Operational Environments to 2028: The Strategic Environment for Unified Land Operations

August 2012

Training and Doctrine Command (TRADOC) G-2

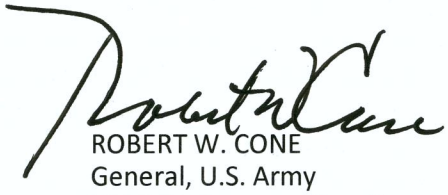
Commanding General's Foreword

As our Army transitions from a decade of war, it is critical for us to focus on the future. Successfully preventing conflict, shaping the environment, and winning our Nation's wars requires substantial preparation across our Army. We must strive to understand the complex future and prepare our Army to operate and adapt in any environment. As we prepare our Soldiers, leaders, and units for the future, this document provides a foundation for us to design training and education, build leader development programs, and develop required capabilities for our Army.

The operational environments we will encounter in the future will differ from Iraq and Afghanistan. Although there may be similarities, the multitude of different actors, interests, and conditions in each conflict create unique and complex environments. While history provides us indicators of the future, it is difficult to predict with any certainty what character future wars will take.

However, we do know some things about the future. The Army must continue to be prepared to answer the call no matter what the task. Our military dominance will shape how potential adversaries perceive us, and the strategies they will employ. Adversaries will seek to deny the United States the advantages of our preferred way of war. They will deny our use of standoff precision weapons, negate our intelligence capabilities, and force the United States into unfavorable positions. Opportunistic adversaries will use the sheer complexity of all the elements interacting in an environment to frustrate commanders and confound senior policy makers.

One thing is certain, in future operational environments, our Army must be operationally adaptable. We must possess agile and innovative leaders organized in versatile units capable of effectively operating across the range of military operations. This strategic environment estimate will serve as the foundation to build, train, and educate the U.S. Army. The intent of this document is not to predict what America's next war will look like. It is to provide potential future environments for commanders, staffs, instructors, and combat developers to use as the basis of training, leader development, education, and capabilities development. Our future success is dependent on building an operationally adaptable force capable of effectively operating in any environment.



ROBERT W. CONE
General, U.S. Army
TRADOC Commanding General

Executive Summary

The Army does not have the luxury of focusing on any one potential adversary or any one mission type across the range of military operations. Instead, leaders and Soldiers must be exposed to the multiple conditions representing threats that exist across the globe. Potential threats will range from standing conventional and unconventional forces, to irregular militias and paramilitaries, to terrorist groups and criminal elements. Training, education, capabilities development, and concept development should reflect this reality.

Currently, in the midst of a global recession, the Army finds itself at a strategically important crossroad as it tries to determine where to wisely invest its limited training, personnel, and materiel resources. The strategic environment (SE) to 2028, with its combination of tough enduring problems and newly developed conditions and characteristics, will add complexity to this challenge.

To help unravel the complexities of current and near-term challenges, the following paper provides a description of the key conditions manifesting across the SE through 2028. Adversarial strategies based on these conditions are also addressed. The concluding chapter explores the military implications of both the conditions and potential adversarial strategies. We know that the current and future strategic environment will be characterized by uncertainty, complexity, and increasingly nuanced relationships. The conditions of the strategic environment must be understood, captured, and factored into Army decision-making. Only then can realistic training, the correct mix of systems and capabilities, and the proper approaches to leader development and education be identified and implemented across TRADOC and the Army in general.

STRATEGIC ENVIRONMENT CONDITIONS

The strategic environment is defined, in the context of this estimate, as the set of global conditions, circumstances, and influences that affect the employment of all elements of U.S. national power. The SE contains multiple potential operational environments (OEs), which are defined as any areas in which U.S forces may operate, from a locale as small as a village to entire regions of the globe.

The strategic environment remains as it has always been: complex. The interaction of the many variables within the environment, including human behavior, assures both fog and friction. The current strategic environment seems more ambiguous, presenting multiple layers of complexity and challenging the Army with requirements beyond traditional warfighting skills and training. Capturing the key strategic conditions is fundamental to understanding current and future military operations. Strategic conditions will be analyzed through the lens of eight OE variables—political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT). The resulting conditions are listed below and explained in detail in **Chapter 2** of this estimate.

POLITICAL CONDITIONS

- Changing International Distribution of Power
- Decline of Global Governance
- Shortfalls in State Governance

MILITARY CONDITIONS

- Global Military Expenditure Rates
- Wide Range of Potential Missions and Adversaries
- Rise of Private Security Organizations (PSOs)
- Weapons of Mass Destruction (WMD) Proliferation
- Importance of the Global Commons
- Continued Vulnerability of the U.S. Homeland
- Emerging and Proliferating Military Technologies

ECONOMIC CONDITIONS

- Economic Shifts
- Income Inequality
- Economic Interdependence

SOCIAL CONDITIONS

- Demographic Transition
- Population Growth
- Persistent Youth Bulge

INFORMATION CONDITIONS

- Proliferation of Information and Communications Technology (ICT)
- Transparency across Societies
- Actor Empowerment
- Controlling the Strategic Narrative
- Technological Vulnerability

INFRASTRUCTURE CONDITIONS

- Urbanization
- Expanding Physical Infrastructure

PHYSICAL ENVIRONMENT CONDITIONS

- Competition over Natural Resources
- Climate Change
- Special Cases

TIME CONDITION

- Cultural Perception of Time

IMPLICATIONS OF THE CONDITIONS

The current and future strategic environment will be—as the above conditions reflect—characterized by multiple actors, adaptive threats, chaotic conditions, and advanced-technology-enabled actors seeking to dominate the information environment. The Army must be operationally adaptive to defeat these complex challenges and adversaries operating within this environment.

Through 2028, the Army will face many unique OEs and simultaneous decisive action operations will be the norm within these environments. Training for sequential operations with clearly defined phases will not suffice. Conflict, post-conflict/failed state, humanitarian, disaster relief, and support and reconstruction operations will occur simultaneously. Such operations will require increased coordination/integration with a range of civilian organizations, both domestic and international. U.S. forces will be required to interact with and to protect nongovernment organizations (NGOs), private voluntary organizations (PVOs), and humanitarian organizations more than ever before.

Long-term implications of the SE conditions are uncertain and can lead to a multitude of potential alternative security futures (ranging from some variant of the status quo, to a more violent world, to a less brutal outlook marked by greater cooperation and more effective international institutions). Future conflicts, moreover, will primarily:

- Require simultaneous operations of varying kinds (combat and reconstruction) vs. sequential, phased operations
- Be identity- (ethnic, religious) and/or deprivation-based
- Occasionally rise to the level of genocide and/or mass atrocity
- Be asymmetric and irregular rather than symmetric (involving at times states but also various types of non-state actors, e.g. terrorist groups, criminal organizations, guerrillas, etc.)
- Occur increasingly in complex terrain to mitigate perceived technological advantages
- Require better cultural understanding to avoid broadening or deepening the conflict

POTENTIALLY CONTENTIOUS OEs AND RELATED MISSIONS

Focusing on OEs likely to see increasing tension or conflict can help us understand the types of environments, conditions, missions, and adversaries we might face. The OEs of Iran, China, Yemen, North Korea, Pakistan, and Nigeria will be presented to highlight types of *possible* environments.[1]

ADVERSARIES IN THE STRATEGIC ENVIRONMENT

The strategic environment is essentially the sum of all the OEs in which commanders and units could find themselves conducting decisive action. **Adversaries take the means provided to them in the strategic environment and use those means in conceptually enduring ways to achieve their ends.** That is adaptive strategy. Adaptation, broadly defined, is the ability to learn and to adjust behaviors based on learning, and is closely linked to one's environment and its variable conditions.

WAYS—THE METHODS OF ADAPTIVE STRATEGY

Success goes to those who master the skills necessary to act, react, and adapt with speed and creativity. Enemies learn quickly and can change, although sometimes haphazardly and incompletely, making the "new" skills difficult to counter. Adversaries will continue to be adaptive in terms of using all available sources of power at their disposal. The methods of adaptive strategy are as follows: **conduct preclusion, control tempo, attack will, neutralize technological overmatch, change the nature of conflict, allow no sanctuary,** and **employ shielding**.

MEANS—THE HUMAN AND PHYSICAL CAPITAL OF ADAPTIVE STRATEGY

While, conceptually, adaptive strategy is the use of available means in the strategic environment to achieve goals, these activities occur in specific OEs. Inside these OEs, the means vary widely. U.S. national interest will also vary widely across the various OEs. The components that exist from which to build an improvised explosive device (IED) in South Asia are not the same as those available in Central Asia or Central America. The means are what change from year to year and OE to OE. However, given our analysis of the strategic environment, we know the means adversaries will need to accomplish their goals and the means available to them. This allows us to draw basic conclusions about the threats that will exist in the strategic environment during this period. **The tactical manifestation of an actor using a hybrid strategy is a hybrid threat**.

HYBRID THREAT

The hybrid threat components of adaptive strategy include two or more of the following:

- Military forces
- Nation-state paramilitary forces (such as internal security forces, police, or border guards)
- Insurgent organizations (movements that primarily rely on subversion and violence to change the status quo)
- Guerrilla units (irregular indigenous forces operating in occupied territory)
- Criminal organizations (such as gangs, drug cartels, or hackers)

Hybrid threats will use a strategic capability that forces any intervening power to adjust operations (WMD, special-purpose forces [SPF], etc). This capability may not be fully developed or developed at all. This will not affect the transition between regular and irregular operations, and the threat of the capability still provides a tool for manipulating the intervening force (e.g. Iraq's WMD capability circa 2001). **All components of a hybrid threat will use cyber operations to either degrade U.S. mission command capabilities, or to conduct global perception management campaigns**.

Hybrid threats have the ability to combine and transition between regular, irregular, and criminal forces and operations and to conduct simultaneous combinations of various types of activities that will change and adapt over time. Such varied forces and capabilities enable hybrid threats to capitalize on perceived U.S. vulnerabilities. Perhaps even more confusing will be when those combinations of threats are uncoordinated and simply seek to maximize their own organizational goals rather than any overarching objective.

TACTICAL DESIGNS

At the tactical level, hybrid threats will employ four key designs that specifically adapt resources available in the strategic environment for use against the U.S. and its partners.

- Exploit Regular/Irregular Synergy
- Employ Range of Technologies
- Information Warfare as Key Weapon System
- Employ Complex Battle Positions and Utilize Cultural Standoff Capabilities

Adversarial challenges will require that the Army be prepared for a wide range of missions over the forecast period. The leader development, training development, capabilities and concepts development implications are significant.

MILITARY IMPLICATIONS

The conditions and strategies highlighted in **Chapter 2, Conditions of the Strategic Environment**, reveal the implications for leader, training, capabilities, and concepts development as well as several implications across Army Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF).

DEVELOPMENT IMPLICATIONS

- Leader Development: Leaders must be able to deal effectively with the complexity and uncertainty of potential OEs, be culturally aware, understand the information environment, master consequence management, and be prepared to conduct decisive actions.

- Training Development: Training venues must reflect an understanding of the influence of various cultures and actors present in potential OEs, must continue the tradition of providing an arena that allows free play, and must adapt to new methods and mediums for training. Current and future Soldiers will demand that the Army keep pace with ICT developments for training.

- Capabilities Development: Capabilities development must anticipate the operational needs of commanders and incorporate the adaptability inherent in “off-the-shelf” technology to support the near future.

- Concepts Development: Accounting for adaptive adversaries requires scenario-based concepts that are informed by collaboration from ongoing operations but look well beyond the current fight.

IMPLICATIONS SHAPING DOTMLPF

Conditions across the strategic environment indicate future conflict will not be confined to one simple category. It will range in scope from major conventional fights to humanitarian support and nation-building missions. Very capable adversaries will continue to challenge U.S. interests globally, while rising military powers, coupled with existing militaries, will work to advance their regional and global interests. Training and preparation against these changing conditions will drive adaptation and flexibility within the Army and ensure U.S. forces are prepared for any potential OE and any potential mission:

- Increasing Challenge of a Wide Range of Threats
- Increasing Multiplicity of Actors across Potential OEs
- Increasing Importance of Gaining a Holistic Understanding of each OE
- Increasing Degree of Uncertainty
- Increasing Occurrence of Simultaneous and Continuous Engagements
- Prepare for Decisive Action
- Increasing Importance of the Information Environment

- Increasing Likelihood of a WMD Event and Consequence Management Activities
- Prepare for Homeland Security/Defense Missions
- Prepare to Defend Access to the Global Commons
- Prepare for Humanitarian Assistance/Disaster Relief Operations
- Prepare for Reconstruction Operations
- Prepare to Counter Threat Anti-Access Capability

Clearly, this estimate of the strategic environment to 2028 demonstrates that any future OE will be complex and demanding. Key themes emerging from analysis of SE conditions and adversaries are proliferation of WMD, hybrid threats, advancements in technology, and an explosion of ICT capabilities among actors of all types. Adaptation will be rampant among adversaries, so we must train and prepare for a multitude of these conditions on a wide array of OEs. Only through these measures will the U.S. military be able to successfully navigate any future OE.

Contents

Chapter 1
Introduction

An operational environment has no constant form or static conditions. Each OE has its own unique flavor and characteristics given that conditions across the strategic environment manifest differently in each potential OE. While such constantly shifting conditions make it difficult to develop a foundation for comprehending the strategic environment and the multiple OEs within that environment, such understanding is essential to all aspects of TRADOC's responsibilities.

Obtaining knowledge of the strategic environment, by observing its key conditions and facts, is the first step in gaining the understanding required to apply resources against ever more capable adversaries—adversaries that are able to create and take advantage of the complexity of the situation. This document is written as TRADOC's view of the near- and mid-term strategic environment (from the present to 2028) to provide leaders at all levels with the knowledge required to make critical decisions across the leader development, training development, capabilities development, and concepts development domains that will shape the Army of the future.

