around BDA, the Global Hawk was indispensable to the precision air campaign against Republican Guard divisions defending Baghdad. Throughout the war, the Global Hawk was also used to provide "last look" assessments to verify that the planned designated mean points of impact (DMPIs) were still up-to-date immediately before in-bound bombers dropped their large payloads of PGMs.[98]

The Emergence of First-Generation Unmanned Combat Air Vehicles

The US military's first built-for-purpose UCAVs, called the X-45A and X-47A, are currently under development by Boeing and Northrop Grumman, respectively.[99] The stealthy, flying-wing X-45A completed

---

[96] Rebecca Grant, "Eyes Wide Open," *Air Force Magazine*, November 2003, p. 41.

[97] Ibid., p. 38.

[98] A designated or desired mean point of impact is the precise, targeting aimpoint assigned as the center for impact of multiple weapons or area munitions to achieve the intended objective and level of destruction. It may be defined descriptively, by grid reference, or by geolocation. Ibid, p. 42.

[99] For additional information on the J-UCAS program see: http://www.darpa.mil/j-ucas/fact_sheet.htm. There are several other armed UAV programs underway including, for example, the development of strike variants of the Fire Scout and Hunter UAVs. DARPA has also recently launched a new program to develop a rotary-wing, armed UAV, called the Unmanned Combat Armed Rotorcraft (UCAR), for the Army. This discussion focuses on the X-45 and X-47 because, in terms of development, they are the most mature, built-for-purpose UCAVs. For additional information on other UCAV efforts, see: Sweetman, "In the Tracks of the Predator," pp. 51-55; and

its first test flight in May 2002 and successfully hit a ground target with an inert, GPS-guided SDB in April 2004. Two X-45A vehicles flew in coordinated flight under the control of single operator in August 2004, demonstrating their ability to maneuver autonomously and hold their position relative to each other. The first six "operational" vehicles, X-45Cs, are slated to be delivered to the Air Force for evaluation in 2007.[100] The X-45 program has been focused mainly upon performing the suppression of enemy air defenses (SEAD) mission because it was "the hardest mission envisioned for a UCAV outside of air-to-air fighter combat" and would implicitly demonstrate the UCAV's capability to conduct many other ground-attack missions.[101] The Air Force is also interested in using the X-45 as an electronic warfare platform.

The X-47A was originally intended as a carrier-based UCAV and designed to perform persistent surveillance and reconnaissance and deep-strike missions for the fleet. It completed its first flight test at the Naval Air Warfare Center in China Lake, California on February 23, 2003. The operational version, the X-47B, is expected to have a radius of over 1,700 miles, an endurance of 12 hours, and a payload capacity of 5,500 lbs.[102]

To enhance coordination, the X-45 and X-47 programs were merged in October 2003 into a joint development program, managed by DARPA, called Joint-Unmanned Combat Air System (J-UCAS). The

---

Robert Wall, "The Latest Leap," *Aviation Week & Space Technology*, September 6, 2004, pp. 46-49.

[100] First flight of the X-45C is expected to occur in 2006. Jefferson Morris, "First Guided Weapon Drop from X-45A Expected in Two Weeks," *Aerospace Daily & Defense Report*, April 12, 2004; and Robert Wall and David Fulghum, "Stage Setting," *Aviation Week & Space Technology*, April 26, 2004, p. 32.

[101] Statement by UCAV Program Manager, Colonel Michael Leahy at a CSBA workshop, October 1, 2001. See also Stanley Kandebo, "SEAD, Other Ground Attack Capabilities Planned for UCAVs," *Aviation Week & Space Technology*, October 2, 2000, p. 69.

[102] Office of the Secretary of Defense, *Unmanned Aerial Vehicle Road Map 2002-2027* (Washington, DC: DoD, December 2002), p. 12; David Fulghum, "First Flight for Pegasus," *Aviation Week & Space Technology*, March 3, 2003, p. 34.

program objectives are for the air vehicles to have an operational radius of 1,300 nautical miles (or 1,000 nautical miles with at least two hours of loiter time) while carrying a 4,500-pound payload, as well as the ability to operate at an altitude of at least 40,000 feet and cruise at Mach .85.[103] Unlike the manned F/A-22 and F-35, which both have a "bow-tie" signature with radar return spikes from either side of the aircraft, J-UCAS vehicles will have all-aspect stealth. They will also be equipped with an extensive sensor suite, including a multi-function SAR, an EO/IR sensor, and electronic-support measures. In addition to meeting the core Service-mandated requirements of SEAD and persistent surveillance and reconnaissance, J-UCAS vehicles could eventually take on myriad other missions including hunting for missile TELs and other time-critical targets, jamming an adversary's communication links, conducting electronic strikes with radio-frequency (RF) weapons, and dropping a wide-range of PGMs on fixed and mobile targets in denied areas.[104]

The impressive performance of the Predator and Global Hawk over the last decade, as well the current flight testing of the first built-for-purpose UCAV, likely foreshadows the rise of other unmanned aircraft over the coming decades. As will be discussed in Chapter IV, stealthy, extremely long-endurance UAVs that can penetrate into denied areas and orbit for weeks, if not months at a time, are on the horizon, as are micro-air vehicles (MAVs) that could be issued to individual soldiers for "over-the-next-hill" tactical reconnaissance. As an indicator of what the future might hold with respect to MAVs, during Operation Iraqi Freedom, US forces took advantage of several different kinds of "small" UAVs to meet their local-area ISR requirements. The First Marine Division, for instance, operated 20 Dragon Eye UAVs, which weigh five pounds and have a wingspan of

---

[103] Tom Goldman (Director, Boeing, J-UCAS Business Development), "Joint Unmanned Combat Air System—Overview and Update," Briefing at CSBA, August 2003; and Robert Wall, "Head-to-Head," *Aviation Week & Space Technology*, February 23, 2004, p. 37.

[104] Office of the Secretary of Defense, *Unmanned Aerial Vehicle Road Map 2002-2027*, p. 11; David Fulghum, "UCAV Spending Spikes in Pentagon Budget Plans," *Aviation Week & Space Technology*, February 17 2003, and Elaine Grossman, "Air Force Mulls Mission Control Issues for Unmanned Combat Aircraft," *Inside the Pentagon*, April 26, 2001, p. 3.

only 45-inches.[105] The "Silver Fox" UAV, which is about five feet long, is currently being used by Marines in Iraq to help pinpoint guerrilla fighters and other potential threats.[106] Similarly, Special Forces operating in Iraq and Afghanistan are using dozens of Battlefield Air Targeting (BAT) mini-UAVs and Pointer UAVs for local-area ISR, as well as to facilitate targeting.[107]

The Emergence of UUVs, UGVs, and USVs

Early prototypes of UUVs and UGVs are also emerging from the laboratory. During Operation Enduring Freedom, for example, five prototype UGVs developed under DARPA's Tactical Mobile Robotics Program were employed operationally. Referred to as "PackBots" because they are small enough to fit inside a soldier's rucksack, these remotely controlled UGVs are very rugged, weigh about 40 pounds, and cost about $40,000 each. Equipped with various sensor packages, they were used to reconnoiter 26 caves, four bunkers, and a building complex for booby traps and hidden Al Qaeda fighters in advance of human troops.[108] Larger UGVs that are currently under development include the 2.5 ton Multifunction Logistics and Equipment (MULE) vehicle, which is designed to shuttle supplies to troops on the field and evacuate wounded personnel, and the 5-ton Armed Robotic Vehicle (ARV), which will be equipped with a gun turret. Both the MULE and ARV are intended to be semi-autonomous, meaning they will require some measure of human oversight. While MULE vehicles, for example, will be unable to navigate independently over complex terrain, they

---

[105] Marine Corps Warfighting Laboratory, "Dragon Eye" Fact Sheet, July 2003.

[106] Dan Moniz, "5-Foot-Long Plane to Run Recon Missions for Marines," *USA Today*, April 26, 2004, p. 8.

[107] Andy Savoie, "UAVs Playing Key Role in Terror War, General Says," *Aerospace Daily & Defense Report*, September 15, 2004; and Mark Hewish, "Folding Micro Air Vehicle Expands the Gaze of Special Forces," *Jane's International Defense Review*, January 2004, p. 17.

[108] The PackBots can also be armed with a grenade launcher and/or a 12-gauge shotgun. See Mark Hewish, "Technology Transformation for Armored Warfare," *Jane's International Defense Review*, April 2003, p. 42; David Buchbinder, "In Afghanistan, A New Robosoldier Goes to War," *Christian Science Monitor*, July 31, 2002, p. 1; and "Robots Go Into Combat," *Army Times*, August 12, 2002, p. 4.

could form a logistics trains behind a single manned vehicle blazing the trail between a rear-area supply depot and forces in the field.

The Navy is experimenting with several classes of UUVs. At present, however, their utility is constrained by the fact that most of them still need to be supervised closely by human operators, have limited range, and have an endurance of, at best, about 24-48 hours.[109] Most UUV development programs currently underway are focused narrowly on mine reconnaissance and mapping.[110] Over the next few years, however, the Navy plans to demonstrate UUVs that can transit autonomously nearly 200 kilometers to a specified operating area and then spend at least 100 hours on station performing a variety of reconnaissance missions. It plans to demonstrate cooperative undersea search and survey operations with multiple UUVs, each able to map a swath of the sea floor nearly 400 meters wide and up to 100 kilometers long.[111] The Navy is also in the early stage of developing a nearly autonomous, mission-reconfigurable UUV that can be outfitted with different "plug-and-play" modules for conducting the following missions: maritime reconnaissance, undersea search and survey (including minehunting and neutralization), communication and navigation support, and submarine track and trail.[112] Over the next decade, UUVs will likely become more autonomous and possess longer endurance. They may also take on additional missions including anti-surface warfare (ASuW), land attack, and logistic supply and support to special forces.

---

[109] Mark Hewish, "Robots from the Deep," *Jane's International Defense Review*, May 2001, pp. 46-53.

[110] The most prominent example of the latter is the Long-Term Mine Reconnaissance System (LMRS). It can operate in up to 460 meters of water and has an endurance of 40-62 hours. See Mark Hewish and Joris Janssen Lok, "Silent Sentinals Patrol the Depths," *Jane's International Defense Review*, April 2003, p. 53.

[111] Hewish, "Robots from the Deep," pp. 46-53.

[112] Richard Scott, "Unmanned, Undersea," *Jane's Defence Weekly*, June 12, 2002, p. 31; and Hunter Keeter, "Navy UUV Acquisition Focuses on Synergy with other Unmanned Systems," *Defense Daily*, July 16, 2002.

The Navy is also exploring the potential of USVs for a diverse array of missions, including minehunting, littoral ISR, ASW, ASuW, and fleet force protection. The largest development project to date has been the Remote Minehunting System (RMS), which uses a semi-autonomous, diesel-powered USV with a side-scanning sonar system in tow to search for mines. Originally developed to provide an organic, "in-stride" mine reconnaissance capability for Arleigh Burke-class destroyers, RMS vehicles will likely be deployed instead on Littoral Combat Ships.[113]

During the 1990s, the Navy experimented with another USV prototype, referred to as Sea Owl Mk II, equipped with starlight, daylight, and infrared cameras, a side-scanning sonar system, and a GPS-based navigation system and commercial autopilot. In a series of sea trials, the Sea Owl demonstrated the capability to perform mine hunting, water-side security, port and harbor surveillance, and maritime interception operations.[114] In parallel with these experiments, the Spartan Scout Advanced Concept Technology Demonstration (ACTD) was launched in 1992 to demonstrate a militarily useful system of USVs for force protection against asymmetric threats (e.g., small boats), networked ISR, precision engagement, and mine warfare. The Spartan Scout USV program uses commercial-off-the-shelf (COTS), rigid-hull inflatable boats (7-meter and 11-meter) outfitted with various mission modules and a "core system," which includes a remote controlled/semi-autonomous command decision system, a basic ISR suite (i.e., navigational radar and a video/infrared camera), a GPS-based navigation system, and a communication suite. Mission modules that have been designed and tested so far have included a side-scanning sonar system for minehunting; an EO/IR surveillance turret, surface search radar, and a stabilized .50-caliber Bushmaster gun for the ISR and force protection mission; and the same module equipped with a stabilized Javelin missile system instead of the Bushmaster for the precision-engagement mission. A fourth module dedicated to ASW is under development. The Spartan Scout ACTD is scheduled to culminate next

[113] Richard Scott, "Nobody at the Helm," *Jane's Defence Weekly*, August 4, 2004, p. 27.

[114] Ibid.

year with a multi-mission demonstration during which several of the "plug and play" modules will be swapped out at sea.[115]

Tactical / Operational Exploitation of Space

Another aspect of the early phase of the RMA is the evolution in the exploitation of space from pre-crisis intelligence gathering and strategic warning to direct force enhancement at the operational and tactical levels of war. As Barry Watts notes:

> The 1990s were a period of transformation in *how* the American military uses space systems to support terrestrial military operations. Whereas U.S. space efforts had concentrated on the *pre-conflict* aspects of central nuclear war and the military competition in Central Europe during 1957-1991, over the last decade, the U.S. military has sought to redirect its space efforts toward the real-time enhancement of ongoing, nonnuclear operations within the earth's atmosphere.[116]

When the first Navstar (Block I) satellite was lofted into orbit on February 22, 1978, GPS was intended primarily as a navigational aid for ships at sea. More than two decades later, GPS is integral to US military operations across all dimensions of the battlespace. The signals transmitted from GPS satellites are not only used to help US forces navigate on land, at sea, and in the air, but also to guide weapons precisely to terrestrial targets, to track friendly forces to avoid "friendly fire" losses, and to facilitate a wide array of other tactical missions.

During Operation Iraqi Freedom, for example, six different kinds of GPS-guided weapons (i.e., TLAM, CALCM, JSOW, JDAM, EGBU-

---

[115] Ibid, pp. 28-29.

[116] Barry D. Watts, *The Military Use of Space: A Diagnostic Assessment* (Washington, DC: CSBA, 2001), p. i.

27, and EGBU-37) were used to attack Iraqi targets. In total, more than 12,000 GPS-guided JDAMs were dropped by US aircraft during Operation Enduring Freedom and Operation Iraqi Freedom. Individual combat controllers on the ground used GPS receivers linked to laser range-finders to determine the precise coordinates of enemy targets, which were in turn relayed to loitering strike aircraft armed with GPS-aided weapons.

Both in Afghanistan and Iraq, US ground forces were equipped with GPS-enabled "blue force tracking" devices, including the Force XXI Battle Command Brigade and Below (FBCB2) system (discussed later as an Army networking initiative) and the Grenadier Beyond Line of Sight Reporting and Targeting (BRAT) system. The latter comprises a handheld GPS receiver linked to a compact, two-pound satellite transponder. Every few minutes, the system transmits the user's GPS coordinates over a secure, difficult-to-detect satellite link and the data is fused and processed at a centralized ground station. The composite data is then sent to field commanders over military UHF satellites. As of April 2003, some 1,500 Grenadier BRAT units had been deployed.[117] Commanders on the ground in Iraq assert that the increased situational awareness made possible by space-enabled blue force tracking systems dramatically reduced the time needed to identify routes through contested areas, minimized friendly fire casualties, especially during poor weather conditions (e.g., sandstorms), and greatly facilitated precision air drops of supplies and equipment to widely dispersed forces.[118]

GPS-derived precision location information also facilitates the execution of myriad combat tasks such as aerial refueling, all-weather air drops, mine laying and clearing, and combat search and rescue. The precise timing signal provided by GPS is used to synchronize

---

[117] Future versions of the Grenadier BRAT system will also be able to process and uplink the precise coordinates of enemy targets pinpointed with integrated laser range finders. Jeremy Singer, "Satellite-Based System Will Make U.S. Troops Safer," *Space News*, April 28, 2003, p. 11.

[118] Jeremy Singer, "DoD to Expand Satellite-Based System Used in Iraq, Afghanistan," *Space News*, July 28, 2003, p. 14; and William B. Scott, "Milspace Technology Coups," *Aviation Week & Space Technology*, January 19, 2004, p. 47.

communications networks (e.g., frequency hopping radios) and cryptological systems.

The current generation of electro-optical imaging satellites can downlink data to ground stations nearly instantaneously, which can then be rapidly processed and enhanced by modern computer systems. SAR satellites regularly provide all-weather, day and night imagery of hot spots around the world.[119] Currently, the information gleaned from some satellites can be exploited in the field almost immediately for mission planning, precision targeting and BDA. Satellite-derived targeting data can, in some cases, be processed and disseminated to US strike assets in a matter of minutes. Civilian and military communication satellites have become indispensable for moving tactical and operational information around the battlefield quickly, reliably, and securely. Between the first and second Gulf Wars, the US military's consumption of satellite bandwidth increased by more than an order of magnitude.

This trend toward increased reliance on space for operational and tactical purposes is certain to continue. For example, the lower-tier of the space-based infrared system (SBIRS), which is currently scheduled for deployment toward the close of the decade, will be tightly integrated with US theater and national missile defense systems.[120] The SBIRS-Low constellation of some 20-30 satellites

---

[119] Currently, the United States has at least two "Lacrosse" SAR satellites in orbit. They are believed to provide imagery with a resolution of between 61 centimeters and three meters.

[120] The SBIRS architecture is divided into two components: high and low. The high portion is essentially a replacement of the Defense Support Program (DSP) satellites designed to detect the launch plume of ballistic missiles. It will comprise four early warning satellites in geosynchronous orbit (GEO) and two satellites in highly elliptical orbits (HEO) that will provide global detection of missile and space launches. The goal is for the SBIRS-Low component, which was officially renamed the "Space Tracking and Surveillance System" in 2002, to have a limited operational capability in 2010 as part of a missile defense "testbed." First launch is slated for 2006. Given the development delays and cost overruns that the overall SBIRS program has encountered over the past several years, however, it appears unlikely that the restructured SBIRS-Low program will meet this timeline. See Amy Butler, "Lord: $1.5 Billion Overrun Estimate for SBIRS High is Solid," *Defense Daily*, June 25, 2004, p. 7; Amy

positioned in LEO, each equipped with sensitive mid- and long-wave infrared sensors, is intended to be used primarily to detect and track ballistic missile warheads in the mid-course portion of their flight. In theory, ground-based missile defense radars will use this cueing information to acquire the missiles and warheads traveling through space and guide interceptors to them. Aside from cueing missile defense systems, SBIRS-Low could be used to detect and track high-flying aircraft against the cold background of space, and with some modifications, it could also be used both for terrestrial surveillance and for tracking objects in space.

The United States is also moving forward with the development of a networked constellation of space-based radar (SBR) satellites designed to provide near-continuous, day-night, all-weather imagery, as well as to find, identify, and track ground vehicles (e.g., tanks, trucks, and missile launchers) over expansive geographic areas throughout the world.[121] The satellites will be equipped with a multifunction SAR with MTI, high-resolution imaging (both strip and spot), and high-resolution terrain mapping capabilities. From the vantage of low- or medium-Earth orbit, these satellites could peer directly down on areas of interest and would be much less affected by terrain features (e.g., mountains) and other obstructions that may block the view of lower flying surveillance aircraft. By virtue of being able to look at the same target from different angles simultaneously, a multiple-satellite SAR constellation could make target identification

---

Butler, "Space PEO: SBIRS High GEO Segment Falls One Year Behind," *Defense Daily*, April 1, 2004, p. 1; Richard Newman, "Space Watch, High and Low," *Air Force Magazine*, July 2001, pp. 35-38; and Amy Butler and Thomas Duffy, "MDA to Unveil SBIRS Low Restructure, Name TRW Prime Contractor," *Inside Missile Defense*, April 17, 2002, p. 1.

[121] Space Based Radar Joint Program Office, "Request for Proposals—Statement of Objectives," January 16, 2004, p. 1. The size of the constellation will depend upon whether the satellites are placed in LEO, MEO, or both. At the low-end of the range, the constellation might comprise ten satellites in MEO, and at the high-end, 36 satellites in LEO. Most of the constellation configurations currently under consideration are reportedly in the 20-25 satellite range. Satellite ground coverage near the poles would be thin or absent. John Tirpak, "The Space-Based Rader Plan," *Air Force Magazine*, August 2002, pp. 62-66. For additional details on the SPR program, refer to the following webpage: http://www.globalsecurity.org/space/system/sbr.htm.

easier and more reliable. Most importantly, it would also be "access-insensitive" in that overflight rights from adjacent states would not be necessary and robust, networked enemy air defenses would not pose a threat.[122] As currently envisioned, the SBR constellation could be directly tasked by the warfighter in the field, and the collected data directly downlinked to the theater for immediate processing and exploitation. Under some circumstances, SBR data might be piped directly into aircraft cockpits, tactical ground vehicles, and ships at sea.[123] The mean response time for typical GMTI taskings or high-resolution SAR imaging requests would likely range from a matter of seconds to a few minutes.[124] Although the first SBR satellite was scheduled to be launched by 2012, owing to recent funding cuts by Congress, it will likely be delayed until the 2015-2017 timeframe. As a result, it is doubtful that a full operational capability will be reached before 2020.[125]

At present, no other countries can match the United States in terms of using space for operational and tactical purposes. As discussed later in this chapter, however, foreign militaries may catch up considerably over the next decade owing to the diffusion of key technologies and commercialization trends. Competitors may also seek to "level the playing field" in space by developing the means to disrupt, damage, or destroy satellites relied upon by the US military.

---

[122] However, as will be discussed in more depth in Chapter III, states could opt to field various types of anti-satellite (ASAT) weapons with which to target a future American SBR constellation. The desire to reduce that threat is apparently one of the reasons why the US military may opt for a MEO constellation, which would place the high-value satellites out of the range of many first-generation ASATs.

[123] Tirpak, "The Space-Based Rader Plan," p. 65.

[124] This is based upon a 24-satellite constellation. See the entry for "Discoverer II" on the Federation of American Scientists' Website at http://www.fas.org/spp/military/program/imint/starlight.html.

[125] Space Based Radar Joint Program Office, "Request for Proposals—Statement of Objectives," January 16, 2004, p. 1; Amy Butler, "Teets Wants Space Based Radar Restructure Options by December," *Defense Daily*, September 16, 2004, p. 1.

Early Network-Based Warfare and Joint-Force Integration

Over the last decade, the US military has significantly enhanced its C3 capabilities at the strategic, operational, and tactical levels of war through the application of modern networking technologies. Those same technologies, combined with new operational and organizational concepts, have also fostered increased integration between the Services.

Defense-Wide and Service Networking Initiatives

Like commercial businesses, the US military has taken advantage of Internet-related technologies to address its C3 needs. The Defense Information Infrastructure (DII) system, which is the US military's information backbone, comprises both the Secret Internet Protocol Router Network (SIPRNET) and the Non-classified Internet Protocol Router Network (NIPRNET).[126] These networks support several critical defense-wide C3 systems such as the Defense Message System, Global Command and Control System (GCCS), Global Combat Support System, and Theater Battle Management Core System.[127] In comparison to their predecessors, these C3 systems offer a number of benefits, including extended geographic reach, enhanced flexibility, increased throughput, greater robustness, and above all, better responsiveness.

DoD is also in the process of dramatically expanding the size of the data "pipes" linking the ever-increasing number of nodes within what is now termed the "Global Information Grid" or "GIG."[128] In the

[126] As their names suggest, both the SIPRNET and NIPRNET use the same network routing protocols, hardware, and software as the civilian Internet. Unlike the Internet, however, all data traffic is encrypted on the SIPRNET and all users must be vouchsafed onto the network. See Major General James Bryan, Commander Joint Task Forces – Computer Network Operations, *Statement before the House Armed Services Committee*, May 17, 2001, p. 3.

[127] George Seffers, "Fit to Fight the Info War," *Federal Computer Week*, March 12, 2001, n.p.

[128] The GIG is officially defined as "a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting,

decade between Operation Desert Storm and Operation Iraqi Freedom, available bandwidth at major forward operations centers grew by a factor of more than 40.[129] Plans are in place to increase the bandwidth accessible at more than 90 critical military and intelligence centers worldwide by an additional two orders of magnitude, to at least ten gigabytes per second.[130] DoD also intends to develop and begin fielding new military COMSATs that will use lasers to transmit data quickly to and from terrestrial nodes, as well as between the satellites themselves. These "Transformational Communications Satellites (TSATs)" will be critical for providing wideband connectivity to mobile users (e.g., airborne C4ISR-related platforms, ships at sea, and ground maneuver units), as well as to fixed nodes located in remote areas where fiber optic lines are unavailable.[131]

The Army has incorporated the FBCB2 system into thousands of combat vehicles (e.g., tanks, infantry fighting vehicles, Apache

---

processing, storing, disseminating, and managing information on demand to the warfighters, policy makers, and support personnel." John P. Stenbit, Assistant Secretary of Defense for Networks and Information Integration, *Statement before the U.S. House Armed Services' Subcommittee on Terrorism, Unconventional Threats and Capabilities*, February 11, 2004, p. 2.

[129] Brigadier General Robert W. Cone, "Briefing on Joint Lessons Learned from Operation Iraqi Freedom," October 2, 2003; and Admiral Edmund Giambastiani (Commander, US Joint Forces Command), *Statement before the House Armed Services Committee*, October 2, 2003.

[130] This is often referred to as the GIG Bandwidth Expansion project. The expansion will be accomplished primarily through increased exploitation of terrestrial, high-capacity, fiber-optic lines and commercially available high-speed switching technologies. John P. Stenbit, Department of Defense Chief Information Officer, *Statement before the U.S. House Armed Services' Subcommittee on Terrorism, Unconventional Threats and Capabilities*, April 3, 2003. See also: Anne Plummer, "U.S. Troops in Persian Gulf Armed with Hefty Bandwidth Upgrades," *Inside the Pentagon*, March 13, 2003, p. 2; and Gail Kaufman and Gopal Ratnam, "U.S. Military Sets Plans for Giant Network," *Defense News*, April 14, 2003.

[131] Contingent upon the outcome of a critical design review of the TSAT constellation in 2008, the launch of the first satellite is currently scheduled for 2011. See Robert Wall, "Fast Connection," *Aviation Week & Space Technology*, December 22, 2003, p. 40.

Longbow attack helicopters, and High Mobility Multipurpose Wheeled Vehicle System).[132] It allows individual vehicles on the network to exchange voice, video, or other data securely, and to gain access to terrain maps, logistics information, and most importantly, a shared situational awareness display indicating the location of friendly and enemy units.[133] Prototype FBCB2 components were evaluated under combat conditions in the Balkans, in Afghanistan, and most recently, in Iraq.[134] Assuming that no major problems surface during testing, the Army plans to install some 60,000 FBCB2 systems into all types of combat vehicles over the next two decades. It also intends to field a

---

[132] As its name indicates, the FBCB2 system is integrated primarily into vehicles at the brigade echelon and below. For theater-wide C3 purposes, however, elements of the FBCB2 system are available at the division and corps level.

[133] The 4th Mechanized Infantry Division was the first Army unit to be equipped with the FBCB2 system and has been experimenting with various pre-production models for several years. Plans are now in place to expand the FBCB2 network to include major theater-wide C4ISR assets (e.g., JSTARS), as well as to beam a modified version of the common operational picture directly into aircraft cockpits. To reduce the current latency in the system, which runs from one to five minutes, as well as to reduce demand for satellite bandwidth, future versions of the FBCB2 system may leverage Link-16 technology, which has a latency measured in milliseconds, and use high-altitude, long-endurance UAVs as airborne communication nodes. George Cahlink, "Better 'Blue Force' Tracking," *Air Force Magazine*, June 2004, pp. 68-69; Rich Tuttle, "Beyond BFT," *Aviation Week & Space Technology*, February 23, 2004, p. 84; Elaine Grossman, "Air Force May Expand on Army Tracking Tool," *Defense Information and Electronics Report*, November 7, 2003, p. 1; and Kim Burger, "U.S. Army Shares Radios to Avoid Gulf Fratricide," *Jane's Defence Weekly*, March 12, 2003, p. 3.

[134] During Operation Iraq Freedom, over 1,200 satellite-linked FBCB2 systems were used by Army units outside the 4th Infantry Division, as well as selected USMC and British units, primarily for "blue force tracking" purposes. Only the 4th Infantry Division, however, was equipped with the software and hardware necessary to support the wireless tactical internet feature of the FBCB2 system. The FBCB2 system was widely credited with reducing coalition friendly fire deaths during combat operations in Iraq. George Cahlink, "Better 'Blue Force' Tracking," *Air Force Magazine*, June 2004, pp. 66-68; and Anne Plummer, "DoD Attempts to Tackle Fratricide Problem That's Lingered Since 1991," *Inside the Army*, March 22, 2004, p. 1.

next-generation wireless tactical internet called the "Warfighter Information Network–Tactical (WIN–T)" that will enable smaller maneuver units and command elements to exchange voice, video and data while on the move.[135]

In the early 1990s, the Navy launched a broad networking initiative called "Copernicus" that sought to make command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems more responsive to the needs of the warfighter.[136] The Copernicus concept was expanded and promulgated under a new moniker, "network-centric warfare" in 1997, and repackaged again in 2002 as "ForceNet," which is defined as:

> ...the operational construct and architectural framework for naval warfare in the information age that integrates warriors, sensors, networks, command and control, platforms, and weapons into a

---

[135] Full-scale development of WIN-T was approved by the Defense Acquisition Board in July 2003. As a positive indicator of WIN–T's technical feasibility, DARPA has already developed and tested a Small Unit Operations Situation Awareness System (SUOSAS) network comprising several local area networks (LANs) that could automatically form and "self heal" in very difficult communication environments (e.g., urban terrain, inside buildings, within forests and dense jungle). The prototype SUOSAS system is being miniaturized and made more robust under the Soldier Level Individual Communications Environment (SLICE) program. Over 100 hockey puck-sized SLICE "pods" are slated to be produced for field trials over the next two years. See Frank Tiboni, "Board Approves U.S. Army's WIN-T Program," *DefenseNews.com*; Rupert Pengelley, "The Military Goes Broadband," *Jane's Defence Weekly*, September 4, 2002, pp. 27-34; and Rupert Pengelley, "Future Tactical Comms: Redefining the Box," *Jane's International Defense Review*, May 2003, pp. 29-39.

[136] Copernicus called for the development of multiple, interconnected networks that would provide warfighters with a common tactical picture of the battlespace; support flexible, robust connectivity between nodes throughout the network; and enable reliable, timely sensor-to-shooter linkages. See US Navy, "Copernicus Forward...C4I for the 21st Century," http://chininfo.navy.mil/navpalib/policy/coperfwd.txt, June 1995. See also: Edward Walsh, "The Copernican Revolution," *Armed Force Journal International*, July 1995, pp. 40-42.

> networked, distributed combat force that is scalable across all levels of conflict from seabed to space and sea to land.[137]

Although the full realization of this very ambitious goal is probably several decades away, the Navy has made incremental progress in this direction with its ongoing Cooperative Engagement Capability (CEC), Joint Fires Network, Information Technology-21 (IT-21), and the Navy-Marine Corps Intranet (NMCI) initiatives.[138]

---

[137] Like Copernicus, the basic thrust of the network-centric warfare (NCW) concept was to link Navy ships, aircraft and shore installations into highly integrated networks. See Ronald O'Rourke, "Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress," *CRS Report for Congress*, (Washington, DC: Congressional Research Service (CRS), January 12, 2001); and Vice Admiral Richard W. Mayo (Commander, Naval Network Warfare Command) and Vice Admiral John Nathman (Deputy Chief of Naval Operations for Warfare Requirements and Programs), "ForceNet: Turning Information into Power," *Proceedings*, U.S. Naval Institute Sea Power 21 Series – Part V, February 2003.

[138] The goal of the CEC effort, which has been underway for about 15 years, is to link US Navy ships and aircraft operating in a particular geographic area into a single, integrated air-defense network in which radar data collected by each platform is transmitted simultaneously to all the other units in the network. With each unit in the network fusing its own radar data with the raw data received from other elements in the network, they can all, in theory, independently generate a common, composite, real-time, air-defense picture. The Navy has also started to develop an offensive analogue to CEC, called the "Joint Fires Network," which would integrate ISR information from disparate sensors within the network; identify, track, and prioritize targets; and then select the best available weapon within the network for striking each target in the queue. The goal of the NMCI program is to field a secure intranet linking more than 300,000 computer stations across 300 Navy and Marine Corps shore installations worldwide. See Ronald O'Rourke, "Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress," pp. 2-4. See also Jason Sherman, "U.S. Navy Shifts Course on CEC," *Defense News*, September 1, 2003, p. 1; Michael Sirak, "U.S. Navy Studies Upgrade Options for CEC System," *Jane's Defence Weekly*, November 13, 2002; Mike McCarthy, "Navy Puts Priority on Networks over Weapons," *Defense Week*, April 16, 2001, p. 8; Archie Clemens, "Standby for Big Reform – A Navy-Marine Corps Intranet," *Navy Times*, March 6, 2000, p. 58; and Joseph Cipriano, "Reinventing

As part of its Sea Dragon wargaming program, the Marine Corps explored the idea of networking relatively small, mobile units with external ISR platforms and fire support systems. It is currently fielding the Data Automated Communications Terminal (DACT) to network maneuver units together, as well as to link up with the national-level GCCS network.[139] In conjunction with the Navy, the Marine Corps has also supported an ACTD called "Extending the Littoral Battlespace," which could enable future expeditionary naval forces to establish rapidly a wide-area, wireless, digital network in littoral operating areas that extends from national- and theater-level assets all the way down to dispersed squads on the move.[140]

The Air Force has focused its networking initiatives on establishing long-distance, high- bandwidth, sensor-to-shooter linkages. By upgrading and expanding the Defense Satellite Communication System and investing in new line-of-sight datalinks, it

---

Maritime Power: The Navy-Marine Corps Intranet," *U.S. Naval Institute Proceedings*, September 2000, pp. 72-74.

[139] The Marine Corps is also developing a rugged, inexpensive personnel identification and location system for urban operations that uses ultra-wideband links and ad-hoc networking technology to determine and report the grid coordinates and elevation within buildings of individual Marines with an accuracy of five centimeters. It can also transmit other useful data such as biometric information, vital signs, and weapons status at a rate of 1,000 bits per second. While the current prototype system is about the size of pager and weighs approximately 130 grams, the next-generation device under development is expected to be the size of a quarter, cost about $10, have a higher data transfer rate (32 kilobits per second), draw less power, and provide positional accuracy of three centimeters out to a maximum distance of 100 meters. Mark Hewish, "USMC to Test UWB Personnel Identification/Location System," *Jane's International Defense Review*, July 2004, p. 24.

[140] The core of this system is referred to as the Wide-Area Relay Network (WARNET). A small-scale version of WARNET was field tested in June 2001. If fielded, the enhanced connectivity provided by a WARNET-like system could allow a common tactical picture of the battlespace—including the geo-location of both friendly and detected enemy forces—to be compiled and shared across the force. Ray Cole, "Networking the Battlespace–DoD Technology Demonstration Extends C3I Connectivity Down to the Squad Level," *Armed Forces Journal*, July 2001, pp. 36-39.

has made major strides in networking airborne, space-based, sea-based, and ground-based communication nodes. During Operation Iraqi Freedom, for instance, Air Force personnel were able to "fly" Predator and Global Hawk UAVs over Iraq from US bases over 6,000 miles away by sending instructions over high-bandwidth, secure satellite datalinks.[141] The Air Force has also dramatically improved communications between aircraft, as well as between aircraft and ground units, using the Joint Tactical Information Distribution System (JTIDS).[142] In some instances, it is now possible to transmit multi-source ISR and targeting information directly into aircraft cockpits.[143] During Operation Allied Force, for example, live battlefield video collected by Predator UAVs was fed directly to modified AC-130 gunships.[144] In the years ahead, the Air Force plans to field a Multi-

---

[141] On at least one occasion, a Predator operator fired a Hellfire missile at a target on Iraqi soil from his command console in the United States. Richard Newman, "War From Afar," *Air Force Magazine*, August 2003, p. 60; and Eric Schmitt, "6,300 Miles from Iraq, Experts Guide Raids," *New York Times*, June 24, 2003.

[142] JTIDS uses the secure, jam-resistant Link-16 datalink system and a wide array of other networking and communications equipment. According to DoD, a multiyear assessment showed that by using JTIDS to network F-15 fighters with a supporting AWACS aircraft, enabling all of the aircraft to contribute to and share a composite tactical radar picture, the air-to-air combat power of the F-15s was increased by about 100 percent. Based on data collected from 10,000 sorties and more than 15,000 flight hours, networking increased kill ratios in daytime engagements by a factor of 2.62 (from 3.1:1 to 8.11:1) and, at night, by a factor of 2.6 (from 3.62:1 to 9.40:1). William Scott and David Hughes, "Nascent Net-Centric War Gains Pentagon Toehold," *Aviation Week & Space Technology*, January 27, 2003, p. 50.

[143] Last year, the Air Force completed a technology demonstration of a new datalink system that enables aircraft to both receive and send real-time text and video data over COMSATs. The demonstration was called the "Integrated Real-time information in cockpit/Real-time information out of the cockpit for Combat Aircraft (IRCA)" effort. See Michael Sirak, "USAF Demonstrates Real-Time Datalink," *Jane's Defence Weekly*, April 17, 2002, p. 7.

[144] Datalinks were also established between several different kinds of manned and unmanned reconnaissance aircraft. See Kim Burger and Andrew Koch, "Afghanistan: The Key Lessons," *Jane's Defence Weekly*, January 2, 2002, p. 23; James Dao, "Newer Technology is Shielding Pilots," *New York Times*, November 29, 2001; and Eric Schmitt and James Dao, "Use of Pinpoint

Sensor Command and Control Constellation (MC2C) that links ground stations, satellites, UAVs, manned ISR aircraft (including a new Multi-sensor Command and Control Aircraft), and strike aircraft into an integrated C4ISR network.[145] As part of this constellation, the Air Force is investigating the possibility of developing "smart tankers" that could serve as airborne routers of heterogeneous data streams while still conducting their primary aerial refueling mission.[146] It is also exploring networking applications for "collaborative targeting" in which different types of sensor systems would not only exchange data, but also actively cue each other regarding the location of potential targets.[147]

The Limits and Promise of Early Networking

The US military's investment in networking technologies over the last few decades has yielded significant dividends in terms of enhanced C4ISR and battle management capability. The ability of the US military to collect sensor data over a wide area, process it, and then relay targeting information to strike and maneuver platforms in a timely fashion has improved dramatically. Tasks that sometimes took days during the first Gulf War were accomplished within hours during Operation Iraqi Freedom. Precision air strikes against more than 150 "time sensitive targets" typically took only a few hours, or in a few

---

Airpower Comes of Age in New War," *New York Times*, December 24, 2001, p. 1.

[145] "Air Force Designing New Constellation of Sensors and Capabilities," *Aerospace Daily*, May 23, 2001, p. 1.

[146] Toward this end, DARPA is developing an airborne communications node that would act as a "switch in the sky," receiving data from numerous sources that use different datalink standards and then routing it rapidly to a wide range of platforms. A prototype airborne communications Link-16 relay, which is reportedly the first in family of "Scalable, Modular, Airborne Relay Terminals (SMART)," was tested aboard a KC-135 refueler in October 2002. See Major General Robert Behler, "Smart Tanker Demonstrated–Special Communications Pallet Provides Beyond-Line-of-Sight-Relay," *ISR Journal*, November 1, 2002, p. 8.