PURPOSE

The purpose of this estimate is to describe the strategic conditions Army forces will encounter as they complete the mission in Afghanistan and prepare for operations beyond the current fight. The primary goal is to provide an overview of the conditions—both current and future—and types of actors in the strategic environment and the many potential OEs that reside within it. To this end, the paper provides the Army's capstone view of the conditions of the SE, the most likely adversaries and their strategies, and the military implications of both.

STRUCTURE

This estimate consists of three chapters and eight annexes which are designed to provide an overview of the key conditions of the strategic environment along with an analytic tool—the Operational Environment Assessment (OEA) framework of analysis—to capture the unique characteristics and conditions of a specific OE. **Chapter 1** provides the introduction, purpose of the paper, and key definitions. **Chapter 2** provides an overview of the strategic environment along with some key examples and presents a discussion of potential adversaries and their associated strategies within that environment. **Chapter 3** offers the implications to the Army of the conditions of the strategic environment.

METHODOLOGY

In order to capture the most significant conditions, the SE is analyzed through the lens of eight OE variables (the OEA framework of analysis; see **Annex A: The Operational Environment Assessment Framework**). The OEA framework allows an analyst to develop a deeper and more robust understanding of the key conditions and characteristics of a specific OE. Key conditions across each variable have been

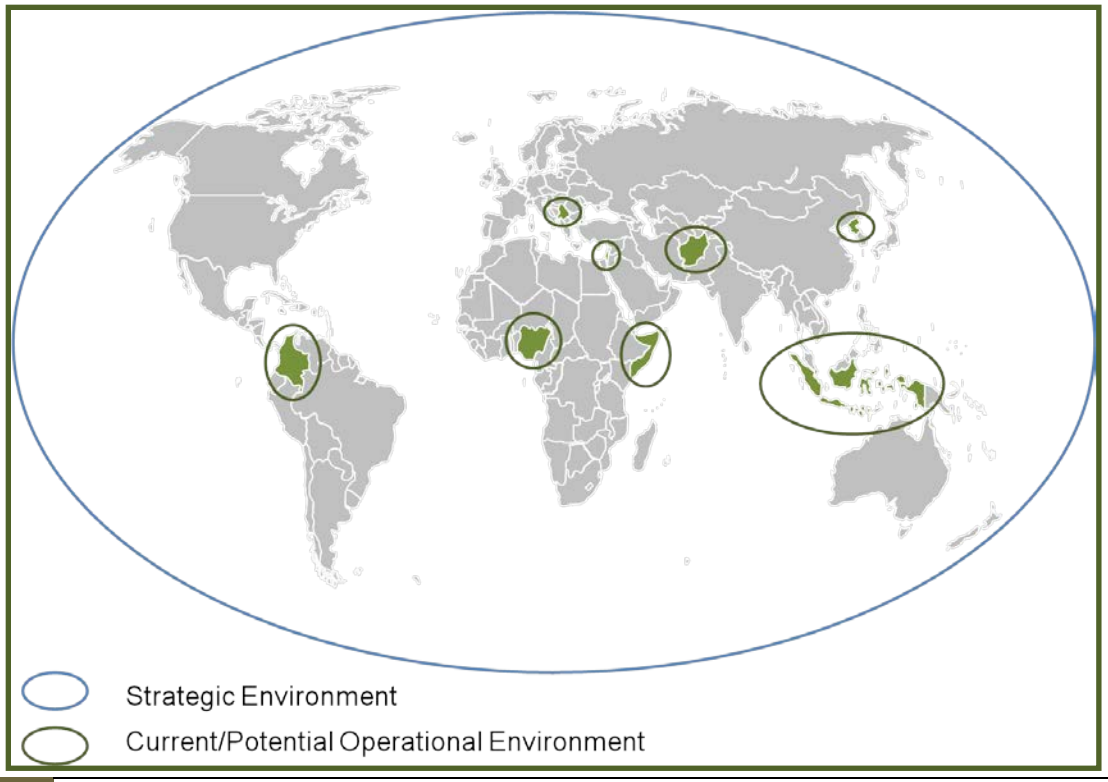
selected for discussion, and only those conditions deemed to have the most important security implications are included in this paper. The selected conditions have current significance and are the most likely to have future implications across the SE. Each variable discussion shows the current and projected future path of each condition.

The OEA framework is typically used to gain a holistic understanding of one specific OE—most often at the state or regional level of analysis. Detailed analysis is required, given that strategic conditions manifest differently across each OE and change constantly. At the operational level, a high degree of resolution is needed to capture the required level of detail for training or pre-deployment. The OEA framework provides such resolution. For use at the strategic level, the framework discussion highlights only the key conditions or observations from each variable that are deemed to have both global reach and significant security implication. Only after the conditions of the strategic environment are articulated can a discussion of the types of adversaries and their potential strategies begin.

Annexes B-G provide regional discussions of the selected conditions. Conditions shaping each region are presented followed by a discussion of potential future Army missions in each region. Finally, **Annex H** presents an overview of additional adversarial designs and capabilities.

THE DIFFERENCE BETWEEN STRATEGIC AND OPERATIONAL ENVIRONMENTS

It is important for the reader to understand the difference between the strategic environment and an operational environment. The SE is the global environment in which the U.S. President employs all the elements of national power (diplomatic, informational, military, and economic). For the purpose of this paper the strategic environment is defined as the set of global conditions, circumstances, and influences that affect the employment of all elements of U.S. national power. The SE contains multiple potential OEs.



Therefore, there is no one operational environment. By Department of Defense (DOD) definition, an OE is "a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander" (JP 3-0). This definition applies to an OE for a specific operation, at any level of command, and any level of analysis. Multiple OEs can and do exist. This distinction becomes important in order to avoid confusion when discussing conditions in the strategic vs. potential operational environments.

CONCLUSION

We know that the current and future strategic environment will be characterized by uncertainty, complexity, and increasingly nuanced relationships. TRADOC must develop an understanding of the conditions of this fluid environment and their interactions. The strategic environment must be discussed, captured, and factored into all decision-making. Only then can the right training, correct mix of systems and capabilities, and suitable approaches to leader development and education be identified and implemented across the Army.

Chapter 2
Conditions of the Strategic Environment

THE COMPLEX STRATEGIC ENVIRONMENT

The strategic environment remains as it has always been: complex. The interaction of the many variables within the environment, including human behavior, assures both fog and friction. The Cold War SE, despite the many variables involved, proved to be a relatively stable and understandable milieu for decision-makers. Both options and limits were considered in the context of an overarching strategic view based on a broad consensus. The nuclear weapons standoff between the U.S. and the U.S.S.R., arguably, produced deterrence and, combined with strong conventional forces, reduced and contained the scale of both proxy wars and simmering ethnic and ideological tensions.

The collapse of Soviet communism has left us with a paradox; there is less threat but also less peace.[2]

General Manfred Woerner, NATO Secretary General

The current strategic environment seems more ambiguous, presenting multiple layers of complexity and a multiplicity of actors challenging the Army with requirements beyond traditional warfighting skills and training. A wide-range of actors across the current and projected SE – friendly and neutrals, malicious actors, and threats – will interact, often in an uncoordinated manner, to produce a complex environment. Neutral or even friendly actors will act in accord with organizational goals that may be contrary to U.S. national interests causing friction. Malicious actors will use violence in pursuit of their goals and will potentially challenge U.S. national interests and vulnerabilities. Threats will use this complexity to their advantage and often employ hybrid strategies. This multiplicity of actors will continue to operate across potential operational environments during the forecast period.

Current ethnic and sectarian tensions within and between countries threaten stability around the world. Economic distress, coupled with the long-term effects of bad governance and revolutionary demands for better governance, have contributed to global unrest. Economic distress is not limited to developing states. The European Union (E.U.) may yet fracture. The strength and influence of the Western alliance in global affairs seems, for the moment at least, in decline. The U.S. remains the most powerful state, but is beset by its own economic and political challenges which further muddy the water through which policy makers and military strategists must peer.

The anticipated strategic environment remains intricate and ambiguous due, in part, to the absence of an overarching consensus on how to approach current and future adversaries and challenges. The national military tools currently available are not always useful in unraveling such complexities in the absence of significant agreement on how to approach the current SE. In some cases, the application of current military tools in an effort to ease tensions has instead exacerbated such problems.

The complexity of today's SE is at least in part a result of U.S. military dominance. Weaker states, in response to U.S. military dominance, have developed strategies to counter U.S. intervention. These states have built conventional forces to coerce and deter neighboring countries while augmenting forces

with irregular elements that provide advantages if the U.S. intervenes. Developing forces that take the U.S. away from its preferred method of warfare—through resources such as WMD, cyber attacks, SPF, or terrorist groups acting as proxies—are believed to significantly reduce the likelihood that the U.S. will choose to enter a conflict.

However, U.S. non-action in this kind of environment can result in two fundamental risks. First, the strategic risk is that non-intervention in a turbulent area could produce an outcome contrary to U.S. interests. For example, in Afghanistan the U.S. supported a "proxy" ground force (the Northern Alliance) with conventional air force assets and U.S. Special Forces. Had the U.S. chosen not to introduce significant ground forces capable of shaping the outcomes, then the probability of an end state incongruent with U.S. interests would have been increased. It may be argued that the current state of affairs in Afghanistan would be no worse had we not introduced ground forces. Even if Afghanistan does not become a functioning liberal democracy, there can be no argument that much of Afghanistan is better off now than under the Taliban.

Second, the risk of failure is accelerated with direct intervention. If ground forces were introduced in Libya, for example, missteps, miscues, and mistakes may have produced the same result as non-intervention—a Libyan government hostile to U.S. interests. Accessibility to cell phone cameras and the Internet ensure that any mistake made is immediately usable for enemy propaganda and perception-management activities. In spite of these challenges and potential opportunities, the failure to place forces on the ground to maintain a guiding presence forfeits the chance to shape the conditions of the environment to be congruent with U.S. national interests.

U.S. intervention into this complex SE will produce many outcomes, some unpredictable. U.S. forces may unwittingly release long-suppressed aggression and create chaotic and dangerous conditions for both U.S. forces and the population. Radical ideologies foster entities that see U.S. involvement in any conflict as an opportunity to weaken the U.S. will while bolstering their own claims to be the righteous purveyor of that radical ideology by attacking the U.S. This opportunistic venture produces its own complexity in an OE that would otherwise have been amenable to the tools U.S. forces bring to the fight. Developing an understanding of these challenges and the complexities they present is critical to comprehending current and future military operations. To foster this understanding, the following discussion provides an analysis of the key conditions that will shape the strategic environment over time.

CONDITIONS SHAPING THE STRATEGIC ENVIRONMENT TO 2028

The eight OE variables—**political**, **military**, **economic**, **social**, **information**, **infrastructure**, **physical environment**, and **time**—provide a valuable lens through which to analyze conditions in the strategic environment. Key conditions across each variable have been selected for discussion. The selected conditions are those conditions with current significance and the most likely to have future implications across the SE. Each variable discussion shows the current and projected future path of each condition.

This approach is based on the OEA framework of analysis (see **Annex A: The Operational Environment Assessment Framework**). The OEA framework is typically used to gain a holistic understanding of one specific OE—most often at the state or regional level of analysis. Detailed analysis is required, given that strategic conditions manifest differently across each OE and change constantly. At the operational level, a high degree of resolution is needed to capture the required level of detail for training or pre-

deployment. The OEA framework provides such resolution. For use at the strategic level, the framework discussion highlights only the key conditions or observations from each variable that are deemed to have both global reach and significant security implications.

The individual variables are each significant, but the convergence point of one or more variables can have the most dramatic impact on an OE or group of OEs. For example, the Arab Spring political revolutions witnessed the convergence of political (shortfalls in state governance) with social (persistent youth bulge), manifesting in poor economic conditions that helped ignite a massive popular uprising against numerous regimes. Information conditions (ICT proliferation) then facilitated the movement. In the final analysis, it was the convergence of at least four variables in the OE that helped manifest the Arab Spring. When appropriate, the following discussion will address potential areas of convergence.

POLITICAL CONDITIONS

CHANGING INTERNATIONAL DISTRIBUTION OF POWER

The most significant political condition over the forecast period is the shifting of the global balance of power. The U.S. faces a balance of power shift "that rivals the end of the Cold War, if not that facing the nation at the conclusion of World War II."[3] By 2028, the U.S. will remain the world's dominant political, economic, and military power, but with a continually decreasing relative advantage over other nations.[4] Emerging state powers and new, more powerful non-state actors will create a multipolar international system of power. The countries with the most potential to substantially increase their power during the forecast period include China, India, Russia, Indonesia, Turkey, and Brazil.[5] History indicates that "emerging multipolar systems have been more unstable than bipolar ones."[6] This shift in the international distribution of power has the potential to produce greater political, military, and economic tensions between those actors who are losing power and those that are gaining in significance. This strategic condition will no doubt converge with economic, social, information, and military conditions across the strategic environment for years to come.

DECLINE OF GLOBAL GOVERNANCE

Over the forecast period, global governance—the collective management of common problems at the international level—will likely decrease due to increasing numbers and influence of non-state actors. Businesses, organizations, and even individuals are liable to form networks or informal groupings and partnerships to address their collective problems, and regional actors will band together to achieve a regional solution.[7]

The number of NGOs, PVOs, PSOs, and non-state actors is expected to increase drastically as the Internet facilitates worldwide contact with low entry costs and low overhead for political and security participants.[8] Both states and non-state actors will continue to be empowered by the proliferation of ICT and will use such capabilities for purposes of governance at the international level. The Army must prepare to deal with a wide range of actors operating in the current and future strategic environment. Over the course of the next sixteen years the number of actors will continue to increase.