[147] David Fulghum, "It Takes a Network to Beat a Network," *Aviation Week and Space Technology*, November 11, 2002, pp. 28-31.

instances, less than an hour to plan and execute.[148] On April 7, 2003, for instance, US Central Command received "potential intelligence" from the Central Intelligence Agency that Saddam Hussein, his two sons, and other high-ranking Ba'ath party officials were meeting in a building adjacent to a popular restaurant in Baghdad's exclusive Mansur neighborhood.[149] Within just over one-half hour the precise location of the building was verified, the attack was authorized, and mensurated GPS coordinates were relayed to an airborne AWACS, which in turn passed them to an orbiting B-1B bomber. Twelve minutes later, the building and the bunker beneath it were obliterated with four, 2000-lb JDAMs.[150] Highlighting the criticality of timely, accurate intelligence, Saddam and the other Ba'ath party leadership targets either escaped just prior to the strike or the tip-off itself was flawed.

As another example of shortened "sensor-to-shooter" links, SAR, EO, and IR imagery of Republican Guard divisions collected by a single Global Hawk UAV operating alongside 15 U-2s and eight JSTARS aircraft was carried by satellite to the Combined Air Operations Center (CAOC) at Prince Sultan Air Base in Saudi Arabia, as well as to Beale Air Force Base in California. The raw data was rapidly processed at Beale (both to acquire new targets and to assess the damage from previous strikes), processed imagery was uplinked to the CAOC, and continually "refreshed" target coordinates were in turn relayed to inbound and loitering strike aircraft using both satellite and line-of-sight communication links.[151] This compression of the targeting cycle overwhelmed Iraqi Republican Guard units—regardless of

---

[148] Lieutenant General T. Michael Moseley, *Operation Iraqi Freedom – By the Numbers*, p. 9; Adam Hebert, "Operation Reachback," *Air Force Magazine*, April 2004, p. 58; and Tony Capaccio, "U.S. Launched More than 50 'Time Sensitive' Strikes in Iraq," Bloomberg.com, April 14, 2003.

[149] Bradley Graham, "'Let's Get the Job Done'," *Washington Post*, April 9, 2003, p. 28.

[150] David E. Sanger and Eric Schmitt, "CIA Tip Led to Strike on Baghdad Neighborhood," *New York Times*, April 8, 2003, p. 1; and Rowan Scarborough, "Saddam Seen at Site," *Washington Times*, April 9, 2003, p. 1.

[151] Nick Cook, "Going Solo?," *Jane's Defence Weekly*, November 19, 2003, p. 23.

whether they tried to maneuver or hunker down in revetments or bunkers, Iraqi ground vehicles were detected, tracked, and destroyed, even during a blinding desert sandstorm. The Services were also better able to coordinate widely dispersed units. For example, during an Army training exercise in 2001 in which the performance of two digitized brigades was evaluated, the commander of the opposing force (OPFOR) observed that, "It is evident that they communicated orders and concentrated fire power far more rapidly than non-digitized units over a greater battlefield area during challenging and continuous operations."[152]

While the US military's various networking initiatives to date are laudable, they represent only the initial stages of network-based warfare. The networks operated by the different Services are still largely "stovepiped" in that they are optimized for internal communications and, in many cases, employ disparate, incompatible datalink standards making lateral, inter-Service communications difficult.[153] Although considerable progress has been made in bridging the Services' various intranets (e.g., SOF combat controllers on the ground in Afghanistan communicating directly with both Air Force and Navy strike aircraft overhead), the US military is still a decade or more away from operating a single, seamless network in which all US force elements can easily pass data back and forth.[154] During Operation Iraqi Freedom, for example, US Army and Marine battalions operating on opposite banks of the Tigris River in Baghdad could not communicate with each other directly because they lacked the necessary encryption and frequency-hopping codes.[155] To avoid

[152] Anne Plummer, "Army Reports Digitized Forces Faring Well in Ft. Erwin Field Exercise," *Inside the Pentagon*, April 12, 2001, p. 15.

[153] See Anthony W. Faughn, "Interoperability: Is it Achievable?" Harvard University – Center for Information Policy Research, September 2001, pp. 7-13, 43-44.

[154] A recent memo from Deputy Secretary of Defense Paul Wolfowitz to the services reportedly sets a 2008 deadline for making all military command and communications systems interoperable. See Sandra Erwin, "Incompatible Battle-Command Systems: There's No Easy Fix," *National Defense*, September 2002, p. 15.

[155] David Zucchino, "Unfriendly Communications Process Raises Risk of 'Friendly Fire'," *Los Angeles Times*, April 13, 2003.

friendly fire incidents, they resorted to face-to-face command post meetings and physically swapped a handful of radios.

With a few notable exceptions (e.g., WIN-T and WARNET), the Services are also currently grafting networking technologies onto platforms that appear to be poorly suited for operating in an advanced RMA regime. To use a historical analogy, when the ARPAnet, later dubbed the Internet, was first created, it was used to network mainframes, which proved useful for swapping large data files between a handful of research facilities distributed throughout the United States. The Internet Revolution was not ignited, however, until digital packet networking technologies were used to link large numbers of desktop computers. At present, the Services are spending most of their resources networking "mainframes." The Navy's CEC and IT-21 efforts, for example, are centered on large, high-signature surface ships that may become increasingly vulnerable in future littoral waters. The Army's digitization effort is focused on plugging networking gear into high-signature, mechanized vehicles (e.g., Abrams main battle tanks and Bradley infantry fighting vehicles) that could face considerable anti-access challenges in the future.

The Services have also been reluctant to adopt flatter, more decentralized organizational structures to harness the power of networking. While there has been some tinkering at the margins, the basic organization of Army divisions, Navy carrier battlegroups, and Air Force squadrons has not changed appreciably since the dawn of the information age in the 1970s. The dawn of mature network-based warfare will be marked by the fielding of systems and the standing up of new organizations optimized for operating as a network. For instance, instead of fielding large, multipurpose platforms that contain many separate systems and subsystems, it could be advantageous to field smaller, single-purpose platforms that can be networked together in innumerable ways for various tasks. There are some signs that the Services may be slowly moving in this direction. As part of the ForceNet concept, for instance, the Navy is entertaining the idea of creating an "expeditionary sensor grid" that would consist of inter-connected networks of UAVs, UUVs, and hundreds of ground- and sea-based unattended sensors. The sensor grid would in turn be linked to a variety of different strike platforms. The Army's Future Combat Systems (FCS) concept envisions a network of comparatively light, distributed platforms (both manned and unmanned) to replace today's concentrated masses of heavy combat forces. Implicit to the FCS concept is the notion of dividing the combat power now aggregated

within large, multi-function platforms among several smaller platforms that can be networked together into an integrated system, which that can be easily reconfigured and optimized for different types of missions and quickly adapt to a dynamic battlefield.

Joint Force Integration

While there was considerable cooperation between the Services at the strategic and operational levels during Operation Desert Storm, the air, ground, and naval components essentially planned and fought their own campaigns. The precision air campaign, for example, preceded the four-day land war and was operationally independent from it. Since then, however, US power-projection operations have become progressively more "joint" in character.

In Operation Enduring Freedom, it would have been impossible for the small number of American and allied special operations forces (SOF) inserted into Afghanistan (i.e., about 300 by the fall of Kandahar)—the only US and allied forces on the ground—to generate the combat power they did without the close cooperation of pilots from the Air Force, Navy, and Marine Corps. Joint air operations were not only conducted simultaneously with ground operations, they were also integrated with them at the *tactical* level. SF teams used a variety of man-portable sensors (e.g., thermal imaging, night-vision goggles, and signals intelligence systems) to find enemy targets. Once a specific target was identified, a laser-designator could be used to "mark" it for destruction by a LGB. More frequently, however, specially trained Air Force combat controllers on the ground determined the target's precise geo-location using a laser range-finder unit linked to a hand-held GPS receiver. The GPS coordinates could then be passed by radio to Air Force, Navy, and Marine Corps pilots in strike aircraft loitering overhead and plugged into GPS-guided JDAMs. In some cases, connectivity between units on the ground and airborne strike assets was established with advanced digital communication systems.[156] As Secretary of Defense Donald Rumsfeld noted:

---

[156] SF units reportedly used the compact Multi-band Inter/Intra Team Radio (MBITR) to enhance their connectivity. The MBITR, which only recently began to be fielded, replaces seven older, narrow-function radios that used to be needed to communicate across the Services.

> In Afghanistan, we saw composite teams of U.S. special forces on the ground, working with Navy, Air Force and Marine pilots in the sky, to identify targets, communicate targeting information and coordinate the timing of strikes with devastating consequences for the enemy. The change between what we were able to do before U.S. forces, special forces, were on the ground and after they were on the ground was absolutely dramatic.[157]

Similarly, in Operation Iraqi Freedom, the ground and air campaigns overlapped from the very outset of the war and were mutually supporting. SOF seized the H2 and H3 airfields in Iraq's western desert for use by US aircraft and helicopters. As in Afghanistan, SOF, along with Army and Marine Corps personnel, designated hundreds of targets for precision air attack. They also conducted probing operations to get Iraqi mechanized units to move and reveal their location, making them vulnerable to precision air strikes.[158]

Joint air power, in turn, was indispensable to the rapid Army and Marine Corps advance from Kuwait to Baghdad. Without it, US ground forces would not have been able to maintain the unprecedented rate of advance that they did, covering over 250 miles in three days, and occupy the Iraqi capital—all while absorbing only light casualties. Before US ground forces even came into contact with major enemy force concentrations, the Iraqi units were substantially weakened by relentless, all-weather strikes by Air Force, Navy, and Marine Corps aircraft. Of the 800-plus tanks that the Republican Guard fielded at the start of the war for the defense of Baghdad, "all but a couple of dozen" were destroyed by air strikes or abandoned by the third week of the war.[159] Reflecting on the destruction of Iraqi

---

[157] Secretary of Defense Donald Rumsfeld, "21st Century Transformation," remarks as delivered at NDU, Fort McNair, Washington, DC, January 31, 2002.

[158] Andrew Krepinevich, *Operation Iraqi Freedom: A First-Blush Assessment* (Washington, DC: CSBA, 2003), p. 21.

[159] General Richard Myers, *DoD News Briefing*, April 7, 2003.

tanks, armored personnel carriers, tracked vehicles and enemy positions by joint air power, Colonel Michael Longoria, commander of the Air Force's 484th Air Expeditionary Wing, commented: "when you can destroy over three divisions worth of heavy armor in a period of about a week and reduce each of these Iraqi divisions down to even 15, 20 percent of their strength, it's going to have an effect."[160] That effect was telling: a ground force one-third the size of the one committed to Desert Storm accomplished a far more demanding mission in about half the time—albeit against a much weaker adversary.

To encourage further joint force integration, DoD is allocating significant resources to the development of "Joint Operations Concepts" for a wide array of contingencies.[161] Building on earlier exercises, it also plans to conduct a series of large-scale, joint training exercises to explore new operational concepts, techniques, and tactics in more detail. As part of this effort, many of the individual services' training sites will be linked together into a new "Joint National Training Capability (JNTC)."[162]

CONTINUED REVOLUTION, REVOLUTION WITHIN THE REVOLUTION, OR SUCCESSOR REVOLUTION?

The rate of change in military capabilities will likely increase substantially over the next couple of decades. Precision-strike capabilities will continue to increase in reach, scale and sophistication. More advanced forms of stealth are in development. Sensors and battle networks will continue to increase in capacity and

[160] Stephen Hedges, "Air War Credited in Baghdad's Fall," Chicago Tribune, April 22, 2003.

[161] Keith Costa, "Rumsfeld Approves Blueprint for Future Joint Military Operations," *Inside the Pentagon*, December 4, 2003, p.1.

[162] Megan Scully, "U.S. Joint Forces Command to Launch Initiative with Massive Exercises in 2004," *Defense News*, December 8, 2003, p. 28.

sophistication. Unmanned systems will become an increasingly important component of force structures. What is not clear at this point is whether we are in the mature, albeit still rapid-growth phase of a revolution in war that began three decades ago, or whether significant discontinuities (a "revolution within the revolution" or a successor revolution) lie ahead.[163] The United States could retain its monopoly on the capabilities underwriting this revolution for several decades. A critical mass of these capabilities, on the other hand, could diffuse to potential competitors, or the United States or a competitor could develop capabilities that result in a new military revolution that displaces the current one.

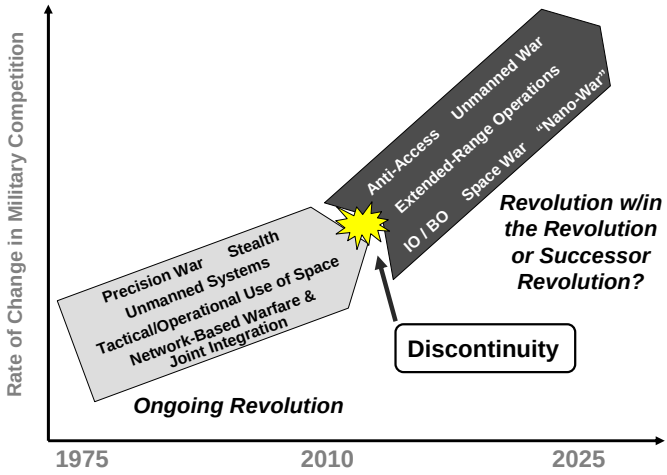
Competitors potentially could respond to the revolutionary changes being pursued by the United States symmetrically (e.g., emulating advanced US capabilities by fielding stealth fighters equipped with advanced PGMs) or asymmetrically (e.g., by focusing on missile-based power projection and other "disruptive" capabilities). Asymmetric competition, the most likely, direct, competitive response to the current revolution in war, if there is one, could lead to the emergence of sophisticated "anti-access/area denial" networks that could pose a significant threat to traditional US power projection capabilities. The ability of the US military to control the air, operate on the ocean's surface in littoral areas and conduct mobile armored warfare—the core of current US power projection capabilities—could be severely challenged. Prospective adversaries could field robust capabilities that allow them to target in-theater ports, airfields, and other installations relied upon by US forces, as well as high-signature aircraft, surface ships, and ground combat formations. Denied access to in-theater bases, US forces could be forced to place much greater emphasis on extended-range operations, stealthy and unmanned platforms, and small footprint, ground combat formations. Asymmetric competition in the current dimensions of the revolution in war is thus likely to be far more disruptive than symmetrical competition.

War could also emerge in new forms and dimensions. The competition in space could shift from continued improvements in the operational and tactical use of near-earth space for terrestrial force

[163] A discontinuity is defined as a fundamental break from current trends.

enhancement to war into, from, through, and within space. Other potential discontinuities include the emergence of new forms of information and biological operations. Such developments could be realized by the US alone or the US and potential competitors. Whether such developments represent aspects of a revolution within the revolution or a successor revolution depends on whether they render obsolete or subordinate the existing military regime in a manner that is rapid, profound and destabilizing. The advent of military capabilities that shattered and rendered obsolete or subordinate the existing military regime (e.g., the dominance of unmanned systems, directed energy or nanotechnology), whether exploited by one or multiple competitors, would represent a successor revolution. (See Figure 1).

Figure 1: Potential Discontinuities in the Revolution in War



How one distinguishes between developments within the ongoing revolution in war, a revolution within the revolution, and a successor revolution could, of course, be a matter of some dispute. It would appear to us, for example, that adversary exploitation of military capabilities that cause discontinuous change in how the United States projects military power (e.g., the emergence of multi-dimensional anti-access/area-denial networks that compel the US military to rely more on stealthy systems and operate from extended range) should, at a minimum, be characterized as a revolution within the revolution. On the other hand, if that change results from the same

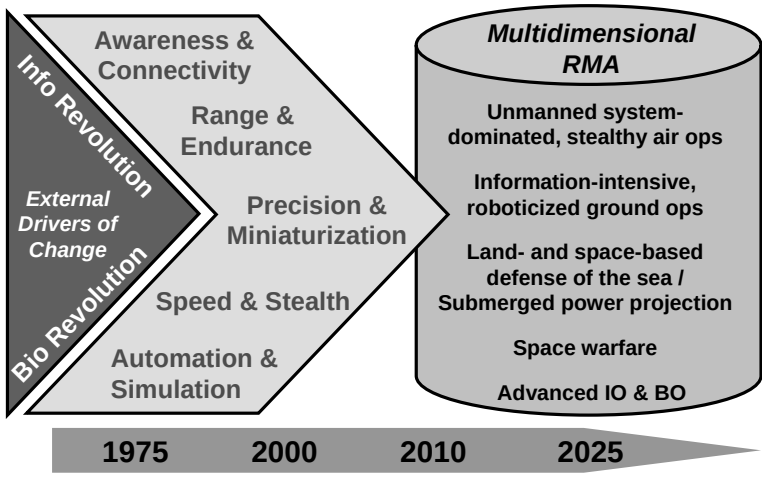
core capabilities that underwrite the ongoing revolution in war (e.g., the ability to target and strike precisely at a distance), even if pursued asymmetrically, it would nevertheless appear to fail the test of a successor revolution: rendering obsolete or subordinate key elements of the current military regime. Similarly, the emergence of war in new dimensions (e.g., war within space) should, at a minimum, be viewed as a revolution within the revolution. The emergence of war in new dimensions, as well as the emergence of new military capabilities more generally, however, may or may not meet the successor revolution test. If advanced forms of unmanned warfare are employed on a scale and scope sufficient to supplant manned warfare, for example, that would, in our view, be termed a successor revolution. Other successor revolutions might conceivably be based upon the exploitation of advanced bio-technologies and nano-technology, but again, only if they displaced key elements of the current warfare regime as opposed to just supplementing them. The key distinction between a revolution within the revolution and a successor revolution is that the former would have more continuity with the current military regime in terms of core military capabilities and patterns of operation and be less strategically discontinuous than the latter. Both, however, would represent significant discontinuities in warfare.

The ongoing revolutions in information technology, and to a lesser extent, biotechnology have had and will likely continue to have an enormous spillover effect on the development of new military capabilities. As depicted below in Figure 2, the combined effect of advances in ten areas—battlespace awareness or "transparency," digital connectivity, range, endurance, precision, miniaturization, speed, stealth, automation, and simulation—could lead to discontinuous, multidimensional change that could have a profound impact on the conduct of war and strategic balances.[164] At a minimum, there is a high probability of a revolution within the revolution occurring within the coming decades.

---

[164] Military revolutions, as opposed to military regimes, typically occur over a two–to–three decade time horizon, though longer periods of revolutionary change (half a century) are evident in the historical record (the "guns and sails" revolution, for example). The contemporary revolution in war certainly fits the traditional pattern of requiring less than three decades to realize. The current period of revolutionary change could be extended, however, through "revolution within the revolution," as discussed above.

Figure 2: Changes in Key Capabilities and Discontinuous Change in Warfare



New classes of commercial and military sensors, combined with more powerful data processing capabilities, could dramatically enhance battlespace awareness. Meanwhile, robust fiber-optic grids, space–based laser communications, computer networking software and hardware, and widely available encryption technologies could enhance the C3 capabilities of military forces by providing them with secure, reliable, broadband communications. Precision-strike systems could diffuse and become progressively more accurate and "brilliant" than their predecessors, exploiting miniaturized terminal seekers, automatic target recognition (ATR) algorithms, and other onboard data-processing features. Given an increasingly transparent battlespace, these systems could dramatically reduce the survivability of high-signature platforms in the air, at sea, and on land. The networking of increasingly capable ISR systems with ever more lethal precision-strike weapons could result in a future warfare environment in which, if you can be seen, you can be killed. This development would, of course, place a premium on stealth, speed, and information operations, including offensive IW and electronic warfare (e.g., jamming, radio-frequency warfare and deception operations), for survivability.

Operational endurance could be extended substantially as a result of new applications of nuclear power and other forms of high-density energy storage (e.g., advanced fuel cells), increased reliance on

unmanned systems unconstrained by human physiology, and the migration of additional capabilities to space. The range and speed of combat operations could continue to increase as militaries take greater advantage of long-range, precision-strike capabilities (e.g., ballistic and cruise missiles and UAVs) and myriad applications of hypersonic and directed-energy technologies. Unmanned systems could increasingly substitute for manned systems across warfare dimensions. Progress in miniaturization could not only result in dramatically smaller versions of traditional platforms and munitions, but could also yield novel systems such as insect-sized ground robots, disposable microsensors and micro "proximity" satellites for space warfare. The exploitation of nanotechnology could result in even more novel systems. Biotechnology could be exploited to create a broad range of novel biological weapons that are more discriminate and lethal in their effects. Advances in computer modeling and simulation could dramatically improve military planning and training.

Key warfare trends and competitions that seem likely to shape the future warfare regime will be discussed in much greater detail in the next chapter. While there is significant uncertainty about how these competitions will play out, key technologies underpinning all ten of the above-mentioned capability drivers of the ongoing revolution in war are already maturing and diffusing, albeit at different rates. As a result, the US military could face significant challenges—different in both form and scale—over the next few decades. Discontinuous change in the conduct of war over the coming decades, in short, could present the United States with both threats to its current dominance, as well as opportunities to extend its dominance.

III. Key Warfare Competitions

While numerous competitions could plausibly shape the future course of the ongoing revolution in war, we believe six will be the most determinative:

1. Evolving anti-access or area-denial capabilities versus current and new forms of power projection;

2. Increased capabilities for preemption versus denial;

3. Hiders versus finders;

4. Space access versus space control;

5. Offense-defense competitions in the areas of missile attack versus missile defense, IW attack versus IW defense, and BW attack versus BW defense;[165] and

6. Increased capabilities for coercion versus counter-coercion.

[165] We combine these three because of their related effects across major strategic functions. They, of course, could also be treated as separate competitions.

We focus on these six because of their potential impact on major strategic functions: forward presence, power projection, dimensional control, and homeland defense. These core competitions also track closely with the "the critical operational goals" outlined in the 2001 Quadrennial Defense Review (QDR) to provide focus for DoD's transformation efforts.[166] How these warfare competitions will play out, of course, will depend fundamentally on the extent and character of strategic competition among state and non-state actors over the next couple of decades. A preliminary assessment of these competitions can be made, however, based on current R&D and modernization plans, foreign military writings, and technology diffusion trends.

The six key competitions overlap to varying degrees. For example, the "hider versus finder" competition is an important element of both the anti-access versus power projection competition, as well as that between missile attack and defense.[167] It could, however, shape the future warfare environment in myriad other ways that warrant separate examination. Similarly, while the outcomes of the key offense-defense competitions and the competition between space access and control have critical implications for power projection in anti-access environments, separate examination of these competitions highlights how the emergence of war in new dimensions of the battlespace (i.e., cyberspace, biological, and near-earth space) could result in much larger military challenges and opportunities. The

[166] The QDR describes six key operational challenges that mandate transformation and provide focus for DoD's transformation efforts: protecting critical bases of operations including the US homeland; assuring US information systems and conducting effective information operations; projecting and sustaining US forces in anti-access or area-denial environments; denying enemies sanctuary; enhancing the capability and survivability of space systems; and leveraging information technology and innovative concepts for more effective joint operations. DoD, *Quadrennial Defense Review Report* (Washington, DC: DoD, September 30, 2001), p. 30. Similarly, the strategic concepts of preemption, coercion, deterrence and reassurance figure prominently in *The National Security Strategy of the United States of America*, released in September 2002.

[167] Both are linked through the sub–competition between stealth and counter–stealth, for example. The hinder–finder competition would still exist, however, in the absence of both the anti–access/power projection competition and the missile attack–defense competition.

missile offense–defense competition, moreover has a strategic (e.g., homeland attack) as well as a theater dimension (e.g., anti–access and missile–based power projection). Finally, while strategic competitions involving coercion and counter-coercion, and preemption and denial are, in part, dependent upon the outcome of the other competitions identified above, they illuminate the potential implications of changes in the efficacy and use of force.

ANTI-ACCESS / AREA DENIAL VERSUS CURRENT AND NEW FORMS OF POWER PROJECTION

In future conflicts, prospective regional allies may be reluctant to host US forces owing to domestic political pressures or because they fear that doing so would invite enemy attacks against their territory. There are numerous precedents for politically motivated base denial in just the last several years. During Operation Desert Fox in 1998, for example, Saudi Arabia, the United Arab Emirates, and Turkey all barred US forces from using bases within their territory for strike operations. During Operational Allied Force in 1999, Greece refused to grant US forces basing and France denied use of its airspace to US bombers based in the United Kingdom, forcing them to fly around Spain and up through the Mediterranean to strike Serbian targets.[168] Rattled by an outbreak of violent protests, Italian authorities yielded to mounting public pressure and threatened to cut off access to its airbases, including the vital airbase at Aviano, unless the coalition immediately focused its air power against Serbian forces conducting atrocities in Kosovo rather than strategic targets such as those in and around Belgrade.[169] In Operation Enduring Freedom, several states that are at least nominally allies of the United States (e.g., Saudi

[168] General John Jumper, "Global Strike Task Force: A Transforming Concept, Forged by Experience," *Aerospace Power Chronicles*, Spring 2001.

[169]Christopher Bowie, *The Anti-Access Threat and Theater Air Bases* (Washington, DC: CSBA, 2002), pp. 41-42. See also: William Booth and Sarah Delaney, "While Accepting Refugees, Italy is Divided over Kosovo," *Washington Post*, April 14, 1999.

Arabia) refused to allow bases on their soil to be used for strike operations against Al Qaeda and Taliban targets in Afghanistan.[170] Most recently in Operation Iraqi Freedom, base access for strike operations was denied not only by Saudi Arabia, but also by Turkey, one of America's NATO allies.[171]

Base access is much more than a political problem, however, that might be remedied through diplomacy or stepped up peacetime presence. Operating from fixed forward bases and within littoral waters could also become militarily untenable over time owing to the emergence and diffusion of increasingly capable anti-access/area-denial capabilities.[172] Highlighting the potential seriousness of this challenge, the 2001 QDR cautioned:

> Future adversaries could have the means to render ineffective much of our current ability to project military power overseas. Saturation attacks with ballistic and cruise missiles could deny or delay US military access to overseas bases, airfields, and ports. Advanced air defense systems could deny access to hostile airspace to all but low-observable aircraft.

---

[170] See David Ottaway and Robert G. Kaiser, "Saudis May Seek U.S. Exit," *Washington Post*, January 18, 2002, p. 1.

[171] As a result, several scores of aircraft had to be dropped from the air campaign because there was not enough capacity at other bases to absorb them, the sortie rate of carrier-based aircraft in the Mediterranean Sea was much lower than anticipated because aerial refuelers could not operate from Turkish bases as planned, and the equipment for the Army's 4th Infantry Division could not be offloaded at Turkish ports in order to open up a northern front against Iraq. Turkey refused to grant US forces base access even though it stood to receive $6 billion in grants that could have been leveraged into more than $20 billion in loans. See Glenn Kessler and Vernon Loeb, "Turkey Wants U.S. to Enhance Aid for Troops to Land," *Washington Post*, February 19, 2003, p.1; and Bill Sammon, "Turkey Risks Losing $6 Billion in Aid from the U.S.," *Washington Times*, March 4, 2003, p.1.

[172] For an assessment of the potential vulnerability of theater air bases see: Bowie, *The Anti-Access Threat and Theater Air Bases*. See also: National Defense Panel, *Transforming Defense: National Security in the 21st Century* (Washington, DC: NDP, 1997), pp. 12-13, 33-36.

> Military and commercial space capabilities, over-the-horizon radar, and low-observable unmanned aerial vehicles could give potential adversaries the means to conduct wide-area surveillance and track and target American forces and assets. Anti-ship cruise missiles, advanced diesel submarines, and advanced mines could threaten the ability of US naval and amphibious forces to operate in littoral waters. New approaches for projecting power must be developed to meet these threats.[173]

As this excerpt from the 2001 QDR makes clear, the anti-access/area-denial challenge could be multidimensional in scope. With the possible exception of China, there are no military competitors on the horizon that have the resources necessary to invest fully in all of the capability areas identified in Table 2. Relatively narrow investments in a handful of these areas, however, could be sufficient to reduce dramatically the effectiveness of many traditional means of US power projection.

[173] *Quadrennial Defense Review Report*, p. 31.

Table 2: Examples of Emerging Multidimensional Anti-Access / Area-Denial Capabilities

Air Dimension	Sea Dimension	Land Dimension	Space Dimension	Information Dimension
Military & Commercial Space-Based Remote Sensing	Military & Commercial Space-Based Remote Sensing	Military & Commercial Space-Based Remote Sensing	Enhanced Space Surveillance & Tracking Capabilities	High-Power Microwave Weapons
ISR UAVs	ISR UAVs	ISR UAVs	Uplink & Downlink Jammers	Transient Electo-Magnetic Devices
Over-the-Horizon (OTH) Radar	OTH Radar	Unattended Ground Sensor (UGS) Networks	GPS Jammers	High-Power Jamming
Integrated, Multistatic Sensor Networks / Counter-Stealth Sensors	Active & Passive Sensor Arrays in Littoral Waters	Missile Barrage Attacks Against Ports, Airbases, Logistics Depots & Staging Areas	"Proximity Operation" Microsatellites	Computer Network Attack / Offensive IW
Missile Barrage Attacks Against In-Theater Airbases	Ground-, Air-, & Sea-Launched, Anti-Ship Cruise Missiles (Stealthy & Supersonic)	Smart PGMs & Anti-Armor Submunitions	Laser Dazzlers	Ballistic & Cruise Missile Attacks against C4 Nodes
Networked, Mobile Long-Range SAMs / Advanced Man-Portable Air Defense Systems	Quiet Attack Submarines (Armed with Wake-Homing Torpedoes)	Large Numbers of Fixed and Mobile Mines	Direct-Ascent / Co-Orbital, Kinetic-Kill, Anti-Satellite (ASAT) Weapons	SOF / Terrorist Attacks against C4 Nodes & Critical Infrastructure
Long-Range Air-to-Air Missiles	Large Numbers of Fixed and Mobile Mines	Wide-Area Effect Weapons (Fuel-Air Explosives)	Directed-Energy ASATS	High-Altitude Nuclear Detonations
Unmanned Combat Air Vehicles (UCAVs)	Maritime Patrol UCAVs	UCAVs	Nuclear Detonation(s) in Low/Medium Earth Orbit (LEO/MEO)	Counter-Space (ASATs, Jamming, Proximity Operations)
Advanced Chemical and Biological Weapons	Small, Fast Boats	Advanced Chemical and Biological Weapons (CBW)	Attacks Against Space Launch & Satellite Control Facilities	C3D2

The competition between maturing anti-access capabilities versus current and new forms of US power projection will likely evolve over time through a series of actions and responses. Over the course of the next ten years, for example, prospective adversaries could potentially exploit widely available ISR capabilities and long-range ballistic and cruise missile to target fixed installations on land (e.g., ports, air fields, depots, and logistics nodes). In response, the US military might shift toward increased reliance upon extended-range strike aircraft that do not require access to in-theater bases (i.e., bombers and UCAVs), carrier-based strike aircraft, missile-armed surface combatants, and ground forces that can be inserted "over the beach" or air-dropped into theater.

Beyond 2010-2015, however, the survivability of aircraft carriers, high-structure surface combatants, and non-stealthy aircraft of all types could increasingly be called into question as maritime, over–the-horizon "area denial" capabilities and extended-range air defense systems continue to mature. To hedge against this possibility, the United States could increase its investment in stealthy, extended-range strike aircraft; submarines and UUV's; and stealthy surface ships and USV's. If prospective adversaries developed the capability to track and target high-signature ground vehicles on the move, the United States might adapt by fielding highly dispersed, information-intensive ground forces supported by stealthy ground vehicles and robotic capabilities.

While it impossible to say with any certainty how specific elements of the anti-access versus power projection competition will evolve the next two decades, it has become increasingly apparent that prospective adversaries (e.g., China and Iran) are interested in pursuing anti-access strategies and many have started fielding relevant capabilities. The sections below briefly examine trends and developments in the following capability areas: battlespace transparency; ballistic and cruise missile arsenals; maritime "area denial" threats; extended-range air defenses; and information- and space-denial capabilities.

Increasing Battlespace Transparency

Given current trends, the ISR information available to prospective adversaries is almost certain to improve significantly over the next two

decades. The advantage in this area that the United States enjoys today could diminish considerably in relative terms. Several prospective adversaries, for example, are actively pursing the development of high-flying, inherently low-observable UAVs capable of performing theater-wide ISR missions. A few are building various kinds of remote-sensing satellites (e.g., China),[174] while others are gaining access to high-resolution satellite imagery by purchasing it from commercial suppliers. Hyperspectral and high-resolution, radar-imaging services are likely to become commercially available within the next several years. Many states are also learning how to network widely dispersed, disparate sensors into an integrated system that is more powerful than the sum of its parts. These networks will become progressively more capable as more advanced sensor technologies diffuse over time, such as unattended ground sensors (UGS), active and passive sonar arrays, OTH radar, infrared search and track (IRST) systems, and SAR systems with GMTI capability.

With more powerful ISR capabilities at their disposal, prospective adversaries will become better able to identify and geo-locate the fixed facilities (e.g., ports, airfields, pre-positioned equipment depots, garrisons, and C3 nodes) upon which US forces currently rely heavily for projecting power. In peacetime, adversaries could build extensive target libraries containing the precise geo-location of thousands of regional fixed targets with potential strategic or operational value. In the event of a conflict with the United States, these same ISR assets (along with intelligence operatives with satellite phones and GPS receivers) could be used to identify which targets in the library were actually being used by US forces, as well as to conduct post-attack BDA.

Given the ongoing diffusion of sensor systems and signal processing technologies, by 2015-2025, if not sooner, prospective adversaries could be able to detect and track some types of mobile ground vehicles and high-signature surface ships operating near their

[174] Two year ago, China launched the second photo-reconnaissance satellite in its Zi Yuan-2 (ZY-2) series. Operating at an altitude of about 500 km, the ZY-2 satellites may have a ground resolution in the range of 10-20 cm. See Phillip Clark, "China Launches New Photo-Reconnaissance Satellite," *Jane's Defence Weekly*, November 6, 2002, p. 14.

coast. For example, the approximate position and course of ships at sea might be determined by using some combination of ground-based, OTH radars; aerostat-borne maritime patrol radars; manned reconnaissance aircraft and UAVs equipped with electronics intelligence (ELINT) gear; pre-deployed passive or active acoustic sensor networks; and satellites carrying reverse-imaging SAR, ELINT, or IR sensor payloads. While these systems may not be able to generate targeting-quality tracking information, they would likely be more than sufficient for vectoring reconnaissance or strike platforms to the vicinity of suspected surface ship contacts.[175] Initial target location inaccuracy could also be overcome somewhat by equipping extended-range missiles with a terminal guidance system. The latter are becoming easier to develop owing to the diffusion of low-cost, high-quality sensors and cheap, but powerful microprocessors.

This is not just a theoretical or academic concern. China, for instance, has several ongoing R&D programs focused on the development of ocean-monitoring satellites, including multi-satellite ELINT/SIGINT and SAR constellations. China has been attempting to develop a "backscatter" OTH radar capability to track maritime movements in its contiguous waters for several years. Currently, it may have as many as three sky-wave OTH radar systems and possibly a prototype surface-wave system operational.[176] To both complement and facilitate indigenous long-term development efforts aimed at fielding modern airborne early warning and control aircraft and long-

[175] Non-stealthy aircraft and stealthy aircraft employing active sensors would be vulnerable to US extended-range air defenses. As a result, adversaries pursuing an anti-access strategy may gravitate toward stealthy UAVs equipped with passive sensors that would be more difficult to detect, track, and engage. The survivability of maritime reconnaissance aircraft—both manned and unmanned—could be enhanced somewhat by flying them within the airspace envelope protected by extended-range ground- and sea-based air defenses. Even in this envelope, however, enemy aircraft would still be vulnerable to attack by stealthy fighter aircraft and/or extended-range missiles.

[176] According to some reports, sky-wave radars have a surveillance range of between 800 and 3,000 kilometers. Kanwa News Agency (Beijing), "China Develops Sky-Wave Backscatter OTH Radar," November 7, 2001. See also: DoD, *Annual Report on the Military Power of the People's Republic of China (2003),* p. 8; and DoD, *Annual Report on the Military Power of the People's Republic of China (2004),* pp. 44-45.

range UAVs, the PLA Navy (PLAN) is attempting to acquire platforms and sensor systems from abroad. China has already procured an aerostat-borne maritime patrol radar that is expected to have an effective range of up to 200 kilometers and the ability to detect, classify, and target ships at sea.[177] DoD reported to Congress in 2002 that "China's procurement of new space systems, airborne early warning aircraft and long-range UAVs, and over-the-horizon radar will enhance its ability to detect, monitor, and target naval activity in the Western Pacific Ocean."[178] It further cautioned that "China may have developed passive acoustic sensors for use in coastal waters" and will probably continue to develop and deploy additional, and more capable, underwater sensors, some of which "may be installed as far offshore as the edge of the continental shelf."[179]

Defenders of high-signature platforms (e.g., large surface combatants and aircraft carriers) frequently assert that competitors will not be able to track mobile targets, particularly surface ships operating over the horizon, for the foreseeable future. This argument, however, hinges on the very debatable assumption that technologies that have enabled the US military to track moving targets, albeit imperfectly, for more than a decade have not and will not diffuse—despite mounting evidence to the contrary. As a point of reference, the basic SAR/MTI technology that allows JSTARS aircraft to track mobile ground vehicles and the ELINT technology that enables the US Naval Ocean Surveillance System (NOSS) to locate and track ships at sea are both already more than two decades old.

---

[177] The radar, which is a modified version of Russia's Novella system, is reportedly capable of operating in four modes: air-to-air detection; long-range surface search; inverse SAR for vessel classification; and target acquisition. See Piotr Butowski, "China's New Radar Watch on Taiwan Strait," *Jane's Defence Weekly*, September 4, 2002.

[178] DoD, *Annual Report on the Military Power of the People's Republic of China (2002)*, pp. 4, 22.

[179] Ibid., p. 29.

Growing Missile Arsenals

Assuming future adversaries have ISR capabilities sufficient to determine the location of ports, airfields, garrisons, and other fixed installations relied upon by US forces to project power, they could potentially target them with waves of ballistic and cruise missiles. While it may not be possible to completely destroy large, heavily defended installations, repeated missile attacks would certainly degrade US military performance and could make the human and material costs of continued American operations prohibitively high. As will be discussed below, although the total number of countries armed with ballistic missiles has not increased significantly over the last decade, several countries have increased the size of their arsenals and have invested in improved missile reliability and performance (e.g., range, payload, and accuracy). Land-attack cruise missiles are falling into the hands of a growing number of prospective adversaries, many of whom are expanding and modernizing their arsenals. By taking advantage of signature reduction, terrain masking, and multi-directional attack tactics, cruise missiles could be very difficult to defend against.

Ballistic Missiles

The number of deployed ballistic missiles in the world with a range between 300 to 3,000 kilometers is expected to increase by at least ten-fold over the next two decades.[180] Ballistic missiles are also improving qualitatively in terms of range, accuracy, reliability, and overall lethality. China, North Korea, India, Iran, and Pakistan, for instance, all have active ballistic missile development programs, and have fielded increasingly capable systems over the last several years.[181]

---

[180] See "National Air Intelligence Center's Missile-Threat Report," *Defense Week*, September 25, 2000, p. 13; Mark Hewish, "Ballistic Missile Threat Evolves," *Jane's International Defense Review*, October 2000, pp. 38-44; and Ben Sheppard, "Ballistic Missile Proliferation: A Flight of Fantasy or Fear?" *Jane's Intelligence Review*, October 1999, pp. 50-54.

[181] Vice Admiral Lowell E. Jacoby, Director, Defense Intelligence Agency, "Current and Projected National Security Threats to the United States," Statement for the Record, Senate Select Committee on Intelligence, February 23, 2004, pp. 7-10. Director of Central Intelligence (Weapons Intelligence, Nonproliferation, and Arms Control Center), *Unclassified Report to Congress*

Several countries are actively investigating countermeasures to US missile defense systems such as maneuvering re-entry vehicles, on-board jammers, decoys, counter-laser cladding, and depressed trajectories.[182] More than a dozen countries could opt to arm their missiles with chemical, biological, or nuclear warheads. As the unclassified summary of the 2002 national intelligence estimate on missile proliferation noted:

> The trend in ballistic missile development worldwide is toward a maturation process among existing ballistic missile programs rather than toward a large increase in the number of countries possessing ballistic missiles. Emerging ballistic missile states continue to increase the range, reliability, and accuracy of the missile systems in their inventories—posing ever greater risks to U.S. forces, interests, and allies throughout the world.[183]

China has at least three classes of theater ballistic missiles in production: the DF-11 (also known as the CSS-7 or M-11) short-range ballistic missile (SRBM), the DF-15 (also known as the CSS-6 or M-9) SRBM, and the DF-21 (CSS-5) medium-range ballistic missile (MRBM).[184] These systems have approximate ranges of 300, 600, and

---

on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January Through 30 June 2002 (Washington, DC: CIA, 2003); and OSD, *Proliferation: Threat and Response* (Washington, DC: DoD, January 2001).

[182] China, for example, has a number of programs underway in this area. See Mark Stokes, "China's Military Space and Conventional Theater Missile Defense Development: Implications for Security in the Taiwan Straits," in Susan Puska, ed., *People's Liberation Army After Next* (Carlisle, PA: Strategic Studies Institute, August 2000), pp. 124–126.

[183] See National Intelligence Council, *Foreign Missile Developments and the Ballistic Missile Threat Through 2015—Unclassified Summary of a National Intelligence Estimate* (Washington, DC: CIA, 2002), p. 7 (electronic version). Available at: http://www.odci.gov /nic/pubs/other_products/ unclassifiedballisticmissilefinal.htm.

[184] Not listed here are China's strategic missiles such as the road-mobile, solid-fueled DF-31, which has a range of 8,000 kilometers; an extended-range, follow-on to the DF-31 (formerly referred to as the DF-41), which is expected

2,000 kilometers, respectively. All three rely on solid propellants and are road-mobile. An extended-range version of the DF-15, which could be used to strike US bases as far away as Okinawa, is under development.[185] China has already taken advantage of GPS to determine the initial location of its missile launchers more accurately, making the missiles themselves considerably more precise. The inertial guidance system incorporated into the most recent generation of SRBMs (e.g., DF-11A and DF-15A) can be updated in flight by GPS. China has recently initiated development of terminal guidance systems to further enhance missile accuracy. In addition, various types of submunitions are being developed to increase the lethality of conventionally armed ballistic missiles, especially against wide-area targets (e.g., airfields, ports, and military bases). China is developing active countermeasures to degrade the effectiveness of US missile defense systems. Finally, China is steadily expanding the size of its missile arsenal. It is expected to have deployed over 600 short-range missiles across from Taiwan by the end of next year and will likely field additional missiles at a rate of approximately 75 per year thereafter.[186] Given current missile production rates and anticipated investment in expanded manufacturing infrastructure, China's ballistic missile arsenal could easily surpass 1,200 by the close of this decade.[187]

Despite a failing economy, North Korea has managed to both expand and qualitatively improve its missile arsenal over the past decade. It is believed to have an inventory of several hundred Scud variants with ranges between 300 and 600 kilometers; dozens of No-

---

to have a range of 12,000 kilometers, and a submarine-launched version of the DF-31, dubbed the JL-2.

[185] DoD, *Annual Report on the Military Power of the People's Republic of China (2003)* (Washington, DC: DoD, July 2003), p. 5.

[186] DoD, *Annual Report on the Military Power of the People's Republic of China (2003)*, pp. 5, 22. See also: Thom Shanker, "U.S. Says China is Stepping Up Short-Range Missile Production," *New York Times*, July 31, 2003; Bill Gertz, "Pentagon Says China Refitting Missiles to Hit Okinawa," *Washington Times*, July 31, 2003, p. 9; and Murray Hiebert, "U.S. Urges Taiwan to Purchase Missiles," *Wall Street Journal*, May 9, 2003.

[187] Assuming a production rate of 75 missiles per year, China could field some 1,200 missiles against Taiwan by 2013. See Bill Gertz, "Chinese Missiles Concern Pentagon," *Washington Times*, April 3, 2002, p. 3.

Dong missiles with an approximate range of 1,300 kilometers; and an unspecified number of Taepo Dong 1 and 2 missiles, which are estimated to have a range of 1,500-2,000 and 3,700-6,000 kilometers, respectively, depending on the weight of the payload.[188] Earlier this year, North Korean began deploying a new land-based, road-mobile, medium-range ballistic missile (MRBM), based on the Soviet-era R-27 MRBM, with an estimated range of between 2,500 and 4,000 kilometers, which is sufficient to reach US bases in Okinawa, Guam, and Hawaii. It reportedly has also developed a sea-launched version of the R-27 with a range of at least 2,500 kilometers that could be launched from submarines (e.g., refurbished Golf-II ballistic missile submarines) or modified merchant ships.[189] Development of a road-mobile, extended-range version of the Taepo-Dong 2 with enhanced accuracy is also reported to be underway.[190] Fueling wider missile proliferation, North Korea has also exported missile systems and missile-related technology—most notably to Iran—to generate badly needed revenue.

Land-Attack Cruise Missiles

More than a dozen countries will soon be deploying land-attack cruise missiles (LACMs) with range capabilities spanning 100 to 1,000 kilometers.[191] Since LACMs can take advantage of GPS-based guidance

---

[188] See OSD, *Proliferation: Threat and Response* (Washington, DC: DoD, January 2001), pp. 11-12; and "NK Exports Large Quantity of Scuds to Middle East," *Korea Times*, September 29, 2003.

[189] The new North Korean MRBM/SLBM is liquid-fueled. See Joseph Bermudez, "North Korea Deploys New Missiles," *Jane's Defence Weekly*, August 24, 2004, p. 6; and Barbara Demick, "N. Korea May Have a Missile That Can Hit Guam," *Los Angeles Times*, May 6, 2004.

[190] See Bill Gertz, "North Korea to Display New Missiles," *Washington Times*, September 9, 2003, p. 1.

[191] China, France, Germany, India, Israel, Italy, Russia, Sweden, and the United Kingdom all build, and in several cases, sell cruise missiles and related technology. The National Intelligence Council estimates that up to two dozen countries "probably will possess a land attack cruise missile capability by 2015 via indigenous development, acquisition, or modification of such other systems as antiship cruise missiles or unmanned aerial vehicles." See National Intelligence Council, *Foreign Missile Developments and the Ballistic Missile*

to navigate throughout their flight, they are generally more accurate than ballistic missiles. Moreover, since many of the technologies needed to develop cruise missiles have commercial applications (e.g., commercial aviation) and can be procured from multiple suppliers, it is even more difficult to stem their proliferation effectively. Vice Admiral Thomas Wilson, director of the Defense Intelligence Agency, has cautioned that:

> ...the potential for widespread proliferation of land attack cruise missiles is high. While the type of missiles most likely to be proliferated will be a generation or two behind the global state of the art, states that acquire them will have new or enhanced capabilities for delivering WMD [weapons of mass destruction] or conventional payloads inter-regionally against fixed targets. Major air and sea ports, logistics bases and facilities, troop concentrations, and fixed communication nodes will be increasingly at risk.[192]

Prospective adversaries are expected to begin fielding LACMs with more accurate GPS-aided guidance, infrared countermeasures, and stealth features as early as 2005.[193] As one example of this trend,

---

Threat Through 2015, p. 17 (electronic version). See also: National Air Intelligence Center, *Ballistic and Cruise Missile Threat* (Wright Patterson Air Force Base (AFB), OH: NAIC, NAIC-1031-0985-99, April 2000), p. 20; Rick Newman, "Cruise Missiles, The Cheap Easy Alternative," *Defense Week*, March 20, 2000, p. 8; and Steven Zaloga, "The Cruise Missile Threat: Exaggerated or Premature?" *Jane's Intelligence Review*, April 2000, pp. 47-51.

[192] VADM Thomas R. Wilson, *Prepared Testimony before the Senate Select Committee on Intelligence*, February 2, 2000. Similarly, in testimony before Congress in March 2002, Director of Central Intelligence George Tenet cautioned, "By the end of the decade, LACMs could pose a serious threat to not only our deployed forces, but possibly even to the U.S. homeland." George J. Tenet, "Worldwide Threat: Converging Dangers in a Post 9/11 World," *Prepared Testimony before the Senate Armed Services Committee*, March 19, 2002, p. 13.

[193] Bryan Bender, "Cruise Control," *Jane's Defence Weekly*, July 22, 1998, pp. 20-22; and David Fulghum, "Stealth, Cheap Technology Complicate Defense Schemes," *Aviation Week & Space Technology*, July 14, 1997, pp. 47-56.

China is currently developing a family of ramjet-powered LACMs with ranges extending from 600 to 3,000 kilometers that could be launched from mobile TELs, ships, submarines, or aircraft.[194] According to some reports, these missiles will be very accurate (i.e., a circular error probable of less than five meters) and incorporate first-generation stealth technologies (e.g., RAM and composite construction).[195] Early this fall, China test-fired a new ground-launched LACM, designated the Dong Hai-10 (East China Sea-10), which can strike targets more than 1,500 kilometers away very precisely owing to an onboard integrated inertial navigation system aided by GPS, a terrain-contour mapping system, and digital-scene-matching terminal homing system. Roughly comparable to an American Tomahawk LACM, the Dong Hai-10 is estimated to have a circular error probable of about 10 meters.[196] As the National Air Intelligence Center has noted, future LACMs are likely to stress air defense systems for a variety of reasons:

> Cruise missiles can fly at low altitudes to stay below radar and, in some cases, hide behind terrain features. New missiles are incorporating stealth features to make them even less visible to radars and infrared detectors. Modern cruise missiles can also be programmed to approach and attack a target in the

---

[194] These LACMs, referred to as the HN-1/-2/-3 family, are reportedly based in part on Russian and French missile technology. See Duncan Lennox, "Cooperation Boosts Missile Proliferation," *Jane's Intelligence Review*, January 2002, p. 40. For an overview of China's LACM programs see: Stokes, "China's Military Space and Conventional Theater Missile Defense Development: Implications for Security in the Taiwan Straits," pp. 127-135; Mark Stokes *China's Strategic Modernization: Implications for the United States* (Carlisle, PA: Strategic Studies Institute, September 1999), pp. 79-86; and Duncan Lennox, "China's New Cruise Missile Programme Racing Ahead," *Jane's Defence Weekly*, January 12, 2000, p. 12.

[195] Lennox, "China's New Cruise Missile Programme Racing Ahead," p. 12; Yihong Zhang, "Beijing Develops New Radar-Absorbing Materials," *Jane's Defence Weekly*, February 24, 1999; and David Fulghum, "Small Stealth Designs within China's Grasp," *Aviation Week & Space Technology*, June 7, 1999, pp. 28-29.

[196] "China Tests New Land-Attack Cruise Missile," *Jane's Missiles and Rockets*, October 2004.

> most efficient manner. For example, multiple missiles can attack simultaneously from different directions....Furthermore, the LACMs may fly circuitous routes to get to the target, thereby avoiding radar and air defense installations.[197]

Competitors may opt to arm ballistic and cruise missiles with WMD payloads to enhance their deterrent value and increase their effectiveness, especially against large, relatively soft area targets such as ports and unhardened airfields. At least 16 states have active chemical weapons (CW) programs and up to a dozen have BW programs.[198] Barrages of ballistic and cruise missiles, some potentially armed with WMD, could be used to deny access to fixed targets such as airfields, ports, prepositioned equipment, C3 facilities, transportation chokepoints, centralized logistics depots, and military garrisons and staging areas.[199]

Of course, the US military can already identify and destroy fixed targets with relative ease, as was demonstrated in Operation Desert

---

[197] NAIC, *Ballistic and Cruise Missile Threat,* p. 19. For a more in-depth explanation of the challenges involved in intercepting cruise missiles, see David Tanks, *Assessing the Cruise Missile Puzzle: How Great the Challenge?* (Washington, DC: Institute for Foreign Policy Analysis, 2001).

[198] George Tenet, Director of the Central Intelligence, *Statement before the Senate Armed Services Committee*, Hearing on Current and Projected National Security Threats, February 2, 1999, p. 3. Vice Admiral Thomas Wilson, Director of the Defense Intelligence Agency, has testified that: "Many potential adversaries believe they can preclude U.S. force options and offset U.S. conventional military superiority by developing WMD and missiles. . . The basic sciences necessary to produce these weapons are widely understood. Most of the technology is readily available, and the raw materials are common. All told, the prospects for limiting proliferation are slim, and the global WMD threat to U.S.-allied territory, interests, forces, and facilities will increase significantly." Vice Admiral Wilson, *Statement before the Senate Select Committee on Intelligence,* February 2, 2000, p. 5.

[199] For an in-depth assessment of the near-term threat missiles could pose to airbases, see: John Stillion and David Orletsky, *Airbase Vulnerability to Conventional Cruise Missile and Ballistic Missile Attacks* (Santa Monica, CA: RAND, 1999). See also: Christopher J. Bowie, *The Anti-Access Threat and Theater Air Bases.*

Storm, Operation Allied Force, Operation Enduring Freedom, and most recently, in Operation Iraqi Freedom. A critical transformation threshold will be crossed, however, once adversaries can deny these same types of facilities to US forces. The Defense Intelligence Agency estimates that during the next decade, "a number of states will develop precision attack capabilities roughly equivalent to what the US fielded in the mid-1990s" and that the diffusion of these capabilities "will increasingly put our regional bases and facilities at risk."[200] Without access to in-theater airfields at which to base US tactical aircraft or ports at which to offload heavy ground combat vehicles, equipment and supplies, the US military will need to rethink much of its current approach to power projection.

As sensor and precision-strike capabilities diffuse, both stationary and moving US ground vehicles will become progressively more vulnerable to detection and attack. Submunitions and terminal guidance system technologies are already proliferating. Given current technology diffusion trends, beyond 2015, there is a reasonable chance that potential adversaries could be armed with anti-armor submunitions that are at least comparable to those available to the US military today (e.g., SFW and the Brilliant Anti-Armor (BAT) system).

Emerging Maritime Area Denial Threats

Since the mobility of surface ships at sea will initially afford them some protection from detection and missile attack, the US Navy may be called upon to perform relatively more of the power projection mission over the next decade or so. The Navy's "Golden Age" of power projection from the sea might be cut short, however, by the ongoing proliferation of extended-range, anti-ship cruise missiles (ASCMs); very quiet diesel attack submarines (SSKs), including ones with air-independent propulsion (AIP) capability; and increasingly

[200] Vice Admiral Lowell E. Jacoby, Director, Defense Intelligence Agency, "Current and Projected National Security Threats to the United States," *Statement for the Record before the Senate Select Committee on Intelligence*, February 11, 2003, p. 16. See also: Jacoby, "Current and Projected National Security Threats to the United States," *Statement for the Record before the Senate Select Committee on Intelligence*, February 23, 2004, p. 10.

sophisticated sea mines.[201] The closer surface combatants come to enemy coasts in order to project power inland, the higher the density and severity of area-denial threats they will likely confront. For example, surface combatants operating a few hundred miles off an adversary's coast might have to contend primarily with limited numbers of extended-range ASCMs and AIP-capable attack submarines armed with wake-homing torpedoes, but within 100 miles they would be subject to attack by a multitude of air-, sea-, and ground-launched ASCMs, thousands of fixed and mobile "smart" mines triggered by different influences, and quiet submarines hidden in the high ambient noise of coastal waters.

Initially, instead of attacking aircraft carriers or major surface combatants directly, prospective adversaries may attempt to derail US maritime power projection by concentrating their attacks upon underway replenishment (UNREP) vessels. A single aircraft carrier consumes approximately 6,500 barrels of JP-5 fuel per day, and with limited onboard storage capacity, has to be refueled on a regular basis.[202] During Operation Desert Storm, for example, aircraft carrier fuel stores were typically replenished about every three days.[203] The turbine-driven power plants of major surface combatants (e.g., destroyers, cruisers, and frigates) are also voracious consumers of fuel.

---

[201] In Senate testimony in February 2003, the director of DIA cautioned, "I am especially concerned about the global availability of affordable and effective anti-surface ship systems (cruise missiles, submarines, torpedoes, naval mines), and a number of other long-range interdiction and area denial technologies." Vice Admiral Lowell E. Jacoby, "Current and Projected National Security Threats to the United States," p. 16. See also: Robert Holzer, "Dangerous Waters: Submarines, New Mines Imperil Ill-Prepared U.S. Fleet," *Defense News*, May 4-10, 1998, p. 1.

[202] See General Accounting Office (GAO), *Navy Aircraft Carriers – Cost Effectiveness of Conventionally and Nuclear-Powered Variants* (Washington, DC: GAO, August 1998), Appendix III-Underway Replenishment Extends the Endurance of Carriers, p. 2.

[203] During Operation Desert Storm, each aircraft carrier consumed about 5,000 barrels (or about 200,000 gallons) of aviation fuel per day. Without JP-5 resupply, carrier aviation would grind to halt in less than a week. Ibid., Appendix V – Operations of Carriers in the Persian Gulf War, pp. 5-6.

Today, the US combat logistic force fleet includes 13 active fleet oilers (T-AO-187 class) and eight fast combat support (AOE) ships. These massive ships, which displace over 40,000 and 50,000 tons, respectively, when fully loaded, have *no* self-defense capability.[204] Oilers, which regularly have to transit outside the protective coverage afforded by the battlegroup to replenish their fuel stores, would be vulnerable to attack while shuttling between known forward ports and the battlegroup. Even when under the defensive umbrella of the battlegroup, decoys used to draw missiles and torpedoes away from the carrier and its escorts, for example, might have the unintended effect of channeling them into high-signature, undefended AOEs.[205]

Anti-Ship Cruise Missiles

ASCMs present a multidimensional threat in that aircraft, surface ships, submarines, and ground-based TELs can all launch them. Since they are powered throughout their entire flight, ASCMs can follow a circuitous path, attacking a vessel at sea from multiple directions. Next-generation ASCMs that are not only longer in range, but also stealthier, faster, and more difficult to intercept than currently fielded systems are expected to become available on world markets within the decade.[206] As part of an assessment of the Navy's capability to defend

---

[204] As a consequence of the Navy's decision to move all of its combat logistics force ships to Military Sealift Command, the AOs were stripped of their limited self-defense capabilities several years ago and the AOEs are in the process of being disarmed. Prior to their conversion, the AOEs were equipped with the Sea Sparrow SAM system, two Phalanx Close-in Weapon Systems, a chaff ejection system, and a towed torpedo decoy.

[205] See Robert Work, "The Department of the Navy and Assured Access: A Critical Risk Assessment," in *Meeting the Anti-Access and Area-Denial Challenge* (Washington, DC: CSBA, 2003), pp. 52-54, 61-62.

[206] Richard Scott, "Global Developments in the ASCM Threat," *Jane's Intelligence Review*, June 2000, pp. 52-55. See also Robert Holzer, "Faster, Craftier Cruise Missiles Bode Ill for U.S. Ships," *Defense News*, May 28-June 3, 2001, p. 36; Robert Holzer, "Deadlier Missiles Threaten Naval Defenses," *Defense News*, July 7, 1999, p. 6; and Naval Studies Board, *Naval Forces' Capability for Theater Missile Defense* (Washington, DC: National Academy Press, 2001).

against modern ASCMs, the General Accounting Office (GAO) characterized the emerging ASCM threat as follows:

> Current anti-ship cruise missiles are faster, stealthier, and can fly at lower altitudes than the missile that hit the *U.S.S. Stark* in 1987, killing 37 sailors....The next generation of anti-ship cruise missiles—most of which are now expected to be fielded by 2007—will be equipped with advanced target seekers and stealthy design. These features will make them even more difficult to detect and defeat.[207]

Weapons sales and technology transfers over the last several years appear to support this assessment. Russia, for example, has reportedly already sold Kh-35 Uran technology (also referred to as Kayak) and SS-N-22 Sunburn (Moskit) ASCMs to China.[208] The former is essentially a Russian version of the US Harpoon system and has a range of about 130-140 kilometers. The latter has a similar range and attacks its target at faster than Mach 2, while making rapid (up to 15-g) turns to evade ship defenses.[209] In a joint venture with India, Russia completed development of a new supersonic ASCM, referred to as the Yakhont (3M-55 Onix), which will probably be available for export within the next few years.[210] This missile has an estimated

---

[207] GAO, *Defense Acquisitions: Comprehensive Strategy Needed to Improve Ship Cruise Missile Defense* (Washington, DC: GAO, July 2000), GAO/NSIAD-00-149, pp. 5-13.

[208] Dmitriy Safonov, "Moskit Has Been Completely Declassified. The Chinese Navy Will Get Unique Russian Missile," *Moscow Kommersant-Daily* (as translated by FBIS), April 14, 1998, p. 2.

[209] The SS-N-22 uses an active radar seeker and carries a 300-kg warhead. China is also reportedly interested in buying sea-skimming 3M54 Alfa ASCMs from Russia that have an effective range of about 300 km. See Yihong Zhang, "China to Acquire Anti-Ship Missiles," *Jane's Defence Weekly*, February 21, 2001; Yihong Zhang, "China Negotiates to Buy Advanced Russian Anti-Ship Cruise Missile," *Jane's Defence Weekly*, August 9, 2000.

[210] The Yakhont appears to be a scaled down variant of the SS-N-19 Shipwreck and SS-NX-26 Onix ASCMs developed by the Soviet Union during the 1980s. As part of the joint venture, India has reportedly helped fund the overall research and development effort and was responsible for developing the

range of 300 kilometers, flies as fast as 750 meters per second, and skims as close as five meters above the water during the terminal phase.[211] Capitalizing on the transfer of technology from Russia, India tested an indigenously developed variant of the Yakhont called the "BrahMos" in 2002.[212]

Capitalizing on a series of technology transfers over the last two decades, primarily from Russia, China has developed three different families (i.e., the FL-, HY-, and C-series) of ground-, sea-, and air-launched ASCMs. It has recently started fielding a standoff, air-launched ASCM called the C-803, which has a range of 250 kilometers (or beyond the range of most of the US Navy's current surface-to-air missiles).[213] China has, in turn, transferred advanced ASCM-related technology to Iran.

With nearly two decades of ASCM manufacturing experience and technical assistance from China and North Korea, Iran can now indigenously produce variants of nearly every Chinese ASCM, including the 120-km range, sea-skimming, turbo-jet powered C-

---

missile's guidance system and software. Russia may package Yakhont ASCMs with Kondor-E radar surveillance satellites as an integrated reconnaissance-strike system. See Michael Jasinski, "Russian and India Step Up Cruise Missile Co-Operations," *Jane's Intelligence Review*, March 2002, pp. 34-36; Steven Zaloga, "Precision Strike Key to U.S. Force Projection," *Aviation Week & Space Technology*, January 14, 2002, p. 179; and Richard Scott, "Russia's 'Shipwreck' Missile Enigma Solved," *Jane's Defence Weekly*, September 5, 2001, p. 28.

[211] The Yakhont ASCM uses an active/passive radar seeker for end-game target acquisition. Richard Scott, "Russia's Anti-Ship Missile Developments," *Jane's Defence Weekly*, August 30, 2000, p. 26. Russian firms hope to tap into what they estimate to be a $10-12 billion market for anti-ship cruise missiles through 2005. Douglas Barrie, "Precision Pursuit," *Aviation Week & Space Technology*, September 8, 2003, p. 51; and Nikolai Novichkov, "Russian Anti-Ship Missile Targets Multi-$B Market," *Jane's Defence Weekly*, June 9, 1999, p. 13.

[212] Bulbul Singh, "India's BrahMos Cruise Missile Has Successful Second Test," *Aerospace Daily*, April 30, 2002.

[213] John Hill, "China's Armed Forces Set to Undergo Face-Lift," *Jane's Intelligence Review*, February 2003, p. 15.

801/802.[214] Iran recently began production of a new sea- and ground-launched ASCM, dubbed the Ra'ad (Thunder), which is reported to have a range approaching 350 kilometers and may be equipped with an advanced active-radar terminal seeker.[215]

When it comes to ASCM defense, the US Navy's strong preference, for obvious reasons, is to "shoot the shooters" before they get into striking range of the fleet with their quivers of ship-killing "arrows." With the diffusion of long-range ASCMs that can be launched beyond the range of most projected US anti-ship and surface-to-air missiles, it may become increasingly necessary to "shoot down the arrows." Defending against early-generation ASCMs like the ubiquitous HY-2 Seersucker and its variants is already a very demanding task. In the event that future ASCM attacks are characterized by large numbers of stealthy, sea-skimming missiles, maneuvering at supersonic speeds, and approaching from multiple directions simultaneously, as current trends suggest, it will be considerably more difficult.

Currently planned US cruise missile defense systems (e.g., the Rolling Airframe Missile, the Phalanx Close-in Weapon System and the Sea Sparrow Surface Missile System) may not be up to the task. Defense against barrages of high-altitude ballistic missiles and low-altitude, multi-aspect, stealthy cruise missiles could be particularly challenging. According to the GAO, several major classes of US surface ships will have, at best, a low to moderate capability to defend

---

[214] The Chinese FL-6, FL-8, FL-9, C-801, C-802, and HY-2 are manufactured in Iran as the Fajr-e-Darya, Kosar, Nasr, Karus, Tondar, Noor ASCMs, respectively. Scott Jones, "Ra'ad Cruise Missile Boosts Iran's Military Capability," *Jane's Intelligence Review*, April 2004, pp. 34-35; Robert Hewson, "Iran Ready to Field Maritime Cruise Missile," *Jane's Defence Weekly*, February 24, 2004, p. 13; and Douglas Barrie, "Iranian Lightweight," *Aviation Week & Space Technology*, February 23, 2004, p. 40.

[215] Some reports indicate the Ra'ad ASCM may be fitted with a dual-mode seeker, combining both radar and infrared homing. The Ra'ad missile incorporates an indigenously developed turbo-jet engine into a modified HY-2 airframe. Hewson, "Iran Ready to Field Maritime Cruise Missile," p. 13; Jones, "Ra'ad Cruise Missile Boosts Iran's Military Capability," pp. 34-35; and Douglas Barrie, "Iranian Cruise Effort," *Aviation Week & Space Technology*, February 2, 2004, p. 45.

themselves against 2012-class cruise missile threats.[216] Even a very low "leaker" rate for future ASCM defenses would likely be problematic because ships at sea cannot absorb repeated hits with modern high-explosive warheads. A few successful missile strikes, or even a single well-placed one, could permanently knock a major surface combatant out of action.

Advanced Diesel-Electric Submarines

While the overall number of submarines is decreasing worldwide, owing in large part to the collapse of the former Soviet fleet, the overall trend is toward quieter, longer-endurance submarines armed with more lethal weapons (e.g., wake-homing torpedoes and advanced ASCMs) and equipped with increasingly sophisticated sensor suites and battle management systems.[217] Over the last decade, Russia has fueled the proliferation of SSK technology by exporting Kilo-class submarines and related-technology to several countries including China, India and Iran.[218]

India currently operates ten Kilo-class submarines and is upgrading several of them with the capability to launch submarine-launched cruise missiles (SLCMs).[219] India reportedly plans to purchase an additional 20 submarines over the next decade, including up to 12 French-built Scorpene-class boats armed with Exocet

---

[216] GAO, *Defense Acquisitions: Comprehensive Strategy Needed to Improve Ship Cruise Missile Defense*, p. 13. See also: Owen Coté, "Assuring Access and Power Projection," *Conference Report*, MIT Security Studies Conference Series, Summer 2001, pp. 31-32.

[217] See Richard Scott, "Submarines Stay the Course," *Jane's Defence Weekly*, October 18, 2000, pp. 32-38.

[218] Other countries operating Kilo-class submarines include Algeria, Poland, and Romania.

[219] At least four of India's Kilo-class submarines have been retrofitted in Russia to operate the Alfa or "Club" SLCM system, which has an effective range of about 180 kilometers. India is also in the process of introducing its PJ-10 BrahMos cruise missile, which can be used to strike both land targets and surface ships, aboard its submarines. See Joris Janssen Lok, "Russian's Amur Diesel Electrics will Follow Kilo Class in Hunt for Exports," *Jane's International Defense Review*, June 2002, p. 68.

ASCMs.[220] China is likewise modernizing its submarine fleet. It purchased four Kilo-class diesel-electric attack SSKs from Russia, which are armed with wake-homing torpedoes, and contracted in June 2002 to buy eight more over the next several years.[221] The new lot of Kilo-class submarines (Project 636) will reportedly be armed with Russian-made 3M-54E ASCMs, heavyweight torpedoes, and the 53-65KE wake-homing torpedoes.[222] There is also a remote possibility that Russia may sell the even more advanced Akula-class, nuclear-powered attack submarine (SSN), or related technology, to China.[223]

Benefiting from substantial technology transfers from Russia, France, Israel, and Germany, China also continues to improve its rapidly growing fleet of indigenously built submarines. The long-awaited Song-class SSK, which is now in serial production, reportedly incorporates an anechoic rubber tile coating for sound dampening, a skewed propeller for enhanced propulsion, an encapsulated ASCM system for firing missiles while submerged, a flank-array sonar system

---

[220] J.A.C. Lewis, "India Set to Sign Scorpene Sub Deal," *Jane's Defence Weekly*, September 25, 2002, p. 3; and David Lague, "We All Live for Another Submarine," *Far Eastern Economic Review*, August 15, 2002, p. 14.

[221] Two of the four Kilos that are now operational are the export design Project 877 EKM and the other two are the more advanced Project 636 type, which were originally designed for the Soviet Navy. Under a deal estimated to be worth about $1.6 billion, all eight Project 636 Kilo-class SSKs are to be delivered by 2007 and will be equipped with Russian 3M-54E anti-ship cruise missiles. According to some sources, Project 636 SSKs are acoustically comparable to US Los Angeles-class SSNs. See Dr. Lyle Goldstein and William Murray, "China Emerges as a Maritime Power," *Jane's Intelligence Review*, October 2004; David Isenberg, "China Buys Russian Vessels to Mount Naval Challenge to U.S.," *Navy News & Undersea Technology*, November 18, 2002, p. 3; John Pomfret, "China to Buy 8 More Russian Submarines," *Washington Post*, June 25, 2002, p. A15; and Nikolai Novichkov, "China's Russian Kilo Buy May Put Song Submarine Future in Doubt," *Jane's Defence Weekly*, June 12, 2002, p. 3.

[222] DoD, *Annual Report on the Military Power of the People's Republic of China (2003)*, p. 7.

[223] Simon Saradzhyan, "Russia Ponders Selling Nuclear Submarines to China," *Defense News*, September 27, 1999, p. 26.

(probably of French design), and diesel engines of German origin.[224] The Song's control room is reportedly equipped with advanced flat-screen monitors for a 360-degree, "digital waterfall broadband sonar display" and a digital fire-control system.[225] Up to eight Song-class SSKs have been launched to date. In July 2004, to the surprise of the US intelligence community, the Chinese suddenly launched the first boat in a new submarine class, the Yuan. Although its basic hullform is similar to a Russian Kilo-class SSK, it incorporates some design features of the Song-class and the Russian Amur-class (e.g., a fin-mounted hydroplane) and appears to be outfitted with an advanced passive sonar system. The Yuan's detailed performance attributes and armament, however, are not yet known.[226] The first Chinese Type-093 SSN, which represents a dramatic improvement over its noisy predecessor, the Han-class, was launched in December 2002, the second in the class was launched in late 2003, and the third is under construction. The first Type-094 nuclear-powered ballistic missile submarine (SSBN) is under construction and is expected to carry up to 16 nuclear-armed JL-2 submarine launched ballistic missiles (SLBMs) with a range of 8,000 kilometers. Two or more Type-094 SSBNs are expected to be in service by 2010.[227]

Prospective US adversaries may also soon be able to acquire SSKs that take advantage of AIP systems and improved energy storage systems to extend their submerged endurance significantly. France, Germany, Italy, Pakistan, Russia, and Sweden all produce or plan to produce AIP submarines for export.[228] Relative to Soviet-era designs,

---

[224] DoD, *Annual Report on the Military Power of the People's Republic of China (2002)*, pp. 21–22.

[225] Goldstein and Murray, "China Emerges as a Maritime Power."

[226] Yihong Chang and Richard Scott, "New Submarine Picture Presents Chinese Puzzle," *Jane's Defence Weekly*, August 4, 2004, p. 8; and Goldstein and Murray, "China Emerges as a Maritime Power."

[227] According to some reports, the performance of the Type-093 SSN may be roughly comparable to first-generation, Los Angeles-class SSNs. Goldstein and Murray, "China Emerges as a Maritime Power," *Jane's Intelligence Review*, October 2004; and "Chinese Puzzle," *Jane's Defence Weekly*, January 21, 2004, p. 28.

[228] Nathan Hodge, "German Design Promises New Capabilities for Non-Nuke Subs," *Defense Week*, April 8, 2002, pp. 3, 9; Richard Scott, "Boosting the

diesel submarines now becoming available on the world market also benefit from lower levels of radiated noise; increased submerged speed; greater diving depth; anechoic coatings and hull designs that make them less detectable by active sonar; and improved sensors, weapons and battle management systems.[229] Russia, for example, may begin exporting its new Amur-class submarine, which is reported to have an acoustic signature that is only 10 percent of that generated by a Kilo-class SSK, which is itself a very quiet submarine when operated competently.[230]

Admittedly, the acquisition of state-of-the-art submarines does not necessarily translate into an effective operational capability. As with any complex weapon system, it takes time and effort to develop the skills needed to operate a submarine proficiently. It is sometimes argued that foreign navies face a particularly steep learning curve and will be unable to exploit the full potential of modern SSKs anytime soon. Putting aside the question of whether such arguments are rooted more in ethnocentrism than sound analysis, there are many other reasons to be cautious about dismissing this emerging threat.

First, today's submarines incorporate a number of technologies (e.g., automated battle management and fire control systems) that actually make them easier to operate than their predecessors. They are also being armed with user-friendly, fire-and-forget weapons, such as wake-homing torpedoes, that can overcome a significant amount of human error. DoD reported to Congress that "even crews with *minimal* proficiency" can employ wake-homing torpedoes

---

Staying Power of the Non-Nuclear Submarine," *Jane's International Defense Review*, November 1999, pp. 41-50; Richard Scott, "Power Surge," *Jane's Defence Weekly*, July 1, 1998, pp. 24-27; and Anthony J. Watts, *Underwater Warfare Systems 2000-2001* (United Kingdom: Jane's Defence Group, January 2000).

[229] David Foxwell, "Sub Proliferation Sends Navies Diving for Cover," *Jane's International Defense Review*, August 1997, p. 30. See also: Coté, "Assuring Access and Power Projection," pp. 23-25.

[230] Joris Janssen Lok, "Russian's Amur Diesel Electrics will Follow Kilo Class in Hunt for Exports," pp. 66-68.

effectively.[231] In short, owing in large measure to the falling price and growing computing power of microprocessors, information technology can partially compensate for a less than fully trained crew by US standards. While SSKs in the hands of relatively inexperienced crews might not pose a major threat to US submarines or surface combatants, they could wreak havoc with noisy sealift vessels, unarmed support ships (e.g., fleet oilers, mine countermeasure ships) and commercial shipping of all kinds. Especially in their home littoral waters and within regional maritime chokepoints, modern SSKs could pose a major area-denial threat in the 2015-2025 timeframe, if not considerably sooner. Second, several navies around the world are making tremendous strides with respect to the professionalism of their submarine personnel. In China, for example, the PLAN is aggressively recruiting technically competent university graduates for its submarine cadre, improving professional military education, and exploiting new training technologies (e.g. computer simulation).

Sea Mines

The number of countries with an offensive sea mining capability has risen by about 40 percent over the last decade.[232] More than 300 different types of mines are now available on the world market, a 75 percent increase since 1990.[233] Many countries are amassing large stocks of cheap, low-technology mines, which, if used properly, could be very disruptive to US power-projection operations. In addition, dozens of countries are investing in modern mines that are triggered by a wide-range of influences (e.g., magnetic, acoustic, seismic, underwater electric potential, or pressure) and incorporate other advanced technologies to improve their lethality, reliability and versatility.[234] By taking advantage of inexpensive microprocessors, for

---

[231] Emphasis added. DoD, Annual *Report on the Military Power of the People's Republic of China (2002)*, p. 22.

[232] Mark Hewish, "Sea Mines, Simple But Effective," *Jane's International Defense Review*, November 2000, p. 45.

[233] Ibid.

[234] The PLA Navy, for example, currently has a huge stockpile of sea mines comprising both vintage Soviet-era designs, as well as more modern mines with a variety of triggers. The variety of mines in China's stockpile include bottom and moored influence mines, mobile mines, remotely controlled

example, modern mines can classify and target specific classes of ships based on acoustic or other signatures. The National Academy of Sciences has estimated that, over the next twenty years, the Navy is likely to confront "smart mine fields" in which diverse kinds of mines—bottom, floating, moored, or propelled and guided—might be controlled by a system of networked sensors that can trigger specific mines in a sequence that would inflict maximum damage on a approaching fleet or shipping train.[235]

Suppliers are also making mines more difficult to detect by crafting irregular-shaped designs, applying anechoic coatings, equipping them with self-burying capabilities, and constructing them of non-magnetic, composite materials. Moreover, a handful of countries, including China, are reportedly developing mines with small motors that enable them to move a short distance at random intervals, which would obviously make mine hunting and mapping even more difficult.[236] With mobile mines, a "cleared" route that was safe one hour could become hazardous the next. The US Navy's Mine Warfare Plan summarized the emerging mine threat as follows:

> Many of these [modern mines] are equipped with microprocessor-controlled target detection devices [TDDs], ship counters, remote control, and delayed arming mechanisms, as well as sweep obstructors to thwart attempts at identification and neutralization.

---

mines, command-detonated mines, and propelled-warhead mines, which are potentially effective in deep waters. China has developed rocket-propelled rising mines and is thought to have developed an acoustically activated remote control system for at least one type of mine. The PLAN is also interested in acquiring submarine-launched, mobile, bottom mines. China is reported to be exporting sea mines widely. DoD, *Annual Report on the Military Power of the People's Republic of China (2003)*, p. 27; and DoD, *Annual Report on the Military Power of the People's Republic of China (2002)*, p. 15.

[235] National Academy of Sciences, *Technology for the United States Navy and Marine Corps, 2000-2035* (Washington, DC, National Academy Press, 1997), Vol. 1, Chapter VII, p. 22 (electronic version). See also: Robert Holzer, "U.S. Navy Seeks Ways to Counter Threat of Mines," *Defense News*, November 10-16, 1997, p. 12.

[236] Mark Hewish, "Sea Mines, Simple But Effective," p. 46.

> Furthermore, microprocessor-controlled TDDs can be used to upgrade obsolescent mines at a fraction of the cost of new mines. Improved sensors, propulsion systems, and deployment methods are also increasing the lethality, versatility, effective range, and countermeasure resistance of propelled warhead mines. All of these technologies are readily available for export.[237]

To further complicate counter-mine operations, adversaries could guard minefields with a few SSKs or, at some point, torpedo-armed UUVs that could quietly patrol for noisy, easy-to-detect mine counter-measure ships. It would be challenging for friendly forces to conduct ASW and countermine operations simultaneously owing to acoustic interference problems. As a result, modern mine networks guarded by SSKs and UUVs could be a very potent area-denial combination that would be difficult to roll back quickly.

Although mine counter-measure technologies have also improved over the last several decades, they appear to be lagging behind the development and diffusion of offensive mining capabilities. Detecting, identifying, and neutralizing mines in littoral waters—especially those in very shallow waters (i.e., less than 40 feet) and in the surf zone (i.e., less than 10 feet)—appears to be becoming more, rather than less difficult. Moreover, the availability of more accurate positional location information with GPS has had the unintended consequence of making offensive mining operations easier and more effective.