SHORTFALLS IN STATE GOVERNANCE

State challenges to provide good governance—basic services and governmental legitimacy—to their populations will remain a constant over the forecast period. Many governments in Africa, the Middle East, Southern Asia, and Latin America face perennial challenges in maintaining political legitimacy in the eyes of their citizens. They lack the institutional, infrastructural, human, and material resources to provide physical security, deliver basic public services, administer justice, and promote economic development. Non-state actors are stepping in to fill this void (e.g. Hezbollah in Lebanon). This trend will likely continue well into the future as other non-state actors step into political roles across various OEs. Over the past two decades, international and bilateral development programs have increasingly targeted governance shortfalls in these regions with little success. Western states are not exempt from this problem, as growing debt loads are forcing countries to institute austerity measures in order to obtain the financing required to avoid default. In Greece, this has caused major reductions in social services and resulted in strikes and riots.[9]

2011 Protests in Yemen

Wikimedia Commons, Yemen Protests, 3 February 2011

Yemen provides the most instructive current example of a state failing to govern. Increasingly divided elites, dwindling state resources, al-Qaeda presence and influence, and strong, unified opposition movements were among the Yemeni state's pre-existing conditions when the Arab Spring ignited. Popular protests and an overly-violent state response may have dealt the regime a fatal blow. Over the past year, the army has split and state authority and influence have contracted significantly, mostly concentrating around the capital city of Sanaa and surrounding districts. Non-state actors, including al-Qaeda in the Arabian Peninsula (AQAP) and the Zaydi revivalist Houthi movement, are quickly filling the void.[10] Areas suffering from poor state governance will remain an attractive locale for actors seeking to establish a base of operations unconstrained by the rules of law. State failure can also trigger destabilizing events on both a regional and global level. For example, protracted state failure in Yemen would likely affect maritime traffic flow in the Gulf of Aden, with severe ramifications for access to the Suez Canal.[11] The Army must be prepared to deal with failing states and those actors seeking to benefit from such conditions.

MILITARY CONDITIONS

GLOBAL MILITARY EXPENDITURE RATES

World military spending for 2011 did not increase for the first time since 1998. The major reason for either reductions or increases in an individual country's military spending relates directly to how particular countries have been impacted by the global financial crisis which began in 2008. Western and Central Europe suffered a particularly strong impact causing a reduction in military spending by 1.9 percent from 2010 to 2011. The inability of the United States Congress to agree on a 2011 budget led to a small real-term reduction in U.S. military expenditures. Africa represented the greatest increase in military expenditures by 8.6 percent. This increase is due, in large measure, to the increasing oil

revenues from countries such as Algeria. Algeria increased military spending by 44 percent due to increased oil revenues, threats from al-Qaeda in the Islamic Maghreb (AQIM), and regional ambitions. Middle Eastern countries increased military spending by 4.6 percent. [12]

Into the future, military expenditures should not rise significantly and may see reductions in some countries. Western Europe is seeing continued demands for "austerity" measures. In the face of high unemployment, diminishing domestic public services, and greater debt, most Western European countries will focus discussions on how to reduce military expenditures through better European Union member country cooperation. The U.S. withdrawal of troops from Iraq and the anticipated pull-out of U.S. forces from Afghanistan should lead to status quo or reduction in U.S. military expenditures into the near future. North African and Middle Eastern countries facing increasing threats from international and local terrorist organizations such AQIM and Nigerian Boko Haram, paired with large oil revenues, will continue to increase military spending.[13]

WIDE RANGE OF POTENTIAL MISSIONS AND ADVERSARIES

Conflict is a constant condition across the strategic environment, with intrastate conflict increasing while state-on-state conventional fights are decreasing.[14] During the forecast period, governments worldwide will face networks of adversaries with a wide range of sophistication, capabilities, and goals.[15] The range of threats across the strategic environment over the forecast period, include **criminal organizations, terrorists, states and non-state actors, insurgents, transnational groups, proxies, technologically-empowered individuals, and paramilitaries**.[16] These actors are increasing in number and capabilities, and may operate as **regular, irregular, or hybrid threats** that can and will challenge conventional military forces.

In addition, traditional armies are investing in more effective, conventional capabilities including armor, air defense, and robotics. China, Russia, and India are examples of traditionally-configured militaries that will grow more capable in the future. Their extensive international military training and sales programs are enabling other states and/or proxies to field highly-capable conventional militaries.

Allegiances and alignments within the complex network of actors, state and non-state, will often change. Adversarial forces will constantly study the military operations of their foes and seek to exploit perceived weaknesses. Transitions in operations of adversarial military forces and changes within the patterns of networks must be constantly monitored and anticipated to avoid surprise and maintain the ability to conduct operations within a designated OE. The Army must be capable of decisive action against a wide array of adaptive threats, and be operationally prepared for a wide range of missions.[17]

Non-state actors and unconventional operational methods will have a greater impact on U.S. military operations. Responding to these types of adversaries "is already blurring the lines between civilian law enforcement and the military; it may also constrain and stress the use of political, economic, and military power."[18] Providing security for the nation in this environment requires the ability to conduct operations across the range of potential military operations. The Army will need to continue to mature its capabilities to counter foreign insurgents and extremists, especially in the Homeland, while maintaining the ability to fight a regular or hybrid threat against state actors and their proxies.

RISE OF PSOs

Beginning in the 1990s, international conditions created an environment ripe for the creation of private security organizations. Several reasons account for this growth. First, post-Cold War downsizing and the increase in small conflicts of little interest to the great powers created a security market opportunity for private sector companies. Second, governments were experimenting with the outsourcing of traditional government jobs and roles to the private sector; security became a natural extension of this experiment. Third, complex military systems required contractors with requisite experience that could train, support, and maintain increasingly sophisticated equipment.[19]

All indications are that PSOs will continue to be an integral part of the strategic environment to 2028. Recent conflicts in Iraq and Afghanistan have brought attention to the use of PSOs, but lesser conflicts all over the world currently use the services of international companies that provide a variety of security services ranging from direct tactical military services, to military consulting, to military support in the form of logistics, intelligence, and maintenance services.[20] One estimate puts the number of PSOs at several hundred global companies with generated revenues of over $100 billion dollars annually.[21] Serious implications have not been completely resolved, including the legal status of PSOs in conflicts, operational and tactical control, and oversight. The consistency of small conflicts around the world, the hesitancy of great powers to intervene with military forces, and the complexity of modern military systems guarantees that PSOs will continue to be an integral part of the strategic environment in 2028.

WMD PROLIFERATION

The proliferation of WMD and related technologies will continue during the forecast period despite non-proliferation being a global priority. WMD capabilities provide actors with a strategic lever to deter their enemies from pursuing certain military strategies. An operational capability may give hostile states and non-state actors a bargaining chip to sue for a negotiated settlement short of complete defeat and regime change. Several extremist organizations are known to be seeking WMD capabilities as well—especially nuclear and biological weapons. The Director of National Intelligence (DNI) predicts that "terrorist or insurgent organizations acting alone or through middlemen may acquire nuclear, chemical, and/or biological weapons and may seek opportunistic networks as service providers."[22] Recent Joint Staff analysis concluded that "considering the efforts by radical, non-State actors to obtain and employ WMD, the likelihood that WMD will be used somewhere in the next 25 years is high."[23]

The proliferation of WMD and related technologies "represents the most serious future threat to America."[24] The DNI recently stated that the "ongoing efforts of nation-states to develop and/or acquire WMDs constitute a major threat to the safety of our nation, our deployed troops, and our allies."[25] The potential for WMD use in warfighting cannot be dismissed across the forecast period. The Army must be prepared to operate in WMD environments and continue to improve its ability to locate and defend against such capabilities.

IMPORTANCE OF THE GLOBAL COMMONS*

Adversaries will seek to deny their enemies access to the global commons, thus limiting their foes' offensive and defensive capabilities. Many states—China, Brazil, India, Russia, Iran, and Saudi Arabia—"are already beginning to orient their militaries toward the global commons, fielding significant maritime capabilities including advanced surface combatants, increasingly capable submarines, sophisticated anti-ship cruise missiles, and (in China's case) ballistic missiles designed to strike major ships at sea."[26] Over the course of the forecast period, there is greater potential for cyberspace or space-based attacks from state, non-state, and proxy actors.[27] China has spoken openly of the "inevitability of space conflict" and the "the requirement of [building] both offensive and defensive space capabilities."[28] Developing countries may be just as much of a concern. The skills required for India and Pakistan to create a nuclear bomb might as easily be used to develop the capability to disrupt space technology-generated images and information. As just one example of current attacks in the cyberspace common, external sources—both governmental and non-state actors—are working daily to penetrate U.S. DOD networks, and foreign intelligence organizations have acquired the capacity to disrupt the U.S. military's information infrastructure. U.S. cyber strategy acknowledges that it is possible that certain systems within DOD's network have been compromised and are as yet undetected.[29]

CONTINUED VULNERABILITY OF THE U.S. HOMELAND

The U.S. Homeland remains vulnerable to attack from extremist groups. Despite success in reducing the effectiveness of al-Qaeda and its affiliates, extremists—both foreign and domestic—will use terrorist tactics in attempts to strike the Homeland during the forecast period. Extremists will continue to recruit members and sympathizers, and religious fervor may not be their only incentive to fight. In addition, the expanding collaboration and cooperation between criminal enterprises and entities associated with extremism and terrorism will exponentially boost their potential for success. The Army must remain prepared to counter threats to the Homeland.

EMERGING AND PROLIFERATING MILITARY TECHNOLOGIES

Over the forecast period, military technologies will continue to proliferate to all types of adversarial actors. If actors have the financial resources, the capabilities are there for the taking. Nanotechnologies will likely provide the impetus for most key emerging military technological breakthroughs over the forecast period. These breakthroughs will probably occur in the areas of ICT, sensor or network technology, biotechnology, and energy storage and transfer. Military leaders will leverage emerging ICT that connects intelligence to enhance their mission command to better visualize, describe, direct, and lead forces against a hostile, thinking, and adaptive enemy. Sensor or network technology will focus on unmanned systems as a means to gain information and intelligence over enemy terrain while reducing physical risk to military personnel.

Biotechnology breakthroughs will have important civilian applications in the areas of medicine, food science, and industrial manufacturing; but they could also lead to new WMD threats to military personnel. It is also probable that biotechnology improvements will provide human strength

* According to the Oxford Dictionary, the *global commons* is "the earth's un-owned natural resources, such as the oceans, the atmosphere, and space." For the purpose of this paper, the domains of the global commons are maritime, air, space, and cyberspace.

augmentation through breakthroughs such as lightweight exoskeleton systems that give the wearer greater protection while increasing physical power. New energy storage technology will range from smaller, lighter, and more powerful batteries that operate military equipment to renewable energy systems that use wind and solar power instead of hydrocarbon fuels. The military may turn to vehicles powered by more accessible biofuels and reduce reliance on gasoline, diesel, and aviation fuel produced from overseas sources. At the extreme end, directed energy weapons may reach the stage where they possess the ability to incapacitate or kill the enemy without collateral damage to either people or infrastructure.[30] Training and education, and leader, concepts, and capabilities development will need to embrace and adapt to key emerging technologies. Adversaries with financial resources will certainly be ready to adapt.

ECONOMIC CONDITIONS

ECONOMIC SHIFTS

Two main global changes in relative wealth and economic power are now underway. The first is a shift from Western to Eastern nations that will continue over the course of the next decade—if not longer. This change will affect the current, global political and military balance of power through the gradual move to a multipolar world, one in which pre-eminence of the West cannot be taken for granted. Nontraditional economic alliances exclusive of the U.S.—such as the BRICS (Brazil, Russia, India, China, and South Africa) alliance—are likely to become stronger, and have the potential to bring another 200 million people with incomes over $15,000 into the world economy by 2050.[31] South Korea, Indonesia, Nigeria, and Chile will also emerge, laying a firm foundation for global economic strength.[32] The second change is that economic alliances between criminal organizations and non-state actors will create new global agents of change, control, and influence in the economic and political realm. The National Intelligence Council estimates that organized crime will continue to grow in influence, with the potential to control several Eastern European governments by 2025.[33] The current and future strategic environment will require the Army to understand such new alliances and shifts and be prepared to deal with the potential tensions stemming from such change.

INCOME INEQUALITY

Income inequality will remain a key economic consideration in the SE. According to the World Bank, over the next several decades the number of people considered to be in the global middle class is projected to increase from 7.6% to 16.1% of the world's population, with most of the new entrants coming from China and India. By 2025-2030, the portion of the world considered poor will shrink by about 23%, but will still constitute 63% of the global population and will be worse off than it is now.[34] Research on trends in armed conflict demonstrates that a disproportionate share of internal conflicts occurs in poor countries with low economic growth rates.

ECONOMIC INTERDEPENDENCE

Globalization has and will continue to raise the level of economic interdependence between states, non-state actors, and individuals across the global economy. While this condition is apt to be an engine for accelerated economic growth, it is also a source of risk, as local markets face increased exposure to destabilizing fluctuations in the global economy.[35] Resources, trade, capital, and intellectual property will rely on complex networks of physical and virtual infrastructure and the supply chains that support

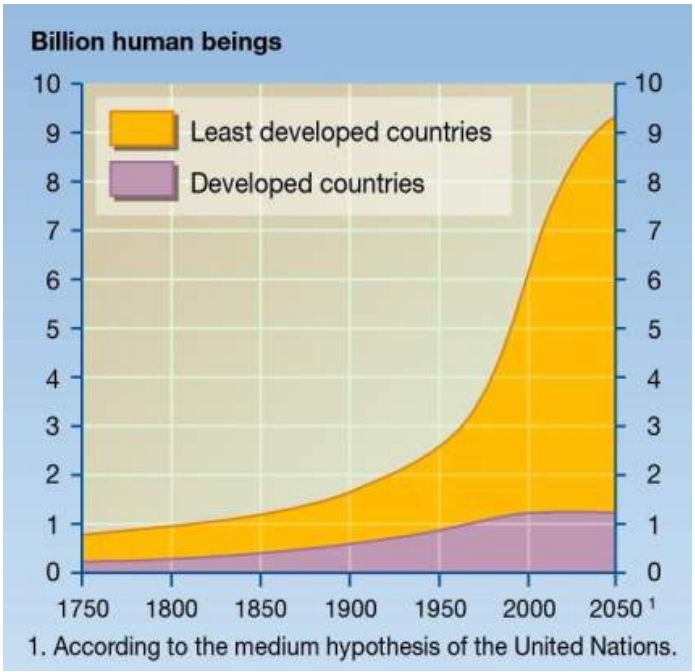
globalization. Disruptions or attacks anywhere along these supply chains risk propelling once-isolated local events into potentially catastrophic global events. Assuring continued access to the global commons may involve the use of military force, while interdependence may shift political power balances in favor of exporting nations over their importing partners or vice versa.

SOCIAL CONDITIONS

DEMOGRAPHIC TRANSITION

Across the strategic environment, states are going through what is referred to as demographic transition—the tendency for families to have increasingly fewer children per household. Developed countries' populations have transitioned to a demographic pattern of low birthrates and slow population decline, presaging an end to the exponential growth of world population during the late 20th century. China, Japan, Russia, Korea, and most of Europe will experience aging populations and gradual population decline that will test their governments' abilities to maintain economic growth, provide health care and pensions to growing senior populations, and provide for national defense. The number of elderly people will likely double in the developed world by 2028.[36]

Aging and even declining populations for many of America's traditional allies in Europe and Asia is already affecting their ability to contribute to collective defense. Even China, which is often posited as a security challenge to the U.S., faces problems associated with a rapidly aging and declining population, especially after 2030. Unlike the already-industrialized countries, these demographic challenges will appear in China before its economy has fully developed and will likely affect the direction and pace of its economic growth. Aging populations might also trigger higher migration levels as states seek to find adequate sources of labor.



Trend in Global Population, 1750-2050

United Nations Dept of Social and Economic Affairs, *World Population Prospects: The 2006 Revision*, February 2007

POPULATION GROWTH

Despite the ongoing transition to fewer children per household, the world is adding the largest numbers to its population in history, with an increase of 83 million annually. The global population reached an estimated seven billion in 2011. Both the six and seven billion marks were reached in a period of 12 years from the previous billion. If birth rates decline as projected, a population of

eight billion will be reached in 2023.[37] By mid-2025, more than a billion will be added to the population of the less developed world while the more developed world will see growth of only 48 million.[38]

Over the past half-century, fertility rates fell dramatically in Europe, particularly in Eastern Europe. Simultaneously, fertility appears to be on the rise in a few countries, such as Burundi and Zimbabwe in Africa, and Kazakhstan and Kyrgyzstan in Central Asia.[39] Russia, Ukraine, Italy, Japan, and almost all countries in Eastern Europe are expected to see their populations decline by several percentage points by 2025. In Russia, Ukraine, and a few other Eastern European countries, these declines could approach or even exceed 10% of the current populations.[40] The U.S. population is projected to grow by more than 40 million, Canada by 4.5 million, and Australia by more than 3 million. India will be the nation with the largest population increase, representing about one-fifth of world growth. India is projected to add about 240 million people by 2025, reaching a population of approximately 1.45 billion. At the same time, China's current population of over 1.3 billion is expected to increase by more than 100 million.[41]

Nearly all of this growth will be in the developing world. The increased world population will fuel greater demand for resources such as energy, minerals, clean water, and food. The competition for resources—aggravated by a larger world population—also heightens the possibility of armed conflict, with populations desperate for essential resources being more likely to resort to extreme measures. The mistreatment of a weaker group by a stronger group could lead to mass atrocities and even genocide, requiring a response from the global community.[42]

PERSISTENT YOUTH BULGE

Many countries around the world are now dealing with a youth bulge, which is defined as a disproportionately large percentage of a population between the ages of 15 and 29. The current youth bulges in Turkey, Lebanon, and Iran will decrease, but those in the West Bank, Iraq, Yemen, Saudi Arabia, Afghanistan, Pakistan, and Sub-Saharan Africa will continue throughout the forecast period.[43] Such a bulge can have either positive or negative effects for a country: it can supply needed workers in a robust economy and a large pool of applicants for military recruitment, or it can create a large population of discontented youths with no prospects for employment or self-improvement.[44] A youth bulge is often accompanied by high unemployment among young men that in turn increases the potential for instability. Nigeria, for example, has thus far been unsuccessful in finding work for its massive youth bulge—almost half the population is under the age of 15, with a staggering 45 million between 10 and 24 years old.[45] The result has been some youth turning toward radicalized elements, particularly the terrorist group Boko Haram in the country's north, as a means of livelihood and an outlet for their frustration. The Arab Spring occurred in countries with the same conditions—large youth bulge and high unemployment. Similar conditions prevail across much of Africa, Asia, and parts of Latin America.

INFORMATION CONDITIONS

PROLIFERATION OF ICT

ICT has evolved tremendously since the creation of the first electric programmable computer in 1941, and will continue to do so during the forecast period and beyond.[46] Items such as cell phones, smart phones, and tablets will continue to become smaller, more powerful, more versatile, and less expensive. As a direct result, the possession of advanced technology is no longer limited to nation-states or wealthy

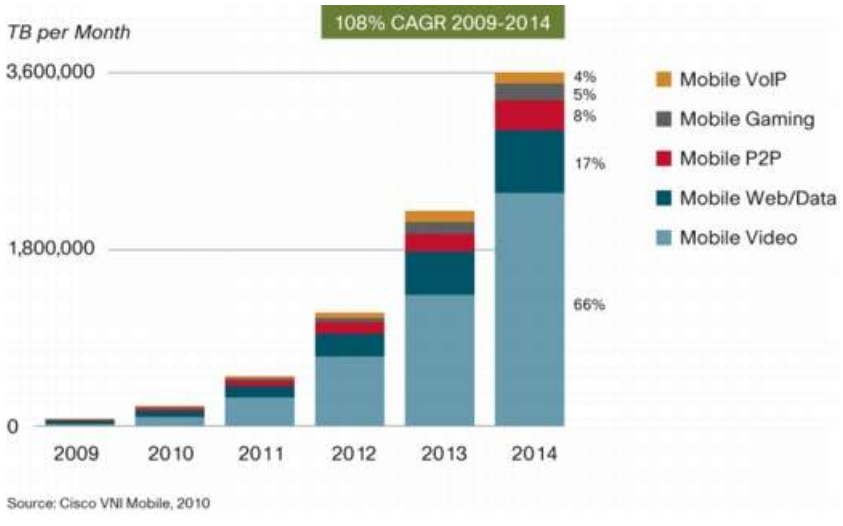
individuals, but is available to even the poorest persons living in the most poverty-stricken countries in the world. For example, a recent survey in India revealed that over half the population—53.2%—owns a mobile phone, and that more households possess televisions than toilets.[47] Many developing nations are taking advantage of technological advances such as "skipping" landlines and building communications infrastructure based on cell phone technology. The implications of technology proliferation are multiple and varied, but four stand out in particular: transparency, actor empowerment, strategic narrative, and technological vulnerability. The Army must be prepared to operate within all types of information environments. Adversaries will attempt to control the narrative and deprive U.S. forces of ICT capabilities across all potential OEs.

Transparency across Societies

Individuals and states can no longer expect to keep the world ignorant of their actions. All military actions and activities have the potential to be digitally captured (perhaps even digitally manipulated) and distributed to a global audience. Information could previously be suppressed through lack of evidence and/or lack of access to broadcast methods, but this is no longer the case. From the beating of Rodney King in Los Angeles in 1991 to the treatment of the "blue bra woman" by Egyptian security forces in 2011, such actions that could formerly be kept hidden are now open for all to see. Regardless of where an event happens, someone will be there with a cell phone, recording it and uploading it to the Internet within minutes. It will become increasingly difficult for actors to conduct diplomacy and military operations with the continuous threat that all their actions and comments are recorded and distributed to a global audience.[48]

Actor Empowerment

The rise of social media, such as Facebook and Twitter, is having a direct impact on the ease with which individuals can communicate with each other. With older software technologies, mass communication was still limited in time and space. The best a person could do was post something to a Web site or send out a mass e-mail, and hope that the intended audience would check the Web site or e-mail account in the near future. Now, an individual can post something with a cell phone, and it is instantly communicated to a large audience via cell phones, computers, and tablets. Others can just as quickly post a response that is seen by the original recipients. This fast,



Trend in Volume of Mobile Communications, 2009-2014

Cisco Systems Inc, *Cisco Visual Networking Index: Forecast and Methodology, 2009-2014*, June 2010

interactive way of communicating can lead to activities as innocuous as "flash mobs," and as serious as full-scale riots. Though the role of social media during the Arab Spring is not yet clearly understood, there is little doubt that it did indeed play a part. As technology is placed in the hands of more and more people, social media will make it easier to instantly mobilize large crowds, be it political, military, or social in nature.

Controlling the Strategic Narrative

With the instantaneous nature of global communications via ICT, the importance of rapid and credible perception management is growing at an exponential rate. In the past, if an event could not be hidden from sight, the actors involved could reveal information slowly and in the manner of their choosing. With mounting transparency and actor empowerment, it is no longer the party that explains his case best that wins the argument, but the one who explains it first. The ability to decide on a narrative and get it out into public view in a timely fashion is paramount: the first narrative presented is seen as authoritative, and those holding other views are automatically put in defensive mode—they must hope to persuade their intended audience of the correctness of their view and the wrongness of the other, whereas the holders of the first narrative have no such difficulties. This has strong implications for both the political and military variables, as modern governments and militaries are usually constrained by some form of approval chain that limits their ability to rapidly respond to events, whereas their opponents have no such constraints.

Technological Vulnerability

The spread of ICT on a global basis and developed nations' dependence on technology will place them at an amplified risk over the forecast period. Cyber attacks, previously the domain of hostile governments, are now easily within the realm of individuals and loosely-knit organizations, such as the hacker group Anonymous. These effects can be felt by both individuals and organizations alike, from the person who discovers his e-mail account has been hacked to the gaming company whose customer names and credit card information are stolen. U.S. cyber strategy has acknowledged that it is possible that certain systems within DOD's network have been compromised and are as yet undetected.[49]

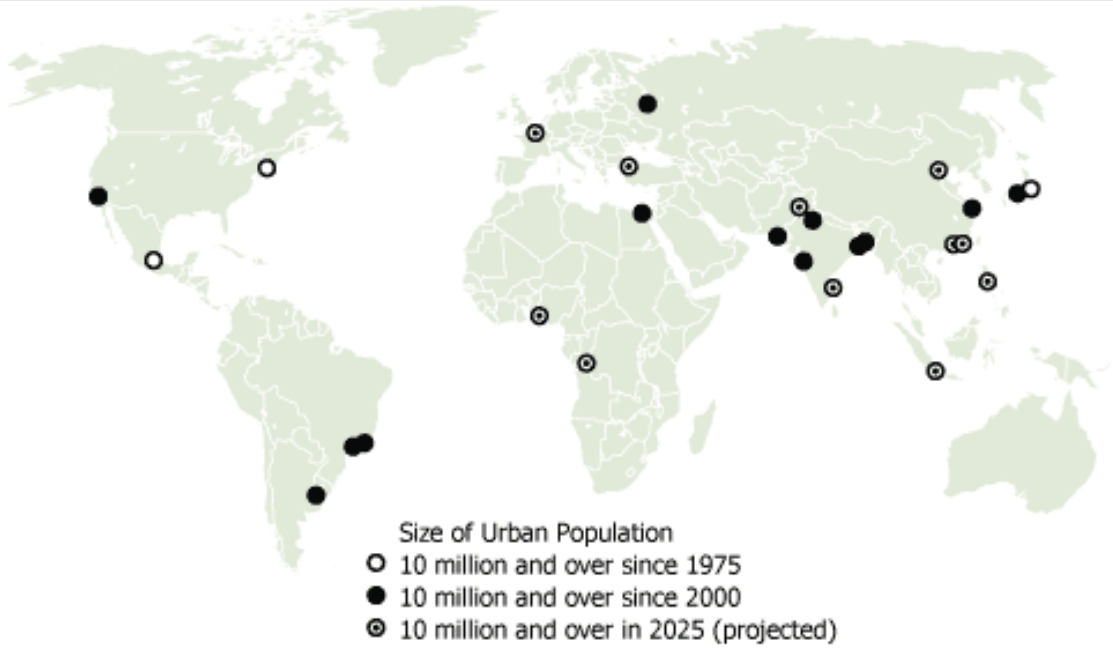
One other risk of dependence is the growing existence and ready availability of technological countermeasures, two examples being cell phone jammers and global positioning system (GPS) jamming/spoofing. Both have been used successfully in military situations: the first by U.S. and affiliated forces as counter-IED measures in Iraq and Afghanistan, and the second by Iran to capture a U.S. drone in 2011.[50] As such devices continue to grow in availability, the technological advantage held by one party over another is reduced or even eliminated. With their heavy dependence on ICT, U.S. forces and other modern militaries may find their opponents equal or even superior to them in some ways.

INFRASTRUCTURE CONDITIONS

URBANIZATION

The urbanization of countries around the globe will continue during the forecast period. According to the National Intelligence Council, "by 2025 about 57% of the world's population will live in urban areas, up from 50% today [2008]."[51] As these areas continue to grow and expand, problems inherent to urban communities will be intensified. Those seeking political change can easily reach and mobilize large numbers of people with effects up to and including the overturning of governments, as occurred during

the Arab Spring of 2011. Urban populations are also difficult to control from a security perspective, as both criminals and insurgents can easily blend into the environment. News and opinions are quickly passed from person to person—either by word-of-mouth or electronically—allowing for freedom of expression and simultaneously making government control of information more difficult. Rising demands on infrastructure will result in larger and more frequent breakdowns of utility and transportation systems. The sheer number of people within a fixed area will make any humanitarian crisis—whether earthquake, famine, or epidemic—more severe in both size and scope. Prolific urbanization has the potential to exacerbate issues faced by a government, military, or organization.