The Extending Reach and Sophistication of Air Defenses

The emergence of more capable integrated air defense systems (IADS) over the next two decades will likely present a growing threat to non-stealthy fighters and bombers, manned and unmanned reconnaissance

[237] Office of the Chief of Naval Operations, *U.S. Naval Mine Warfare Plan – Programs for the New Millennium* (Washington, DC: U.S. Navy, 1999), Appendix A.

aircraft, and strategic mobility aircraft (i.e., refuelers and transports). Many potential adversaries are upgrading legacy air defense systems with advanced electronics and signal processing capabilities.[238] They are also seeking to make them more resistant to suppression through increased exploitation of passive sensors (e.g., signals intelligence and infrared tracking), multistatic configurations, and robust C3 links (including fiber optics).

In addition, the effective range of SAM interceptors available on the world arms market is steadily increasing. Variants of the Russian-built SA-10/20 and other "double-digit" SAMs, which can intercept non-stealthy aircraft at extended range and are difficult to disable with electronic countermeasures, are expected to proliferate over the coming decade.[239] The SA-10E (S-300PMU2 Favorit) has an effective range of nearly 200 kilometers and the newly developed export model, the S-400 Triumph, reportedly has a range of up to 400 kilometers and incorporates advanced electronic counter-countermeasures.[240] These systems can intercept non-stealthy, land-attack cruise missiles (e.g., TLAMs) and, under some circumstances, may also pose a limited threat to current generation stealth aircraft.[241] China, among other prospective adversaries, has purchased SA-10, SA-15, and SA-20 air

---

[238] Mohammed Ahmedullah, "Russia Upgrades SAMs to Fight NATO Planes," *Defense Week*, October 2000, p. 16; David Fulghum, "Upgrades Increase Air Defense Threat," *Aviation Week & Space Technology*, March 15, 1999, p. 55; and David Fulghum, "Improved Air Defenses Prompt Pentagon Fears," *Aviation Week & Space Technology*, July 6, 1998, pp. 22-24.

[239] Mark Hewish and Charles Gibson, "Into The Valley of Death," *Jane's International Defense Review*, October 2001, pp. 34-40; and John A. Tirpak, "The Double-Digit SAMs," *Air Force Magazine*, June 2001, pp. 48-49.

[240] David Fulghum and Robert Wall, "Russia's Top Designers Claim Anti-Stealth Skills," *Aviation Week & Space Technology*, October 8, 2001, pp. 82-83; and Christopher Foss, "Russia's S-400 Missile Tests Near Completion," *Jane's Defence Weekly*, June 2, 1999, p. 12.

[241] For instance, according to some reports, the S-300PMU2 can detect some stealthy aircraft at a range of 50-60 miles. David Fulghum and Robert Wall, "Russia's Top Designers Claim Anti-Stealth Skills," *Aviation Week & Space Technology*, October 8, 2001, p. 83.

defense systems.[242] While these Russian systems are currently very expensive, and thus beyond the financial reach of most countries, more affordable, reversed-engineered versions will likely be produced and exported by China and others within the next 10 years.

Foreign militaries are learning how to better protect their air defense systems from attack. Having witnessed the rapid dismantling of Iraq's relatively modern air defense network during the first Gulf War, militaries are taking advantage of mobility and C3D2 techniques to reduce the vulnerability of their air defense assets. During Operation Allied Force in 1999, for example, Serbian forces routinely moved SAM launchers (mostly SA-3s and SA-6s) and radars every few hours to evade detection, turned radars on and off sporadically, used smoke to obscure targets, exploited camouflage (e.g., burying missile launchers in haystacks), and made extensive use of a wide range of decoys. These measures proved effective. Of Serbia's 25 known mobile SA-6 batteries, only three were reportedly destroyed over the course of the war.[243]

Finally, the diffusion of advanced man-portable air defense systems (MANPADS) such as the French *Mistral*, Russian *Igla*, Chinese FN-6, and Pakistani *Anza* systems will likely exacerbate the "close in" air threat. While far less capable than "double-digit" SAMs, these man-portable units are affordable enough to buy in quantity and can be easily dispersed and hidden, which makes them very difficult to

---

[242] In September 2004, China finalized its fourth major purchase agreement for the S-300 family of air defense missile systems, export variants of the Russian-built SA-10/20. For close to $1 billion, it will receive a vehicle-mounted battle management post, an S-band acquisition radar with an effective range of 300 kilometers, and eight firing batteries—each comprising a multi-purpose illumination and guidance radar (X-band); an all-altitude target designation radar with a multiple-beam, phased-array antenna; and eight launcher units armed with four missiles apiece (plus reloads). This purchase follows the 1993 contract for 32 self-propelled launchers and 384 missiles (128 in transport and launch containers, 256 in reserve), the 1994 contract for 32 launchers and 196 missiles, and the 2004 contract for 32 launchers and 198 missiles. Jiang Jintao, "China Becomes First Export Customer for S-300 PMU2," *Jane's Defence Weekly*, September 1, 2004, p. 7.

[243] Ben Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Perspective* (Santa Monica, CA: RAND, 2001), p. 111.

suppress or eliminate. Especially when cued by early-warning radars, widely dispersed troops equipped with modern MANPADS could present a significant anti-access threat to low-flying aircraft and helicopters.

Emerging Information- and Space-Denial Capabilities

Radio-frequency (RF) weapons and IW attacks could be used to deny US forces unimpeded access to the electromagnetic spectrum, as well as to degrade the overall performance of US C4ISR capabilities. ASATs, jammers, and other offensive "space control" capabilities could be used to deny or degrade US access to imagery satellites, COMSATs, GPS, and other space-based assets.

Active Information Denial

RF weapons, including both narrow-band, high-power microwave (HPM) devices and broadband Transient Electromagnetic Devices (TEDs), disrupt, damage or destroy electronic equipment by releasing very short, but powerful pulses of energy (i.e., billions of watts within nanoseconds).[244] These "spikes" of energy offer a potentially potent means for burning out the sensitive electronic equipment upon which

[244] HPM systems radiate a short, but continuous wave of energy over a relatively narrow band. They are most effective when tuned to the target's operating frequency or specific frequencies that exploit known "backdoor" vulnerabilities. TEDs generate a short burst (i.e., measured in 100s of pico-seconds) of energy with a very high peak power that occupies a very large spectrum space (e.g., 100 MHz to several GHz). Mr. David Schriner, "The Design and Fabrication of a Damage Inflicting RF Weapon by 'Backyard' Methods'," Testimony before the Joint Economic Committee of the U.S. Congress, February 25, 1998 [http://www.fas.org/irp.congress.1998_hr/s980225ds.htm]. See also: Carlo Kopp, "The Electromagnetic Bomb – A Weapon of Electrical Mass Destruction," available online at http://www.globalsecurity.org/military/library/report/1996/apjemp.htm; and Curt Weldon (chairman), Hearing on EMP Threats to U.S. Military and Civilian Infrastructure, House Armed Services Subcommittee on Military Research and Development, October 7, 1999.

the US military depends.[245] Unhardened computers, communications equipment, and sensor systems (e.g., radar) are particularly vulnerable to RF weapons. They can be attacked directly through antennas or other sensor openings, which is referred to as a "front door" strike, or through the "back door" via coupling with telephone wires, power lines, network cabling, and cooling and ventilation grills.

While the key enabling technologies for RF weapons (e.g., explosively pumped flux compression generators, magneto-hydrodynamic generators, virtual cathode oscillators, electron accelerators, and spark-gap switches) have been available for many years, in some cases, for several decades, worldwide interest in them has surged recently. Several countries, including Russia, China, and France, are aggressively pursuing development of RF weapons.[246] A Russian firm, *Rosoboronexport*, is marketing a mobile HPM system, which they call a "radio frequency canon," called Ranets-E that can supposedly disable the electronics of PGMs at ranges up to 10 kilometers.[247] While China probably does not have a high-power RF weapon deployed at this time, DoD estimates that: "Within the next decade, China may be able to develop and field air defense RF weapons intended to defeat missiles or aircraft by targeting the electronics in guidance, altimeter, fire-control, communications, navigation, and other critical subsystems."[248] The PLA probably also

---

[245] David Ruppe, "Emerging Threat: Radio Frequency Weapons," *Defense Week*, March 2, 1998, p. 1; David Fulghum, "Microwave Weapons Await a Future War," *Aviation Week & Space Technology*, June 7, 1999, p. 30; and Roger Fontaine, "EMP's No Longer Science Fiction," *Washington Times*, July 14, 1997, p. 10.

[246] Ibid. See also: Ruppe, "Emerging Threat: Radio Frequency Weapons," p. 13.

[247] The Ranets-E system is available in both mobile and fixed versions. It reportedly has an output power of 500 megawatts, operates in the centimeter-wave band, and emits pulses 10-20 nanoseconds long. See Nikolai Novichkov, "Russia Plans to Export Non-Lethal Beam Weapon," *Jane's Defence Weekly*, November 21, 2001, p. 18; and Mohammed Ahmedullah, "Russia Unveils Radio-Frequency Arms," *Defense Week*, December 10, 2001, pp. 1, 15.

[248] DoD, *Annual Report on the Military Power of the People's Republic of China (2002)*, p. 34.

has a program in place to develop explosively driven RF warheads suitable for use in missiles and gravity bombs.[249]

The apparent diffusion of RF weapons is especially troubling because in recent years the US military has started to rely more upon unhardened COTS components and equipment to reduce costs, especially in the information-technology area.[250] Emerging very-short-pulse RF weapons (i.e., pulse durations measured in nanoseconds or less) may be able to defeat even "hardened" military systems designed to survive nuclear electromagnetic pulse (EMP) effects and lightening strikes.[251]

Adversaries could also conduct IW attacks not only against the US military's C4ISR networks, but also against critical, information-dependent, civilian infrastructures with the US homeland. Several prospective US adversaries—including China, Iran, and North Korea—are investing in computer network attack (CNA) and other offensive

---

[249] DoD, *Annual Report on the Military Power of the People's Republic of China (2003)*, pp. 9, 38.

[250] Semiconductors, which operate at very low voltages (3-5 volts), are very sensitive, for example, to voltage spikes produced by EMP weapons. Furthermore, the heat generated within a semiconductor when exposed to EMP-induced currents may not be able to dissipate quickly enough, especially at small junction areas within the semiconductor, to avoid permanent damage from overheating.

[251] According to an expert on RF weapons from the US Army's Space and Missile Defense Command: "[T]here is an increasing variety of equipment capable of generating very short RF pulses that are capable of disrupting sophisticated electronics. These pulses are not addressed by current design standards and will challenge existing front-end RF protection and other forms of EMI [electromagnetic interference] protection. New capabilities are needed to reject high-power, very-fast RF pulses and to minimize their effect on systems. We believe that common EMI and EMP mitigation techniques will not provide adequate protection against nanosecond and sub-nanosecond pulses from future radio frequency weapons, since active mitigation device response times are typically several nanoseconds to microseconds." Dr. Ira Merritt, "Proliferation and Significance of Radio Frequency Weapons Technology," Statement before the Joint Economic Committee of the U.S. Congress, February 25, 1998.

IW capabilities.[252] As will be elaborated upon later in this monograph, since the financial and technical barriers to developing such capabilities are comparatively low, it stands to reason that both state and non-state actors alike will likely pursue this element of the RMA in the years ahead. As George Tenet, then Director of Central Intelligence, testified to Congress in 2000:

> A surprising number of information warfare-related tools and "weapons" are available on the open market at relatively little cost....Already, we see a number of countries expressing interest in information operations and information warfare as a means to counter U.S. military superiority. Several key states are aggressively working to develop their IW capabilities and to incorporate these new tools into their warfighting doctrine....Information warfare has the potential to be a major force multiplier.[253]

---

[252] Bill Gertz, "Military Fears Attacks From Cyberspace," *Washington Times*, March 29, 2001, p. 3.

[253] George J. Tenet, "The Worldwide Threat in 2000: Global Realities of Our National Security," *Testimony before the Senate Select Committee on Intelligence*, February 2, 2000. Available on-line at http://intelligence.senate.gov/0002hrg/000202/tenet.htm. Similarly, the Defense Intelligence Agency has concluded that "numerous potential foes are pursuing information operations capabilities as a relatively inexpensive means to undermine domestic and international support for U.S. actions, to attack U.S. national infrastructures, or to challenge our information superiority. The threat from information operations will expand significantly during the next decade or so. . .Software tools for network attack, intrusion, and disruption are globally available over the Internet, proving almost any interested U.S. adversary a basic computer network exploitation and attack capability." Vice Admiral Thomas Wilson, "Global Threats and Challenges," *Statement before the Senate Select Committee on Intelligence*, February 6, 2002, p. 7. See also: Vice Admiral Thomas Wilson, "Global Threats and Challenges," *Statement before the Senate Armed Services Committee*, March 19, 2002, p. 15; and Vice Admiral Lowell E. Jacoby, Director, Defense Intelligence Agency, "Current and Projected National Security Threats to the United States," *Statement for the Record before the Senate Select Committee on Intelligence*, February 23, 2004, p. 11.

While it is unclear how the competition between various offensive and defensive IW capabilities will turn out, network-on-network warfare will almost certainly be a central feature of future, high-end warfare.

Space Denial

As will be addressed in more depth in an upcoming discussion on the emerging competition between space access and space control, future adversaries may develop myriad means for contesting the freedom of operation in space now enjoyed by the US military. The Defense Intelligence Agency has characterized the space denial threat between now and 2015 as follows:

> The U.S. reliance on (and advantages in) the use of space platforms is well known by our potential adversaries....By 2015, future adversaries will be able to employ a wide variety of means to disrupt, degrade, or defeat portions of the U.S. space support system. A number of countries are interested in or experimenting with a variety of technologies that could be used to develop counter-space capabilities. These efforts could result in improved systems for space object tracking, electronic warfare or jamming, and directed energy weapons.[254]

Multidimensional Anti-Access: Implications for Defense Planning

While they are diffusing at different rates, the capabilities summarized earlier in Table 3-1 are gradually finding their way into the hands of potential US adversaries. As a result, they will become better able to deny US forces access into a theater of operations and the ability to

[254] Vice Admiral Wilson, *Statement before the Senate Select Committee on Intelligence*, 2001, p. 6. In testimony before the Senate Armed Services Committee in March 2002, Admiral Wilson moved up the timeline for the emergence of such counter-space capabilities to 2010. See Vice Admiral Thomas Wilson, "Global Threats and Challenges," *Statement before the Senate Armed Services Committee*, March 19, 2002, p. 17.

operate in littoral waters at an acceptable level of risk, as well as to prevent US forces from freely exploiting near-earth space and the information sphere. Over the next 10-15 years, the operational impact of these emerging anti-access and area-denial threats may be limited to making US power projection operations more difficult, time consuming, and costly in terms of both casualties and material resources. Assuming current proliferation and technology diffusion trends continue, however, the traditional US approach to power projection could be completely up-ended by 2020, if not sooner.

Assuming that the United States wishes to continue wielding the same amount of military influence abroad as it does today, it will likely need to adopt new means for projecting power and controlling the various dimensions of the battlespace. Promising approaches for doing so will be discussed in the next chapter, including the following:

- Extended-range, increasingly unmanned, stealthy air operations;
- Increased use of special operations forces (SOF), and information-intensive, highly roboticized, ground force operations that place a premium on signature management;
- Submerged power projection;
- Maritime surface operations that rely on networked, stealthy, surface combatants—both manned and unmanned;
- Offensive and defensive space control operations;
- Offensive and defensive IW; and
- New types of defensive BW operations.

INCREASED CAPABILITIES FOR PREEMPTION VERSUS DENIAL

The diffusion and continued maturation of offensive capabilities that are stealthy, long-range, rapid, and increasingly lethal could substantially increase both capacity and incentive for preemptive attack. Examples include the following:

- Stealthy, long-range missiles and other precision strike capabilities (e.g., sub-orbital strike systems) that can strike rapidly, without warning, and are difficult to defend against;

- IW and BW capabilities that can be developed and employed covertly; and

- Directed-energy weapons that can strike at the speed of light.

By increasing the prospect of successfully surprising adversaries and elevating the magnitude of anticipated damage, these types of capabilities would likely increase the attractiveness of preemption strategies.[255] A preemptive strategy, for example, might involve massive missile barrages on the armed forces and critical national infrastructure of a neighboring state as a precursor to invasion. These attacks might be supported by a series of offensive IW strikes and advanced BW attacks initiated in "peacetime."[256] By striking first, the aggressor would not only have a chance of at least partially knocking out an adversary's retaliatory capabilities, but could also significantly degrade its defensive capabilities as well. Simultaneous attacks against airfields, ports, military garrisons, C3 nodes, the electrical power grid,

[255] Similarly, during the Cold War, the combination of long-range strike capabilities (e.g., long-range ballistic missiles and bombers) armed with nuclear warheads created powerful incentives for preemption. Mutual fear of adversarial preemption led the United States and the Soviet Union to implement a myriad of costly offsetting measures such as erecting distant early-warning radar networks; sustaining continuous airborne bomber alerts; developing solid rocket motors so that it would be possible to launch ballistic missiles more quickly (i.e., before enemy missiles struck); building super-hardened missile silos and mobile missile launchers; increasing reliance on difficult-to-find submarines for deterrence; and developing, fielding, and operating ballistic missile defenses. While the United States seriously contemplated atomic preemption against the growing Soviet threat following the end of World War II, it was deterred first by Soviet ground force superiority in Europe and, after August 1953, by the retaliatory threat posed by Soviet thermonuclear weapons.

[256] Computer Network Attack (CNA) tools could be inserted secretly into the targeted state's C4ISR systems during peacetime and triggered once hostilities began. Similarly, BW agents or vectors could be introduced clandestinely into the targeted state's population several days before an overt attack commenced.

and other supporting infrastructures could rapidly and seriously undermine the targeted state's ability to mount either offensive or defensive military operations.

These strikes might also coincide with a preemptive attack against pre-positioned equipment, forward presence forces, and space assets belonging to the targeted state's allies to undermine their ability to mount an effective extended-range defense. While the targeted state and its allies were still reeling from these initial "bolt from the blue" strikes, the aggressor could potentially follow-up with rapid air, sea, and ground assaults oriented on key nodes or other valuable terrain. Having achieved a fait accompli, the aggressor state could then pursue an anti-access/area-denial strategy to prevent opposing forces from restoring the status quo ante.

Conversely, from the moment hostilities began, allies of the targeted state could attempt to derail the aggressor's power-projection efforts by attacking its invading forces with extended-range, precision strikes (e.g., cruise missiles launched from ships at sea) and survivable, rapid-response, power-projection capabilities (e.g., stealthy bombers and UCAVs launched from peripheral bases). The effectiveness of such a conquest-denial strategy could also be enhanced significantly by providing threatened allies with survivable anti-access capabilities of their own during peacetime. Long-endurance UAVs equipped with modular sensor payloads, UGS networks, and various types of maritime sensor networks (e.g., active and passive sonar arrays) could provide early warning of an attack and improve the effectiveness of defensive systems by cuing them to specific avenues of attack. Active defenses might include, for example, ballistic and cruise missile interceptors, long-range SAMs, MANPADS, ASCMs, and diesel-electric attack submarines. Threatened allies might also be armed with a large inventory of brilliant mines, as well as a survivable, mine-laying capability (e.g., AIP submarines). Bristling with such weapons, a relatively weak state in terms of offensive striking power would probably appear much less appetizing to bellicose neighbors. While this "porcupine strategy" might not deter a determined aggressor state from attacking, it would increase the price of conquest significantly and slow down an aggressor's invasion timetable. With more time available, allies of the targeted state might be able to mount a more successful defense—precluding the attack from rapidly achieving a fait accompli.

In short, future power-projection operations could be conducted in the face of opposing denial strategies. Consider, for example, two major RMA powers vying over a less powerful state—one seeks to annex the weaker state, while the other hopes to defend it. Assuming that both major powers had long-range, precision-strike capabilities secured within their homeland, each could potentially deny the other from achieving their respective war aims by holding at risk key economic and political infrastructure in the contested state. In most circumstances, the aggressor could be denied the spoils of war with a relatively low level of force. A few missile strikes now and again could prevent the aggressor from tapping the economic potential of the "conquered" state. Precision strikes could, for example, make it impractical to export valuable commodities or import needed natural resources (e.g., energy). Oil and gas pumping stations and pipelines could easily be rendered unusable. At the same time, however, the aggressor could use the same means to prevent the defender from restoring critical utilities and reestablishing local government control in the beleaguered state.

Thus, increased opportunities for preemption notwithstanding, denial strategies may actually prove more powerful and could make war termination very difficult. As will be explored later, frustration stemming from an inability to attain war aims could carry with it the risk of vertical or horizontal escalation. Adversaries may also be more likely to employ coercion strategies, which could, paradoxically, be more difficult to deter and counter than the overt use of force.

HIDERS VERSUS FINDERS

The side that is better able to find, track, and target the opposing side's forces will have an enormous advantage in future conflicts. Given current trends in sensor and data-processing technologies, the ability to find opposing forces (and the corresponding ability to destroy or neutralize what one can find) seems almost certain to increase dramatically over the next two decades. In response, an increased emphasis will likely be placed on stealth, decoys, jamming, offensive IW, and other forms of information protection. Meanwhile, the value of traditional physical protection (e.g., armor and active defenses) could erode over time.

As mentioned earlier in our discussion of emerging anti-access challenges, over the next 20 years, the battlespace is likely to become more transparent. Sensor systems will continue to become smaller, cheaper, and more capable owing, in no small part, to the steadily dropping cost and increasing performance of microprocessors. Signal processing, in particular, has benefited tremendously from the semiconductor industry's success in upholding "Moore's law." Although only a few militaries have access to today's state-of-the-art signal processing algorithms, they will become both more widely available and more powerful by 2015-2025. Myriad sensor systems will also mature and proliferate over this time horizon. Commonly available sensors might include, for example, the following:

- High-range-resolution (HRR) radar systems with the ability to track and accurately classify moving targets;

- Foliage penetration (FOPEN) radar systems that can reliably find and track combat vehicles hiding under trees or other vegetation;[257]

- Hyperspectral imagery (HSI) systems that can not only detect the presence of specific materials on the battlefield (e.g., kevlar), but also reduce the effectiveness of traditional C3D2 measures;

- LADAR and Light Detection and Ranging (LIDAR) systems that can form high-resolution, three-dimensional images of suspected targets;

---

[257] It might also be possible to map trails and roads that are concealed beneath a foliage canopy. A FOPEN SAR prototype installed aboard an Army RC-12 Guardrail has demonstrated the ability to detect, but not classify, targets hidden under "limited" foliage at a range of 20-25 kilometers. With the requisite investment, a smaller, lighter, more capable version of this FOPEN SAR could be fielded within a decade and potentially mounted on rotary- or fixed-wing UAVs, as well as other platforms. For a detailed discussion of a SAR concept for FOPEN imaging, see Michael F. Toups, "Foliage Penetration Radar Synthetic Aperture Radar Concept," in DSB 1996 Summer Study Task Force, *Tactics and Technology for 21st Century Military Superiority* vol. 2. See also: Timothy R. Gaffney, "Better Sensors Sought from Researchers," *Dayton Daily News*, May 2, 2000, p. 1B; and Andrew Koch, "U.S. Army to Field Radar that Can Penetrate Trees," *Jane's Defence Weekly*, August 29, 2001.

- UGS networks comprising cheap, compact, easily deployable devices that can be disseminated over a wide area;[258]

- Rapidly deployable, highly sensitive, passive and active, multistatic acoustic arrays that can detect and track ships and submarines operating over a wide area more effectively than is currently possible;[259] and

---

[258] Current UGS under active development include complementary combinations of acoustic, infrared, optical/electro-optical, seismic, and magnetic sensors. An individual UGS package might contain both an acoustic sensor, which would be used mostly at night when background noise is often relatively low, and an optical sensor that would be used during the day to take advantage of available light. Sensors could be disseminated by UAVs, manned aircraft, robots, or simply planted by hand. DoD currently has over a dozen major UGS-related development programs underway. For example, the Smart Sensor Web concept envisions thousands of inexpensive sensors sprinkled throughout the battlespace. These sensors would collect data and relay it back to distributed fusion points where it could be aggregated or fused into a single, comprehensive picture of the battlespace and then disseminated to the warfighter. The goal is for the sensors to become essentially disposable, costing as little as $10 each. See Mark Hewish, "Little Brother Is Watching You," *Jane's International Defense Revi*ew, June 2001, pp. 46-52; Bryan Bender, "DoD Eyes Sensors to Give 'Urban Canyon' Visibility," *Jane's Defence Weekly*, February 16, 2000, p. 14-15; George Seffers, "U.S. Army May Employ Microsensor Force," *Defense News*, January 10, 2000, p. 3; and Mark Hewish, "Silent Sentinels Lie in Wait: Unattended Ground Sensor," *Jane's International Defense Review*, January 1998, pp. 48-52.

[259] Future undersea sensor arrays could be similar in concept to the Advanced Deployable System (ADS) currently being developed by the US Navy. ADS is a passive acoustic array that can be deployed by aircraft, surface ships, or submarines in matter of weeks and can operate for six months to a year on battery power. Future ADS arrays might employ an all-optical (AO) laser sensor to pick up acoustic signals and then transmit the data through a fiber optic cable to a processing node (e.g., a submarine). ADS is scheduled to enter operational evaluation in 2004. Building upon the ADS program, the Navy is currently funding several cutting-edge undersea sensor programs including Deployable Low-Frequency Active (LFA) Multistatic arrays; Compact Deployable LFA Receivers (Super ADAR) that incorporate in-buoy signal processing and GPS-based positional information; and the Deployable Shallow Water Autonomous System that can be laid rapidly from aircraft, submarines, or surface ships to form a 100 square-mile acoustic sensor network For

- Portable, see-through-wall radar systems that can be used by soldiers to peer into buildings and rooms before attempting to enter and clear them.[260]

These and innumerable other sensors will not only be incorporated into existing ISR platforms, but also into new ones such as stealthy, long-endurance UAVs, man-portable MAVs, UUVs, UGVs, and constellations of small satellites. As the endurance and quantity of these platforms increases over time, it will become progressively more difficult to conceal troop movements or other military activities by exploiting temporal or spatial gaps in sensor coverage. The effectiveness of current stealth designs and techniques could also wane as militaries around the world become better able to integrate widely distributed sensors (e.g., IRST devices, bistatic and multistatic radar, passive coherent location systems, low-frequency radar, advanced electro-optical surveillance, and maybe even laser-radar systems) into a common counter-stealth architecture.[261]

---

additional information on the ADS program, see: Lisa Troshinsky, "Navy's Future Undersea Sonar System Will Be Tactical; Might Use All Optical Sensor," *Navy News & Undersea Technology*, April 24, 2000, p. 1; and Mark Hewish, "Listening for Whispers," *Jane's International Defense Review*, September 2001, pp. 40-41.

[260] Under laboratory conditions, it is possible to detect and track concealed weapons and monitor humans moving on the other side of a building wall with only a small amount of distortion. When mature, this technology would be a tremendous force multiplier in urban settings. One prototype system currently being tested has a detection range of between 25 and 50 meters for people behind a building wall, depending on thickness and type of wall material. The user can stand 4-5 meters away from the wall. From the images the radar generates, it is not only possible to visualize the movement of arms and legs, but also heartbeats and breathing. Joris Janssen Lok, "TNO Offers Through-the-Wall Radar for Special Operations," *Jane's International Defense Review*, August 2004, p. 19; and DSB 1996 Summer Study Task Force, *Tactics and Technology for 21st Century Military Superiority*, Vol. 2, Section VII. See also David Sun and Jay Sklar, "Through-the-Wall CSAR System Concept," in the same volume.

[261] David Fulghum, "Stealth Retains Its Value, But Its Monopoly Wanes," *Aviation Week & Space Technology*, February 5, 2001, pp. 53-57.

If advances in finding were to dominate advances in hiding capabilities completely, operational movement of any kind would be stymied. However, advances in sensor and data processing technologies will almost certainly trigger the development and diffusion of more sophisticated information-denial techniques, including counter-sensor capabilities (e.g., RF weapons, jamming and offensive IW) and new approaches to signature reduction. As a harbinger of this future competition, militaries around the world are already beginning to adopt more sophisticated C3D2 techniques.[262] The hider-versus-finder competition should be seen as an action-reaction contest that will seesaw back and forth over time. As sensor networks become more powerful over time, military forces could respond in some or all of the following ways:

- Applying signature reduction techniques and design principles to military platforms of all types, including strategic mobility aircraft, surface ships and ground combat vehicles;

- Increasing reliance upon submerged platforms that can hide in the world's oceans since electromagnetic radiation attenuates rapidly in water;

- Using multispectral decoys to confuse sensor systems;[263]

- Developing advanced materials for camouflage netting that reduce radar, infrared, and other signatures;[264]

---

[262] The DIA concluded in 2001 that "Many potential adversaries – nations, groups, and individuals – are undertaking more and increasingly sophisticated C3D2 operations against the United States . . . Advances in satellite warning capabilities, the growing availability of camouflage, concealment, deception, and obscurant technology, advanced technology for and experience with building underground facilities, and the growing use of fiber optics and encryption, will increase the C3D2 challenge." DIA Director Vice Admiral Thomas Wilson, "Global Threats and Challenges Through 2015," *Statement before the Senate Select Committee on Intelligence*, February 7, 2001.

[263] The ability of the Serbs to fool NATO pilots in Operation Allied Force with very crude decoys provides a glimpse of the potential effectiveness of sophisticated, multispectral decoys. John Barry and Evan Thomas, "The Kosovo Cover Up," *Newsweek*, May 15, 2000, p. 23.

- Jamming and dazzling imagery satellites and other sensor platforms to mask force movements and other activity;

- Exploiting miniaturized platforms such as micro-robots and MAVs that are inherently difficult to locate, track and engage;

- Emphasizing force mobility and dispersion, including logistics, C4ISR and combat service support functions;

- Relying more upon fiber-optic networks and passive sensor systems to reduce electronic transmissions; and

- Building military-related facilities deep underground.[265]

Based on current trends, it appears that the maturation of information-denial capabilities will generally keep pace with the development of new sensor and information acquisition technologies. In the contest between hiders and finders, in all likelihood, stealth, broadly conceived, will remain practicable and no dimension of the battlespace will become completely transparent by 2025.[266] Signature management and information protection, however, will likely become increasingly central to force protection.

---

[264] Sweden, for example, currently manufactures a material which, when draped over a tank, reduces its radar signature by more than half and its infrared signature by about two-thirds. George Seffers, "New Stealth Material Dulls U.S. Smart Missiles," *Defense News*, June 29-July 5, 1998, p. 3.

[265] The number of underground facilities worldwide has risen steadily over the last decade. The US intelligence community suspects with "a reasonable certainty that there are over 10,000 potential HDBTs [hardened and deeply buried targets] worldwide and their numbers will increase over the next 10 years. See Department of Defense, *Report to Congress on the Defeat of Hard and Deeply Buried Targets*, submitted in response to Section 1044 of the National Defense Authorization Act for Fiscal Year 2001, July 2001, p. 8.

[266] This conclusion is also supported by analysis completed by the Northrop Grumman Analysis Center. See Robert P. Haffa and James H. Patton, "Analogues of Stealth," Northrop Grumman – Analysis Center Papers, June 2002.

SPACE ACCESS VERSUS SPACE CONTROL

Over the coming decade, satellites that can be exploited for secure, long-haul communications and wide-area, terrestrial ISR will become both more capable and more widely accessible. As the Defense Intelligence Agency recently cautioned:

> Worldwide, the availability of space products and services is accelerating, fueled by proliferation of advanced satellite technologies, including small satellite systems, and increased cooperation among states and increased activity by consortia. These developments provide *unprecedented* communications, reconnaissance and targeting capabilities to our adversaries because most space systems have military as well as civil applications.[267]

Hundreds of new civilian and military COMSATs are scheduled to be launched into orbit over the next several years.[268] In addition, the data throughput that can be sustained by individual satellites is steadily increasing.[269] During recent operations in Afghanistan and Iraq, US military forces were provided with more than 3,000 megabits per second of COMSAT bandwidth, which was thirty times higher than

---

[267] Emphasis added. Vice Admiral Lowell E. Jacoby, Director, Defense Intelligence Agency, "Current and Projected National Security Threats to the United States," *Statement for the Record before the Senate Select Committee on Intelligence*, February 23, 2004, pp. 22-23.

[268] A few years ago, it was estimated that nearly 2,000 commercial COMSATs would be launched over the next decade. However, several multiple satellite programs have been delayed or have gone bankrupt. See Barry Watts, *The Military Use of Space: A Diagnostic Assessment* (Washington, DC: CSBA, 2001), pp. 51, 121-122.

[269] In the case of COMSATs in geostationary orbit, for example, the average number of transponders per satellite grew from 26.3 in 1994–95 to 30.5 in 1998–99, and that number could soon exceed 40. The incorporation of on-board circuit switching and advanced networking capabilities will further increase the average throughput supported by next-generation satellites. Ibid., p. 51.

in Operation Desert Storm. What is even more staggering, however, is that commercial COMSATs were responsible for about 82 percent of that bandwidth.[270] Foreign militaries will undoubtedly take advantage of encrypted COMSAT links as well to enhance their C3 capabilities. For instance, the secure, long-haul connectivity COMSATs provide could be used to better coordinate geographically dispersed units and to integrate widely separated elements of future anti-access networks.

The US firm DigitalGlobe (formerly EarthWatch Inc.) now offers images sharp enough to distinguish objects as small as 60-70 centimeters across and Space Imaging Inc. is planning to follow suit.[271] This degree of resolution is sufficient for detecting and characterizing a wide array of objects of military interest. For example, it is not only adequate for identifying a particular object as an aircraft, but also for characterizing it as a specific type of aircraft. DigitalGlobe intends to launch a satellite with panchromatic resolution of one-half meter or better in 2006. Only five days into Operation Enduring Freedom, DoD's National Imagery and Mapping Agency (NIMA) signed an exclusive contract with US-based Space Imaging that prohibited the company from "distributing, releasing, sharing or providing to any other entity" images generated by its Ikonos satellite.[272] The Ikonos satellite is capable of producing monochrome and full-color images with a resolution of one meter and multispectral ones with a resolution of four meters. By reaching such an agreement, DoD ensured that Ikonos images that could potentially compromise US operations overseas would never find their way into the hands of Al Qaeda

---

[270] Michael Sirak, "US Bid to Shield Vital Satellites," *Jane's Defence Weekly*, June 16, 2004, p. 17; and Molly Peterson, "Defense Improves Network-Centric Warfare, Tech Expert Says," *National Journal's Technology Daily*, May 6, 2003. The Air Force asserted that the average amount of satellite bandwidth consumed during Operation Iraqi Freedom was approximately 500 megabits per second, of which, about 70 percent was carried by commercial COMSATs. It is unclear, however, whether those figures encompass the entire joint force. See Lieutenant General T. Michael Moseley, *Operation Iraqi Freedom – By the Numbers*, p. 12.

[271] DigitalGlobe lowered the planned orbit of its QuickBird satellite in order to achieve higher resolution.

[272] Pamela Hess, "DoD Locks Up Commercial Space Pix," *United Press International*, October 12, 2001.

terrorists or their supporters. The question it raises, however, is how will DoD prevent such imagery from being distributed when it can no longer control access to space through "checkbook shutter control"?

Following the US lead, companies in Canada, France, India, Israel, Russia, and China either already offer high-resolution imagery for sale or will likely do so within the next several years. In addition to offering high-resolution, EO images, commercial firms are also expanding the range of spectral imaging options (i.e., multi- and hyper-spectral products) and reducing the lag time between when a tasking is received and when the final product is electronically transmitted or shipped to the customer.[273] As an early indicator of the growing menu of commercially available imaging services, Canadian-owned and operated Radarsat International offers SAR imagery that has a resolution as fine as three meters. This development is significant because radar-imaging satellites can peer through clouds and collect images at night as well as during the day. In terms of reduced latency, the Israeli-owned Imagesat Corporation now allows selected customers to directly task its Eros-A satellite and download raw data in real time.[274] As the chairman and CEO of Imagesat summarized:

> Our customers, in effect, acquire their own reconnaissance satellite in an agreed-upon footprint at a fraction of the cost than it would take to build their own...There is no shutter-control with our satellite....They do not have to ask for the satellite imagery from someone else. They do not have to

[273] As one means of reducing this lag time or "latency," firms are setting up regional affiliates in different regions of the world that can task satellites and directly receive raw imagery data.

[274] Satellite operating partner (SOP) customers can task the Eros-A satellite with complete secrecy. Later this year, Imagesat plans on launching the Eros-B1 satellite, which is expected to have a ground resolution significantly better than one meter. Elizabeth G. Book, "Non-U.S. Firms Provide Niche Imagery Products," *National Defense*, May 2003, p. 38.

> reveal where or when they are imaging, and they do not have to share the imagery with anyone.[275]

In a similar vein, France-based SPOT Image guarantees image delivery within 24 hours and, in many cases, it fills imaging requests within six hours. For customers that have a mobile imagery receiving station, image delivery can be completed in as few as 30 minutes.[276] While the highest resolution currently offered by SPOT Image is 2.5 meters, the firm plans to launch a new constellation of imaging satellites, referred to as the "Pleiades" series, which are expected to have a resolution of one-half meter. Given current trends, the quality and diversity of commercially available satellite imagery and value-added products will increase substantially over the next decade.[277]

Several prospective adversaries will be able to complement commercial products with imagery and data collected from remote-sensing satellites dedicated to military use. Four new capabilities, for instance, are slated to be incorporated into China's military-space architecture by the close of this decade: SAR satellites, ELINT and SIGINT satellites, mid-to-high resolution EO satellites, and a new generation of high-resolution, optical-imaging satellites that rely upon a film recovery system.[278] In October 2002, China launched the second EO reconnaissance satellite in the Zi-Yuan-2 series, which may have a ground resolution measured in tens of centimeters.[279] Prospective

---

[275] Ibid.

[276] Ibid.

[277] For an overview of commercial space-based remote sensing, see: John C. Baker, Kevin O'Connell, and Ray Williamson (ed.), *Commercial Observation Satellites: At the Leading Edge of Global Transparency* (Santa Monica, CA: RAND, 2001).

[278] Mark Stokes, "China's Military Space and Conventional Theater Missile Defense Development: Implications for Security in the Taiwan Straits," pp. 112-118; and Desmond Ball, *"China Pursues Space-Based Intelligence Gathering Capabilities,"* *Jane's Intelligence Review*, December 2003, pp. 36-39. See also: Robert Sae-Liu, "Beijing Aims High," *Jane's Defence Weekly*, January 17, 2001, p. 21; and Bill Gertz, "Chinese 'Civilian' Satellite a Spy Tool," *Washington Times*, August 1, 2001, p. 1.

[279] Phillip S. Clark, "China Launches New Photo-Reconnaissance Satellite," *Jane's Defence Weekly*, November 6, 2002, p. 14.

adversaries could exploit increasingly available satellite imagery in myriad ways, including: conducting indications and warning analysis, planning offensive and defensive military operations, geo-locating fixed targets, conducting BDA, and enhancing overall theater-level situational awareness. As noted earlier, space-based remote sensing could be an integral element of an anti-access or area-denial strategy.

Foreign militaries also stand to benefit from more accurate civilian GPS signals. Although GPS was always intended as a dual-use system, its primary purpose was to enhance the effectiveness of US and allied military forces. Over the last decade, however, it has evolved into more of a shared global utility. This trend culminated in 2000 with the Clinton Administration's decision to turn off selective availability, an artificial error that was intentionally introduced into the civilian signal to degrade its accuracy. As a result, the geo-positional accuracy of non-military receivers increased literally overnight by almost an order of magnitude from an average of about 45 meters to slightly more than six meters.[280] This shift in policy has, of course, benefited many users, including potential adversaries.

Military forces around the world use the signals from GPS satellites to navigate at sea, on land, and in the air. They also take advantage of the GPS "utility" for conducting field surveys, optimizing weapons emplacement, precision targeting, and synchronizing the timing of communications systems and computer networks.[281] Several countries have successfully integrated GPS receivers into ballistic and cruise missile guidance systems to improve their accuracy. It is inevitable that these and other applications of GPS will find their way into an ever-increasing array of foreign military equipment and

---

[280] With selective availability, the US government assured 100-meter accuracy 95 percent of the time. On the last day of selective availability, the National Oceanographic and Atmospheric Administration's National Geodetic Survey showed that 95 percent of the GPS position plots actually fell within a radius of 45 meters. When selective availability was turned off, position plots fell with a 6.3-meter radius of ground truth 95 percent of the time. See Bruce Nordwall, "Major Upgrades on the Way for Civil, Military GPS Users," *Aviation Week & Space Technology*, September 10, 2001, p. 56.

[281] Synchronized timing is important, for example, in configuring cryptographic systems and computer network security systems.

concepts of operation over time. While it would be technically possible for the US government to re-introduce selective availability in time of war, this option is rapidly becoming impractical due to growing civilian reliance upon the more accurate signal for functions that cannot be easily suspended.[282] For example, ships depend upon the signal to navigate in restricted harbors and waterways throughout the United States, and commercial aircraft use it for in-flight navigation in crowded air traffic corridors, as well as for landing at airports. Computer systems used in banking, telecommunications networks, and other critical civilian infrastructures (e.g., electrical power) have become increasingly dependent upon GPS for precision timing.

Since prospective adversaries will be able to derive progressively more military benefits from space in the years ahead, the US military has a strong incentive to develop and field space denial capabilities. In the spring of 2000, the Defense Science Board Task Force on Space Superiority recommended development of a "viable, quick-reaction, 'reversible' ability to disrupt, deny, degrade or deceive information available to an adversary from space" and "an option to deploy a non-reversible, lethal capability to destroy space systems when in the U.S. interest to do so."[283] The Air Force's Deputy Chief of Staff for Air and Space Operations, Lieutenant General Charles Wald observed in 2002 that the fielding and use of space control capabilities to deny future adversaries access to space and to assure the survivability of US satellites is inevitable. As he put it, "We're going to have to go down that path eventually—like it or not."[284] It appears that DoD is, in fact, already well down that path. Over the past several years, the US military has made significant progress developing and fielding the capabilities needed to enhance US situational awareness in space, temporarily deny space-based imagery and communication services,

---

[282] Commercial GPS is currently the basis for a $12 billion global industry. See "Accuracy is Addictive," *The Economist – Technology Quarterly*, March 16, 2002, pp. 24-25.

[283] The Task Force's recommendations are reprinted in *Inside the Pentagon*, March 30, 2000, pp. 13-15.

[284] Remarks by Lieutenant General Charles Wald at the 2002 National Defense Industrial Association (NDIA) conference. Kerry Gildea, "Air Force Space Officials Believe U.S. Use of Weapons in Space is Inevitable," *Defense Daily*, February 28, 2002, p. 2.

and disrupt access to GPS and other space-based navigational services to future adversaries.[285] Admiral James Ellis, head of US Strategic Command, recently asserted that developing and fielding both defensive and offensive space-control capabilities was "a vital national security interest."[286] Capabilities that are, or soon will be, in the US military's space-control "toolbox" include the following:

---

[285] The defense budget for FY 2002 included about $33 million for the development of various space-control capabilities including a small, transportable system, referred to as a Counter-Communication System (CCS), to incapacitate satellite communication systems using a "reversible and temporary means" and a second system, dubbed the Counter-Surveillance and Reconnaissance System (CSRS), designed to disrupt and degrade surveillance and reconnaissance satellites exploited by future adversaries. The FY 2003 budget included about $300 million for space control initiatives, including $24 million for the CSRS effort and $9 million for the CCS program. Funding was also earmarked for these and other space-control programs in the FY 2004 and 2005 budgets. Although Congress recently zeroed out funding for the politically contentious CSRS system, cutting some $53 million in the FY 2005 defense appropriation, General Lance Lord, chief of Air Force Space Command, has asserted that the requirement for a counter-surveillance system remains and noted that "as we continue to work this mission area you could see another kind of capability and another version of that system." See Amy Butler, "Lord: CSRS is Out, But Capability is Still Needed," *Defense Daily*, October 8, 2004, p. 1; Air Force Space Command, *Strategic Master Plan FY06 and Beyond* (Peterson AFB, CO: HQ AFSPC/XPXP, 2003), pp. 21-26; and Adolfo J. Fernandez, *Military Role in Space Control: A Primer* (Washington, DC: CRS, 2004), pp. 8-11, 17-20. See also: John A. Tirpak, "Securing the Space Arena," *Air Force Magazine*, July 2004, pp. 32-34; Andrew Koch, "US Seeks Solution to Space Threats," *Jane's Defence Weekly*, August 13, 2003, p. 7; Michael Sirak, "USAF Plans 'Space Control'," *Jane's Defence Weekly*, October 31, 2001; General Accounting Office, *Military Space Operations* (Washington, DC: GAO, September 2002), p. 8; and Office of the Under Secretary of Defense (Comptroller), *RDT&E Programs (R-1) – Department of Defense Budget Fiscal Year 2003* (Washington, DC: DoD, February 2002), pp. F4-F5.

[286] William Scott, "Control 'Out There'," *Aviation Week & Space Technology*, April 12, 2004, p. 69.

- Terrestrial- and space-based space surveillance systems;[287]
- High-power jammers designed to interfere with satellite uplinks and downlinks;[288]
- GPS jammers and spoofers;[289]

---

[287] The US Air Force is currently developing a constellation of space-based optical telescopes that will provide a dramatically enhanced, all-weather ability to detect, characterize, and track objects in space and monitor their activities. Referred to as the Space Based Space Surveillance (SBSS) system, it will comprise up to eight satellites that are slated to be on-orbit by around 2012-2013. SBSS will be followed by the Orbital Deep-Space Imager system that will be designed to maneuver within geo-synchronous orbit and inspect objects of interest at close range. Air Force Space Command, *Strategic Master Plan FY06 and Beyond*, pp. 21-22, 24; Fernandez, *Military Role in Space Control: A Primer*, pp. 16-17; Tirpak, "Securing the Space Arena," pp. 32-34; Michael Sirak, "US Air Force in Bid to Boost Space Awareness," *Jane's Defence Weekly*, April 14, 2004, p. 8; and Koch, "US Seeks Solution to Space Threats," p. 7.

[288] A first-generation version of the CCS—most likely a mobile, ground-based, high-power COMSAT jammer—was fielded in 2004. Two more CCS units are scheduled for delivery in early 2005. A second-generation system is already under development. The program, which is also referred to as the Counter-Satellite Communications System (CSCS), received $6.24 million in funding for FY 2005. Department of the Air Force, *Fiscal Year (FY) 2005 Budget Estimates, Research, Development, Test, and Evaluation (RDT&E)—Descriptive Summaries*, Volume II, Budget Activities 4-6, February 2004, pp. 871-874; Air Force Space Command, *Strategic Master Plan FY06 and Beyond*, pp. 23-24; Fernandez, *Military Role in Space Control: A Primer*, pp. 18-19; Michael Sirak, "Pentagon Eyes Near-Term Ability to Block SATCOM," *Jane's Defence Weekly*, July 24, 2002, p. 8; Tirpak, "Securing the Space Arena," pp. 32-34; and Koch, "US Seeks Solution to Space Threats," p. 7.

[289] Jamming refers to overpowering GPS signals with noise. Spoofing refers to a false GPS signal that is accepted by the receiver causing it to generate inaccurate positional information. While all radio frequency systems are vulnerable to jamming, GPS is particularly susceptible because it uses a relatively low-power signal. The United States intends to field a sophisticated Counter Navigation System (CNS) to deny an adversary use of satellite navigation signals by around 2017. Tirpak, "Securing the Space Arena," pp. 32-34; and Koch, "US Seeks Solution to Space Threats," p. 7.

- Relatively low-power lasers that can temporarily blind or "dazzle" electro-optical and infrared sensors;[290]

- Lasers with sufficient power to induce thermal overload in targeted satellites; and

- IW capabilities that can be directed not only against the satellites themselves (e.g., sending false commands), but also against terrestrial nodes (e.g. satellite command and control facilities, data processing installations, etc.).

Over time, US space-control capabilities will probably migrate to space. In terms of the physics involved in jamming a satellite's uplinks and downlinks, it is highly desirable to deploy jammers in closer proximity to targeted satellites.[291] Other types of non-destructive "proximity operations," which would cause little or no space debris that might inadvertently damage other satellites, might include fogging the optics of imaging satellites, applying an opaque coating to a satellite's solar panels, severing the power cables leading from a satellite's solar panels, or simply nudging a satellite into a useless orbit. One way to conduct such proximity operations would be to place small, specially designed microsatellites into orbit that could maneuver clandestinely toward a targeted satellite and shadow it during peacetime. In the event of war, the microsatellites could be

---

[290] The CSRS, which was slated for initial deployment in the 2008 timeframe before it was terminated by Congress in the FY 2005 defense budget appropriation, reportedly would have used a laser to blind electro-optical sensors temporarily and electronic warfare technology to jam radar-imaging satellites. Fernandez, *Military Role in Space Control: A Primer*, p. 19; Air Force Space Command, *Strategic Master Plan FY06 and Beyond*, pp. 23-26; Tirpak, "Securing the Space Arena," pp. 32-34; Koch, "US Seeks Solution to Space Threats," p. 7; and Jerry Singer, "Air Force Develops Satellite Blinder," *Defense News*, October 15-21, 2001, p. 1.

[291] Holding other variables constant, the closer a jamming source is to a targeted satellite, the lower the amount of radiated power required to disrupt its communication links effectively. The effective power of a jamming signal diminishes in inverse proportion to the distance squared. Reducing jamming distance could be particularly critical when attempting to disrupt future satellites that use high-power, narrow-beam communication links.

instructed to carry out various types of space-denial operations.[292] Alternatively, manned space operations vehicles (SOVs) could be used in this role.

Denying adversaries access to commercial space services, however, could prove rather problematic. First, it may be difficult to identify which firms throughout the world are providing services to a given US adversary. This challenge will only be exacerbated by the current trend toward increased global connectivity (i.e., the ability to move data rapidly across national borders using terrestrial communication networks) and the widespread availability of increasingly powerful encryption tools. Second, assuming that service provider information can be obtained in a timely fashion, the US government could be self-deterred from interfering with foreign-owned or operated systems owing to the probable diplomatic and economic repercussions. Lastly, even assuming the US government was willing to act, effectively denying an adversary access to

[292] The United States is currently developing a first-generation proximity-operations capability. As part of the Advanced Spacecraft Technology program funded in the 2004 budget, the Air Force plans to develop and test a microsatellite to demonstrate "operations around a non-cooperative resident space object." Related enabling technologies are also being developed as part of the Experimental Satellite Series (XSS) program. The XSS-11 experiment, which is slated for November 2004, is intended to demonstrate autonomous microsatellite operations, as well as to gain experience with command and control of proximity operations. During the experiment, a 100-kilogram satellite will fly several hundred kilometers away from its expended booster and then return to within 10 meters to inspect it autonomously with an onboard sensor payload. The satellite will circumnavigate the expended booster several times. While the Air Force claims that the XSS effort is focused narrowly on the development of a proximity-operations capability needed for identifying unknown objects in space, carrying out on-orbit satellite maintenance and upgrades, and possibly refueling future satellites, it would also have an inherent offensive space-control capability. See Elaine Grossman and Keith Costa, "Small, Experimental Satellite May Offer More than Meets the Eye," *Inside the Pentagon*, December 4, 2003, p. 1; Theresa Hitchens and Jeffrey Lewis, "Arms Race in Space?" *Defense News*, September 1, 2003, p. 35; Mark Hewish, "U.S. Air Force to Test Lockheed Microsatellite," *Jane's International Defense Review*, September 2001, p. 8; and Office of the Secretary of Defense, *Space Technology Guide FY 2000-01* (Washington, DC: DoD, 2001), pp. 12.5-12.10.

commercial services could be a daunting task from an operational perspective, especially if future service providers invest in proliferated architectures comprising dozens of distributed, cross-linked satellites.

As the US military relies more heavily on space for both force enhancement (e.g., precision navigation, long-haul communications, imaging, and target tracking) and perhaps even force application (e.g., sub-orbital strike platforms or military space planes), competitors will undoubtedly attempt to develop and field their own space control capabilities. As the former commander of US Space Command, General Charles Horner cautioned, "Our military forces are so dependent on space that it's created a vulnerability for us. . . We may be faced with a Pearl Harbor in space."[293] The congressionally mandated, blue-ribbon Commission to Assess United States National Security Space Management and Organization reached a similar conclusion:

> The relative dependence of the U.S. on space makes its space systems potentially attractive targets . . . Those hostile to the U.S. possess, or can acquire on the global market, the means to deny, disrupt, or destroy U.S. space systems by attacking satellites in space, communications links to and from the ground or ground stations that command the satellites and process their data . . . An attack on elements of U.S. space systems during a crisis or conflict should not be considered an improbable act.[294]

As an early confirmation of the Commission's finding, Iraq activated an unspecified number (at least six) of Russian-made GPS jammers during Operation Iraqi Freedom in an attempt to degrade the effectiveness of American PGMs. Although the jammers were quickly destroyed—ironically, in several cases, by GPS-guided JDAMs—the

---

[293] Comments made at a Heritage Foundation Forum. See Andrea Stone, "Dependence on U.S. Satellites Makes U.S. Vulnerable," *USA Today*, January 11, 2001, p. 5.

[294] See Donald Rumsfeld (chair), *Report of the Commission to Assess United States National Security Space Management and Organization* (Washington, DC: January 2001), p. viii.

commander of the Army Space and Missile Command noted that the critical lesson that should be drawn from the experience is that other states clearly "recognize the value of space and will try to take it away from us."[295] Echoing that view, General Lance Lord, commander of Air Force Space Command, recently cautioned:

> Space...is the center of gravity. We must not let it become a vulnerability. Our future adversaries understand that we have this advantage, and I think they are trying to develop capabilities right now to thwart that.[296]

Since ASAT weapons that physically destroy targeted satellites by colliding with them or by detonating an explosive warhead in close proximity to them would create large fields of space debris, most militaries will probably eschew them to avoid inadvertently harming their own satellites or those of their friends and allies. Instead, like in the United States, foreign militaries will likely gravitate—at least initially—toward terrestrially based, "soft-kill" ASAT capabilities like jammers and dazzlers.

Many countries already have significant military jamming capabilities that could be adapted to a counter-space role, including China and Russia, as well as Cuba, Iran, and North Korea.[297] A few years ago, Indonesia successfully jammed a transponder on a Chinese-owned satellite, and Iran and Turkey have jammed satellite television

---

[295] Lt. Gen Joseph Cosumano as quoted in Ann Roosevelt, "Space Control Vital for Future Operations, General Says," *Defense Daily*, November 3, 2003; Major General Victor Renuart, CENTCOM Operation Iraqi Freedom Briefing, March 25, 2003; and Lieutenant General Michael Moseley, Coalition Forces Air Component Command Briefing, April 5, 2003. According to the director of OSD's space policy office, Colonel David Trottier, "the effectiveness of these jammers [has] been hotly debated in the months since the war ended." See Cortes, "OSD's Space Policy Office Director Cites Multifaceted Threats Facing Space Assets," p. 5.

[296] As quoted in Robert Dudney and Peter Grier, "New Orbit for American Space Power," *Air Force Magazine*, February 2004, p. 40.

[297] Rumsfeld, *Report of the Commission to Assess United States National Security Space Management and Organization*, p. 19.

broadcasts.[298] Between 2002 and 2003, Cuba periodically jammed the Telsat-12 commercial COMSAT on behalf of Iran.[299] Similarly, several foreign countries are reportedly developing or buying GPS-jamming capabilities. The Russian firm Aviaconversia has displayed a hand-held GPS jammer for $4,000 at a number of trade shows over the last several years.[300] China is also reported to be developing and producing GPS jammers for both domestic use and export markets. China, India, Israel, and Russia are all believed to be developing ground-based lasers than can "dazzle" or temporarily disrupt imaging satellites. DoD has estimated that "China already may possess the capability to damage, under specific conditions, optical sensors on satellites that are very vulnerable to damage by lasers" and "given China's current interest in laser technology, it is reasonable to assume that Beijing would develop a weapon that could destroy satellites" within the 2010-2020 timeframe.[301]

---

[298] Ibid., p. 20. See also: Damien McElroy, "Iran 'Jams' US-based Satellite Channels after Clashes," *London Sunday Telegraph*, June 15, 2003.

[299] The government of Iran reportedly used a COMSAT jammer located in Cuba to jam Farsi-language radio broadcasts from an Iranian-born businessman in California carried over the Telsat-12 satellite. See Lorenzo Cortes, "OSD's Space Policy Office Director Cites Multifaceted Threats Facing Space Assets," *Defense Daily*, October 30, 2003, p. 5; and Andrew Koch, "US Seeks Solution to Space Threats," *Jane's Defence Weekly*, August 13, 2003, p. 7.

[300] Sales representatives claimed that the 4-watt jammer had an effective range of up to 150-200 kilometers. Russia is also marketing a handheld, one-watt GPS jamming system, the size of a cigarette pack that is reportedly able to interfere with a GPS out to 80 kilometers. Sandra Erwin, "Threat to Satellite Signals Fuels Demand for Anti-Jam Products," *National Defense*, June 2000, p. 23-27; David Foxwell and Mark Hewish, "GPS: Is it Lulling the Military into a False Sense of Security," *Jane's International Defense Review*, September 1998, p. 33; Richard Newman, "The New Space Race," in *U.S. News On-Line*, November 8, 1999, pp. 1-8; Ann Marie Squeo, "U.S. Military's GPS Reliance Makes A Cheap, Easy Target," *Wall Street Journal*, September 24, 2002; and Rumsfeld, *Report of the Commission to Assess United States National Security Space Management and Organization*, p. 20.

[301] DoD, *Future Military Capabilities and Strategy of the People's Republic of China* (Washington, DC: DoD, November 1998).

Prospective adversaries may also develop and deploy *space-based* denial capabilities over the next 10-20 years. Today, several countries use nanosatellites and microsatellites, weighing between 10 to 100 kilograms, to perform satellite inspection, imaging and other functions. The possibility that these satellites could be adapted into weapons was highlighted by the Commission to the Assess United States National Security Space Management and Organization, which cautioned:

> Placed on an interception course and programmed to home on a satellite, a microsatellite could fly alongside a target until commanded to disrupt, disable, or destroy the target. Detection of and defense against such an attack could prove difficult.[302]

Chile, China, Malaysia, Pakistan, Portugal, Singapore, South Africa, South Korea, Thailand, and Turkey have all participated in training programs focused on the development and deployment of microsatellites systems.[303] Aside from American and British firms, companies in Canada, Israel, Russia, and Sweden are heavily involved in advancing the state-of-the-art in microsatellite technology.[304] According to some reports, China is already developing a microsatellite system for space-denial missions.[305] As a possible step in this direction, in April 2004, China successfully placed into orbit a

---

[302] Rumsfeld, *Report of the Commission to Assess United States National Security Space Management and Organization*., p. 20.

[303] Ibid., p. 21.

[304] Ibid. Although 38 microsatellites were launched over the last two years, none of them were launched by the United States. See Marc Selinger, "DOD's TacSat-1 Micro-Satellite Slated for Launch in March," *Aerospace Daily*, December 4, 2003.

[305] The system apparently comprises a small carrier satellite that is capable of carrying and launching various types of micro-sized "parasitic satellites" that weigh several kilograms to tens of kilograms. These parasitic satellites supposedly attach themselves to a targeted satellite during peacetime, and interfere with or destroy their host satellite upon command. See Cheng Ho, "China Eyes Anti-Satellite System," Space Daily, January 8, 2000. Available on-line at: http://www.spacedaily.com/news/china-01c.html.

55-pound satellite with a "technology demonstration payload," which the Chinese declined to identify.[306]

The proliferation of space-denial capabilities will inevitably spawn the development of a range of defensive countermeasures. Future military satellites will likely be equipped with warning sensors to alert operators on the ground if they are being jammed, tracked with radar, lased, or have otherwise come under attack. To counter RF jamming, satellites might employ laser datalinks, or narrow-beam, high-power transmissions. Not coincidentally, DoD is currently funding the development of both a satellite-attack warning system and laser-linked COMSATs.[307] GPS satellites that have reached the end of their operational life will be replaced with modified Block IIR and Block IIF versions that have a military-only, "M-code" signal that is considerably stronger and more resistant to jamming than the current signal. The GPS-III series of satellites, which are expected to enter into service starting in 2012, will have an even more powerful spot-beam signal for military users.[308]

---

[306] Craig Covault, "China Surges Again," *Aviation Week & Space Technology*," April 26, 2004, p. 37.

[307] As part of its Rapid Attack Identification, Detection and Reporting System (RAIDRS) initiative, Air Force Space Command is developing a network, which will comprise ground- and space-based sensors, information processing nodes, and a global reporting architecture, designed to detect an attack on US military space platforms, identify and locate the responsible party, and then disseminate pertinent information to operators and users. The first elements of the RAIDRS network are expected to be in place by 2008-2009. Under the TSAT program, DoD plans to begin launching laser-linked satellites by around 2011. Fernandez, *Military Role in Space Control: A Primer*, p. 19; William Scott, "Tattletale Milsats," *Aviation Week & Space Technology*, December 23, 2003, p. 61; Mark Hewish, "US Eyes 'Transformational' Communications," *Jane's International Defense Review*, May 2003, p. 2; Craig Covault, "Military Satcom, Relay Programs Boost Industry, Enhance Warfare," *Aviation Week & Space Technology*, January 6, 2003, p. 43; Amy Butler, "Wolfowitz Boosts MILSATCOM by Billions, Outlines Additional Buys," *Inside the Air Force*, December 20, 2002, p. 1; and Jeremy Singer, "U.S. Laser-Link Satellites Likely to Launch after 2010," *Space News*, July 1, 2002, p. 11.

[308] The GPS III program may be accelerated by up to two years. GPS III satellites are expected to have "100 to 500 times the anti-jam capability of

More sophisticated protection systems (e.g., baffles, filters, and shutters) might be designed into future imaging satellites to reduce the effectiveness of laser dazzlers. Reflective or ablative coatings might be used to thermally shield satellites from high-power lasers. Space-faring nations might increasingly rely upon constellations of small, single-purpose satellites that are comparatively robust and easy to replenish instead of large, expensive, difficult-to-replace multipurpose ones.[309] Although a more distant prospect, military satellites could also shift their orbits periodically to complicate an adversary's tracking and targeting challenge. Given limited onboard fuel capacity, this tactic would likely require that future satellites be designed with an on-orbit refueling capability. Satellites might also be equipped with electronic counter measure (ECM) systems designed to lure approaching ASATs away or to detect and jam the terminal sensors of an inbound ASAT. Alternatively, states might field "guardian" satellites, equipped with a suite of active defenses, to escort high-value satellites during periods of increased tension.[310]

If these defensive countermeasures prove effective, they could create new incentives for disadvantaged states to field hard-kill ASATs that physically destroy their targets, regardless of the attendant

---

current satellites." See Jefferson Morris, "GPS III Options To Be Presented to Teets in Mid-April," *Aerospace Daily*, April 1, 2003; Mark Hewish, "What is Happening with GPS?" *Jane's International Defense Review*, July 2003, pp. 53-54; and Kerry Gildea, "Air Forces Halts GPS III Program, Competition Put Off Until 2006," *Defense Daily*, January 21, 2003, p. 5.

309 As illustrated by the upcoming "Operationally Responsive Space Experiment Tacsat-1" sponsored in part by DoD's Office of Force Transformation, the US military is beginning to focus increased attention and resources on the development of operationally useful, easily reconstituted micro-satellites. See OSD Office of Force Transformation, "Operationally Responsive Space Experiment Tacsat-1," *Transformation Trends*, October 17, 2003, pp. 1-3; and Marc Selinger, "DOD's TacSat-1 Micro-Satellite Slated for Launch in March," *Aerospace Daily*, December 4, 2003.

310 Early development of these types of guardian or "sentry" satellites may already be underway within the United States. See Scott, "Control 'Out There'," p. 70; and Tirpak, "Securing the Space Arena," p. 34. For a summary of additional satellite-defense options, see: Fernandez, *Military Role in Space Control: A Primer*, pp. 11-13.

diplomatic and economic costs of creating fields of destructive space debris. The United States and the former Soviet Union successfully developed hard-kill ASATs with technology that is now more than 25 years old.[311] Today, the technological barriers associated with developing a modest hard-kill ASAT capability could be surmounted by several states. For those with indigenous space-launch vehicle (SLV) or long-range ballistic missile programs, the primary challenge in fielding a rudimentary direct-ascent, explosive-kill ASAT would be developing a reliable end-game interceptor.[312] In light of the widespread availability of key enabling technologies (e.g., propulsion, sensors, and microprocessors) and open-source information on US and Soviet designs from the Cold War, developing one would be within the technical grasp of many prospective adversaries. According to some experts in the field, effective ASAT interceptors and supporting systems could be developed and fielded by a determined,

[311] The United States and the Soviet Union experimented extensively with both nuclear and conventional hard-kill ASATs during the Cold War. The Soviets tested a radar-guided, co-orbital ASAT system on 20 separate occasions between 1968 and 1982 that was capable of reaching satellites at altitudes up to 5,000 kilometers. The Soviets also developed and successfully tested an air-launched, kinetic-kill ASAT in September 1985 that could be released from a MiG-31. In addition to these programs, the Soviets experimented with a wide-range of more exotic ground- and space-based directed energy systems including high-energy lasers, particle beams and high-power microwave weapons. For a historical overview of US and Soviet ASAT programs during the Cold War, see Joan Johnson-Freese, "The Viability of U.S. Anti-Satellite Policy," *INSS Occasional Paper 30*, Space Policy Series, January 2000, pp. 3-18; Office of Technology Assessment (OTA), *Anti-Satellite Weapons, Countermeasures, and Arms Control* (Washington, DC: GPO, 1985). See also: Daniel Gonzales, *The Changing Role of the U.S. Military in Space* (RAND, MR-895, 1999), pp. 27-28; "Russia Alters MiG-31 for ASAT Carrier Roles," *Aviation Week & Space Technology*, August 17, 1992, p. 63.

[312] Aside from the world's four top-tier space launch providers (e.g., China, European Space Agency countries, Russia, and the United States), other countries with a space launch capability include, at present, Brazil, India, Israel, Japan, and the Ukraine. Countries that have a sufficient ballistic-missile technology base to pursue this path would arguably include Iran (Shahab 4), North Korea (Taepo Dong 2), India (Agni II), and Pakistan (Ghauri II). For more discussion on the possible adaptation of ballistic missiles to direct-ascent ASATs see Mark Mateski, "Managing ASATs: The Threat to U.S. Space," *Jane's Intelligence Review*, May 1999, p. 52.

technologically savvy adversary within a few years of the decision to do so.[313]

While it is not possible to predict exactly how the contest between space access and space control will play out over the coming decades, near-Earth space is almost certain to become an arena of intensifying military competition. As discussed above, the US military is already taking steps to ensure freedom of action in space for the United States and its allies, as well as to deny prospective adversaries from exploiting space-based capabilities.[314] Conversely, prospective adversaries will not only take greater advantage of space systems to enhance their own military effectiveness in the years ahead, but are also in the early stages of developing capabilities to deny the US military and its allies unimpeded access to space. Barring a verifiable arms control treaty proscribing the development of offensive space-control capabilities, which seems exceedingly unlikely, it seems probable that this competition will ineluctably lead to the deployment of progressively more lethal and more numerous space-control capabilities over time.[315]

---

[313] Allen Thomson, "Time to Plan for Satellite Warfare," *Space News*, April 22-28, 1996, p. 19. Similarly, Gregory Canavan of Los Alamos has concluded: "Simple anti-satellites (ASATs) can be based on current, conventional technology available to most countries. ASATs based on radar-guidance could release pellets in front of a satellite to destroy it or consume its maneuver fuel." Gregory Canavan, "An Entry Level Conventional Radar-Driven Rocket Anti-Satellite," (Los Alamos National Laboratory, LA-12297-MS, November 1993).

[314] See Department of Defense Directive 3100.10, July 1999. See also: Office of the Secretary of Defense, *Department of Defense Space Technology Guide FY 2000-2001* (Washington, DC: DoD, January 2001), pp. 10.1-10.2.

[315] A treaty banning the development of offensive space-control capabilities would be extraordinarily difficult to verify and enforce. Except for the testing of direct-ascent ASAT systems, it would be impractical to verify that all parties were honoring their commitment to eschew development of offensive space-control capabilities. Terrestrially based jammers and DE-ASATs, for example, could be developed and tested with almost no risk of detection. It is also highly unlikely that countries would be willing to subject highly sensitive military satellites to intrusive foreign inspection. As a result, it would be impossible to verify that they did not contain hidden space-control capabilities. Given that

KEY OFFENSE-DEFENSE COMPETITIONS

At some level all military operations represent a competition between offensive and defensive capabilities. However, beyond the overarching competitions discussed earlier (i.e., anti-access versus new forms of power projection, preemption versus denial, hiders versus finders, and space access versus space control), we believe the following three subordinate competitions deserve particular attention because of their potentially profound impact on the ability of the US military to perform its core missions of forward presence, power projection, dimensional control, and homeland defense over the next two-to-three decades:

- Missile attack versus missile defense;
- Offensive IW versus IW defense; and
- Advanced BW versus novel BW defenses.

The outcome of these pivotal competitions is, at present, uncertain. Each will be discussed briefly below.

Missile Attack Versus Active Defenses

Currently envisioned theater missile defense (TMD) systems (e.g., Patriot variants, Theater High Altitude Air Defense (THAAD), and Navy Mid-Course) will likely have difficulty handling repeated barrage attacks that combine both low-level, cruise missile and high-altitude, ballistic missile threats. Moreover, if future adversaries amass large enough missile arsenals, they could potentially exhaust interceptor stocks that are immediately available within a given geographic area. The application of stealth technologies and hypersonic propulsion systems to low-flying cruise missiles will make them even more

---

proximity-operation capabilities could dramatically lower the life-cycle cost of satellites through on-orbit upgrades, repairs, and refueling, space-faring nations would likely be reluctant to forego their development. These systems, however, would have an inherent offensive space-control capability.

difficult to detect, track and engage. Meanwhile, the increasing sophistication of penetration aids, including multispectral decoys and active jammers, for ballistic missile warheads could further complicate the target discrimination challenge. Lastly, the high-power radars and computerized battle management systems used in active missile defense systems are currently, and will likely remain, vulnerable to attack by anti-radiation missiles and RF weapons, respectively.

A number of technologies that are expected to mature substantially over the next two decades, however, could make a valuable contribution to missile defense. Long-endurance UCAVs, hypersonic missiles and next-generation loitering PGMs, for example, could provide a potent means for destroying enemy missile TELs, and under some circumstances, intercepting ballistic missiles in their boost phase. Missile defense systems that use directed-energy beams (e.g., high-power lasers) to intercept incoming missiles offer the prospect of rapid engagements, a relatively low cost-per-shot, and a deep "magazine." Space-based interceptors (e.g., "Brilliant Pebbles") could potentially provide near global coverage against a limited number of long-range ballistic missiles, but not against shorter range or depressed-trajectory missiles. The combination of advanced data processing capabilities and multispectral sensing could make envisioned penetration aids and decoys less effective. Of course, in response to these defensive developments, one can imagine all kinds of offsets that could enhance the striking power of the offense. For example, the effectiveness of directed-energy defenses could be degraded by applying ablative or reflective coatings to the outer skin of missiles, or in the case of ballistic missiles, rotating the missile around its longitudinal axis during its boost phase.

Although the ultimate outcome of this competition remains uncertain, it seems increasingly likely that large numbers of high-precision, low-observable missiles could limit the practical effectiveness of active defenses, especially for protecting "close in" targets. Given finite resources, over the coming decades, foreign militaries will probably opt to field more short- to medium-range missiles (i.e., less than 1,000 miles) than long-range ones because the former are more affordable and provide sufficient regional striking power. Accordingly, missile-barrage intensity will likely decline as a function of distance. In addition, greater distance also affords the defender increased warning time and more intercept opportunities. Thus, all else being equal, the further away a target is from a missile-armed opponent, the easier it will be to defend; and conversely, the

closer it is, the more difficult it will be to defend. In short, while potentially very useful, active defenses are unlikely to be a panacea—a significant fraction of future adversary's missiles will likely reach their intended targets.

Information Warfare

The increased importance of information infrastructures and information-intensive forces to economic and military power will make offensive IW capabilities highly valuable. For obvious security reasons, the capabilities and likely effectiveness of specific IW tools and techniques are highly classified and compartmentalized within the US intelligence, military and policy-making communities. The manual outlining Joint Doctrine for Information Operations (Joint Pub 3-13), for instance, sheds little light on the conduct of offensive information operations (IO) beyond the assertion that:

> Offensive IO are conducted across the range of military operations at every level of war to achieve mission objectives. The employment of IO to affect an adversary's or potential adversary's information or information systems can yield a tremendous advantage to US military forces during times of crisis and conflict.[316]

Joint Pub 3-13 later states that "IO may be used to effectively attack strategic targets, while minimizing potentially devastating social, economic, and political effects normally associated with conventional military operations."[317] Similarly, a presidential commission on critical infrastructure protection in 1997 noted simply that "offensive IW, in brief, uses computer intrusion techniques and

[316] Joint Chiefs of Staff (JCS), *Joint Doctrine for Information Operations* (Washington, DC: Joint Pub 3-13, October 9, 1998), p. II-1.

[317] Ibid, p. II–10.

other capabilities against an adversary's information-based infrastructures."[318]

At the tactical-operational level, offensive IW strikes could be directed against an adversary's battlefield C4ISR networks and combat forces. At the strategic level, IW attacks could target information-dependent civilian and military infrastructures such as transportation; energy generation, transmission and distribution; emergency services; banking and finance; telecommunications; and computer networks.[319] The electronic equipment upon which both battlefield networks and strategic information-dependent infrastructures depend could either be physically attacked by kinetic or non-kinetic means, or rendered functionally inoperable (but physically intact) by CNA operations.

Fiber-optic links, radio transmitters, network switching hubs, and data-processing nodes, for example, could be physically damaged or destroyed with various types of PGMs. As alluded to earlier, critical electronic systems could also be disrupted or permanently damaged

---

[318] *Critical Foundations – Protecting America's Infrastructures* (Washington, DC: President's Commission on Critical Infrastructure Protection, October 1997), p. 17. Hereafter referred to as the *Marsh Commission Report*.

[319] The Marsh Commission focused on eight inter-related infrastructures: telecommunications; electric power; banking and finance; transportation; oil and gas delivery and storage; water distribution; emergency services; and continuity of government services. Water distribution has been omitted here because of the relatively limited vulnerability of this infrastructure to information warfare in most countries. Water pumping and treatment facilities remotely controlled by computer-based Supervisory Control and Data Acquisition (SCADA) systems, however, might be vulnerable to IW attacks. The SCADA system for a sewage treatment plant in Australia was successfully attacked in 2000, resulting in the release of about 264,000 gallons of raw sewage into nearby rivers and parks. In January 2003, the Microsoft SQL Server worm (more commonly known as "Slammer") disabled the safety-monitoring system and plant process computers at the David-Besse nuclear power plant in Oak Harbor, Ohio for about six hours. See Robert F. Dacey (Director, Information Security Issues, US General Accounting Office), "Critical Infrastructure Protection: Challenges to Securing Control Systems," Testimony before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, October 1, 2003, Document No. GAO-04-140-T, p. 17.

with non-kinetic RF weapons.[320] The US military made significant progress throughout the 1990s developing and testing single-use HPM warheads for cruise missiles, glide bombs and other precision standoff weapons. Current prototype designs reportedly have an effective range of about 1,000 feet.[321] The US military is expected to field a HPM warhead in the next 2-4 years that can be mated to the JASSM, the conventional air-launched cruise missile (CALCM), or the Tomahawk LACM.[322] The United States and the United Kingdom have also investigated TEDs, which operate across a broader spectrum (10 MHz to 1 GHz) than HPM weapons and could potentially be effective against a wider array of electronic equipment.[323] These devices can reportedly be made small enough to be carried to their target by small, disposable UAVs.[324] Reusable RF weapons are also being developed for future electronic-strike UCAVs. In addition to the United States and its close allies (e.g., the United Kingdom and Australia), China,

---

[320] Semiconductors, which operate at very low voltages, are very sensitive, for example, to voltage spikes produced by EMP weapons. Furthermore, the heat generated within a semiconductor when exposed to EMP-induced currents may not be able to dissipate quickly enough, especially at small junction areas within the semiconductor, to avoid permanent damage from overheating. EMP fields can penetrate any and all types of openings in the housing of an electronic device and induce current flows in the circuits therein. They will also couple to any electrical conductors they encounter (e.g., power and telephone lines, data cables and antennas) inducing currents that can permanently damage any electronic devices connected to them.

[321] David Fulghum, "EMP Weapons Lead Race for Non-Lethal Technology," *Aviation Week & Space Technology*, May 24, 1993, p. 61; and David Fulghum, "Microwave Weapons May be Ready for Iraq," *Aviation Week & Space Technology*, August 5, 2002, p. 24. See also: Fulghum, "Microwave Weapons Await a Future War," p. 31.

[322] David Fulghum, "Thug Zapper," *Aviation Week & Space Technology*, July 26, 2004, p. 34.

[323] These broadband RF weapons reportedly have an effective range measured in "tens of meters." See David Fulghum, "U.S. Funds British Energy Weapon Tests," *Aviation Week and Space Technology*, September 16, 2002, p. 22.

[324] They could also be carried by Miniature Air-Launched Decoy (MALD) systems. David Fulghum and Robert Wall, "Small UAVs to Carry Disposable Pulse Weapons," *Aviation Week & Space Technology*, October 28, 2002, p. 60.

France, Russia, and Ukraine also have relatively advanced RF weapons programs under development and Germany, Israel, South Korea, Sweden, and Taiwan are believed to have nascent capabilities.[325]

Battlefield C4ISR networks and information-dependent infrastructures could also be subject to CNA attacks that target the communication protocols, databases, program applications, and other software systems upon which they depend.[326] Assuming an adversary's computer network security barriers could be penetrated or bypassed successfully, CNA operations might include some combination of the following: damaging or altering software applications; erasing or corrupting valuable data files; manipulating network protocols in order to interfere with the routing of data packets; and/or inserting malicious code.[327]

However, the prospect of successfully hacking into a well-defended system and then carrying out such attacks is, at best, uncertain given the growing availability of increasingly powerful network security software and hardware. Many countries, for example, are already taking advantage of commercially available firewall

[325] Ruppe, "Emerging Threat: Radio Frequency Weapons," p. 13.

[326] For additional information on the offensive IW techniques discussed below, see *Report of the Defense Science Board Task Force on Information Warfare-Defense,* Section 2, pp. 11–17. See also *Joint Doctrine for Information Operations*.

[327] Some of the weapons that might be used to carry out such attacks include logic bombs that consume the processing capacity of the host platform at a rapid rate as soon as some triggering event occurs; self-replicating viruses and worms that infect progressively larger volumes of data and greater numbers of computer systems over time (viruses require human involvement to propagate such as opening an infected file or email attachment, whereas worms do not); and Trojan horses, which can perform a wide array of pre-scripted functions while hiding within a legitimate computer program. Rather than a direct information strike, an adversary's computer network could also be disabled indirectly by network flooding, or the introduction of an unmanageable quantity of traffic into the adversary's network (e.g., sending thousands of messages per second to a targeted server). The goal of such an attack would be to overwhelm the system and prevent legitimate users from accessing and using the network. This type of information strike is often referred to as a "denial of service" attack.

products, automated intrusion detection systems, virus protection software, public key infrastructure (PKI) and public key enabled (PKE) applications, and extremely strong encryption software to better protect their computer networks. Given current trends in encryption, protected files could soon become practically impossible to decrypt, especially within operationally useful timelines.[328] Over time, prospective adversaries may also take advantage of commercially available biometric user-authentication systems (e.g., facial recognition and fingerprint, iris, and retinal scans) to secure their military and sensitive civilian-sector networks from unauthorized access.