Largest Urban Agglomerations, 1975, 2000, 2025

United Nations, World Urbanization Prospects: The 2007 Revision, Population Reference Bureau, 12 April 2012

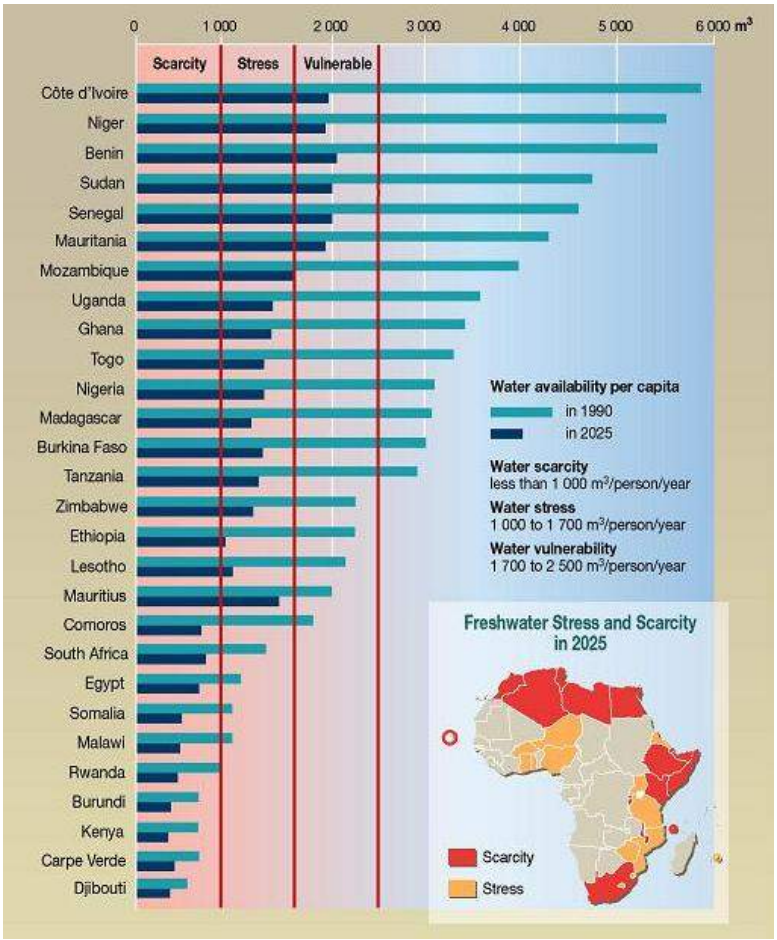
EXPANDING PHYSICAL INFRASTRUCTURE

Physical infrastructure, such as road, utility, and communications systems, will expand and improve during the next sixteen years. China is expanding its road infrastructure with the goal of having a network "suitable for the entire Chinese population by 2020," including at least 27 new highways.[52] The country is also making bilateral agreements with other nations whereby natural resources are exchanged for infrastructure improvement programs. For example, in 2007 China signed an agreement with the Democratic Republic of Congo (DRC) in which China provides $5 billion for infrastructure improvements in exchange for rights to DRC's natural resources.[53] Access to electricity is of major import as well: in light of global concerns over hydrocarbon resource levels and nuclear power safety issues, hydroelectric power projects will expand worldwide. Turkey is currently working on an extensive project that includes multiple dams and hydroelectric plants on the Tigris and Euphrates Rivers, and the Supreme Court of Chile recently ruled to allow the HidroAysen dam project in Patagonia to proceed.[54] ICT infrastructure will also continue to grow in both developed and developing countries, such as the current project to build a land-based fiber-optic system linking the countries of Sierra Leone, Guinea, and Liberia in West Africa.[55]

PHYSICAL ENVIRONMENT CONDITIONS

COMPETITION OVER NATURAL RESOURCES

Competition over limited natural resources—such as water, hydrocarbons, metals, and rare earths—will continue to intensify during the upcoming decades, fueled by regional economic and population growth; unequal resource distribution and limited supply; unstable political, military, and/or physical environments in source regions; and a distinct lack of suitable alternatives for the resources sought. Of particular note is that hydrocarbons will continue to experience mounting demand—and prices—as both developed and developing countries increase their energy consumption. Reactions to this struggle over natural resources will mainly occur in the political, military, and economic arenas, and may manifest in such ways as the arms-for-oil agreement between Venezuela and Belarus; the mining of conflict diamonds in camps run by Zimbabwean security forces; and the current lawsuit brought by the U.S., E.U., and Japan against China regarding Chinese production and use of rare earths.[56]



Trend in Water Availability in Africa, 1990-2050

United Nations Environment Programme, *Global Environment Outlook 2000*, 1999

CLIMATE CHANGE

Global weather patterns have diverged significantly from the norm in recent years.[57] While a discussion on the prospect of global climate change is not within the purview of this paper, a consideration of possible implications is both appropriate and relevant. Potential effects of lasting weather shifts generally fall into two broad categories: short-term and long-term. Short-term effects include catastrophic events that are inherently one-time in nature—e.g. hurricanes, typhoons, tornados, and mudslides—and may or may not be severe enough to require a U.S. humanitarian response. Long-term changes in regional climate are characteristically slower and more lasting, and include expanding or

shifting deserts, changes in average annual temperature or rainfall, and increases in seasonal flooding. The effects of such changes play out through the economic, social, political, and military variables.

SPECIAL CASES

Two specific physical environment conditions bring together the interplay of natural resources and climate change, namely access to fresh water and the opening of the Arctic Ocean. Changing weather patterns will cause a decrease in available water in some regions, leading to a loss of arable land, population movement, increased social and political conflict, and potential military clashes. For example, Turkey's Southeastern Anatolia Project centered on dam construction and increased irrigation of Turkish farmland. The project focused on the Tigris and Euphrates Rivers as the main sources of water, leading to reduced levels of fresh water flowing to Iraq and causing major tension between the two countries.[58]

Reduced levels of ice in the Arctic Ocean have opened up northern waters to a host of possible activities, two of which are natural resource exploration and maritime commerce. As much as 22% of the world's undiscovered oil and natural gas may lie in the Arctic, and use of the Northeast Passage for shipping goods between Asia and Europe promises significant time and cost savings over the current route through the Suez Canal and the Strait of Malacca.[59] Greater activity in the area may lead to political conflict over international borders, as well as possible militarization of the region by bordering countries.

TIME CONDITION

CULTURAL PERCEPTION OF TIME

Political and military decision-makers need to understand that perceptions of time are not universal, but vary depending on the country, culture, or government under consideration. Western cultures tend to have a view of time that is concrete and short-term, whereas Eastern cultures are more likely to focus on the long term and make decisions accordingly. Recognizing the manner in which time is viewed by a particular group of people is necessary to understand its actions toward, and reactions to, other actors in a given operational environment. If one party is working from a five-year plan and its opponent is working from a twenty-year plan, the first party will find itself at a distinct disadvantage. If the opponent sees time in terms of centuries, then the first has already lost. Unless the first party achieves total control through either annihilation or conquest and assimilation, its opponent will simply wait until the opportune time—be that ten, fifty, or two hundred years later—and then reassert itself. Successful interactions across political, military, economic, and social variables require a thorough understanding of all parties' perceptions of time in order to effect lasting change.

IMPLICATIONS OF THE CONDITIONS

The current and future strategic environment will be—as the above conditions reflect—characterized by multiple actors, adaptive threats, chaotic conditions, and advanced-technology-enabled actors seeking to dominate the information environment. The Army must be operationally adaptive to defeat these complex challenges and adversaries operating within this environment.

Over the course of the forecast period, the Army will continue to deploy to a multitude of distinct OEs, and concurrent decisive action operations will be the norm within these environments. Training for sequential operations with clearly defined phases will fail to prepare forces for the realities of an OE. Conflict, post-conflict/failed state, humanitarian, disaster relief, and support and reconstruction operations will occur simultaneously. Such operations will require better coordination/integration with a range of civilian organizations, both domestic and international. U.S. forces will be required to interact with and to protect NGOs, PVOs, and humanitarian organizations more than ever before.

Many of the longer-term implications of these conditions are murky. Depending on how they play out over the next sixteen years, a multitude of alternative security futures are possible (potentially ranging from some variant of the status quo, to a more violent world, to a less brutal future marked by greater cooperation and more effective international institutions). Yet clearly, they also suggest that armed conflicts and crises will continue to occur. These conflicts, moreover, will primarily:

- Require simultaneous operations of varying kinds (combat and reconstruction) vs. sequential, phased operations
- Be identity- (ethnic, religious) and/or deprivation-based
- Occasionally rise to the level of genocide and/or mass atrocity
- Be asymmetric and irregular rather than symmetric (involving at times states but also various types of non-state actors, e.g. terrorist groups, criminal organizations, guerrillas, etc.)
- Occur increasingly in complex terrain to mitigate perceived technological advantages
- Require better cultural understanding
- Require all elements of national power to achieve success

OE variable conditions across the SE portend future events such as new failing states, the rise of new political and military actors, the possibility of terror attacks, persistent cyber and space events, higher potential for humanitarian disasters, continuing WMD proliferation, and demographic challenges potentially triggering conflict across the current and future strategic environment.

The interaction of the OE variables depicted in the previous paragraphs describes a world that is increasingly interconnected but more fractious. The ubiquitous spread of information through technological advances, both true and false information, seems to be failing to empower understanding and instead is stimulating friction. Economic woes and demographic indicators point to decreasing influence of the traditional world powers in bending the course of world events to suit their needs. Rising influence of non-state organizations and nations with demographics and conditions favoring economic solvency are gaining power in shaping the world to accommodate their desires. Although not a popular prediction over the next 20 years, the former “world powers” may be relegated to second chair, including the United States. The implications of this are profound and at this point in no way certain. The trajectory of the OE variables indicates that course, but there are many national choices yet to be made between now and 2028. Those choices will set the stage for the range of missions the U.S. Army must accomplish in the conditions described.

POTENTIALLY CONTENTIOUS OEs AND RELATED MISSIONS

Geographical areas where variable conditions converge may point to areas of potential friction and possible conflict. If such areas also hold U.S. national interests, then such friction can lead to U.S. military action. The following discussion will highlight a sampling of such areas. This discussion is not all

inclusive, nor is it an attempt to predict the next location for U.S. Army actions. It is not a list of upcoming adversaries of the U.S. Instead, it is a discussion to inform Army leaders and Soldiers of types of potential flashpoints—based on converging conditions and U.S. national interests—they are likely to encounter over the course of the forecast period. Whether the U.S. Army conducts missions in one or more of the following OEs will be the result of political decisions based on criteria not within the scope of discussion of this estimate. Focusing on OEs likely to see increasing tension or conflict, however, can help us understand the types of environments, conditions, missions, and adversaries we might face. The OEs of Iran, China-Taiwan, Yemen, North Korea, Pakistan, and Nigeria will be presented to highlight types of possible environments.[60]

IRAN

The converging variable conditions manifesting in Iran include WMD proliferation, domestic political problems, a stalling economy, political elite infighting, and ICT empowerment of political opposition groups. Such conditions not only sow the seeds of budding internal discord, but also potentially germinate regional and global actions counter to U.S. national interests. The state sits on a major strategic chokepoint that it has threatened to close, is pursuing a nuclear weapons program, and is a confirmed supporter of terrorism, all of which challenge U.S. national interests in the region. Iran is regionally aggressive, and is openly hostile to the U.S. A 2012 DNI statement concludes that "Iran's intelligence operations against the United States, including cyber capabilities, have dramatically increased in recent years in depth and complexity." The DNI concludes his statement with the assessment that Iran will remain a top threat to the United States in the coming years.[61] Possible missions related to this OE include counter access-denial operations to open the Strait of Hormuz or counter-proliferation missions.

Iran would most likely present a highly adaptive threat, using both high- and low-tech threat capabilities. Regular, irregular, and criminal elements would combine to counter U.S. forces and employ anti-access strategies. Iran would use its large, conventional force to employ advanced missiles, air defense, rockets, and naval assets. Its irregular force would focus on clandestine and covert operations with proxies and sleeper cells prepared to act. Iran would also conduct well-organized and well-executed information warfare activities against the U.S. Electronic warfare and computer warfare attacks would be significant. Iran may also conduct terrorist operations against the U.S. homeland or against targets in state friendly to the U.S., including threatening to use long-range surface-to-surface missiles.

CHINA

Converging variable conditions directly impacting China include changes in the international distribution of power as it begins to rise in economic and military stature, proliferation of ICT, and emerging and abundant military technologies. Further, China clearly understands the importance of the global commons and will seek to maximize its position in the cyber and space commons, potentially challenging U.S. national interests. Over the course of the last decade, China has pursued a robust military modernization program. Gathering lessons learned by watching the U.S. operate in DESERT STORM and the Balkans, China "responded by investing in shorthand medium-range ballistic missiles, modern naval platforms, improved air and air defense systems, counterspace capabilities, and intelligence, surveillance, and reconnaissance (ISR) to support over-the-horizon military operations."[62] While unlikely to challenge the U.S. with direct military confrontation, China does pose a regional challenge of ownership of territory in the South China Sea (Spratly Islands), and presents a potential challenge to the strategic chokepoint of the Strait of Malacca, both of which counter U.S. national interests in the region.

Some believe that the U.S. would be drawn into action if China launched operations against the Spratly Islands or if support to regional allies (e.g. the Philippines) became necessary.[63] Although at first glance this appears to be primarily a Navy and Air Force problem set, there are many ways the Army might be involved, from theater missile defense to "shaping" the theater.

YEMEN

An excellent example of shortfalls in state governance resulting in a failing state is Yemen. Demographic challenges of young, disenfranchised males help set the conditions for instability and violence. Recent youth protests helped spark a movement for political reform in Yemen. Poor state governance has allowed a safe haven for al-Qaeda in the Arabian Peninsula (AQAP) and associated groups in Yemen and across the globe in similar environments. The Intelligence Community concluded in 2012 that AQAP "will remain committed to the group's ideology, and in terms of threats to U.S. interests will surpass the remnants of core al-Qa`ida [sic] in Pakistan."[64] Potential challenges to the U.S. include issues related to the closure of the Bab-el Mandeb Strait, to exports of hydrocarbons to the U.S., to a direct threat posed by terrorist groups with freedom of maneuver across Yemen. The most likely missions related to this OE would be for counterterrorism or support and stability operations.