The outcome of the competition between offensive and defensive CNA capabilities is very much an open question. Although breakthroughs in CNA could dramatically and suddenly reshape the military competition, current trends suggest that computer network defenses may have the upper hand. Growing dependence upon unhardened, COTS electronic equipment that is vulnerable to RF attack, however, could prove to be the Achilles' heel of information-age militaries and economies.

---

[328] Modern encryption is achieved with algorithms that use a "key" to encrypt and decrypt messages. The longer the key, the more computing power required to crack the code. To decipher an encrypted message by brute computational force, one would need to try every possible key. Encryption keys are made of "bits" or binary units of information having the value of zero or one. Therefore, an eight-bit key, for instance, has 256 (2 to the eighth power) possible values. A 56-bit key creates 72 quadrillion possible combinations. Given the current power of computers, 56-bit and 128-bit keys can both be cracked, but it requires an enormous amount of time and computing power, especially for 128-bit keys. According to the US Air Force Scientific Advisory Board: "*Unbreakable* codes will exist as *standards* throughout the world . . . the knowledge is already widespread, and the development of standards, cheap coders, and transparent interfaces will inevitably follow." See US Air Force Scientific Advisory Board, *New World Vistas – Air and Space Power in the 21st Century: Information Technology Volume* (Washington, DC: Department of the Air Force, 1995), p. 21.

Biological Warfare

The pace of technological advances over the last decade in DNA sequencing and mapping, bioinformatics, genetic engineering, and proteomics is well documented. Perhaps the best illustration of the rapid progress in the first two areas is the successful sequencing of the human genome that was completed in 2001.[329] Among other benefits, advances in genetic engineering and proteomics have led to disease-resistant, high-yield plants and have enabled pharmaceutical companies to develop new drugs to combat human diseases.[330]

While the ongoing revolution in biotechnology offers many potential benefits, future adversaries could harness it for malevolent ends. John Lauder, serving as chief of the CIA's Nonproliferation Center in 1999, testified to Congress that, "Rapid advances in biotechnology present the prospect of a wholly new array of toxins or live agents that will require new detection methods and preventative measures, including vaccines and therapies."[331] It is already possible to alter traditional BW agents to make them more virulent, more difficult to detect and identify, more resistant to antibiotics, and less susceptible to environmental factors (e.g., increased tolerance to ultraviolet radiation).[332] Between 1970 and 1990, for instance, Soviet scientists reportedly developed a wide range of genetically engineered pathogens, including hybrid viruses (e.g., a combination of encephalomyelitis and smallpox viruses) and strains of pneumonic

---

[329] J. Craig Venter et al, "The Sequence of the Human Genome," *Science*, February 16, 2001, pp. 1304-1357.

[330] Charles Mann, "Biotech Goes Wild," *Technology Revie*w, July-August 1999, pp. 38-43; and Antonio Regalado, "Mining the Genome," *Technology Review*, September-October 1999, pp. 57-63.

[331] David Abel, "U.S. Knowledge of Bioweapons Largely 'Obsolete'," *Defense Week*, March 8, 1999, p. 7.

[332] Barbara Starr, "U.S. DoD Reveals Horrific Future of Biological Wars," *Jane's Defence Weekly*, August 13, 1997, p. 6. See also Al Venter, "Keeping the Lid on Germ Warfare," *Jane's International Defense Review*, pp. 26-29; and William Broad, "Gene-Engineered Anthrax: Is It a Weapon?" *New York Times*, February 14, 1998, n.p.

plague and pulmonary anthrax that had resistance to up to ten different antibiotics.[333]

Owing to the development and diffusion of recombinant DNA technology, it is now relatively simple to manufacture "stealth pathogens" by hiding pathogenic genetic material inside bacteria that are relatively harmless. During the mid-1980s, Soviet scientists reportedly inserted the gene that produces the protein myelin, which helps transmit nerve signals, into *Legionnella*, the bacteria that causes Legionnaire's disease.[334] In tests, rabbits exposed to the altered pathogen became ill with mild pneumonia-like symptoms. Two weeks after completely fighting off the *Legionnella* infection, however, the apparently healthy rabbits developed severe neurological paralysis and died as their immune systems attacked the myelin around their own nerves, as if it were an invading pathogen.[335] Similarly, during the 1980s, South African scientists reportedly produced a variety of stealth pathogens under a top-secret program called "Project Coast." As one example, they spliced a toxin-producing gene from *Clostridium perfringens*, which causes a severe form of gangrene, into *Escherichia coli*, a common bacterium found in the human digestive tract and in a variety of foods.[336] By virtue of having the outward appearance of a common bacterium, stealth pathogens would be very difficult to detect

---

[333] Interview with Sergei Popov, former Soviet BW scientist, NOVA Bioterror Special, original air date November 13, 2001. Transcript is available online at: http://www.pbs.org/nova/bioterror.

[334] Soviet BW scientists also reportedly successfully inserted the encephalomyelitis virus (and possibly smallpox and Ebola as well) into Yersinia pestis, the bacteria which causes bubonic plague. Ibid.

[335] Ibid.

[336] Scientists working on Project Coast also reportedly explored, but never produced, pathogens that could selectively target South Africa's black majority population. See Joby Warrick and John Mintz, "Lethal Legacy: Bioweapons for Sale," *Washington Post*, April 20, 2003, p. 1; and Joby Warrick, "Biotoxins Fall into Private Hands," *Washington Post*, April 21, 2003, p. 1. According to some reports, the Japanese Aum Shinrikyo cult successfully inserted the toxin-producing genetic sequence of the botulism bacterium into *E. coli*. Barbara Starr, "DARPA Begins Research to Counteract Biological Pathogens," *Jane's Defence Weekly*, October 15, 1997, p. 8.

using current BW agent sensor systems and effective medical diagnosis and treatment would be extraordinarily difficult.

It may also become possible to assemble synthetic pathogens from a diverse set of component genes within the next decade or two. As a result of research conducted in laboratories around the world, the DNA and protein sequence of more than 70 major bacterial, fungal, and parasitic pathogens of humans, animals, and plants will be publicly available in the next few years.[337] These databases essentially provide a "parts list" for genes involved in pathogenicity and virulence, adhesion and colonization of host cells, immune response evasion and antibiotic resistance from which to pick and choose the most lethal combinations.[338] Through trial and error, these genetic "parts" could be assembled into viable "super" pathogens optimized for various applications.

Another biotechnology spin off of concern is the potential manipulation of bioregulators, which are organic chemicals produced by the human body that regulate cell processes and a broad range of functions such as bronchoconstriction, vasodilation, muscle contraction, blood pressure, heart rate, body temperature, and immune responses.[339] Owing to new biotechology-based production processes developed in the pharmaceutical and food industries, it is now possible to produce these chemicals, or more potent variants thereof, in large batches. (With recombinant DNA technology, it would also be possible to design outwardly benign organisms that produce bioregulator compounds once inside the human body.) Assuming the agent could be successfully disseminated and introduced into the human body, bioregulator weapons could be used to induce fear, fatigue or depression in targeted individuals; to render them

---

[337] Claire M. Fraser and Malcolm Dando, "Genomics and Future Biological Weapons: The Need for Preventive Action by the Biomedical Community," *Nature Genetics*, Volume 29, November 2001, p. 254.

[338] Ibid, p. 255.

[339] Central Intelligence Agency, *The Biological Chemical Warfare Threat*, (Washington, DC: CIA, 1997), pp. 2-3.

unconscious; to cause reversible physical incapacitation; or to trigger heart attacks and paralysis.[340]

Recent advances in biotechnology could eventually lead to pathogens designed to cause disease in certain types of people, depending on their genetic makeup.[341] In 1997, the World Medical Association (WMA) issued the following public warning: "The potential for scientific and medical knowledge to contribute to the development of new weapons systems, targeted against specific individuals, specific populations or against body systems is considerable."[342] Similarly, a recent British Medical Association report observed:

> While modern biotechniques are revolutionizing medicine and agriculture, the possibility exists of their misuse for political ends, for clandestine production and refinement of biological weapons (BW), and for future development of weapons of mass extermination, which could be used for genocide.[343]

---

[340] Canadian Delegation to the Biological and Toxin Weapons Convention, *Novel Toxins and Bioregulators: The Emerging Scientific And Technological Issues Relating To Verification And The Biological And Toxin Weapons Convention*, September 1991, pp. 45-46, 51.

[341] Former President Bill Clinton reportedly held a private discussion in April 1998 with government and private sector experts on the threat posed by the use of genetic engineering to develop advanced biological weapons, such as ethnically specific weapons. Some experts assert that the threat of genetically specific weapons is overblown because analysis of the human genome sequence to date has not revealed any polymorphisms that can be used to *absolutely* define racial groups. See Fraser and Dando, "Genomics and Future Biological Weapons: The Need for Preventive Action by the Biomedical Community," p. 256; and Barbara Starr, "Clinton Briefed on Genetic Engineering Threat," *Jane's Defence Weekly*, April 22, 1998, p. 13. See also: Starr, "U.S. Department of Defense Reveals Horrific Future of Biological Wars," p. 6; and British Medical Association, *Biotechnology, Weapons, and Humanity* (Canada: Harwood Academic Publishers, 1999), pp. 53-67.

[342] Starr, "Bio Agents Could Target Ethnic Groups, Says CIA," p. 6.

[343] The report concluded that, for example, "a mixture of influenza or diphtheria could be designed to affect mainly blacks; a 'designer toxin' could

Finally, biotechnology could also give birth to modern forms of "agrowar," or the use of naturally occurring or genetically engineered agents and pests to devastate crops and livestock.[344] Agrowar offers an insidious means of waging strategic warfare that is inexpensive, relatively easy to conduct in both a technical and operational sense, and very difficult to defend against. Depending on the means of delivery and the type of agent, it could be practically impossible to discriminate between agricultural warfare and a natural outbreak of disease. As Colonel Robert Kadlec, a US Air Force expert on BW, has cautioned, "Agroterror offers an adversary the means to wage a potentially subtle yet devastating form of warfare, one which would impact on the political, social and economic sectors of society and potentially threaten national survival itself."[345]

---

be aimed exclusively at Serbs; or people with blue eyes might be given Alzheimer's disease." See British Medical Association, *Biotechnology Weapons and Humanity* (Amsterdam, The Netherlands: Harwood Academic Publishers, 1999), p. 57.

[344] The easiest approach might be to increase the virulence and hardiness of naturally occurring pathogens. More than a dozen animal pathogens have the potential to impact severely US livestock populations. Candidate pathogens include foot and mouth disease, classical swine fever, African swine fever, rinderpest virus, Rift Valley fever virus, avian influenza virus, Exotic Newcastle Disease virus, bluetongue virus, sheep and goat pox virus, swine vesicular disease, vesicular stomatitis virus, lumpy skin disease virus, and African horse sickness virus. Peter Chalk, *Hitting America's Soft Underbelly—The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry* (Santa Monica, CA: RAND, 2004), pp. 14-16; and Peter Chalk, "The U.S. Agriculture Sector: A New Target for Terrorism?" *Jane's Intelligence Review*, February 2001, pp. 12-15.

[345] Peter Chalk, "The U.S. Agriculture Sector: A New Target for Terrorism?," p. 14.

The United States may be especially vulnerable to agrowar.[346] According to some assessments, the natural tolerance of US livestock to disease has fallen in recent years as a result of intensive antibiotic and steroid programs, and husbandry changes designed to elevate the quality and quantity of meat production.[347] Most sectors of the livestock industry are highly concentrated, which make them lucrative agrowar targets. For example, less than 10 percent of the cow and calf production facilities in the United States account for 75 percent of the sales of those commodities. Most dairy farms house at least 1,500 lactating cows at any one time and some of the largest facilities contain upward of 10,000 animals.[348] The combination of crowded livestock populations and the long distances over which the animals are regularly transported (i.e., from rearing locations, to sales yards, and then on to slaughter and meat-packing plants) would make it extraordinarily difficult to contain a deliberate agrowar attack. Similarly, heavy reliance on a relatively small number of genetically enhanced seed stocks has reduced the genetic diversity of key crops, making American farms particularly vulnerable to engineered plant diseases. It is all too easy to imagine, an altered variant of soybean rust, ear rot (corn), wheat stem rust, karnal bunt (wheat), or wheat smut spreading like wildfire across America's agricultural heartland.[349] A combination of several pests or pathogens could be introduced simultaneously at multiple locations to complicate containment,

---

[346] The two most detailed, publicly available analyses of US vulnerability to "agrowar" are: Committee on Biological Threats to Agricultural Plants and Animals, *Countering Agricultural Bioterrorism* (Washington, DC: National Academies Press, 2002); and Peter Chalk, *Hitting America's Soft Underbelly—The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry* (Santa Monica, CA: RAND, 2004).

[347] Examples of husbandry changes that have increased livestock and poultry stress levels, lowering their resistance to infection, include: overcrowding, branding, dehorning, hormone injection, castration, and disinfectant sterilization. Chalk, *Hitting America's Soft Underbelly*, p. 9.

[348] Henry S. Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat* (Washington, DC: National Defense University, 2002), McNair Paper No. 65, p. 12; and Chalk, *Hitting America's Soft Underbelly*, p. 8.

[349] There are more than a dozen plant pathogens with agrowar potential. Parker, *Agricultural Bioterrorism*, p. 18.

overwhelm US response capabilities, and maximize damage. As one analyst from the US Department of Agriculture (USDA) has cautioned:

> American agriculture is often concentrated, highly accessible, vertically integrated, and of limited genetic diversity; historically it has been free of major disease outbreaks, so vaccines are not routinely used. Consequently, pathogens could be introduced easily and spread rapidly...Advances in genetic engineering have raised the prospect of transgenic pathogens and pests that are resistant to conventional control methods...Signs of infection may be manifested slowly, delaying effective response by authorities. Finally, attacks against agriculture may be less risky to perpetrators than attacks against humans because many anti-agriculture pathogens are comparatively safe to work with.[350]

The outbreak of foot and mouth disease (FMD) in Taiwan in 1997 provides a valuable glimpse of the potential, long-term strategic implications of agrowar. Within six weeks, FMD spread throughout the country and necessitated the slaughter of more than eight million pigs. The cost of eradicating the disease was over $4 billion and estimates of the value of lost exports run as high as $15 billion.[351] Similarly, the FMD outbreak that began in the United Kingdom in the spring of 2001 quickly spread to the Netherlands, France, and Ireland and resulted in four million cattle, swine, sheep, and goats being culled in an effort to contain the disease. The cost of an earlier outbreak of bovine spongiform encephalopathy (BSE) or "Mad Cow" disease in the United Kingdom, which reached epidemic proportions in the early 1990s, is conservatively estimated at more than $10 billion.[352] Not

---

[350] Ibid, p. x.

[351] The origin of the outbreak was reportedly traced to a single infected pig from Hong Kong, which may have been deliberately introduced into Taiwan. Ibid, p. 15.

[352] The cost estimate cited here includes over $1.6 billion in compensation paid to farmers and laid-off workers, an estimated $4 billion in tourism losses, and over $5 billion in agricultural export losses. Some estimates of the economic cost are as high as $30 billion. Ibid, p. 14. See also: Committee on Biological

surprisingly, agricultural exports from the United Kingdom plummeted following the BSE and FMD outbreaks and have yet to recover fully.[353]

Despite their prospective strategic value, the United States will not develop offensive BW for legal, political, and moral reasons. Future military competitors, however, may not be similarly self-constrained. Fortunately, new technologies may help to reduce the threat posed by advanced BW. Major strides, for example, are being made in small, robust, low-power sensors that could be able to detect and identify low concentrations of BW agents with very few false positive and false negative alarms.[354] Antibody-based sensors and miniaturized mass spectrometers may eventually be able to provide rapid, accurate identification of all known BW agents.[355] It may also be feasible to develop tissue-based sensors that use the physiological response of biological cells and tissues to detect the presence of previously unidentified or engineered CBW agents.[356]

While traditional immunization practices can offer protection against specific known agents, they are not adequate for protecting against genetically engineered variants. Under its "Unconventional Pathogen Countermeasures Program," DARPA is investigating a wide range of possible countermeasures including multi-agent immunizations to be used prior to exposure, as well as advanced medical therapeutics against toxins, bacteria, and viruses (e.g., broad

---

Threats to Agricultural Plants and Animals, *Countering Agricultural Bioterrorism*, p. 23; Sean Henahan, "Mad Cow Disease – The BSE Epidemic in Great Britain," *Access Excellence*, 1996; and Janet Ginsburg, "Bio Invasion," *Business Week*, September 11, 2000, p. 72.

[353] British beef exports in 2000 were still down 99 percent relative to 1995. Janet Ginsburg, "Bio Invasion," pp. 72-74.

[354] Fernandez, *Testimony before Subcommittee on Emerging Threats and Capabilities of the Senate Armed Services Committee*, pp. 6-7.

[355] Dr. Jane Alexander, Acting Director of the Defense Advanced Research Projects Agency (DARPA), *Testimony before Subcommittee on Emerging Threats and Capabilities of the Senate Armed Services Committee*, June 5, 2001, p. 4.

[356] Ibid., p. 5

spectrum anti-viral and antibiotic drugs).[357] DNA vaccination, which entails administering antigen-encoding DNA that causes antigens to be directly synthesized within the human body, is another promising technology area. It offers a number of benefits over traditional vaccines such as ease of production, stability, and transport; elimination of the need to cultivate dangerous infectious agents; and the ability to vaccinate against multiple pathogens in a single shot.[358]

However, all of these improvements in BW defenses have their own limitations or counters. While it might be possible to develop sensors, vaccines, and gene therapies that are effective against a wide variety of traditional pathogens, it may prove impractical to do so in a timely manner against an innumerable array of never-before-seen, genetically engineered variants. As the US government notes in the Fifth Review Conference on the Biological Warfare Convention (BWC), the very advances in biotechnology that have put new capabilities in the hands of those conducting legitimate biological research could "make developing biological and toxins weapons much easier than developing adequate defenses against them."[359]

INCREASED CAPABILITIES FOR COERCION VERSUS COUNTER-COERCION

As suggested earlier in the discussion pertaining to preemption and denial, the likelihood of outright invasion and conquest may be on the wane since friends and allies of a beleaguered state may increasingly be able to use precision-strike capabilities to deny an aggressor the spoils of conquest. Precision-strike capabilities, however, could also be

[357] Ibid, pp. 4-5.

[358] Fifth Review Conference on the States Parties to the Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, *Background Paper on New Scientific and Technological Developments Relevant to the Convention* (Geneva, Switzerland, Convention Secretariat, 2001), p. 16.

[359] Ibid, p. 15.

used by a prospective adversary to pressure neighboring countries into acquiescing to its demands.[360] Ballistic and cruise missiles, for example, could be particularly useful in this regard because they offer a relatively low-cost means of striking over extended distances that is difficult to defend against. As Secretary of Defense Donald Rumsfeld cautioned in testimony before the US Senate in 2001:

> The regimes seeking ballistic missiles and nuclear, chemical and biological weapons see them not only as weapons to use in war, but as *tools of coercion – means by which they can intimidate their neighbors* and prevent others from projecting force to defend against aggression.[361]

For example, as foreshadowed by its missile launch "exercises" in the waters near Taiwan in 1995 and 1996, China could use the implicit or explicit threat of missile strikes as a means of coercing Taiwan's political leadership.[362] Alternatively, China could leverage its recent investments in minelaying capabilities, difficult-to-detect SSKs, and ASCMs to threaten to blockade major Taiwanese ports and interdict commercial shipping.[363] These same capabilities could also be used to

---

[360] These demands would have to be limited in nature such as economic or foreign policy concessions favorable to the aggressor state (e.g., denying base access to US forces) in order for a coerced state to acquiesce without a fight. It is hard to imagine that any state, for instance, would capitulate to coercive pressure if doing so would result in its annexation and subjugation.

[361] Emphasis added. Secretary of Defense Donald Rumsfeld, *Prepared Testimony to the Senate Armed Services Committee*, June 21, 2001, p. 2.

[362] According to the Defense Intelligence Agency, China is "rapidly expanding its conventionally-armed theater missile forces (particularly the road-mobile, solid-propellant, 300-kilometer CSS-7), in large measure to give it leverage against Taiwan and, to a lesser extent, other U.S. Asian allies." See VADM Wilson, *Prepared testimony before the Senate Select Committee on Intelligence*, February 2, 2000.

[363] Tom Christensen of MIT asserts that this type of coercive operation seems more likely to be adopted by China and might actually serve Beijing's political purposes better than an invasion would. He argues that the limited nature of China's political goals (i.e., preservation of the one China concept) "might convince Beijing elites that a coercion campaign far short of an amphibious invasion will likely succeed in convincing Taiwan and its potential

threaten the commercial shipping of neighboring states in a bid to shape regional trade flows to better accommodate China's interests.

Prospective adversaries could also employ offensive information operations and, as suggested in the citation above, advanced BW attacks for coercive purposes. In doing so, it might be possible to take advantage of the inherent reversibility of such attacks. An IW attack could be used to disable critical economic and governmental infrastructure (as well as enemy forces), but might also be easily reversed with the requisite software or computer codes. Similarly, advanced BW capabilities might not only be precisely targetable against a particular ethnic group or individual, but also treatable with an easily supplied antidote or vaccine. Depending upon an opponent's response to an ultimatum, these remedies could be either supplied or withheld. Moreover, the pain induced by these attacks could be gradually ratcheted up or down in order to maximize their coercive effect and ensure compliance.

There would appear to be two basic strategies for reassuring friends and allies facing these types of threats and deterring prospective adversaries from making them. The first would be to provide the former with robust defensive capabilities that reduce the anticipated effectiveness of threatened missile, IW, BW, or other attacks. Providing them with state-of-the-art IW defenses (e.g., strong encryption, sophisticated firewalls, and virus protection) and BW defenses (e.g., broad-spectrum drugs and novel vaccines) would be expected to reduce the coercive value of IW and BW threats. Similarly, theater missile defenses, even if only partially effective, could take some of the sting out of missile threats.

The second strategy would be to extend formal security assurances to them. The effectiveness of this strategy—both in terms of deterring prospective adversaries and reassuring friends and allies—would depend upon the perceived ability and willingness of the United States to conduct punitive reprisals in response to coercive acts (i.e.,

---

international supporters that fighting a prolonged battle to avoid such an outcome simply is not worth it." Thomas J. Christensen, "Posing Problems Without Catching Up – China's Rise and Challenges for U.S. Security Policy," *International Security*, 25, No. 4, Spring 2001, pp. 23-25.

holding at risk those things that are valued by the power contemplating coercive acts). While it is almost certain that the US military would have the ability to carry out such attacks, the willingness of the US government to do so may be more open to question, especially when only limited American interests were at stake. Reassuring friends and allies that the US government would be willing to initiate conventional strikes against the homeland of a nuclear-armed adversary in response to coercive acts (e.g., interdicting a ship at sea or launching a missile into a commercial port), for example, would be a particularly difficult diplomatic hurdle to overcome.

Unlike deterring the outright use of force in which the behavior to be deterred is unambiguous (e.g., military forces crossing over a well-demarcated international border), deterring political-military coercion is complicated by the fact that there often may be no clearly discernable acts to trigger a response. In a RAND study of the possibility of Chinese military coercion aimed at influencing the outcome of democratic elections or political decision-making in Taiwan, Abram Shulsky notes:

> How much Chinese "saber rattling" would call into question the voluntariness of the Taiwanese decision making process? The United States may find it hard to draw a clear line separating "acceptable" Chinese pressure on Taiwan from what it would seek to deter by means of some sort of retaliation.[364]

Given that the United States could not hope to specify in advance every possible form of coercion to be deterred, either by China or any other prospective regional adversary, it would likely have to rely on an ambiguous threat to respond in some undisclosed way to vaguely defined acts of coercion. Regional powers that sought to erode US influence would likely respond to ambiguous threats through

[364] Abram Shulsky, *Deterrence Theory and Chinese Behavior* (Santa Monica, CA: RAND, 2000), p. 25.

"brinkmanship" or probing US commitments with frequent challenges at or near the perceived threshold for triggering a response.[365]

For example, assume China launched a handful of missiles into relatively remote areas of Taiwan, Japan, or some other East Asian ally of the United States. Would proportional attacks against the Chinese homeland inflict sufficient pain on the leadership in Beijing to alter their long-term, cost-benefit calculus and deter them from such behavior in the future? Paradoxically, the political leadership in Beijing could actually perceive proportional American reprisals as beneficial. By facilitating domestic mobilization within China and by creating a sense of crisis, US strikes could afford Beijing an opportunity to extract diplomatic concessions or make other strategic gains that would otherwise be unattainable.[366] The creation (and manipulation) of a crisis could, for example, provide a useful way to probe American intentions, to create divisions between the United States and its regional allies, and to undermine US popular support for military involvement in the region.[367]

Disproportionate retaliatory attacks would be more likely to deter future acts of coercion, but would also introduce a considerable amount of escalatory risk into the equation. For deterrence purposes, therefore, an uneasy balance would need to be struck between ineffective pinpricks and attacks that carry an unacceptably high risk of escalating out of control. The prospect of miscalculation by either side would likely be quite high. Another option for deterring coercion

---

[365] Adopting a strategy of brinkmanship would offer at least three benefits to the coercing power. First, it would force the United States to clarify the ambiguity of its commitments over time, which would likely leave the coercing power with a better understanding of the maneuvering room it has for conducting subsequent political-military coercion without risking US retaliation. Second, it would compel the United States to expend time and resources continually positioning itself to respond to potential acts of coercion, whether real or feigned. And lastly, if the United States periodically failed to respond to above-the-threshold challenges, this policy could, over time, erode the confidence of friends and allies in the ability and willingness of the United States to honor its commitments.

[366] Abram Shulsky, *Deterrence Theory and Chinese Behavior*, pp. 38-40.

[367] Ibid., p. 39.

might be to threaten various forms of horizontal escalation. For instance, rather than threatening punitive missile strikes, the United States could threaten to cut off the coercing state's access to external energy supplies (e.g., severing pipelines and interdicting tankers) or valuable imports and exports. The problem of reassuring allies and deterring political-military coercion could emerge as a core strategic challenge for the United States over the next two decades.

IV. Warfare in an Advanced RMA Regime

Depending on how the key warfare competitions described in Chapter III unfold over time, by 2025, war could be substantially transformed within existing dimensions and emerge in new ones. Developments in these competitions could also have major ramifications for military operations at the upper and lower ends of the spectrum of conflict. In this chapter, we assume that significant discontinuities in warfare lie ahead. We assume that the US loses its monopoly on the revolution in war, and that asymmetric, disruptive exploitation of the military capabilities underwriting continued change in war by strategic competitors at both the high-and low-ends of the conflict spectrum leads to a revolution within the revolution.[368]

This chapter is organized into two major sections. In the first, we discuss how high-end conventional war could change within each dimension of the future battlespace. This discussion assumes intensified strategic competition in which most of the capability trends

[368] Many of the advanced RMA capabilities we describe here might be pursued even if the United States retains a monopoly on the revolution in war. The purpose, however, would not be to adapt to adversary acquisition of disruptive capabilities, but rather to extend US dominance and increase its strategic freedom of action.

associated with an advanced, discontinuous phase of the RMA have been realized. The discussion is focused principally on high-end warfare against a near-peer competitor. Although we argue that new capabilities and operational and organizational concepts will be needed to fight effectively in this environment, legacy and early-phase RMA capabilities will remain sufficient for operations involving less demanding contingencies. The second section of this chapter explores how an advanced phase of the RMA could affect the war on terrorism, intra-state conflict (including stability operations), and strategic warfare.

ASYMMETRIC, HIGH-END WARFARE

Based on our current assessment of the key competitions shaping the ongoing revolution in war, we believe that the modes of warfare that are presently dominant in the air, on land, and at sea could be rendered obsolete or subordinate within the next two to three decades. New forms of warfare in space, the information spectrum, and the biological realm could also emerge.[369] Clashes between competing network architectures and organizational forms will likely become a central feature of warfare within all dimensions of the future battlespace.

Air warfare could be transformed from a regime dominated by manned, theater-range, air superiority aircraft to one dominated by networks of extended-range, unmanned, and stealthy platforms. The conduct of land warfare could shift from a regime dominated by mobile, combined-arms, armored forces to one that is dominated by much lighter, stealthier and information-intensive forces that make heavy use of robotics. War at sea could be transformed by the emergence of anti-navy capabilities that allow nations to assert a degree of surface control over adjacent maritime areas out to several hundred miles. This development could, in turn, lead to new forms of naval power projection, including increased reliance on undersea platforms and relatively small, stealthy, networked surface vessels. In

[369] The discussion that follows extends upon Michael G. Vickers, *Warfare in 2020: A Primer* (Washington, DC: CSBA, 1996).

all likelihood, increased commercial and military use of space will lead to the emergence of a wide range of offensive and defensive space control capabilities—both terrestrially based and in near-earth space. CNA tools and RF weapons will likely be widely used to attack civilian and military information infrastructures and information-intensive combat and supporting forces. Advanced biological operations may also figure prominently in an advanced RMA regime.

Militaries will likely pursue different paths within this multidimensional RMA. Some competitors may invest heavily in a few dimensions of the battlespace, but not in others. Even within a particular warfare dimension, militaries may pursue divergent paths. For example, in the air dimension, some advanced militaries may rely mainly upon ballistic and cruise missiles, while others emphasize UAVs and UCAVs. In all likelihood, the forces of advanced RMA militaries will be highly asymmetric. In the sections that follow, we attempt to describe what war in each dimension of the battlespace might be like in an advanced RMA regime.

War in the Air

Over the next 15-20 years, air power could be transformed by three developments: the denial of close-in theater bases, the large-scale substitution of unmanned for manned systems; and the application of signature-management technologies to a much wider range of aircraft than is the case today.[370]

Assuming that TMD systems are less than fully effective, which seems probable, air power's principal operational challenge over the next two decades will likely be the growing vulnerability of fixed

[370] These developments could affect the conduct of air operations in limited, but significant ways within the coming decade. For example, UAVs will likely supplant manned reconnaissance aircraft in performing a wide-range of ISR missions; ballistic and cruise missiles threats will almost certainly make it more risky to conduct operations out of in-theater air bases; and the proliferation of advanced, networked, mobile, long-range SAMs could make it much more difficult to suppress enemy air defenses. However, the full effect of these developments will probably not be felt until 15-20 years hence.

bases.[371] Given current technology diffusion trends, future adversaries may be able to render in-theater airbases inoperable for an extended period of time by launching waves of long-range, highly precise ballistic and cruise missiles armed with conventional warheads, wide-area submunitions, WMD payloads, or RF warheads. Aircraft lacking intercontinental range or whose operational task requires them to land in theater could be forced to operate from dispersed, unimproved, transitory airfields with the active support of information operations.

The increased prevalence of long-range cruise and ballistic missiles, as well as stealthy UAVs and UCAVs able to loiter at high altitudes could make it difficult to gain control of the air dimension. The traditional air control task of sweeping the skies of enemy fighters could be subordinated in importance to counter-missile and counter-UAV operations. The application of signature-reduction technologies to aircraft of all kinds could reduce the effective range of surveillance sensors and place a renewed emphasis on short-range engagements. As a result, traditional air superiority, to the extent it can be achieved, could be confined to relatively small geographic areas.

Over time, a steadily wider array of missions may migrate from manned fighters to long-endurance, fully autonomous UCAVs (see Table 3).[372] Both manned and unmanned aircraft may be armed not only with hypersonic missiles, but also high-energy laser (HEL) systems that can engage enemy targets at the speed of light.[373]

---

[371] As discussed previously, in-theater airbases could also be unavailable for political reasons. In some parts of the world, in-theater air bases may be limited in number (and austere), or may not even exist.

[372] Unlike pilots that get tired and whose alertness begins to fade after a few hours on patrol, UAVs and UCAVs could technically remain aloft, ever vigilant, for days on end. Unmanned aircraft might also be more maneuverable in that their ability to "pull g's" would be limited only by the physical tolerance of the airframe, not by human physiology.

[373] According to the DSB, with the requisite investment, a HEL fighter could be ready for engineering and manufacturing development (EMD) in approximately 10-15 years. The technology "long poles" that need to be addressed include the power-to-weight/volume ratio of the laser system, beam control in a high vibration/acoustic environment, and thermal management.

Table 3: Transformation to an Advanced RMA Air Warfare Regime

Mission	Mid-Term	Long Term
ISR	Stealthy, Long-Endurance UAVs	Stealthy, Extremely Long Endurance UAVs
Air-to-Air	Short-Range, Stealthy Manned Fighters 1st Generation, Stealthy UCAV Prototypes	Long-Range, Stealthy, Highly Autonomous UCAVs UAV Tenders
Deep Strike	Small Number of Stealthy Bombers Small Number of 1st Generation, Stealthy UCAVs Extended-Range PGMs	Long-Range, Stealthy, Highly Autonomous UCAVs Long-Range, Stealthy, Highly Autonomous UCAVs UAV Tenders Advanced, Extended-Range PGMs/Hypersonics
Close Strike	Stealthy, Ground-Attack Fighters Small Number of 1st Generation, Stealthy UCAVs	Long-Range, Stealthy, Highly Autonomous UCAVs UAV Tenders
Strategic Mobility	Small Number of Stealthy Refueler & Transport Prototypes	Large Fleet of Stealthy Refuelers & Transports

See Larry Welch and Donald Latham (chairmen), *Report of the DSB Task Force on High Energy Laser Weapon Systems Applications* (Washington, DC: DoD, June 2001), pp. xii, 65-72.

Stealthy, autonomous UAVs will likely play an increasing role performing ISR missions at all levels of warfare. At the strategic and operational levels, stealthy, high-altitude, extremely long endurance (ELE) UAVs could provide a valuable complement to space-based remote sensing.[374] Able to operate unescorted in contested airspace for days, weeks, or even months at a time, they could provide persistent surveillance over a wide swath of ground using passive sensor suites (e.g., EO, IR, ELINT and SIGINT) or low-probability-of-intercept, advanced electronically scanned array (AESA) radar systems.[375] Stealthy, high-flying, ELE UAVs could be very valuable for finding and tracking mobile, time-critical targets such as missile TELs and SAM launchers. They could also provide a meaningful hedge against the

---

[374] Building upon extended endurance UAV concepts developed under the AARS program in the 1980s, a "Tier III" UAV design was proposed to the Services in 1992. This UAV reportedly could have loitered in the sky for several days at a time. The Special Projects Department of Sandia National Laboratories has proposed developing an extremely long-endurance vehicle (ELEV) or "air breathing satellite" that could fly at 70,000 feet and stay on station for six months to a year with up to a 5,000-lb. payload. It would be powered by a conventional engine during take-off and landing, and by a compact, nuclear-powered engine while on-station. The basic design concept for the nuclear engine is over 40 years old and has already been demonstrated. According to Sandia, building a modern nuclear-turbojet engine would not be an R&D project, but rather an engineering development effort that could culminate in a flight test within a decade. Although significant political obstacles would have to be overcome to field a nuclear-powered UAV, it appears to be both practical and safe from a technical perspective. See Thomas P. Ehrhard, *A Comparative Study of Weapon System Innovation: Unmanned Aerial Vehicles in the United States Armed Services* (John Hopkins University PhD Dissertation, 2000), pp. 136-158; David Fulghum and Robert Wall, "Long-Hidden Research Spawns Black UCAV," *Aviation Week & Space Technology*, September 25, 2000, p. 28; and Sandia National Laboratory, Unclassified briefings on "Extremely Long Endurance Covert UAV," February 2001 and "Air-Breathing Satellite," May 3, 2002.

[375] AESA radars incorporate a number of techniques for reducing the probability of intercept while emitting, including minimizing side lobes and reducing beam width. The signature could be further reduced by using two or more UAVs simultaneously, with each aircraft taking a turn emitting a radar pulse that would then be received and processed collectively. See David Fulghum, "Stealthy UAVs Snag Rumsfeld's Attention," *Aviation Week & Space Technology*, June 4, 2001, p. 30.

potential loss of imaging and communications satellites to enemy space-denial operations.

At the tactical level, cheap, rugged, bird-sized MAVs could revolutionize forward scouting and surveillance.[376] For example, a soldier could take one out of his rucksack and instruct it to fly over an adjacent hill or down to the next city block to determine if enemy units were in the vicinity. To conserve energy, MAVs could "perch" on buildings, trees, or other elevated positions and "stare" at areas of interest using a variety of onboard sensor systems. Swarms of MAVs could fly into buildings, subways, and other urban structures in advance of ground troops to map the interior layout, as well as to determine the location of booby traps, enemy forces, and noncombatants.

Stealthy intercontinental bombers and long-range UCAVs will likely come to dominate the airborne, penetrating component of deep-

[376] In 1996, DARPA launched a program to develop MAVs, which were defined as being no larger than 15 centimeters in any dimension. It was subsequently expanded to no more than 12 inches in any dimension. A variety of propulsion alternatives are being explored, including fixed-wing, rotary-wing and flapping-wing designs. Considerable progress has been made in four critical enabling technologies: aerodynamic control and platform stabilization in a low Reynolds-number regime; high-density energy storage (e.g., next-generation batteries and fuel cells); ultra-light, low-power sensors and communication systems; and artificial intelligence required for autonomous operations. Several prototypes, including a flapping-wing or ornithopter design, have been flown under laboratory conditions. Based on the status of ongoing R&D programs, it should be possible to procure battlefield MAVs by around 2015 that could perform local-area ISR missions, drop microsensors, relay communications, and even identify, track and tag high-value enemy assets based upon ATR algorithms. Moreover, given current trends in MEMS technology, there is good reason to believe that MAVs could also be cheap enough to issue to individual soldiers. See OSD, *Unmanned Aerial Vehicles Roadmap: 2002-2027* (Washington, DC: DoD, 2003), pp. 18-19; Mark Hewish, "Small, But Well Equipped," *Jane's International Defense Review*, October 2002, pp. 53-62; Mark Hewish, "A Bird in the Hand," *Jane's International Defense Review*, November 1999, pp. 22-28; and James M. McMichael and Col. Michael Francis, "Micro Air Vehicles – Toward a New Dimension in Flight," DARPA Concept Paper, August 1997 (Available on-line at: http://www.darpa.mil/tto/mav/mav_auvsi.html).

strike forces. Aside from dropping large numbers of smart, relatively low-cost PGMs on both fixed and mobile targets, stealthy bombers might also be relied upon to deliver large gravity bombs and heavy earth-penetrator weapons needed to destroy hardened and deeply buried targets.[377] Owing to their extended endurance, and thus, loiter time, UCAVs would be particularly valuable for attacking all types of mobile, time-critical targets on land and at sea.[378] Specialized electronic warfare UCAVs might be used to attack enemy information systems with RF weapons, to jam enemy sensors, or to spoof them with false-signature generators.[379]

Stealthy, loitering UCAVs may eventually be relied upon for much of the close-strike mission as well. Engaged ground troops could call upon UCAVs orbiting overhead for rapid-response fire support. As a consequence of the dramatically increased effectiveness of multidimensional long-range strike forces (e.g., shorter time-of-flight

---

[377] DARPA's Quiet Supersonic Platform (QSP) program could create the foundation for a future supersonic UCAV that could travel about three times as fast as the B-2. Robert Wall, "Bomber Becomes Focus of Quiet Aircraft Effort," *Aviation Week & Space Technology*, May 6, 2002, p. 28; Bill Sweetman, "Supersonic Bomber Revival," *Jane's International Defense Review*, March 2002, pp. 60-62; and Michael Sirak, "DARPA Selects Two to Develop Supersonic Aircraft," *Jane's Defence Weekly*, March 13, 2002.