NORTH KOREA

The converging conditions manifesting in North Korea include WMD proliferation and shortfalls in state governance. A recent DNI testimony stressed the severity of the threat from North Korea and its challenge to the U.S. national interest of nonproliferation of WMDs. The DNI states:

> North Korea's nuclear weapons and missile programs pose a serious threat to the security environment in East Asia. Its export of ballistic missiles and associated materials to several countries, including Iran and Syria, and its assistance to Syria—now ended—in the construction of a nuclear reactor (destroyed in 2007) illustrate the reach of the North's proliferation activities. Despite the October 2007 Six-Party agreement—in which North Korea reaffirmed its commitment not to transfer nuclear materials, technology, or know-how—we remain alert to the possibility that North Korea might again export nuclear technology.[65]

Openly hostile to both its southern neighbor and the U.S., multiple possible mission types related to the OE include a response to an invasion of South Korea, counterproliferation missions and activities, and stabilization and stability efforts after a collapse of the North Korean regime. Much like Iran, North Korea would present the U.S. with the challenges of countering a hybrid threat. It would utilize both its conventional forces and irregular elements to conduct hit-and-run attacks and terrorist acts. SPF would be deployed and several proxy actors would be used to assist in terrorist activities possibly targeting the U.S. Homeland. Access denial strategies and operations would be used. North Korea would also apply sophisticated information warfare activities against U.S. forces both in the region and at home.

PAKISTAN

WMD proliferation, direct threat to the Homeland, terrorist organizations, and regional tensions with India are examples of the key converging variable condition for this OE. Shortfalls in state governance in Pakistan have produced safe havens for various insurgent and terrorist organizations. For example, al-

Qaeda is relying on "ideological and operational alliances with Pakistani militant factions to accomplish its goals within Pakistan and to conduct transnational attacks" resulting in a direct challenge to U.S. national interests.[66] Poor economic performance in Pakistan is also fostering tensions and conditions that extremist groups can use to their advantage. This, coupled with a potentially vulnerable stockpile of nuclear weapons and terrorist groups dedicated to harming the U.S., makes this OE a potential flashpoint. Possible scenarios requiring U.S. action include an internal coup causing regime collapse and "loose nukes," stabilization efforts, and counterproliferation and counterterrorist actions.

NIGERIA

Converging variable conditions for Nigeria include persistent youth bulge, income inequality, shortfalls in state governance, and competition over natural resources. According to a recent DNI testimony, "Nigeria is critical to U.S. interests—it is Africa's most populous nation and the source of 8 percent of total U.S. oil imports."[67] A young population has severely strained economic development in Nigeria. Shortfalls in governance have lead to regional tensions, violence, and the rise of terrorist groups such as Boko Haram. Evidence suggests that Boko Haram and al-Qaeda in the Islamic Maghreb (AQIM) are strengthening ties and coordination with stated interests in hitting Western targets in the area.[68] Stabilizing the government to counter an expansion of transnational terrorism in the region would be a possible reason for U.S. actions in this OE.

CONCLUSION

All the conditions discussed have the potential to create friction and tensions across the highlighted OEs. While it is impossible to determine when or if a condition will actually trigger a conflict, it is possible to study such conditions to better understand the environment and the Army's potential actions in such an environment. Adversaries are certainly aware of and studying the SE conditions to determine their best course of action. They will seek both purpose and opportunity in the conditions of the current and future strategic environment. The commonalities of the OEs and threats represented in the foregoing discussion include the potential use of proxies, possession of WMD, and the possible use of a hybrid approach to challenge regional contenders while remaining resilient to the threat of a U.S. intervention. In the next section, potential adversary strategies and likely methods of operation will be described.

ADVERSARIES IN THE STRATEGIC ENVIRONMENT

The character of emergent threats will depend on how the United States focuses its resources. Paradoxically no matter what it emphasizes, the military threats the United States is—or will be—most capable of defeating are the ones it is least likely to face, since potential adversaries will be deterred and seek other ways of confrontation.[69]

Horowitz and Shalmon, "The Future of War and American Military Strategy," 2009

Reviewing the key conditions of the strategic environment is fundamental to develop an understanding of potential adversarial strategies. **Adversaries take the means provided to them by the strategic environment and use those means in conceptually enduring ways to achieve their ends.** That is adaptive strategy.

ADAPTATION

Success goes to those who master the skills necessary to act, react, and adapt with speed and creativity. Enemies learn quickly, and can change unconstrained by rules or bureaucracy. Because these changes occur so quickly and often incompletely, they are difficult to counter. Adversaries will continue to be adaptive in terms of using all available sources of power at their disposal. Adaptation, broadly defined, is the ability to adjust behaviors based on learning, and is closely linked to one's environment and its variable conditions.

Adversaries can approach adaptation from two perspectives: natural and directed. Natural adaptation occurs as an actor (state or non-state) acquires or refines its ability to apply political, economic, military, or informational elements of power. Natural adaptation may be advanced through the acquisition of technology or key capabilities, resources (financial and materiel), effective organization, and effective use of the information environment or even key regional or global alliances. Directed adaptation is based specifically on lessons learned to counter U.S. power and influence. Such counters to U.S. actions will be ever-changing and likely conducted by an adaptive threat. Adversaries will offer a mix of capabilities along the range of military operations, and will learn from U.S. operations what works and what needs refinement. They will be whatever the U.S. is not. Adversaries will attempt to sidestep the U.S.' preferred way of war.

ENDS—THE GOALS OF ADAPTIVE STRATEGY

The ends that actors in the SE strive to achieve are based on the timeless motivations of:

- Wealth
- Resources
- Political authority
- Influence
- Sovereignty
- Identity
- Legitimacy[70]

These pursuits are the motivations of any actor in the strategic environment. It is when these ends are at odds with our interests or, in the view of the actor, require harm to U.S. people or property, that the actor becomes an adversary. Entities pursue those ends by cooperation, competition, or conflict. The choice of the means to pursue those ends sets the conditions for the U.S. response. The choice of the response is a national policy issue and not in the purview of the Armed Forces to decide. As a result, the decision to employ the military tool of national power will be driven by U.S. elected officials' tolerance level for world conditions that are not congruent with U.S. national interests. Understanding the motivational impetus of the ends described above provides insight on what types of military operations may be helpful in assisting or thwarting other nations to achieve goals that support U.S. international security goals. Thus the Army must prepare for the widest range of employment that is affordable and retain the ability to rapidly adapt to the actual needs of the moment. "Getting it right" is simply not possible with the vagaries of the SE and shifting U.S. national interests. The best course is to train, prepare, and equip to high levels of task proficiency that minimize the degree of adaption required.

Adversaries are those human actors who employ violence and fear to oppose our interests, harm our people, and attack our will. To oppose the U.S. is a dangerous undertaking. We are strong, resolved, well-equipped, and possessed of the finest fighting force in the world. Adversarial strategies are designed to increase costs beyond political benefit, as opposed to trying to defeat U.S. military might. Therefore, adversaries are likely to—and have long shown a marked predilection to—exploit any and all ways and means available to them in order to pursue courses of action that make the cost of the mission too high to pay.

WAYS—THE METHODS OF ADAPTIVE STRATEGY

There are a number of ways in which adversaries will act. These ways are the conceptually enduring methods that bring about desired ends. While a wide array of methods is available to our adversaries across the SE, the one method currently perceived to be unavailable to them is to defeat us in a conventional battle. Instead, any aggregated violence will be designed not to defeat us on the battlefield, but to cause enough damage, both real and perceived, in both the physical and informational spheres, that we cannot sustain our will through to mission accomplishment. Such a strategy requires two major lines of effort: attacks that cause this damage, and actions that extend the time to mission accomplishment so it does not occur before sufficient damage is caused. Likely adversarial courses of action are the nexus of the need to move along these two lines of effort and the means available in the near-term SE. These methods of adaptive strategy are **conduct preclusion**, **control tempo, attack will, neutralize technological overmatch, change the nature of conflict, allow no sanctuary,** and **employ shielding**.

Conduct Preclusion

Anti-access is defined as those actions and capabilities, usually long-range, designed to prevent an adversary from entering an operational area. Area denial includes actions and capabilities, usually of shorter range, that are not designed to keep an adversary out, but rather to limit its freedom of action within the operational area. Preclusion refers to the combination of anti-access and area denial methods, and seeks to influence an extraregional enemy's ability to introduce forces into the theater and sustain combat power.

Adversaries use preclusion to selectively deny, delay, and disrupt entry of extraregional forces into the region (anti-access), and to compel extraregional forces to keep their operating bases beyond continuous operational reach (area denial). This is the easiest manner of preventing the accumulation of enemy combat power in the region and thus defeating or denying victory to a technologically-superior enemy.

Capable adversaries will attempt a comprehensive anti-access strategy that aims to prevent the Army from getting involved in conflicts in the first place. Potential adversaries have noted the repositioning of Army units from overseas bases to the continental U.S., along with ongoing U.S. investments in strategic mobility and joint forcible entry capabilities. As a result, the first element of their strategy will be to deter the U.S. government from making the political decision to initiate an overseas deployment. For example, an adversary might exploit and manipulate international media to paint foreign intervention in a poor light, decrease U.S. domestic and international resolve, and affect the force mix and rules of engagement (ROE) of potentially deploying extraregional forces. It might also seek to prevent potential U.S. allies, coalition partners, and NGOs from offering military, logistical, and political support, basing, and overflight rights to U.S. forces via diplomacy, economic, or political connections; information

campaigns; and/or hostile actions. Basing rights are of particular import: while it is possible for the U.S. to conduct an air and missile campaign without forward basing, a campaign using exclusively strategic—rather than a mix of strategic and operational reach—would be greatly diminished in its effectiveness and tempo. These effects, when combined, may prove sufficient to deter the U.S. from deploying forces to the region.

Should this fail, the next step taken by the adversary will be to limit the accumulation of applicable U.S. combat power to a level and location(s) that do not threaten the accomplishment of its goals through interdicting ingress routes, denying bases, and undermining international support. The adversary will use any means at its disposal to strike U.S. forces along routes to the region, at transfer points en route, at aerial and sea ports of embarkation (APOEs and SPOEs), and even at troop home stations. If unsuccessful, it will attempt to limit or interrupt our deployment through actions against aerial and sea ports of debarkation (APODs and SPODs) in the region.[71] An adversary will also try to disrupt and isolate U.S. forces that are in the region or coming into it, so that it can destroy them piecemeal. It will threaten and attack forward bases and supplies via operational fires and recruitment of host-nation individuals to conduct terrorist activities against U.S. logistics systems, including contamination of fuel and water and theft of supplies during transit. This raises the risks to U.S. forces, hinders operational phasing, and diminishes host nation support for protection of U.S. lines of communication (LOCs). The adversary might also attack population and economic centers for the intimidation effect.

Potential adversaries may now or in the near future have access to multiple weapons platforms to assist in conducting preclusion. Medium- and long-range, precision strike munitions—including the Iranian Fatah-ll0, the Chinese DH-10 land attack cruise missile, the YJ-83 cruise missile, the Russian AS-18 KAZOO air-to-surface missile, Club K missile, and SS-N-27 cruise missile—can provide the ability to target deploying forces, strategic mobility assets, forward operating bases, staging areas, and LOCs. Proliferation of long-range air defense systems such as the Russian SA-20 and the more advanced SA-21—with an estimated engagement range of 250 miles—could present significant challenges as adversaries attempt to exclude or limit U.S. access to areas where the Army is forced to deploy by air. Other adversarial platforms may include unmanned aerial vehicles (UAVs), such as the Chinese ASN 207 that employs a GPS jammer, space-based sensors, anti-satellite and EW capabilities, sea mines, Akula-II and Kilo class submarines, WMD, SPF, and cyber capabilities. In addition, readily available commercial imagery and omnipresent media sources provide early warning of U.S. actions that will become increasingly difficult to elude.[72]

Chinese Unmanned Aerial Vehicle ASN-207

TRADOC Intelligence Support Activity-Threats, Worldwide Equipment Guide, December 2011, 4-11

Control Tempo

An adversary will employ rapid tempo in an attempt to conclude regional operations before an extra-regional force can be introduced. It will also use rapid tempo to set conditions for preclusion operations before the extraregional force can establish a foothold in the region. Once it has done that, it needs to be able to control the tempo—to ratchet it up or down—as is advantageous to its own operational or tactical plans.

During the initial phases of an extraregional force's entry into the region, an adversary may employ a high operational tempo to take advantage of the weaknesses inherent in enemy power projection. (Lightly equipped forces are usually the first to enter the region.) This may take the form of attack against enemy early-entry forces, linked with diplomatic, economic, and informational efforts to terminate the conflict quickly before the main force can be brought to bear.

VIGNETTE

The young man nervously played with the switch in his hand; he wondered what he would feel when he killed the Americans. His leader had told him that they were barbarians and no better than animals, but after working around them for weeks he had seen that they were much like him. It did make him feel better that his target was a military storage site where the United States had stockpiled weapons to be used on his people when they came to steal the resources they badly needed to escape from poverty. As the soldier locked the gate to the warehouse, the young man flipped the switch and was rewarded with a huge explosion that engulfed the warehouse and the soldier. As huge plumes of black smoke billowed skyward, his only thought was, "I have struck a blow for the freedom of my people from the Americans." Hours later, a video of the attack was on the Internet emphasizing that a U.S. military target was struck as a prelude to other attacks on U.S. military interests in the region. The message to the American people was clear in the posting: "This is a local affair, if you remove your forces from the region they will not come to harm."

If an adversary cannot end the conflict quickly, it will likely take steps to slow the tempo and prolong the conflict. Adversaries realize the importance of coalitions for their self-preservation. They have observed successes and failures of U.S.-led coalitions. If timely victory does not occur, U.S. public backing begins to wane and ultimately influences political decisions. Therefore, threats will seek protraction of conflict to keep U.S. forces engaged to weaken resolve and drain military and economic resources. The preferred tactics during this period would be those that avoid decisive combat with superior forces. These activities may not be linked to maneuver or ground objectives, but may instead be intended to inflict mass casualties or destroy flagship systems, both of which will reduce the U.S.' will to continue the fight.