[378] By leveraging R&D associated with the development of the B-2, the F-35 JSF, the Global Hawk HALE UAV, and the J-UCAS program, it appears to be possible to build a stealthy, highly autonomous, global-strike UCAV with a 6,000-mile unrefueled range, a 20,000-pound payload, and a high-subsonic cruising speed within the next decade. (Authors' discussions with Northrop Grumman representatives regarding the Unmanned Global Strike System (UGSS) concept.) See also: Donald Hicks/Northrop, "The Unmanned Global Surveillance-Strike System (UGSSS) and Military Transformation," White Paper prepared for the 2003 DSB on Future Strategic Strike Systems, August 2003.

[379] Foreshadowing this possibility, the Air Force is exploring the technical possibility of using the X-45 UCAV in an electronic strike role. See David Fulghum and Robert Wall, "USAF Tags X-45 UCAV as Penetrating Jammer," *Aviation Week & Space Technology*, July 1, 2002, p. 26; David Fulghum, "UCAVs also Tagged to Carry Energy Weapons," *Aviation Week & Space Technology*, July 8, 2002; and Michael Sirak, "US Mulls Electronic Attack Potential of Strike Drones," *Jane's Defence Weekly*, August 21, 2002.

made possible by hypersonic propulsion, in-flight retargeting capabilities, and brilliant submunitions that can identify and attack specific targets), the unique loitering capability of UCAVs, and the challenges associated with inserting heavy, difficult to supply, short-range artillery in an anti-access environment, the latter could largely disappear from the future battlefield.

As air forces are forced to mount air-to-air and ground-attack operations from extended ranges, new platforms may need to be developed to compensate for the loss of in-theater airbases. For example, one candidate system might be the "UAV Tender," envisioned as an intercontinental-range, high-endurance, stealthy aircraft capable of launching, controlling, recovering, rearming, and refueling a squadron of relatively short-range strike and air-control UCAVs.[380] Supported by an enlarged fleet of stealthy and non-stealthy air refuelers, UAV Tenders could be critical in an enabling air power to be surged forward early on in a crisis. Swarms of tender-supported, ground-attack UCAVs could be invaluable, for example, in halting a large-scale ground invasion or in providing responsive, high-volume, precision fire support (i.e., airborne artillery) for engaged ground forces. UAV Tenders and their complement of strike and air-control UCAVs could also work to gain and maintain some measure of air control within contested airspace.

Low-observable refuelers might be used to extend the endurance of stealthy aircraft operating in the heart of an adversary's anti-access defenses.[381] By obviating the need for strike and air-superiority aircraft to return all the way back to a remote peripheral base outside the

---

[380] Taking advantage of the fact that they would not have to take-off or land from the ground, these UAVs could have a significantly smaller wingspan than traditional UAVs and would not need landing gear. To fit within the limited confines of the tender, they would necessarily be relatively small (and thus, short-range) and would carry miniaturized PGMs and air-to-air weapons.

[381] Lockheed Martin reportedly developed a preliminary concept for developing a low-observable tactical tanker/transport for the US Air Force. See "Stealth Technology May Help to Develop LO Transport," *Jane's Defence Weekly*, May 6, 1998, p. 6. The development of a stealthy transport aircraft was also endorsed by the 1996 DSB Summer Study Task Force. *Tactics and Technology for 21st Century Military Superiority*, pp. VI-10, C-10.

range of the enemy's missiles or to uncontested airspace to refuel, a low-observable refueling capability could dramatically increase their on-station time.

In order to insert and sustain ground forces safely into a theater overwatched by an adversary armed with robust anti-access capabilities, it will likely be necessary to apply stealth technologies to both inter- and intra-theater air transports. New forms of precision resupply, perhaps using stealthy, GPS-guided parafoils, might also be required. Force extraction could become a very high-risk endeavor for future air mobility forces because of the need to land and the time it takes to onload troops and equipment. During that relatively brief window in time, even a stealthy transport would be vulnerable to detection and attack by an adversary's reconnaissance-strike systems.

War on Land

The threat posed by the proliferation of sensors linked to progressively more capable precision-strike weapons will probably require advanced RMA ground forces to adopt a stealthy means of insertion and sustainment (see Table 4). Today's high-signature insertion platforms would almost certainly be vulnerable to detection and attack. For example, large sealift vessels moored at known, fixed ports would generate signatures that could be easily detected, especially while off-loading troops and equipment. Once detected, these vessels, as well as the port itself, would be very vulnerable to attack. Similarly, large non-stealthy airlifters would not only have difficulty penetrating airspace defended with next-generation IADS, but would also become lucrative targets for precision strikes once they landed at fixed airbases within the theater of operations.

As maritime area-denial capabilities diffuse, surface amphibious ships located offshore will become progressively easier to target. Even if their "sea base" was somehow secured, amphibious units inserting via surface craft would still need to navigate through concentrated fields of increasingly sophisticated mines that can move, share information, and recognize and attack specific targets. Given the prevalence of SAMs with extended-range intercept capability, as well as ubiquitous MANPADS, high-signature, low-flying tilt-rotor transports (e.g., V-22s) would likely fare no better ferrying troops and equipment from ships to inland objective areas.

Table 4: Transformation to an Advanced RMA Land Warfare Regime

Missions	Mid-Term	Long Term
Insertion & Sustainment in Anti-Access Environments	Stealthy Airlifter Prototypes for SOF GPS-Guided Parafoils Submerged Insertion Limited to Small Number of SOF (SSNs/SSGNs)	Large-Scale, Stealthy Air Insertion Operations Large-Scale, Submerged Insertion Operations
Maneuver, Close Combat, and Urban Warfare	Future Combat System "Objective Warrior" UGV Prototypes MAV Prototypes	Stealthy, Electric-Drive Advanced Combat Vehicles & IFVs Stealthy UCAVs Exoskeleton-Equipped Troops Specialized, Information-Intensive, High-End Infantry Advanced Robotics – UAVs, MAVs, UGVs & Microrobots Multispectral Decoys and Holographs
Deep Strike	Unmanned, Remotely Fired Missile Pod Prototypes (e.g., the "NetFires" program)	Advanced, Unmanned, Remotely Fired Missile Pods

Consequently, at least early on in a conflict, future ground forces may have to be inserted via stealthy airlifters; stealthy, high-speed, over-the-beach, surface insertion vessels; and submerged, troop-carrier platforms (initially, modified SSGNs). Even with such insertion platforms, an emphasis would likely need to be placed upon concepts

of operation that further minimize the probability of detection, such as the following:

- Conducting extensive information preparation of the battlespace (IPB) prior to inserting forces, including selectively blinding enemy ISR assets and conducting operational-level deception operations (e.g., disseminating large numbers of multispectral decoys and conduction information operations to mislead or "spoof" enemy ISR systems);

- Entering the theater rapidly at a large number of geographically dispersed insertion points in order to avoid large, possibly detectable concentrations of otherwise stealthy forces;

- Relying upon air drops with parachutes or precision-guided parafoils for force and supply insertion to the greatest extent possible, and when necessary, landing and rapidly offloading stealthy transports on dispersed, remote, unimproved runways (e.g., strips of road); and

- Conducting airdrops primarily at night in order to reduce the chances of detection by EO sensors.

These operational constraints would place severe limits on the type and number of ground forces that could be successfully inserted into theater and subsequently sustained. In light of these limits, it would be important to maximize the combat power of those relatively few deployed forces. This might be accomplished, for example, by endowing them with advanced C4ISR capabilities, equipping them with various kinds of robotic support, and by networking them closely with units operating in the other dimensions of the battlespace. A large portion of their firepower, for example, would likely reside in stealthy surface ships and submerged strike platforms waiting offshore, or aboard UCAVs orbiting overhead.

Ground combat could take on many of the attributes of special operations today. Once inserted, ground forces might move immediately toward enemy objectives or small, dispersed hide sites. When the moment was favorable, these widely distributed forces could take advantage of their advanced C4ISR capabilities and mobility to launch coordinated, multi-axis attacks on enemy targets and then return to different hide sites to await mission orders for the next sortie. Rather than rely upon centralized stockpiles of supplies that

would be vulnerable to attack, ground forces could maneuver to widely distributed, geo-located caches of supplies dropped from stealthy airlifters as part of each offensive pulse or sortie. Alternatively, robotic, vertical-takeoff-and-landing (VTOL) transports could carry tailored resupply loads directly to widely dispersed ground units.[382]

If ground forces are to be more than spotters for external, long-range precision strike (LRPS) systems, they will likely require significant advances in lethality, operational mobility and protection. One promising technology that could potentially be fielded in the decade after next is the exoskeleton—a self-powered, robotic suit worn by dismounted infantry and special operations forces. Exoskeletons could dramatically increase the organic firepower of individual soldiers by making it possible for them to carry heavier weapons, more ammunition, or a wider array of weapons. They could also enable soldiers to move cross-country at a relatively high sustained speed and carry a more extensive suite of sensors, communications equipment, ballistic protection, and information protection (e.g., decoys and false-image generators) than would otherwise be possible. DARPA recently launched an R&D program called, "Exoskeletons for Human Performance Augmentation," to explore the feasibility of developing precisely this type of capability. The program is focused on developing technologies that:

> [E]nhance a soldier's physical performance to enable him, for example, to handle more firepower, wear more ballistic protection, carry larger caliber weapons and more ammunition, and carry supplies greater distances. This will provide increased lethality and survivability to ground forces in combat environments, especially for soldiers fighting in urban terrain....[W]e plan to explore systems with varying degrees of sophistication and complexity, ranging

[382] Air-dropped supplies could be positioned at specific coordinates on the ground by taking advantage of GPS-guided parafoils or semi-rigid wing systems. Boeing has completed conceptual design studies for a VTOL transport, dubbed the Light Aerial Multipurpose Vehicle, which would be capable of carrying a 1,500 payload nearly 2,000 kilometers. See David Fulghum, "VTOL Transport Planned," *Aviation Week & Space Technology*, September 22, 2003, p. 31.

from an unpowered mechanical apparatus to full-powered mechanical suits.[383]

The performance objectives for an initial operational prototype, which is expected to be available for field testing as early as 2008-2010, are an unrefueled endurance of up to 24 hours under normal operating conditions, a payload capacity of 100-200 pounds exclusive of the exoskeleton's weight, and the ability to move at an average sustained pace of 4-6 miles per hour (mph).[384] By 2020-2025, it is technologically possible that exoskeleton-equipped soldiers could operate in the field for days without being refueled, move over uneven terrain at a sustained pace of over six mph, dash short distances as fast as world-class sprinters (e.g., 100 yards in ten seconds), ascend or descend multiple flights of stairs very quickly, and bound over urban obstacles (e.g., piles of rubble, fences, and walls). A number of subsystems could be integrated into the basic exoskeleton "platform" including various C4ISR systems; situational awareness and navigation systems; a shoot-on-the-move, stabilized weapon system; and medical treatment systems. Individual exoskeleton-equipped soldiers could also have organic MAVs, UGVs and robotic porters for surveillance and logistics support.

The relatively well-defined fronts of opposing forces that characterize conventional land warfare in the current regime could give way to non-linear combat formations in a LRPS-dominant regime. Advanced RMA ground units would likely fight from dispersed, non-contiguous positions and with a 360-degree

---

[383] Alexander, *Testimony before Subcommittee on Emerging Threats and Capabilities of the Senate Armed Services Committee*, pp. 29-30. See also Fernandez, *Testimony before Subcommittee on Emerging Threats and Capabilities of the Senate Armed Services Committee*, p. 29.

[384] Proof-of-concept demonstrations of lower-body components, including power and actuation controls, were completed in 2003. Demonstrations of self-powered, full-body exoskeleton suits are scheduled for 2005-2006. Core technological enablers for the exoskeleton include high-density power sources, energy-efficient actuators, haptics and active-control approaches that sense and enhance human motion, ergonomics and human-machine interfaces, and complex system design and integration. See Dr. John Main, EHPA Program Briefing, February 2004.

orientation (i.e., enemy positions and sensors could *routinely* be in front, behind, or to the sides of friendly positions). In addition, network forms of small unit organizations could emerge to take full advantage of available C3 capabilities.

The lethality of multidimensional, precision-strike capabilities linked to robust sensor networks could lead to an "emptying" of the ground battlespace. The relatively small number of ground forces inserted into a given theater would probably be dispersed over a wide area to minimize their footprint and reduce the chances of being detected by the opposing side's ISR systems. While the resulting reduced force-to-space ratio might create substantially enhanced opportunities for maneuver, the lack of enemy force concentrations could frequently limit the effects of ground maneuver to the tactical level. In other words, although the existence of open terrain and enhanced mobility could facilitate ground maneuver, there may not be any large enemy force concentrations against which to gain an advantageous position. As a result, future ground campaigns might be characterized by many relatively small tactical engagements and few, if any, grand decisive battles. Furthermore, the combination of stealth and improved mobility could make it easier for small, dispersed ground forces to decline battle. In which case, conventional ground operations could, in some respects, come to resemble high-intensity guerrilla warfare.

The traditional role of indirect fires supporting maneuver forces is likely to remain relevant in an advanced RMA regime. For instance, indirect fires could facilitate maneuver by suppressing or destroying enemy precision-strike units, and by impeding the movement of enemy maneuver units. However, the reverse relationship—maneuver units operating in support of indirect fires—may become much more common. Maneuver units may be increasingly used to lure or compel enemy forces out of either physical or information-based concealment in order to enable precision strikes from remote platforms. In short, friendly maneuver forces may need to fix the enemy—becoming the *cheng* (or shaping) force in Sun Tzu's lexicon—to better allow LRPS systems to serve as the *ch'i* (or killing) force.

Seizing territory may be easier to accomplish than physically holding it. In an advanced RMA regime, controlling terrain would be complicated by the fact that stationary troops holding ground, just like any other fixed target, would be vulnerable to detection and attack by an opponent's reconnaissance-strike assets. Against a regional

adversary with a relatively small missile force, it might be possible to eliminate or exhaust its missile arsenal over time. However, this might be difficult to achieve against a peer or near-peer competitor with a large missile arsenal that could be regenerated over time and the ability to launch missiles from a secure homeland sanctuary. As a result, the best that might be hoped against some competitors may be to control ground indirectly with survivable, long-endurance sensors linked to precision-strike systems and a mobile force-in-being that could project force on the ground whenever necessary, but that is not tied down to a specific, identifiable piece of terrain. This might be accomplished, for example, by linking UGS networks, sentry and scout robots, and UAVs to a network of orbiting UCAVs, ground-based missile launchers, maritime fire support assets, and dispersed, rapid-response close combat forces. If enemy forces tripped the sensor grid, strike and maneuver units could quickly be brought to bear.

Adversaries will continue to be drawn toward urban areas because they contain valuable material resources, military-related infrastructure (e.g., ports, airfields, radio and television broadcast stations), and the physical apparatus of government. Based on demographic projections, by 2025, over 85 percent of the world's population will reside in urban areas.[385] Future adversaries will also likely gravitate toward these areas to diminish US C4ISR and precision-strike advantages. Evicting enemy units from the sprawling urban megacities of tomorrow will likely be excruciatingly difficult. The combination of ubiquitous sensor systems; local and theater-range, precision-strike systems; and micro-scale capabilities (e.g., MAVs and microrobots) will limit both the quantity and form of force that can be projected into these areas (and sustained after entry), and impose severe constraints on operations. Large garrisons and military C3 nodes within a city, for example, would be easy targets for PGMs. Even with the full range of next-generation C4ISR systems at their disposal, it will remain a daunting challenge for a relatively small

[385] General Accounting Office, *Military Capabilities: Focused Attention Needed to Prepare US Forces for Combat in Urban Areas* (Washington, DC: February 2000), p. 6; and Central Intelligence Agency, *Global Trends 2015: A Dialogue About the Future with Non-governmental Experts*, (Washington, DC: NIC 2000-02, December 2000, GPO #041-015-00211-2).

number of friendly forces to find and evict enemy units hiding in large urban enclaves.

With comparatively small forces, it would be problematic for either side in a conflict to gain and maintain control over a city housing potentially tens of millions of inhabitants. The combination of dense sensor coverage, advanced C3 systems, and increased mobility could allow advanced-phase RMA forces to police urban areas much more efficiently than in the past. Nevertheless, conducting urban control operations, especially in an anti-access environment, will likely remain exceedingly difficult. Winning over the population will likely be essential for gaining an upper hand in urban eviction and control campaigns. This requirement may place a premium on psychological and information operations. An advantage could also be gained by developing irregular forces and employing robotic forces as force multipliers. For instance, microrobots and MAVs could be employed as a "stay behind force" to monitor and defend cleared areas such as secured buildings, neighborhoods, utilities, or other important urban nodes.

War at Sea

The ability to dominate the surface of littoral waters using land- and space-based assets, and the replacement of manned aircraft with missiles and UCAVs for naval strike, could transform war at sea. A reconnaissance-strike architecture comprising maritime-reconnaissance satellites (e.g., SAR, EO, infrared, and ELINT satellites); OTH radar; land-based UAVs and UCAVs; and ground-, air-, and sea-launched ASCMs could enable small naval powers to contest control of the sea for extended distances from their borders (see Table 5).

Table 5: Transformation to an Advanced RMA Naval Warfare Regime

	Mid-Term	Long Term
Area Denial	UAVs & Satellites OTH Radar AIP Attack Submarines Stealthy, Long-Range ASCMs with Terminal Guidance Wake-Homing Torpedoes Advanced Mines	Stealthy HALE UAVs & Next-Generation Satellites (SAR/MTI, IR, and ELINT AIP & Nuclear Attack Submarines Stealthy, Very Long-Range ASCMs Anti-Navy UCAVs "Brilliant" Mobile Mines Advanced Sensor Nets
Surface & Air Warfare	Carrier-Based JSFs / First-Generation UCAVs Stealthy Frigate Prototypes (Littoral Combat Ship) Advanced Munitions (e.g., Tactical Tomahawk)	Networked Fleet of Stealthy Frigates / Unmanned Surface Vessels Carrier-Based, Long-Range UCAVs Next-Generation Munitions
Undersea Warfare	SSNs Semi-Autonomous, Medium-Endurance UUV Prototypes Unmanned Undersea Strike Module Prototypes SSGNs (Converted SSBNs)	Submarine After Next Built-for-Purpose SSGNs Advanced Undersea Strike Modules Fully Autonomous, Long-Endurance UUVs Sensor Nets Undersea Amphibious Assault Vessels Submerged Mine Countermeasure Ships Submerged Fleet Replenishment & Logistics Ships

This type of basic "anti-navy" architecture could be made more effective by incorporating increasingly sophisticated mines, active and passive sea-based sensor networks, and quiet attack submarines. Such architectures would have far lower barriers to entry (cost and learning) than carrier battlegroup operations, potentially enabling those competitors who pursue them to leapfrog the carrier era and become major maritime competitors, at least in littoral waters. Establishing sea control against an adversary with a robust, multidimensional, area-denial network could require winning not only the undersea and surface battles, but the space (satellite reconnaissance), air (manned and unmanned ISR and strike platforms), and land battles (ASCM launchers) as well.

In response, absent a revolutionary breakthrough in ASW, naval power-projection operations could be driven sub-surface.[386] Since electromagnetic energy attenuates rapidly in water, submerged platforms will, in all likelihood, remain more difficult to locate than traditional surface vessels. As an alternative to going undersea, it might also be possible to rely upon distributed networks of relatively small, stealthy surface ships. In either case, however, missiles and UCAVs could, in large measure, supplant manned aircraft as the principal basis for naval strike.

The capital ships of the future fleet might be built-for-purpose SSGNs armed with a mix of several hundred ballistic and stealthy, hypersonic cruise missiles and outfitted with a flexible ocean interface for launching and recovering a variety of autonomous, multi-mission UUVs and UAVs.[387] A distributed, power-projection navy might

---

[386] We assume that the ability of submerged vessels to operate quietly and manage non-acoustic signatures will stay ahead of developments in ASW technology. Despite the emergence of new sensors and sensor platforms (e.g., UUVs and anti-navy UAVs), detecting and localizing sub-marine vessels operating in a vast ocean will probably continue to be a labor intensive *and* time consuming enterprise. If that assumption proves unfounded, naval power projection platforms would likely be driven toward speed and active defenses.

[387] According to some estimates, SSGN-like vessels could carry as many as 2,000 missiles of different sizes and ranges. Eric Labs, *Budgeting for Naval Forces: Structuring Tomorrow's Navy at Today's Funding Level* (Washington, DC: CBO, October 2000), Chapter III.

include several classes of SSGNs, as well as stealthy surface ships, unmanned undersea strike modules,[388] submerged mine countermeasure ships (employing autonomous UUVs for mine detection and mapping), undersea amphibious assault vessels (with embarked submerged troop-insertion vehicles), and submerged fleet replenishment and logistics prepositioning ships. Legacy surface ships would be used mainly for peacetime engagement and presence functions, as well as for power-projection operations in relatively benign threat environments.

As suggested above, autonomous UUVs could take on a much broader array of missions than is the case today.[389] In addition to mine

---

[388] The Defense Science Board (DSB) endorsed the "undersea strike module" concept in 1998. It was envisioned as a stealthy, unmanned, submerged platform containing a large quantity of missiles that could be towed to an area of interest by an attack submarine. Once in theater, the module would be released above the continental shelf in up to 500 feet of water. It would then bottom on the seafloor, self-anchor, or both. All non-essential equipment would be powered down to a "sleep" mode to preserve energy and keep the module's radiated signature as low as possible. In this mode, it could remain on station for up to 12 months, and be awakened at any time by an encoded extremely low frequency (ELF) message or acoustic signal. Once on-board command and control systems were up and running, the module could receive targeting coordinates, or alternatively, coded references to preset target packages that had already been downloaded into its digital library. After rising to launch-depth and firing a missile salvo, it would wait for additional instructions, and after a pre-defined period of time had elapsed, return to its sleep mode. SSNs could tow deployed modules to ports around the world for refueling and rearming as part of their routine mission taskings. See DSB 1998 Summer Study, *Joint Operations Superiority in the 21st Century* Vol. II (Washington, DC: Office of the Undersecretary of Defense for Science & Technology, 1998), pp. 5-14.

[389] As a step in this direction, the Navy recently launched the Mission Reconfigurable UUV program that seeks to develop and field an autonomous, multi-mission capable UUV by 2007. The US Naval Undersea Warfare Center's Unmanned Undersea Vehicle Initiative is focused on the development of autonomous UUVs capable of carrying a range of interchangeable mission payloads in order to execute a variety of complex missions (e.g., above-water ISR, mine reconnaissance, tactical oceanography, and ASW) in non-permissive, high-threat environments. An early prototype and testbed for future technologies, called the Manta Test Vehicle, began trials in 1999.

reconnaissance and mapping, they might be used for offensive mining, precision mapping of the sea floor, covert ISR missions in littoral waters, laying fiber-optic cable for undersea littoral communications, acting as a relay node for undersea communications, ASW and anti-surface warfare (ASuW) operations, and precision-strike operations against land targets.[390] In some cases, "packs" of relatively small, short-range UUVs hosted by a mothership (e.g., SSGNs and SSNs with a flexible ocean interface or conformal docking points outside the pressure hull) might be used to saturate a given area of interest quickly. Minehunting, underwater object location and recovery, and hydrographic and bathymetric survey missions, for example, might be conducted most efficiently by packs of cooperating UUVs. In contrast, independent UUVs with an endurance measured in weeks or months might be used to track and trail enemy submarines, as well as to conduct independent ISR, ASW, and ASuW operations.

In comparison to today, future amphibious operations could be far smaller in scope and may come to rely on more covert insertion methods. As area-denial threats mature, amphibious forces might be forced to conduct their assaults and sustain their operations from *under* the sea rather than upon it. Furthermore, given that it will likely be impossible to isolate a contested beach in a deep-fires environment, amphibious entry will likely be conducted against remote, undefended coastal areas where enemy forces and sensors are known to be either limited or absent.

Future countermine operations will likely seek to detect, mark and map hostile mines clandestinely rather than destroying them in place, which would generate a detectable signature and give away the location of friendly forces. In cases where it is impossible to maneuver through a mine field without channeling friendly forces into suspected enemy sensor nets or submarine patrol areas, or when mobile mines are present, it may be necessary to use multiple UUVs, UCAVs, or

---

Richard Scott, "Unmanned, Undersea – Future Undersea Battlespace," *Jane's Defence Weekly*, June 12, 2002, pp. 29-34.

[390] Ibid. See also: Mark Hewish and Joris Janssen Lok, "Silent Sentinels Patrol the Depths," *Jane's International Defense Review*, April 2003, pp. 49-54; and Christian Bohmfalk, "Submarine Studies Point to Unmanned Vehicles, Advanced Weapons," *Inside the Navy*, April 30, 2001, p. 1.

other assets to disable simultaneously many widely separated mines. The goal would be to create so many gaps through which friendly forces could potentially transit that it would be impractical for the enemy to fix them to a specific avenue of approach.

Space Warfare

Space warfare should not be equated simply with the stationing and use of weapons in space. Such a definition would artificially exclude a range of activities that should unquestionably be captured as elements of space warfare. It would be logically untenable, for instance, to assert that destruction of one state's satellites by another's ground-based ASATs should not be considered space warfare just because the ASAT interceptors themselves were not fired from space. Space warfare should be construed more broadly to include combat to, within, through, or from space in order to gain military advantages or to deny them to potential adversaries. Through a series of incremental, escalatory steps in the mission areas of space control, terrestrial strike, and missile defense, it is entirely conceivable that space will become extensively weaponized by multiple states by 2020-2025, if not sooner (see Table 6).

Most thinking about the emergence of space warfare assumes that it will come about as the result of a sudden discontinuous change in the strategic competition. It is far more likely, however, that space warfare will emerge through a gradual fielding of less controversial capabilities. The pace of change will likely be affected by a number of variables, including the rate at which relevant technologies diffuse, shifting political or cultural barriers to the weaponization of space, and evolving military requirements. As discussed in Chapter III, initially, some states might employ broadband jammers because the enabling technology is widely available; there are few political or cultural constraints related to their use; and, by interfering with satellite uplinks and downlinks, they could significantly degrade an enemy's ability to exploit COMSATs for military purposes. Over time, however, those same states may field more threatening space warfare capabilities as new technologies become available, as the threshold for what is considered an acceptable military use of space rises, and as new military requirements come to the fore.

Table 6: Transformation to an Advanced RMA Space Warfare Regime

Mission	Mid-Term	Long Term
Space Control	Terrestrial Uplink & Downlink Jammers GPS Spoofers Low-Power Laser Dazzlers First-Generation "Proximity Operations" Microsatellites Direct-Ascent, Kinetic Kill ASATs	Advanced "Proximity Operations" Microsatellites Manned/Unmanned Space Maneuver Vehicles Directed-Energy ASATs Advanced Jammers & Spoofers
Space Strike	Unmanned Suborbital Strike System Prototypes	Robust Fleet of Unmanned Suborbital Strike Systems Manned Trans-Atmospheric Vehicles & Space Planes
Missile Defense	Ground-Based Interceptors with Space-Based ISR Cueing (SBIRS)	Space-Based Kinetic Interceptors (e.g., Brilliant Pebbles) Space-Based Lasers

Based on current investment trends, described previously, it appears likely that the United States and/or its competitors will develop and field the following types of space warfare capabilities over the next few decades:

- Robust terrestrial- and space-based space surveillance systems for characterizing and tracking objects in space;
- Directed-energy ASAT systems based on airborne, ground, sea, or space platforms that can damage or destroy targeted satellites by causing thermal overload or radiation damage;
- Microsatellites that can stalk an adversary's satellites in peacetime and then jam, damage or destroy them on command;
- Unmanned, re-useable, two-stage, suborbital strike systems capable of rapidly hitting targets anywhere in the world;

- Manned and unmanned trans-atmospheric vehicles (TAVs) or space planes that can conduct offensive or defense space control missions in near-earth space, repair or refuel satellites, or release precision-guided projectiles against terrestrial targets; and

- Space-based ballistic missile defense systems (e.g., space-based lasers or "Brilliant Pebble" interceptors).

The balance between offensive "space control" capabilities and defensive countermeasures is unlikely to be stable. Given that an attack in space could be initiated with little or no warning and individual strikes could occur very quickly—in some cases, at the speed of light—competitors would have a strong incentive to put their defensive systems and retaliatory capabilities on hair-trigger alert, especially during periods of heightened tension. A premium would be placed on early warning and survivable space situational awareness capabilities. The apparent feasibility of mounting rapid, surprise attacks in space would make preemption attractive both as a means of protecting one's space-based assets and for disarming one's opponent.[391] To hedge against a disarming surprise attack, states might develop robust, survivable space reconstitution capabilities (e.g., mobile or sea-based SLVs and micro-satellites), as well as terrestrial replacements for space-based capabilities (e.g., extremely long-endurance UAVs and lighter-than-air, near-space vehicles for long-haul communications, wide-area ISR, and precision navigation).

Currently several countries have the ability to conduct terrestrial strikes through space with long-range ballistic missiles or modified SLVs (e.g., the United States, Russia, China, North Korea, France, Israel, India, and Japan). Over the next two decades, militaries may attempt to expand their options for conducting terrestrial strikes

[391] In many respects, the future offense-defense balance in space could mirror the balance between US and Soviet strategic nuclear forces during the Cold War, especially early on when warhead inventories were comparatively small and delivery systems were vulnerable to attack. The analogy, however, is limited. It is hard to imagine, for instance, a space-based parallel to the elements that proved critical to the creation of a Soviet and American "assured second strike" capability such as super-hardened, land-based silos and highly survivable, stealthy SSBNs.

through or from space. For instance, with declining access to forward basing overseas and motivated by the strategic need to project power to distant corners of the globe, the US military may develop an unmanned, rocket-powered, sub-orbital vehicle for terrestrial-strike missions. Outfitted with an upper-stage containing Common Aero Vehicles (CAVs), a suborbital vehicle could strike fixed and possibly mobile targets as distant as halfway around the earth in tens of minutes after launch.[392] The US military is also actively pursuing the development of a re-useable space plane, referred to as a Hypersonic Cruise Vehicle (HCV), which could take-off and recover like traditional aircraft on standard military runways. The HCV is expected to be capable of striking multiple, diverse, and widely dispersed targets up to 9,000 nautical miles away with up to 12,000 pounds of munitions

[392] The CAV is expected to be flight tested in late 2006 and is slated to become operational by 2010. It is basically a cone-shaped, maneuvering reentry vehicle that can carry and dispense a munitions payload of up to 1,000 pounds (i.e., LOCAAS, SDB, BAT submunitions, or other PGMs). Under a new program called Project Falcon (Force Application and Launch from CONUS), the CAV would be boosted into orbit by a disposable, low-cost, small launch vehicle. The goal is for the boosted CAV to have a range of over 5,000 kilometers, a flight time of less than 15 minutes, and an overall system accuracy of better than three meters. If used as a unitary penetrator weapon, the CAV re-entry glide vehicle would have an impact velocity of 4,000 feet per second. The longer term goal is to develop an "enhanced CAV" that can carry a 2,000-pound payload and can be launched by a reusable SLV or space plane. With this configuration, the CAV is expected to have a range in excess of over 16,000 kilometers with a flight time of 50 minutes. After separation, the CAV would have a cross-range maneuver capability of over 5,000 kilometers. The enhanced CAV is slated for testing in early 2009. See John Tirpak, "Spaceplanes," *Air Force Magazine*, December 2003, pp. 67-68; Mark Hewish, "US Eyes Global Strike within Two Hours with Hypersonics," *Jane's International Defense Review*, August 2003, p. 3; Michael Sirak, "Pentagon Eyes Global Strike System," *Jane's Defence Weekly*, July 2, 2003, p. 8; and Robert Wall, "Global Strike," *Aviation Week & Space Technology*, July 14, 2003, p. 37. Alternatively, a Space Maneuver Vehicle (SMV) upper-stage could be placed atop the SLV for conducting space-control operations. The SMV could refuel friendly satellites, repair damaged satellites, jam enemy satellites, launch co-orbital ASATs, or conduct other offensive and defensive space control missions. William B. Scott, "Wargames Zero in on Knotty Milspace Issues," *Aviation Week & Space Technology*, January 29, 2001, p. 52.

or weapon-delivery vehicles (e.g., CAVs) in less than two hours.[393] The many advantages of conducting terrestrial strikes from space were highlighted by the blue-ribbon Commission to Assess United States National Security Space Management and Organization, which concluded:

> It is possible to project power through and from space in response to events anywhere in the world. Unlike weapons from aircraft, land forces or ships, space missions initiated from earth or space could be carried out with little transit, information or weather delay. Having this capability would give the U.S. a much stronger deterrent and, in a conflict, an extraordinary military advantage.[394]

Over the next 10-15 years, space systems are likely to play only a limited, supporting role in ballistic missile defense. The US SBIRS-low constellation, for example, is being developed to detect and track ballistic missile warheads in the mid-course portion of their flight and cue ground- or sea-based radars and interceptors. Driven by the operational desire to intercept missiles in the boost phase of flight (i.e., before they release their payload of warheads and decoys) and the strategic imperative to reassure friends and allies confronting worrisome missile threats, the United States may eventually opt to deploy missile interceptors (e.g., "Brilliant Pebbles" or SBLs) in space as part of a global missile defense network.

---

[393] The HCV would fly, either autonomously or with a human crew, at Mach 8 while outbound and between Mach 3 and Mach 4 during the return to base. First flight of a prototype HCV is slated for late 2009 or early 2010. An IOC is not anticipated, however, until 2020-2025. The HCV builds upon the Hyper-X technology development program that has been underway for several years. Mark Hewish, "Making Space Fast and Cheap," *Jane's International Defense Review*, February 2004, p. 55; and Tirpak, "Spaceplanes," pp. 67-69.

[394] Donald Rumsfeld (chair), *Report of the Commission to Assess United States National Security Space Management and Organization*, p. 33.

Advanced Information Operations

The information spectrum or "cyberspace" will almost certainly emerge as a warfare dimension in its own right affecting all levels and all other dimensions of warfare. The information aspects of war—information acquisition and denial, information strikes, information-based protection and movement—will likely permeate all military operations. Maneuvers on information "terrain," such as CNA strikes, could become essential to maneuver on physical terrain, and, to a significant degree, information-based protection could supplant traditional notions of physical protection. The emergence of war in the information spectrum, moreover, could add a qualitatively new means for destroying enemy targets and disrupting enemy operations. Electronic commerce and financial flows, for example, might be most effectively attacked through IW.

IW at the strategic, operational and tactical levels could be an important means of gaining a relative advantage over an adversary. It may well be that greater operational advantage will accrue from making the enemy's environment more opaque (through destruction or deception) than it will from making one's own environment more transparent. As discussed in Chapter III, outright control of the information dimension will probably not be achievable given that competitors will almost certainly have access to intelligent, self-healing communication networks; redundant, global communication links that are based not only upon radio waves, but also fiber optic, laser or other waveforms; and sophisticated firewall software, encryption algorithms and anti-jamming techniques.

The basic objective of future IW operations will undoubtedly be about the same as today: defending one's own information networks while at the same time degrading, denying, deceiving, exploiting, or destroying those information systems upon which adversaries rely. The resources dedicated to waging war in cyberspace, however, will likely be qualitatively improved and quantitatively expanded relative to today (see Table 7). Based on his preliminary analysis of this area of competition, Andrew W. Marshall surmises that:

> [P]rotecting the effective and continuous operation of one's own information systems and being able to degrade, destroy, or disrupt the functioning of the opponent's information systems will become a major focus of the operational art. Obtaining early

> superiority in the information realm will become central to success in future warfare. *It has always been important: it will soon be central.*[395]

Table 7: Transformation to an Advanced RMA Information Operations Regime

Mission	Mid-Term	Long Term
IW Defense	Strong Encryption Digital Signatures & Time Stamping Firewalls / Automated Intrusion Detection Advanced Virus Detection & Quarantine Tools	Computationally Unbreakable Encryption Intelligent Agents for Computer Network Defense Biometrics
IW Offense	Early CNA Tools RF Weapons Sensor Spoofing	Advanced CNA Tools Multispectral Decoys & 3-D Holographs

It is easy to imagine a future warfare environment in which thousands of specially recruited and trained information warriors armed with state-of-the-art computer hardware, sophisticated IW-related software and redundant access to global, wideband data links clash over control of the information realm. An important IW task will almost certainly be deceiving enemy information systems as to the location and disposition of friendly forces. This might be accomplished, for example, by spoofing enemy sensors, inserting false data into enemy communications links, launching CNA strikes on data processing nodes, or through the creative use of multispectral decoys and three-dimensional holographs. Information warriors might attempt to orchestrate "virtual feints" to lure the enemy's attention

[395] Zalmay Khalilzad, John P. White, and Andrew W. Marshall, *Strategic Appraisal: The Changing Role of Information in Warfare* (Santa Monica, CA: RAND, 1999), pp. 5-6.

away from sensitive areas (e.g., force insertion and extraction points) at key moments in time.

At the operational and tactical levels, what might be termed "information baiting" operations might be used to support precision-strike missions, as well as maneuver and close combat. The goal of such operations would be to induce an adversary's forces to move, power up active sensors, fire weapons or otherwise engage in activity that reveals their location or places them in a more vulnerable position. For example, sensor-spoofing techniques, perhaps augmented by the seeding of physical multispectral decoys and selective jamming, could be used to bait an adversary into firing missiles at false targets. If successful, this ploy would not only cause an opponent to waste its finite inventory of missiles, but would also expose the missile batteries themselves to counter-strikes.

At the strategic level, future competitors will likely try to map each others' C4ISR networks clandestinely during peacetime in hopes of finding unprotected entry points and vulnerable nodes. Competitors that manage to gain access to a rival's computer network may attempt to leave behind trap doors, which if not discovered, could allow them to by-pass security measures during a subsequent attack. Alternatively, they might hide Trojan horses within legitimate software programs that could perform a wide array of pre-scripted CNA functions when triggered by an external cue or some predefined event (e.g., a specific date is reached or a specific order is issued). A strategic IW campaign might encompass sustained CNA operations against mapped nodes in an adversary's C4ISR network, as well as strikes with RF weapons against known or suspected C4ISR-related infrastructure. Targets for RF weapons might include not only elements within civilian and military telecommunications networks, but also critical supporting infrastructures such as the adversary's power grid and transportation networks.

At a minimum, the goal of such an IW campaign would be degrade an adversary's C4ISR capabilities sufficiently for friendly forces to gain a relative advantage. IW operations might even be able to turn some of an adversary's weapons against him. At the extreme, an offensive IW campaign could potentially be decisive by intentionally causing cascading failures within an adversary's national-level C4ISR networks, inducing strategic and operational paralysis.

Advanced Biological Operations

The biotechnology revolution could potentially spawn a variety of extremely potent biological weapons, including genetically tailored agents capable of targeting specific ethnic groups and stealth pathogens that are very difficult to detect and counter (see Table 8). Future adversaries could, for example, stockpile hundreds of altered strains and novel pathogens in peacetime and employ them in rapid succession during periods of war. Since it will often take time to identify and develop appropriate counters to them, defensive options could frequently be limited and ineffective in the immediate aftermath of an attack. Barring a dramatic breakthrough in broad-spectrum vaccines, BW defenses will likely lag behind offensive capabilities.