Attack Will

Victory does not always go to the best-trained, best-equipped, and most technologically advanced force. The collective will of a state or non-state organization encompasses a unification of values, morals, and effort among its leadership, its forces, and its individual members. Through this unification, all parties are willing to individually sacrifice for the achievement of the unified goal. The interaction of military actions and other instruments of power, conditioned by collective will, serve to further define and limit the achievable objectives of a conflict for all parties involved. These factors can also determine the duration of a conflict and conditions for its termination.

Adversaries will try to inflict highly visible and embarrassing losses on U.S. and partner forces to weaken domestic resolve and national will to sustain the deployment or conflict. Modern wealthy nations have shown an apparent lack of commitment over time. They have also demonstrated sensitivity to domestic and world opinion in relation to conflict and seemingly needless casualties. Potential adversaries believe they can have a comparative advantage against superior forces because of the collective psyche and will of their own forces and leadership to endure hardship or casualties, while we may not be willing to do the same.

Potential adversaries also have the advantage of disproportionate interests. The extraregional force may have limited objectives and only casual interest in the conflict, while our adversary will approach it from the perspective of total war and the threat to its aspirations or even survival. Our adversaries will be willing to commit all means necessary, for as long as necessary, to achieve strategic goals. They will try to influence public opinion in the Homeland to the effect that the goal of intervention is not worth the cost. They will use violence, intimidation, and coercion against U.S. supporters and partners.

Adversaries will exploit the lack of cultural understanding inherent in U.S. forces. They will conduct information campaigns dedicated to portray the U.S. culture as an institution bent on political and economic global domination in the name of "Western" democracy. Information campaigns will paint U.S. military forces as brutal and unconstrained by the accepted rules of warfare. They will also exploit instances of U.S. missteps due to cultural differences. The fabrication and exaggeration of U.S. cultural shortcomings are designed to alienate the populace from supporting the U.S. and aid in recruiting people to support the threat.

Neutralize Technological Overmatch

Against an extraregional force, adversarial forces will forego massed formations, patterned echelonment, and linear operations that would present easy targets. They will hide and disperse forces in areas of sanctuary that limit the ability to apply our full range of technological capabilities. However, an adversary will attempt to retain the ability to rapidly mass forces and fires from those dispersed locations for decisive combat at the time and place of its own choosing.

Adversaries will attempt to use the physical environment and natural conditions to neutralize or offset the technological advantages of modern reconnaissance, surveillance, and intelligence operations. Forces will be practiced in operating in adverse weather, limited visibility, rugged terrain, and urban environments that shield them from the effects of our high-technology weapons and deny us the full benefits of advanced mission control and related systems.

Adversaries will also look to use our robust array of reconnaissance, surveillance, and intelligence systems against us. Large numbers of sensors can overwhelm a unit's ability to receive, process, and analyze raw intelligence data and provide timely and accurate intelligence analysis. Adversaries seek to add to this saturation problem by using deception to flood sensors with masses of conflicting information. Conflicting data from different sensors at different levels (such as satellite imagery conflicting with data from UAVs) can significantly degrade situational awareness.

The destruction of high-visibility or unique systems employed by our forces offers exponential value in terms of adversarial goals. These actions are not always linked to military objectives; they also maximize effects in the information and psychological arenas. High-visibility systems that could be identified for destruction might include stealth aircraft, attack helicopters, counterbattery artillery radars, aerial

surveillance platforms, or rocket launcher systems. Losses among these premier systems may undermine U.S. morale, degrade operational capability, and inhibit employment of these weapons systems.

If available, precision munitions can degrade or eliminate high-technology weaponry. Camouflage, deception, decoy, or mockup systems can degrade the effects of sensor systems. Also, adversaries can employ low-cost GPS jammers to disrupt precision munitions targeting, sensor-to-shooter links, and navigation. Lethal weapon systems such as advanced missiles, advanced air defense, sensor and EW weapons, UAVs, precision-guided artillery, and directed energy weapons will all be used to degrade U.S. capabilities. Another way to operate on the margins of U.S. technology is to maneuver during periods of reduced exposure, those periods identified by a detailed study of our capabilities and patterns.

Basic low-tech counters to U.S. capabilities provide the threat with near-peer or even niche advantages. Counter-collection capabilities such as counter-signal GPS jammers, radar scattering, landlines, couriers, and language itself create effective counters to U.S. technical signals intelligence collection and will increase the importance of U.S. human intelligence (HUMINT) capabilities. Threat actors may purchase military and commercial technology that can easily be modified for collection or analytical purposes. Examples include UAVs with multiple sensors and weapon packages, commercially-available satellite imagery, image intensifiers, first-generation forward-looking infrared (FLIR), computer geographic information systems, and EW technologies.

Rocket-propelled grenades (RPG) and man-portable anti-tank (AT) missiles are easily concealed, withstand detection from anti-radar detection systems, can be cached and carried in large numbers, and make an attractive low-cost alternative for the threat in lieu of conventional surface-to-air missiles.
Adversaries may have access to commercial products to support precision targeting and intelligence analysis. This proliferation of advanced technologies permits organizations to achieve a situational awareness of deployments and force dispositions formerly reserved for selected militaries. Intelligence can also be obtained through greater use of HUMINT assets that gain intelligence through noncombatants or local workers contracted for base operation purposes. Similarly, technologies such as cellular telephones are becoming more reliable and inexpensive. It is becoming harder to discriminate between the use of such systems by civilian and military or paramilitary actors.

Change the Nature of Conflict

Adversaries will try to change the nature of conflict to exploit the differences between friendly and enemy capabilities. To do this, they can take advantage of the opportunity afforded by phased deployment of an extraregional force. For example, following an initial period of regionally-focused conventional operations, an adversary could change its operations to focus on preserving combat power and exploiting enemy ROE. This change of operations will present the fewest targets possible to the rapidly growing combat power of the intervening coalition. It is possible that coalition power-projection forces, optimized for a certain type of maneuver warfare, would be ill suited to continue operations. An example would be a heavy-based projection force confronted with combat in complex terrain.

Any adversary will likely have different criteria for victory than the extraregional force—a stalemate may be good enough. Similarly, its definition of victory may not require a convincing military performance. For example, it may call for inflicting numerous casualties to the enemy. The adversary's perception of victory may equate to its survival.

Allow No Sanctuary

Our adversaries seek to deny our forces safe haven during every phase of a deployment and as long as they are in the region. The resultant drain on manpower and resources to provide adequate force-protection measures can reduce our strategic, operational, and tactical means to conduct war and erode our national will to sustain conflict. Along with dispersion, decoys, and deception, adversaries will use urban areas and other complex terrain as sanctuary from the effects of our forces. Meanwhile, their intent is to deny U.S. forces the use of such terrain. This forces us to operate in areas where adversary fires and strikes can be more effective. Terror tactics are one of the effective means to deny sanctuary. Terrorism has a purpose that goes well beyond the act itself: the goal is to generate fear. Adversary SPF can also use terror tactics and are well equipped, armed, and motivated for such missions.

Adversaries are prepared to attack our forces anywhere across the strategic environment, at overseas bases, at home stations, and even in military communities. They will attack our airfields, seaports, transportation infrastructures, and LOCs. These attacks feature coordinated operations by all available forces, using not just terror tactics, but possibly long-range missiles and WMD. Targets include not only military forces, but also contractors and private firms involved in transporting troops and materiel into the region. The goal is to present us with a nonlinear, simultaneous operational environment. Striking such targets will not only deny sanctuary, but also weakens national will.

Employ Shielding

Adversaries will use any method necessary to protect key elements of combat power from destruction by an extraregional force, particularly by air and missile forces. This protection may come from use of any or all of the following:

- Complex terrain
- Noncombatants
- Risk of unacceptable collateral damage
- Countermeasure systems
- Dispersion
- Fortifications
- Information campaigns

Adversaries will employ a wide variety of counter-precision techniques that include camouflage, concealment, and deception; GPS jamming; terminal defenses; forcing close-in fights; advanced aircraft; and extended-range precision munitions. Adversaries will seek shielding by exploiting civilian populations and cultural sites to hide weapons systems and shape the battlefield. They will reduce U.S. air defense system reaction times with technology such as penetration aids on missiles, low observable aircraft, and jamming. Adversaries will increasingly employ hardened and buried facilities and multispectral decoys of key, operational-level targets such as short-range ballistic missiles (SRBMs) and surface-to-air missiles (SAMs). Many adversaries have invested in short- and medium-range missile systems, such as the Russian Smerch and Chinese PHL-03, capable of counterfires with ranges out to 150km. Improved air defense systems including counter-TBM [tactical ballistic missile] capabilities will provide protection to these advanced fires capabilities.

MEANS—THE HUMAN AND PHYSICAL CAPITAL OF ADAPTIVE STRATEGY

While, conceptually, adaptive strategy is the use of available means present in the strategic environment to achieve goals, these activities occur in specific OEs. Inside these OEs, the means vary widely. The components that exist from which to build an IED in South Asia are not the same as those available in Central Asia or Central America. The means are what change from year to year and OE to OE. However, given our analysis of the SE, we know the ways adversaries might use to accomplish their goals and the means available to them. This allows us to draw basic conclusions about the threats that will exist in the strategic environment during this period.

The tactical manifestation of an actor using adaptive strategy that will be encountered by our forces is a threat employing hybrid strategies. The hybrid is the natural result of a political entity arming and organizing to coerce or deter other entities in the region. As a result of arming in this fashion and pursuing interests, however, there is the fear of intervention by the U.S. and the resultant existential threat. Such threats provide the operational and tactical space for moving rapidly from conventional operations against a neighbor to decentralized irregular operations against an intervention. The combinations of forces also create opportunities to exploit discovered vulnerabilities against any adversary. The enemy of our future is a highly-resolved fighter that mixes the characteristics of those who fight outside the law with those who fight using deadly weapons in a reasoned manner. This fighter will steal, murder, conduct assaults, snipe, bribe, prepare defenses, and execute cyber attacks. He will equally be able to choose a rocket launcher firing position as to shoot a mayor from a moving car. He will, possibly in the same day, dress in a host-nation uniform, no uniform, or one of our uniforms.

HYBRID THREAT

Generally speaking, a threat that employs a hybrid strategy or strategies can be defined as a hybrid threat. A hybrid threat is the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects (ADRP 3-0). Hybrid threats can combine state-based, regular military forces with attributes usually associated with irregular forces and criminal organizations. Regular forces are governed by international law, military tradition, and custom. Irregular forces and criminal elements are unregulated and as a result act with no restrictions on violence or targets for violence. To be a hybrid, these forces cooperate in the context of pursing their own internal objectives. For example, criminal elements may steal parts for a profit while at the same time compromising the readiness of a U.S. force's combat systems. Militia forces may defend their town or village with exceptional vigor as part of a complex defensive network. Some hybrid threats will be a result of a state (or states) sponsoring a non-state actor.

Hybrid Threat Components of Adaptive Strategy

The key components of a hybrid threat are two or more of the following:

- Military forces
- Nation-state paramilitary forces (such as internal security forces, police, or border guards)
- Insurgent organizations (movements that primarily rely on subversion and violence to change the status quo)
- Guerrilla units (irregular indigenous forces operating in occupied territory)
- Criminal organizations (such as gangs, drug cartels, or hackers)

Hybrid threats will use a strategic capability that forces any intervening power to adjust operations (WMD, SPF, etc). This capability may be undeveloped or only partially developed. This will not affect the transition between regular and irregular operations, and the threat of the capability still provides a tool for manipulating the intervening force (e.g. Iraq's WMD capability circa 2001). All components of a hybrid threat will use cyber operations to either degrade U.S. mission command capabilities or to conduct perception management campaigns.

Hybrid threats have the ability to combine and transition between regular, irregular, and criminal forces and operations and to conduct simultaneous combinations of various types of activities that will change and adapt over time. Such varied forces and capabilities enable hybrid threats to capitalize on perceived U.S. vulnerabilities.

Examples of Hybrid Threats

Although the term hybrid threat has emerged only recently, such combinations are not new. History is full of examples:

- 1754 to 1763: Regular British and French forces fought each other amidst irregular Colonialists fighting for the British and American Indians fighting for both sides.
- 1814: The Peninsula War ended after the combination of regular and irregular allied forces from Britain, Portugal, and Spain prevented France from controlling the Iberian Peninsula.
- 1954 to 1976: The Viet Cong and the People's Army of Vietnam combined irregular and regular forces in fighting the French and U.S. forces. Viet Cong would organize into conventional and irregular units.
- 2008: Russian-Georgian conflict in the breakaway regions of Abkhazia and South Ossetia, in which both sides used combinations of regular forces, irregular forces, and criminal elements.

Iran and North Korea would most likely present a hybrid threat. Regular, irregular, and criminal elements would be combined to challenge U.S. forces. Iran would utilize its large conventional force to employ advanced missile, air defense, rockets, and naval assets. Its irregular force would focus on clandestine and covert operations with proxies and sleeper cells prepared to act. North Korea would likewise use its conventional forces and irregular elements. Irregular and criminal forces would conduct hit-and-run attacks and terrorist acts. SPF would be deployed and several proxy actors (Hezbollah, etc.) would be tapped to assist in terrorist activities possibly targeting the U.S. Homeland. Access denial strategies and operations would be implemented as well as the employment of ballistic missiles and mining of sea lanes. Both states would also use sophisticated information warfare activities, SPF, and perhaps even criminal elements against the U.S. Both states are examples of a hybrid threat prepared to employ varying combinations of forces and capabilities against the U.S.

Potential Evolution of Threats through 2028

As various actors observe the effectiveness of threats in recent conflicts, they are more likely to unite their resources and capabilities into a similarly successful type of threat. Although states and various non-state actors may continue to pursue their own particular goals and objectives, they are apt to seek

out alliances or at least loose affiliations with other actors in order to exploit the synergy of their collective capabilities to achieve mutual benefit.