Table 8: Transformation to an Advanced RMA Information & Biological Operations Regime

	Mid-Term	Long Term
BW Defenses	BW Sensors Individual Protective Gear Anti-Viral & Antibiotic Drugs Agent-Specific Vaccines	Advanced BW Sensors Lightweight, Breathable Protective Gear Broad Spectrum Drugs DNA Vaccines & Therapies
Offensive BW	Bio-Engineered Agents Bioregulator Weapons Agricultural Warfare	Genetically Specific Weapons “Stealth” Pathogens Novel “Super Agents”
Other Bio-Based Capabilities	Bio-Sensors Bio-Materials Human Performance Enhancement	Bio-Electronics Bio-Computing

As mentioned earlier, advanced BW could also be leveraged as a new tool of political-military coercion. For example, it might be possible to target segments of an adversary's population or leadership with non-lethal agents that make them ill, or with bio-regulator weapons that upset normal bio-chemical processes within the human body. Vaccines or other antidotes that mitigate or reverse the effects of these agents could then be made available in exchange for some desired political action or decision.

Biotechnology could also have a myriad of non-offensive applications including biosensors, bio-electronics, biocomputing, materials, bio-based power sources, and human performance enhancement.[396] There would appear to be great potential for technological surprise or breakout in all of these areas.

THE REVOLUTION IN WAR AND THE SPECTRUM OF CONFLICT

To this point, our discussion has focused on the potential implications of the advanced phase of the RMA on high-end, conventional warfare. As will be addressed below, the ongoing revolution in war could also substantially increase the intensity and lethality of low-end operations. Meanwhile, the strategic scope of the RMA will likely be truncated by the continued dominance of nuclear weapons.

The Nuclear Overhang and Expansion of Strategic Strike

Nuclear weapons can be expected to have a continuing, truncating effect on the strategic scope of the RMA.[397] This nuclear overhang will

---

[396] See National Resource Council, *Opportunities in Biotechnology for Future Army Applications* (Washington, DC: National Academy Press, 2001), pp. 16-72.

[397] Vickers, *Warfare in 2020: A Primer*, p. 13. See also: Andrew Krepinevich and Robert Martinage, *The Transformation of Strategic-Strike Operations* (Washington, DC: CSBA, March 2001), pp. 47-49.

likely limit not only the strategic scope of new conventional capabilities, but also new forms of strategic warfare. The continued dominance of nuclear weapons at the strategic level of warfare is one of the characteristics that makes the structure of the current military revolution unique historically.

To be sure, the ongoing RMA could expand the menu of strategic warfare options available to belligerents. There could, for example, be some substitution of conventional LRPS and space warfare capabilities for nuclear weaponry in strategic war planning. Moreover, a few new means of carrying out strategic attack could be added to the menu (i.e., IW and more lethal forms of BW).[398] But in a general war between competitors with robust strategic nuclear deterrents, both sides will likely grant their opponent's homeland some degree of sanctuary status. At a minimum, nuclear-armed adversaries will probably be deterred from attempting to change the regime of the opposing side through the direct application of military force.

The presence of nuclear weapons could have a similar politically limiting effect on lesser contingencies. A regional power armed with a small, but survivable arsenal of deliverable nuclear weapons could hold at risk an opponent's theater bases and visible, forward-deployed forces thereby compelling the abandonment of traditional means of conventional power projection.

Terrorism and Intra-State Conflict

The ongoing military revolution may also be unique historically in its potential to affect the lower end of the conflict spectrum.[399] States will

---

[398] See Andrew Krepinevich and Robert Martinage, *The Transformation of Strategic-Strike Operations*, pp. 47-49; and Kurt Guthe, *The Nuclear Posture Review: How is the "New Triad" New?* (Washington, DC: CSBA, 2002).

[399] One of the key uncertainties associated with the ongoing RMA is whether it will ultimately undermine or strengthen state structures and institutions. In some advanced states, the effects could well be centripetal, meaning that the central government will be able to exert control more effectively. States who see their power increased are likely to be the most competitive economically and coherent politically. For the majority of states, the dominant effects of the

not have exclusive access to many of the key enabling technologies underpinning both the early and advanced phases of the ongoing revolution in war. Many militarily useful systems will likely become available in either the open or black market. For nearly a decade, drug traffickers smuggling contraband into the continental United States have been equipped with state-of-the-art night-vision devices, encrypted radio sets, cellular phones, and GPS receivers.[400] In the future, insurgents, terrorists, organized criminals, and other non-state actors could exploit many of the RMA-related capabilities described in previous chapters. In some cases, non-state actors may exploit these capabilities more quickly or more skillfully than states. In any event, owing in part to the diffusion of these technologies, future low-end operations could increase substantially in intensity and lethality.

Connectivity and Awareness

One of the consequences of the ongoing information revolution is that states have become less able to control the flow of information into and within their borders. As a result, the future will likely see an upsurge in the frequency and formidability of challenges to state authority. With unprecedented access to information, sub-national groups could become more aware of their relative deprivation, form higher expectations, and impose increasing demands on state governments. In states that are unable to satisfy those demands, rising social discontent could create a fertile environment for the emergence of insurgent groups championing populist sentiments and exploiting communal identities (e.g., ethnic, religious, socio-economic, etc.). Insurgents could exploit the global information network to gain political support, recruit, and raise funds, as well as to organize, plan and coordinate activities from multiple locations around the globe. If the experience of the last several years is any guide, future non-state

---

RMA could well be centrifugal, empowering sub-national groups and dissidents. If the latter proves to be the case, state failures could become more prevalent, as would civil wars, insurgencies, and other forms of low-intensity conflict. See Vickers and Martinage, *The Military Revolution and Intrastate Conflict*.

[400] William Branigin, "Drug Gangs Terrorize the Texas Border – Ranchers Seek Bigger U.S. Military Role Against Sophisticated Outlaws," *The Washington Post*, September 25, 1996, p. A4.

actors will not only be equipped with the weapons of war, but also with the tools of information connectivity—portable satellite phones, computers with Internet access and strong encryption algorithms, and satellite links to international television networks. Large segments of a population might be mobilized and their energies directed against state authority more rapidly and efficiently than ever before.

Furthermore, the increased transparency resulting from the commercialization of remote sensing from space, the proliferation of dual-use UAV systems, and the diffusion of militarily-relevant sensors (e.g., UGS and MAVs) will also benefit non-state actors as well as states. Some states will be able to take advantage of heightened transparency to identify and respond to insurgent activities (e.g., riots, demonstrations) more quickly and perhaps more effectively. However, insurgent groups, terrorist organizations and other non-state actors, which have heretofore relied almost exclusively on robust human intelligence networks, will benefit tremendously from the unprecedented amount of information from technical sources to which they stand to gain access. They will be better able to locate and target high-value state assets, conduct information-intensive guerrilla warfare against a state's military and police forces, and threaten to deny access to ports, airfields and other facilities to foreign powers attempting to come to the aid of a besieged state.

New Means of Attack

The combination of increased transparency and connectivity, access to precision location information (i.e., GPS), and availability of affordable standoff weapons could dramatically increase the striking power of non-state actors of all types. Easily transportable standoff weapons that will likely become available on the world arms market over the next two decades include precision-guided mortars, fiber-optic guided missiles (FOGMs), and MANPADS. Insurgents, terrorists, and other non-state actors may also exploit offensive IW tools, both infectious and contagious BW pathogens, and low-tech, but highly disruptive radiological dispersal devices (RDDs).

Precision-guided mortars employ a range of targeting systems including laser, IR, millimeter-wave radar seekers, and fiber-optics. Britain, Germany, Sweden, and the United States all have systems in various stages of development. Though intended by their producers to be primarily anti-armor weapons, precision-guided mortar rounds could be used against a wide variety of targets, providing future non-

state actors with an unprecedented indirect, fire-and-forget, point-target-kill capability. Not only would the range and destructive effects of mortar attacks be increased, but the time and rounds needed to execute attacks would also be reduced, increasing mortar crews' survivability (through reduced exposure to counter-battery fire) and mobility (through reduced logistics burden).[401] Mortar attacks like that on the British Prime Minister's residence at No. 10 Downing Street in February 1991 by the Provisional Wing of the IRA could become far more effective.[402] Similarly, with pinpoint targeting accuracy (e.g., the ability to strike specific government buildings, police barracks, military bases, and infrastructure targets), repeated mortar attacks like those that have caused hundreds of civilians and military casualties during the current insurgency in Iraq could reasonably be expected to have an even greater strategic impact.

FOGMs are non-line-of-sight, precision, standoff weapons designed for use primarily against armored vehicles and low-flying helicopters. They can be used, however, to strike any type of mobile or fixed target within striking range (i.e., several kilometers). The missile transmits an optical or IR image to the operator's display via fiber-optic cable and receives its guidance in the same manner. Aside from the United States, countries that have developed or are developing FOGM products include a consortium of European states (France, Germany and Italy), Brazil, Israel, Japan, and Spain. Future designs will likely include man-portable, modular versions that could be reassembled once a suitable target has been identified.[403] In the hands of insurgents, FOGMs could be a potent means of striking government facilities, as well as military and police vehicles of all types. In the hands of terrorists, they might be used to strike economic or political

---

[401] Ibid., p. 50.

[402] "Mortar Attack on Downing Street," *News Digest,* February 1991, p. 38019. Three bombs were launched from improvised pipe mortars inside a van which had parked about 200 meters from Downing Street. One landed in the garden behind 10-12 Downing Street, shattering windows in the room where 15 ministers and officials of the Gulf War cabinet were meeting. The two other bombs landed nearby but failed to explode fully.

[403] David A. Shlapak and Alan Vick, *Check Six Begins on the Ground* (Washington, DC: RAND, 1995), p. 50.

icons, popular entertainment venues, and public modes of transportation (e.g., ferries, trains, and buses).

With over 150,000 systems in circulation internationally and an estimated 350,000 in storage, it is not surprising that MANPADS are widely available on the world arms market.[404] A half dozen different MANPADS—including variants of the Soviet-designed SA-7 Grail and SA-14 Gremlin, as well as the British Blowpipe and the American FIM-92 Stinger—are reported to be in service with nearly 30 non-state groups around the world.[405] Even more sophisticated systems will likely become available in the near future. Advanced MANPADS could be particularly lethal when employed in air ambush tactics near airbases to attack planes just after take-off or on their landing approach. Insurgents or terrorists operating from urban rooftops could expand their line-of-sight engagement envelope while at the same time taking advantage of their opponents' likely unwillingness to inflict large numbers civilian casualties through counterattacks. These systems could create a low-altitude, air anti-access environment that would necessitate stealthy means of transport for traditional low-altitude air operations such as urban force insertions.[406]

The threat MANPADS could pose in the future was foreshadowed in the Soviet war in Afghanistan (1979-1989). The introduction of the US Stinger enabled the Mujahideen to reduce dramatically the effectiveness of Soviet and Democratic Republic of Afghanistan (DRA) air operations. Soviet and DRA fixed-wing aircraft were forced to fly either high (over 10,000 feet) or low and fast, which made it considerably more difficult to find and kill targets on the

---

[404] David Kuhn, "Mombasa Attack Highlights Increasing MANPADS Threat," *Jane's Intelligence Review*, February 2003, p. 28.

[405] See Thomas Hunter, "The Proliferation of MANPADS," *Jane's Intelligence Review*, September 2001, pp. 42-45; David C. Isby, "MANPADS Proliferation Threatens Helicopter Operations," *Jane's Missiles & Rockets*, January 29, 2001; and Glenn W. Goodman, "Counter-SAM Tactics," *Armed Forces Journal International*, November 2001, p. 52.

[406] Defense Science Board 1996 Summer Study Task Force, *Tactics and Technology for 21st Century Military Superiority*, (Washington, DC: OSD, October 1996), p. V36. See also: Stacey Evers, "USAF Special OPS Seeks Stealthy VTOL," *Jane's Defence Weekly*, April 23, 1997, p. 26.

ground. Soviet pilots also started making riskier, high-gradient climbs at take-off to reach safe altitudes more rapidly. The Stinger threat also forced Soviet helicopter pilots to fly low and use techniques that brought them within effective range of the Mujahideen's anti-aircraft artillery. According to US Army estimates, the Mujahideen scored 269 hits out of 340 Stinger firings during the period before the Soviet withdrawal.[407]

A decade later, in the skies over Chechnya, insurgents downed several Russian aircraft (e.g., Su-25 and Su-24 fighter-bombers) and helicopters with MANPADS.[408] The persistent MANPADS threat was also reportedly a significant factor in the US decision not to commit deployed Apache helicopters to combat in and around Kosovo during Operation Allied Force.[409] Since October of 2003, at least nine military helicopters have been shot down over Iraq with RPGs and MANPADS. An official Army review team concluded that a few of the helicopters may have been downed with SA-14 and SA-16 shoulder-fired missiles, which are significantly more difficult to counter than the ubiquitous SA-7.[410] The insurgents are also beginning to implement new tactics for countering American defenses, including using MANPAD teams to launch attacks from multiple directions simultaneously and using ground fire to steer helicopters into the engagement envelope of shoulder-launched missiles.[411] In addition, American fixed-wing aircraft taking off and arriving at Baghdad International Airport and at other Iraqi airfields have come under missile attack on more than a score of occasions. Fortunately, whether owing to operator error on the ground, the evasive measures of the pilots, or the effectiveness of the self-defense systems with which the targeted aircraft were

---

[407] Anthony H. Cordesman and Abraham R. Wagner, *The Lessons of Modern War* (Boulder, CO: Westview Press, 1990), pp. 176-177.

[408] Thomas Hunter, "The Proliferation of MANPADS," *Jane's Intelligence Review*, September 2001, p. 43.

[409] Glenn W. Goodman, "Counter-SAM Tactics," *Armed Forces Journal International*, November 2001, p. 54.

[410] Eric Schmitt, "Iraq Rebels Seen Using More Skill to Down Copters," *New York Times*, January 18, 2004, p. 1.

[411] Robert Wall, "Facing the Threat," *Aviation Week & Space Technology*, March 8, 2004, p. 58.

equipped, nearly all of the attacks were unsuccessful. Thus far, only three transport aircraft, including a C-5 and a C-17, have been seriously damaged during their climb out from Baghdad International Airport and all have managed to recover safely.[412]

Terrorist use of MANPADS against unprotected civilian airliners and commercial cargo aircraft, however, could potentially prove far more costly. On November 28, 2002, terrorists linked to al Qaeda attempted to shoot down an Israeli 757-300 airliner leaving Mombasa International Airport in Kenya with 271 civilians onboard using a pair of Soviet-designed *Strela* 2M (SA-7B) MANPADS.[413] Although operator error caused this attack to fail, there is scant reason to be sanguine about the outcome of future attacks. As the Defense Intelligence Agency cautioned in February 2004:

> A MANPAD attack against civilian aircraft would produce [a] large number of casualties, international publicity and a significant impact on civil aviation. These systems are highly portable, easy to conceal, inexpensive, available in the global weapons market and instruction manuals are on the internet. Commercial aircraft are not equipped with countermeasures and commercial pilots are not

[412] Although Iraq is believed to have stockpiled over 5,000 MANPADS launchers, less than one-third have been recovered. See Mark Hewish and Joris Janssen Lok, "David versus Goliath," *Jane's International Defense Review*, April 2004, pp. 46-55; David Fulghum, "SAMs Threaten," *Aviation Week & Space Technology*, February 2, 2004, p. 43; Eric Schmitt, "Attack Highlights a Constant Threat Faced by Aircraft in Iraq," *New York Times*, November 3, 2003; Hampton Stephens, "CENTAF: Missile Attacks on Military Aircraft in Iraq have Decreased," *Inside the Air Force*, November 21, 2003, p. 1; and John Daniszewski, "Shoulder-Launched Missiles Miss U.S. Plane in Iraq," *Los Angeles Times*, September 8, 2003.

[413] The attack apparently failed due to operator error. It appears that the missiles were fired before the airliner reached the *minimum* engagement range for the Strela 2M system. David Kuhn, "Mombasa Attack Highlights Increasing MANPADS Threat," p. 28.

> trained in evasive measures. An attack could occur with little or no warning.[414]

Offensive IW capabilities are also likely to be exploited by non-state actors in the years ahead. For a variety of reasons, IW provides a means of attack that is particularly well suited to the needs of non-state actors. Some of its many advantages included the following:

- IW attacks can be conducted across global distances and can originate from almost any location;
- The hardware and software required for conducting CNA requires a minimum of capital investment and is widely accessible;
- With the advent of increasingly powerful laptop computers, modems and personal satellite communication services, CNA capabilities are inherently mobile;
- CNA attacks can be conducted in a very clandestine fashion, making it very difficult for states to track down and punish the perpetrators; and
- RF weapons, which can be easily built with widely available COTS technology costing only hundreds of dollars, could potentially cause extensive damage to the unprotected electronic equipment upon which modern economies (and militaries) rely.[415]

---

[414] Vice Admiral Lowell E. Jacoby, Director, Defense Intelligence Agency, "Current and Projected National Security Threats to the United States," *Statement for the Record, Senate Select Committee on Intelligence*, February 23, 2004, p. 3.

[415] As part of a DoD-funded "Red teaming" exercise, a pair of scientists reportedly assembled simple, but effective RF weapons using easily obtainable, off-the-shelf components (e.g., automotive ignition coils and fuel pumps, capacitors, copper tape, and television dish antennas). The first weapon took the team only two weeks to build and cost about $500. Initial tests indicated that the signal was at a sufficiently high power level to damage military equipment and civilian infrastructures at ranges suitable for terrorist usage. See David Shriner, "The Design and Fabrication of a Damage-Inflicting RF Weapon by 'Backyard Methods'," Statement before the Joint Economic Committee of the US Congress, February 25, 1998; David Wood, "Scientist

Potential strategic information targets for non-state actors include telecommunication nodes, power grids, air traffic control networks, and electronic bank clearing systems. Would-be attackers could gain valuable insight into techniques and tactics for attacking such sites on the Internet. World Wide Web sites and hacker bulletin boards could easily be set up specifically for the purpose of broadcasting target vulnerabilities. According to the Central Intelligence Agency, since the mid-1990s "hackers have shared increasingly sophisticated and easy-to-use software on the Internet that can be readily used by any computer-literate adversary for computer network reconnaissance, probing, penetration, exploitation, or attack."[416] Although not necessarily lethal, IW strikes could be extremely disruptive and financially costly.

BW could also become a prominent feature of future intrastate war and transnational terrorism. For instance, government forces might use biological agents to eradicate livestock and crops in rebel-held territory, or insurgents could use them to weaken the government's hold over a disputed area.[417] Terrorists could use them to inflict mass casualties, especially within enclosed spaces such as large office buildings, government buildings, subway systems, shopping malls, and entertainment venues.

Builds Fearsome Electronic Weapon," New Orleans Times-Picayune, April 29, 2001, p. 30; and Kenneth Timmerman, "U.S. Threatened with EMP Attack," Insight Magazine, May 28, 2001, p. 16.

[416] The CIA has similarly cautioned, "Advanced technologies and tools for computer network attack operations are becoming more widely available, resulting in a basic, but operationally significant, technical cyber capability for U.S. adversaries." See Lawrence Gershwin, National Intelligence Officer for Science and Technology, *Testimony before Joint Economic Committee*, Hearing on "Cyber Threat Trends and U.S. Network Security," June 21, 2001, p. 3. See also John Schwartz, "Securing the Lines of a Wired Nation," *New York Times*, October 4, 2001.

[417] See Lt. Col. Robert P. Kadlec, USAF, "Biological Weapons for Waging Economic Warfare," in Barry R. Schneider and Lawrence E. Grinter, eds., *Battlefield of the Future: 21st Century Warfare Issues* (Maxwell AFB, AL: Air University Press, September 1995).

Defending against biological terrorism could prove difficult. First, it is extremely challenging to detect the development and production of the agents themselves. An easily hidden, small-scale BW production facility could be created using equipment that is widely available in mail-order catalogs and requires, at most, a graduate-level education in biotechnology.[418] Once released, BW particulates in the air are nearly invisible. Although highly specialized sensors might be able to detect the presence of a BW agent, they have to be in the right place at the right time. Second, it may be difficult to determine whether an outbreak is the result of a natural occurrence or a deliberate attack. Because of the incubation period for typical pathogens, it often takes at least three or four days for symptoms to manifest themselves, which provides ample time for terrorists (who could be immunized ahead of time) to flee the area. Third, some pathogens (e.g., smallpox, Ebola, plague, and cholera) are highly contagious and can spread rapidly, making containment difficult, especially in highly mobile societies. Finally, even after it has been determined that a deliberate BW attack has occurred, assembling a trail of evidence leading to the perpetrators may prove exceedingly problematic. As discussed in Chapter III, the ongoing revolution in molecular biology could make this situation substantially worse, with ethnically discriminating weapons and stealth pathogens being just two of the possibilities.

The prospect of biological terrorism was demonstrated, albeit in limited form, by the anthrax scare in the United States in the fall of 2001.[419] Although anthrax-laced letters proved exceedingly disruptive,

---

[418] Under Project Baccus, DoD created just such a facility to demonstrate how easy it would be to do. Using off-the-shelf equipped order by mail, the DoD team successfully produced simulant bacteria with qualities very similar to anthrax. Taped interview with Jay Davis, former director the Defense Threat Reduction Agency, on NOVA Bioterror Special, original air date November 13, 2001. Transcript is available online at: http://www.pbs.org/nova/bioterror.

[419] As an earlier example of non-state interest in BW, in 1995, it came to light that the Aum Shinrikyo cult had ordered sophisticated molecular design software that could be used to reengineer the molecular structure of chemicals or microorganisms to make them more lethal. In a subsequent raid on the cult's facilities, the Japanese police seized large quantities of *Clostridium botulinum*, the bacterium that causes botulism. See Lt. Col. Terry N. Mayer, USAF, "The Biological Weapon: A Poor Nation's Weapon of Mass

especially to the nation's postal system, the number of casualties was fortunately very low. Future terrorists, however, may devise much more effective agent delivery means. Offering a chilling omen of this possibility, then Director of Central Intelligence George J. Tenet noted, "Documents recovered from Al Qaeda facilities in Afghanistan show that bin Laden was pursuing a sophisticated biological weapons research program."[420] Al Qaeda was apparently trying to develop several different biological and chemical agents for attacking people, livestock, and crops.[421] Two production centers in Afghanistan that were preparing to manufacture botulinum and salmonella toxins, and possibly anthrax, were found and destroyed by Coalition forces in 2001. Since then, traces of ricin, an extremely lethal biological toxin, have been discovered along with related production equipment during raids on al Qaeda-affiliated cells in Britain, France, Spain, Russia, Georgia, and Kurdish-controlled northern Iraq.[422]

Non-state actors may also attempt to develop radiological dispersal devices (RDDs) designed to cause radiation sickness and

---

Destruction," in Schneider and Grinter, eds., *Battlefield of the Future: 21st Century Warfare Issues*, pp. 211-212, 216.

[420] As quoted in Michael Gordon, "U.S. Says it Found Al Qaeda Lab Being Built to Produce Anthrax," *New York Times*, March 23, 2002, p. 1. See also Judith Miller, "Lab Suggest Qaeda Planned to Build Arms, Officials Say," *New York Times*, September 12, 2002; and Judith Miller, "Qaeda Videos Seems to Show Chemical Tests," *New York Times*, August 19, 2002, p. 1.

[421] Judith Miller, "Lab Suggest Qaeda Planned to Build Arms, Officials Say," *New York Times*, September 12, 2002; Michael Gordon, "U.S. Says it Found Al Qaeda Lab Being Built to Produce Anthrax," *New York Times*, March 23, 2002, p. 1; Jonathan Weisman, "Possible Anthrax Lab Unearthed," *USA Today*, March 26, 2002, p. 10; and "Al-Qaeda Bioterror Study Went Further than Thought," *USA Today*, January 8, 2003, p. 6.

[422] Although a pinhead-quantity of ricin can be fatal if introduced directly into the bloodstream, a substantially larger quantity (approximately 3 micrograms per kilogram of body weight) must be inhaled to kill a healthy adult. It can also be introduced into the body by the consumption of contaminated food or water. Ricin, which is derived from commonly available castor beans, is relatively easy to produce, but difficult to weaponize. Joby Warrick, "An Al Qaeda 'Chemist' and the Quest for Ricin," *Washington Post*, May 5, 2004, p. 1. See also: http://www.bt.cdc.gov/agent/ricin/facts.asp

environmental contamination. There are three basic types of RDDs that non-state actors could construct from radioactive material (e.g., Cesium-137, Strontium-90, and Cobalt-60) commonly available in hospitals, universities, and factories. The most basic type of RDD is nothing more than an unshielded container of radioactive material that could be easily hidden in congested, heavily trafficked areas (e.g., rail stations, subways, or shopping malls). People walking by or lingering in close proximity to the hidden container could be exposed to unhealthy, but probably not life-threatening, levels of radiation. The second type of device, referred to as explosive RDDs or "dirty bombs," are devices that use explosive force to disperse small particles of radioactive material over a wide area (e.g., a container of radioactive material blanketed with high explosive charges). The third type, atmospheric RDDs, requires the conversion of radioactive material into a very fine powder that could be aerosolized into a particulate cloud and easily transported by air currents.[423] Unless radioactive material could be obtained "off-the-shelf" in the required form, it would be necessary to mill larger pieces (e.g., pellets) into micron-sized particles, which would be both hazardous to those involved and technically challenging.

Black-market trafficking in radioactive materials has reportedly increased significantly over the last several years. In May 2003, an individual transporting two capsules of strontium and cesium was intercepted by police in Tbilisi, Georgia. In June 2002, over a pound of uranium was seized at the Georgia-Armenia border.[424] While RDDs could, under some circumstances, cause radiation sickness in relatively confined areas, they are unlikely to cause large numbers of fatalities. Explosive RDDs, for instance, would likely cause more prompt casualties from high-explosive blast and shrapnel than from radiation.[425] RDDs could, however, have a powerful psychological

---

[423] CIA, *Terrorist CBRN: Materials and Effects (U)*, CTC 2003-40058, May 2003, p. 4.

[424] Joby Warrick, "Smugglers Targeting Dirty Bombs for Profit," *Washington Post*, November 30, 2003, p. 1.

[425] According to a study by the Center for Technology and National Security Policy at the National Defense University, casualties from an explosive or atmospheric RDD, which generate radioactive particles in a "respirable form," could be higher than previously thought because of under-estimated damage

"shock effect." Moreover, cleaning up the contamination from an explosive or atmospheric RDD, especially in urban areas, could be extraordinarily expensive and cause significant economic disruption. One recent study, which included a detailed computer simulation, concluded that the detonation of an explosive RDD containing *less than two ounces* of Cesium-137 in Manhattan would spread contamination over an area covering sixty square blocks and take years to clean up at a cost of tens of billions of dollars.[426]

---

to the lungs, digestive system, and immune system. The study concluded that a well-executed RDD attack in a densely populated urban area "could cause tens to hundreds of fatalities" and would also cause "great panic and enormous economic losses." Joby Warrick, "Study Raises Projection for 'Dirty Bomb' Toll," *Washington Post*, January 13, 2004, p. 2.

[426] Warrick, "Smugglers Targeting Dirty Bombs for Profit," p. 1; and Douglas Frantz, "Threat of 'Dirty Bomb' Growing, Officials Say," *Los Angeles Times*, May 9, 2004, p. 1.

V. Conclusion

A revolution in war has been underway for nearly three decades. To date, it has been principally characterized by:

- The emergence of all-weather precision war;
- The advent of stealth;
- The rise of unmanned systems;
- The tactical and operational exploitation of space; and
- The emergence of early forms of network-based warfare and joint-force integration.

Thus far, the US military has enjoyed a monopoly on the revolution in war. Within the next two decades, however, the revolution could shift from a purely opportunity-based one for the United States to one that portends significant threats, as well as opportunities. If there is competition within the revolution in war, it is likely to be highly asymmetric. It is entirely conceivable, moreover, that a competitor could "leapfrog" the United States in some areas of future competition.

Major advances in the core military capabilities that are underwriting the revolution in war are likely over the next one–to–two decades. The future course of the revolution in war could range from a

continuation of current trends and the existing warfare regime, to a "revolution within the revolution" due to asymmetric exploitation of disruptive capabilities by strategic competitors, to a successor revolution that would involve a much greater break with the ongoing revolution in war. While the emergence of a revolution within the revolution or a successor revolution is still highly uncertain, we believe that the outcome of six warfare competitions will be determinative of the character of the future warfare regime:

- Evolving anti-access and area-denial capabilities versus current and new forms of power projection;

- Increased capabilities for preemption versus increased denial capabilities;

- Hiders versus finders;

- Space access versus space control;

- Offense-defense competitions in the areas of missile attack versus missile defense, IW attack versus IW defense, and BW attack versus BW defense; and

- Increased capabilities for political–military coercion versus capabilities for counter–coercion.

As these key warfare competitions unfold, discontinuous change could occur within and across the primary warfare dimensions of air, land and sea. New forms of war could emerge in several other dimensions: space, information and the advanced biological. Air warfare could be transformed from a regime dominated by manned, theater-range, air superiority aircraft to one dominated by extended-range, unmanned, stealthy platforms. The conduct of land warfare could shift from a regime dominated by mobile, combined-arms, armored forces to one that is dominated by much lighter, stealthier and information-intensive forces that make heavy use of robotics. War at sea could be transformed by the emergence of "anti-navy" capabilities that allow nations to assert a degree of surface control over adjacent maritime areas out to several hundred miles. This development would likely lead to new forms of naval power projection, including increased reliance on undersea warfare and relatively small, stealthy, networked surface vessels. Increased commercial and military use of space could lead to the emergence of a wide range of

offensive and defensive space control capabilities. CNA tools and RF weapons could be widely used to attack information infrastructures and information-intensive forces. Designer BW and the emergence of biological operations could also figure prominently in an advanced RMA regime.

At the lower end of the conflict spectrum (e.g., the war on terrorism, intra-state conflict, and stability operations), non-state actors could become far more virulent and insurgency-induced state failures could become far more prevalent. At the highest-end, the strategic scope of the revolution in war (including a prospective revolution within the revolution and potential successor revolutions) will likely be truncated by the continued "overhang" of nuclear weapons, though new forms of strategic warfare will likely also emerge.

Although it has grown increasingly dominant in the ongoing revolution in war, the US military is by no means adequately hedged at present for the prospect of discontinuous change within or across military regimes (a revolution within the revolution or a successor revolution). Failure to adequately hedge represents a significant future risk.[427]

---

[427] See Michael G. Vickers, "The 2001 Quadrennial Defense Review, The FY 2003 Defense Budget Request and The Way Ahead for Transformation: Meeting the 'Rumsfeld Test'," *CSBA Backgrounder*, June 19, 2002.

Appendix: Glossary

AARS	Advanced Airborne Reconnaissance System
ACTD	Advanced Concept Technology Demonstration
ADS	Advanced Deployable System
AESA	Active Electronically Scanned Array
AFB	Air Force Base
AIP	Air-Independent Propulsion
AO/AOR	Area of Operations/Area of Responsibility
AOE	Fast Combat Support Ship
ARV	Armed Robotic Vehicle
ASAT	Anti-Satellite
ASCM	Anti-Ship Cruise Missile

ASuW	Anti-Surface Warfare
ASW	Anti-Submarine Warfare
ATACMS	Army Tactical Missile System
ATD	Advanced Technology Demonstration
ATO	Air Tasking Order
ATR	Automatic Target Recognition
AWACS	Airborne Warning and Control System
AWASM	Autonomous Wide-Area Search Munition
BAT	Brilliant Anti-Armor
BDA	Battle Damage Assessment
BRAT	Beyond Line of Sight Reporting and Targeting
BSE	Bovine Spongiform Encephalopathy or "Mad Cow"
BW	Biological Warfare / Biological Weapons
BWC	Biological Weapons Convention
C3	Command, Control and Communications
C3D2	Cover, Camouflage, Concealment, Deception, and Denial
C3I	Command, Control, Communications, and Intelligence

C4	Command, Control, Communications, and Computers
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CALCM	Conventional Air-Launched Cruise Missile
CAOC	Combined Air Operations Center
CAV	Common Aero Vehicle
CBRN	Chemical, Biological, Radiological, and Nuclear
CBW	Chemical and Biological Weapons / Chemical and Biological Warfare
CCS	Counter-Communications System
CEC	Cooperative Engagement Capability
CEP	Circular Error Probable
CIA	Central Intelligence Agency
CNA	Computer Network Attack
CNS	Counter-Navigation System
COMSAT	Communications Satellite
CONUS	Continental United States
CORM	Commission on Roles and Missions
COTS	Commercial Off the Shelf
CRS	Congressional Research Service

CSCS	Counter-Satellite Communications System
CSRS	Counter-Surveillance and Reconnaissance System
CW	Chemical Warfare / Chemical Weapons
DACT	Data Automated Communications Terminal
DARPA	Defense Advanced Research Projects Agency
DDR&E	Director of Defense Research and Engineering
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DMPI	Designated Mean Point-of-Impact
DoD	Department of Defense
DRA	Democratic Republic of Afghanistan
DSB	Defense Science Board
DSP	Defense Support Program
ECM	Electronic Countermeasures
EGBU	Enhanced Guided-Bomb Unit
EHPA	Exoskeletons for Human Performance Augmentation
ELE	Extremely Long Endurance
ELEV	Extremely Long Endurance Vehicle

ELF	Extremely Low Frequency
ELINT	Electronic Intelligence
EMD	Engineering and Manufacturing Development
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EO	Electro-Optical
FBCB2	Force XXI Battle Command Brigade and Below
FCS	Future Combat System
FMD	Foot and Mouth Disease
FOFA	Follow-On Forces Attack
FOGM	Fiber-Optic Guided Missile
FOPEN	Foliage Penetration
FSE	Future Security Environment
FY	Fiscal Year
GAO	General Accounting Office (now Government Accountability Office)
GCCS	Global Command and Control System
GEO	Geosynchronous Orbit
GIG	Global Information Grid
GMTI	Ground Moving Target Indicator
GPS	Global Positioning System

HALE	High-Altitude, Long-Endurance
HARM	High-Speed Anti-Radiation Missile
HCV	Hypersonic Cruise Vehicle
HDBT	Hardened and Deeply Buried Targets
HEL	High Energy Laser
HEO	Highly Elliptical Orbit
HPM	High-Power Microwave
HRR	High-Range-Resolution
HSI	Hyperspectral Imagery
IADS	Integrated Air Defense System
ICBM	Intercontinental Ballistic Missile
IO	Information Operations
IPB	Intelligence Preparation of the Battlespace
IR	Infrared
IRBM	Intermediate-Range Ballistic Missile
IRST	Infrared Search and Track
ISR	Intelligence, Surveillance, and Reconnaissance
IT-21	Information Technology--21
ITASS	Intended Target Acquisition and Strike System
IW	Information Warfare

JASSM	Joint Air-to-Surface Stand-Off Missile
JCS	Joint Chiefs of Staff
JDAM	Joint Direct Attack Munition
JDAM-ER	Joint Direct Attack Munition--Extended Range
JSF	Joint Strike Fighter
JSOW	Joint Stand-Off Weapon
JSTARS	Joint Surveillance and Target Attack Radar System
JTIDS	Joint Tactical Information Distribution System
J-UCAS	Joint Unmanned Combat Air System
LACM	Land-Attack Cruise Missile
LADAR	Laser-Radar
LAN	Local Area Network
LCS	Littoral Combat Ship
LEO	Low-Earth Orbit
LFA	Low-Frequency Active
LGB	Laser-Guided Bomb
LIDAR	Light Detection and Ranging
LMRS	Long-Term Mine Reconnaissance System
LO	Low-Observable

LOCAAS	Low-Cost Autonomous Attack System
LRPS	Long-Range Precision Strike
MALD	Miniature Air-Launched Decoy
MANPADS	Man-Portable Air Defense System
MAV	Micro Air Vehicle
MBITR	Multi-Band Inter/Intra Team Radio
MC2C	Multi-Sensor Command and Control Constellation
MDA	Missile Defense Agency
MEMS	Micro-Electromechanical System
MEO	Medium-Earth Orbit
MLRS	Multiple Launch Rocket System
MRBM	Medium-Range Ballistic Missile
MTI	Moving Target Indicator
MTR	Military-Technical Revolution
MULE	Multifunction Logistics and Equipment Vehicle
NCW	Network-Centric Warfare
NDU	National Defense University
NIMA	National Imagery and Mapping Agency (now the National Geospatial-Intelligence Agency)
NIPRNET	Non-Classified Internet Protocol Router Network

NMCI	Navy-Marine Corps Intranet
NOSS	Naval Ocean Surveillance System
OPFOR	Opposing Force
OSD	Office of the Secretary of Defense
OTA	Office of Technology Assessment
OTH	Over the Horizon
PGM	Precision-Guided Munition
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PLA	People's Liberation Army (China)
PLAN	People's Liberation Army-Navy (China)
QDR	Quadrennial Defense Review
QSP	Quiet Supersonic Platform
R&D	Research and Development
RAIDRS	Rapid Attack Identification, Detection, and Reporting System
RAM	Radar-Absorbing Materials
RCS	Radar Cross Section
RDD	Radiological Dispersal Device
RDT&E	Research, Development, Test and Evaluation
RF	Radio-Frequency

RMA	Revolution in Military Affairs
RMS	Remote Minehunting System
RPG	Rocket-Propelled Grenade
SAB	Scientific Advisory Board
SAM	Surface-to-Air Missile
SAR	Synthetic Aperture Radar
SBIRS	Space-Based Infrared System
SBR	Space-Based Radar
SBSS	Space-Based Space Surveillance
SCADA	Supervisory Control and Data Acquisition
SDB	Small Diameter Bomb
SEAD	Suppression of Enemy Air Defense
SF	Special Forces
SFW	Sensor-Fuzed Weapon
SIGINT	Signals Intelligence
SIPRNET	Secret Internet Protocol Router Network
SLBM	Submarine-Launched Ballistic Missile
SLCM	Submarine-Launched Cruise Missile
SLICE	Soldier Level Individual Communications Environment
SLV	Space-Launch Vehicle

SMART	Scalable Modular Airborne Relay Terminal
SMV	Space Maneuver Vehicle
SOF	Special Operations Forces
SOP	Satellite Operating Partner
SOV	Space Operations Vehicle
SRBM	Short-Range Ballistic Missile
SSBN	Nuclear-Powered Ballistic Missile Submarine
SSGN	Nuclear-Powered Guided Missile Submarine
SSK	Diesel-Powered Attack Submarine
SSN	Nuclear-Powered Attack Submarine
SUOSAS	Small Unit Operations Situational Awareness System
TacTom	Tactical Tomahawk
TAV	Trans-Atmospheric Vehicle
TDD	Target Detection Device
TED	Transient Electromagnetic Disruption
TEL	Transporter-Erector-Launcher
THAAD	Theater High-Altitude Air Defense
TLAM	Tomahawk Land Attack Missile
TMD	Theater Missile Defense

TSAT	Transformational Communications Satellite
UAV	Unmanned Aerial Vehicle
UCAR	Unmanned Combat Armed Rotorcraft
UCAV	Unmanned Combat Aerial Vehicle
UGS	Unattended Ground Sensors
UGSSS	Unmanned Global Surveillance-Strike System
UGV	Unmanned Ground Vehicle
UHF	Ultra-High Frequency
UNREP	Underway Replenishment
USAF	United States Air Force
USDA	United States Department of Agriculture
USMC	United States Marine Corps
USV	Unmanned Surface Vehicle
UUV	Unmanned Underwater Vehicle
VLAAS	Vertical Launch Autonomous Attack System
VLS	Vertical Launch System
VTOL	Vertical Take-Off-and-Landing
WARNET	Wide-Area Relay Network
WASAAMM	Wide-Area Search Autonomous Attack Miniature Munition

WCMD	Wind Corrected Munition Dispenser
WIN-T	Warfighter Information Network--Tactical
WMA	World Medical Association
WMD	Weapons of Mass Destruction
XSS	Experimental Satellite Series