Threats may employ sophisticated weapons in specific niches to attack perceived U.S. weaknesses. They may threaten to employ WMD, targeting concentrations of U.S. forces and urban centers. When projecting power into a region, Army leaders may find themselves without one or more of the advantages they normally have. U.S. forces encountering new and unanticipated enemy capabilities have to rapidly adapt while engaging in operations. Enemies may organize themselves for highly decentralized operations over a protracted period. They will work to secure the active support of other regional powers and supporters. Enemies seek to create disruptive effects oriented toward U.S. activities within the Homeland through cyber attacks and terrorism.

TACTICAL DESIGNS

At the tactical level, threats will employ four key designs that specifically adapt resources available in the strategic environment for use against the U.S. and its partners.

Exploit Regular/Irregular Synergy

Adversaries understand that the environment that would produce the most challenges to U.S. forces is one in which conventional military operations execute in concert with irregular warfare. Units that are well-trained and equipped for counterinsurgency (COIN) operations often do not retain the precise skills, equipment, and mindset for conventional combat and vice versa. In addition, there is a synergy to the simultaneous use of conventional and unconventional methods by both regular and irregular forces that is difficult to counter. Synergy will be achieved in one of two basic ways: by a threat state actor executing conventional operations that ensure the U.S. is also simultaneously presented with an irregular warfare environment; or by a threat non-state actor conducting irregular warfare that integrates conventional means and tactics into its operations.

Non-state threat actors will continue to seek and employ paramilitary capability. They will organize, train, and equip themselves as cohesive units. This training will continue to require sanctuary—training facilities and industrial partners, or covert/protected supply lines will be necessary for acquiring modern equipment.

Employ Range of Technologies

Adversaries will employ niche technologies at the tactical level that are just as sophisticated, and sometimes more so, than those possessed by the local U.S. unit and its partners. Tandem-warhead anti-tank guided missiles (ATGMs), sophisticated EW, communications and encryption devices, and modern air defense missiles are just some examples of the many types of systems in which threat actors can and will achieve parity or superiority in tactical actions. This is not to say that threat actors will not continue to employ improvised devices of many types. On the contrary, the trend will be for threat actors to employ modern niche technologies in a synergistic manner with improvised devices.

One of the most important areas in which threat actors will seek to operate in the future is in the acquisition and employment of sophisticated EW systems. Threat actors understand the continued reliance the U.S. places on communications, intelligence and surveillance, and visualization technologies. These technologies are vulnerable to disruption and exploitation by systems far easier to

obtain and simpler to master. The cycle of threat acquisition of EW technology will continue to operate inside the cycle of U.S. acquisition of major communications, intelligence and surveillance, and visualization systems.

The enemy's use of countermeasures (both traditional and nontraditional) will limit the U.S. military's ability to achieve overmatch against a determined enemy in restricted terrain. Forces will have to engage in close combat to find and defeat the enemy. In addition, future enemies will attempt to counter our most significant advantages in communications, surveillance, long-range precision fires, armor protection, and mobility. Tactical units will require a suite of adaptable combined arms capabilities and the ability to integrate joint effects.

Information Warfare as Key Weapon System

Adversarial tactical actions will be designed to achieve information warfare objectives rather than purely military ones. Causing U.S. casualties; exposing weaknesses in training, equipment, or resolve; and forcing redeployment will be paramount over such considerations as seizing or retaining terrain features or battlefield victory. Adversaries will attempt to deny and degrade U.S. mission command by constant cyber and EW attacks.

Employ Complex Battle Positions and Utilize Cultural Standoff Capabilities

Adversaries reduce exposure to stand-off fires and reconnaissance, surveillance, and intelligence by utilizing complex battle positions (CBPs) and cultural standoff. CBPs are locations designed to protect the occupants from detection and attack while denying their seizure and occupation by the enemy. They are not necessarily tied to an avenue of approach. CBPs protect forces while providing sanctuary from which to launch attacks. Camouflage, concealment, and deception measures are critical to the success of a CBP. These efforts and actions include, but are not limited to, underground facilities, complex/urban terrain, fortification, false and decoy positions, and information warfare support.

Cultural standoff is the act of using social aspects of the environment to provide protection and freedom to maneuver. Cultural standoff tactics, techniques, and procedures (TTP) employed by threat actors include integrating religious, medical, and other sensitive facilities into CPBs; employing human terrain for deception purposes; and exploiting a population using information warfare.

CONCLUSION

Adversarial challenges will require that the Army be prepared for a wide range of missions over the forecast period. Based on the conditions discussed above, Army missions could range from major combat operations to humanitarian and disaster relief operations. The leader development, training development, and capabilities and concepts development implications are significant and are addressed in **Chapter 3, Military Implications**, along with key implications based on conditions of the strategic environment presented in this chapter.

Chapter 3
Military Implications

INTRODUCTION

Conditions across the strategic environment indicate future conflict will not be confined to one simple category. It will range in scope from major conventional fights to humanitarian support and nation-building missions. Very capable adversaries will continue to challenge U.S. interests globally, while rising military powers, coupled with existing militaries, will work to advance their regional and global interests. The U.S. could potentially face a variety of missions and adversaries operating in a wide range of OEs. The Chief of Staff of the Army, General Raymond T. Odierno, captured this outlook in his statement from January 2012:

Our standing as the most dominant land force on the planet can never be up for debate. We must be able to operate across any operational environment, in a broad mission set, including regular and irregular warfare, stability operations, counterinsurgency, humanitarian assistance, and any other mission that is out there.[73]

Training and preparation against these changing conditions will drive adaptation and flexibility within the Army and ensure U.S. forces are prepared for any potential OE and any potential mission. The TRADOC focus areas discussed below will fall across the four domains of leader development, training development, capabilities development, and concepts development to varying degrees. Some implications are more important to one domain over another, but most apply to all of the domains in both impact and applications.

LEADER DEVELOPMENT

Army leaders will need to embrace the concept of complexity and fluidity and understand that they will have to operate in a decentralized manner and function with some level of uncertainty across the various OEs. The strategic environment and potential OEs require adaptive leaders who are intuitive, recognize changing patterns, and can solve problems through critical thinking and adaptive decision-making skills. Leaders will need to discern patterns and have broad perspective so that they can deal with the range of potential threats and military operations. Leaders and units must be taught continuous recognition and response skills.

Leaders must be **culturally aware and sensitive**. They must understand the human dimension of an OE and factor this dimension into all facets of leadership, decision-making, and training. Culture matters.

Leaders must be able to **understand the implications of the information environment**—from the human side of developing and controlling a narrative to the technical side of developing effective filtering and management strategies—so Soldiers do not become overwhelmed by the large volume of data. Knowledge management skills and advanced analytical skills (in an age of too much information vs. too little analytic competency) need to be continuously honed at all levels.

Leaders must be able to **master consequence management:** understand second- and third-order effects of actions or inaction and be willing to apply risk analysis to critical decisions. They must develop skills to lead adaptively and allow creativity and new approaches to emerge across the force. They must be willing to allow for more creative and free thinking from subordinates and to encourage and foster such an environment.

TRAINING DEVELOPMENT

Just as with leader development, the training environment—whether live, virtual, or constructive—must be imbued with the complexities of potential OEs. This includes the development of scenarios and drivers that contain conditions of the SE and adversarial strategies as part of their base design.

Training venues must reflect an **understanding of the influence of various cultures** and incorporate the increasing array of actors that will be present in any OE, from NGOs, PVOs, and PSOs to allied partners. Each actor has the potential of working side by side with the Army as it conducts operations. Each of these actors will bring its own culture, agenda, and operating procedures to the situation. U.S. forces working directly with such actors will need to be trained to deal with the unique requirements each will bring.

Training venues must continue the tradition of **providing an arena that allows free play**. Training events must contain adaptive, intelligent, and innovative opposing forces (OPFOR), organized and equipped in a flexible fashion that can replicate a mix of regular and hybrid threats capable of pushing units to failure in an effort to expose shortfalls. Adversarial portrayal must reflect current strategic environment realities while helping to identify potential future adversaries.

Training venues and events must **quickly adapt to new methods and mediums for training**. Distributed content and more, personally-tailored training methods will overtake the more traditional "schoolhouse" approach. Advanced ICT capabilities are and will continue to change how we educate the Army. Current and future Soldiers will demand that the Army keep pace with ICT developments for training. Advanced educational platforms and applications must be rapidly absorbed, and the content of training must be updated as quickly as possible to stay relevant and effective.

CAPABILITIES DEVELOPMENT

To provide Soldiers the capabilities they will need requires a much more **agile capabilities-development process**. It must anticipate the operational needs of commanders and incorporate the adaptability inherent in "off-the-shelf" technology to support the near future. At the same time, it must look deep enough into the future to anticipate the "fight after next."

Capabilities development must quickly and effectively incorporate technological advances, developments in strategic partner capacities, ICT advances, and science and engineering developments. The Army must develop a capabilities approach that allows for a quick and continuous absorption of scientific advances. Our adversaries are doing this now. Leaders and Soldiers must be trained to operate in such a technologically fast-paced environment and to understand how threat actors are responding to this environment.

CONCEPT DEVELOPMENT

As with other TRADOC core competencies, the strategic environment has implications for approaches to concept development. Accounting for the adaptive, transitioning adversaries described in this environment calls for concepts that are explored and validated through robust experimentation. Accomplishing this requires scenario-based concepts that are informed by collaboration from ongoing operations yet look well beyond the next five years. Once initiated, key ideas from these concepts need to be integrated, examined, and critiqued as part of leader development.

KEY MILITARY IMPLICATIONS SHAPING DOTMLPF

The strategic environment conditions and adversarial strategies presented in **Chapter 2** lead to several military implications requiring consideration across the areas of Army Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF).

INCREASING CHALLENGE OF A WIDE RANGE OF THREATS

While the existence of innovative adversaries is not new, today's strategic environment demands that U.S. forces prepare for a range of conflicts and potential adversaries. These may involve states that employ protracted forms of warfare, possibly using proxy forces to coerce and intimidate, or non-state actors using operational concepts and high-end capabilities traditionally associated with states.[74]

The Army does not have the luxury of focusing on any one potential adversary or any one mission type across the range of military operations. Instead, leaders and Soldiers must be exposed to the multiple conditions representing various types of threats that exist across the globe. Potential threats will range from standing conventional and unconventional forces, to irregular militias and paramilitaries, to terrorist groups and criminal elements. The Army must build and sustain capabilities to deter threats ranging from counterterrorism, to counterinsurgency, to aggressive states conducting major combat operations. Training, education, capabilities development, and concept development should reflect this reality.

INCREASING MULTIPLICITY OF ACTORS ACROSS POTENTIAL OEs

The Army must be prepared to face an ever-changing array of actors in any potential OE. Nation-states still matter, but the stage is becoming more and more crowded. Conflicts involving non-state actors are progressively becoming the norm, and non-state actors will be a key component of any future OE. For example, between 2007 and 2008, "non-state conflicts—violent confrontations between communal groups, rebels, or warlords that do not involve a state as a warring party—increased by a startling 119%."[75] Conversely, during roughly the same period, there were virtually no interstate conflicts except a small border conflict between Eritrea and Djibouti in 2008.[76]

Given the widespread and rapid dissemination of technology, non-state actors are more able to challenge state-based militaries. Access to such technology is leveling the playing field. The likelihood that the U.S. Army will find itself operating with or against a technologically sophisticated non-state actor is extremely high.

Operations in a JIIM environment are apt to be the norm in the future. Current operations already illustrate the capabilities that NGOs, PVOs, PSOs, and international organizations bring and their overall importance to supporting various types of operations. Conditions in the strategic environment indicate the importance of these organizations will continue. It will become increasingly more important for Army forces to know and act within the unique legal requirements such operations will bring. The Army must also enhance its ability to integrate with partners.

From humanitarian relief to reconstruction, units will be required to work alongside a number of non-DOD organizations. Leaders and Soldiers must understand these organizations and their capabilities to assess how they can shape any OE. The Army must "be able to work with other government agencies, indigenous forces, and international partners to build unity of effort."[77] Achieving this unity of effort will require focused training along with education and leadership development. Concept and capabilities development will need to address issues of organizational interoperability and communication system compatibility. Training should reflect various types of actors, with varying types of political, military, and economic goals. Training, education, capabilities development, and concept development should reflect the proliferation of technology and related capabilities. The investment in language, regional expertise, and cultural knowledge of multiple OEs will be required over the forecast period.

INCREASING IMPORTANCE OF GAINING A HOLISTIC UNDERSTANDING OF EACH OE

In addition to understanding the wide range of actors, leaders and Soldiers must be able to analyze and understand the strategic environment and each potential OE that U.S. forces may operate within. Leaders and Soldiers will also need to develop a mindset that allows for quick and competent adaptation across various OEs. Each OE will present different and challenging conditions, and such variations must be taken into consideration. OEs will be distinguished by unique and particular political, military, economic, social, infrastructure, information, physical environment, and time conditions and characteristics. Leaders and Soldiers must be able to function in any environment with the forces on hand and be "culturally astute enough to operate effectively among the people."[78] This requires a knowledge and understanding of each OE and the conditions and characteristics of the PMESII-PT variables inherent in each OE. Leaders must actively promote the value of a holistic look at and understanding of an OE and prepare for operational adaptability at all times. For more detail on the OEA framework, see **Annex A: The Operational Environment Assessment Framework**.

INCREASING DEGREE OF UNCERTAINTY

Predicting the future of human endeavors is an inherently difficult task. As a result, we have to educate for uncertainty by providing opportunities for Army leaders and Soldiers to learn and understand basic principles and enduring concepts relative to any OE. This is a critical skill that must be stressed across all leader development and training venues. Before the U.S. deploys units to a conflict, there will be much energy devoted to gathering information about the area of operations, but there will remain much that is still unknown. Training and education venues must prepare leaders and Soldiers to become accustomed to and even thrive in situations of uncertainty. As the Chairman of the Joint Chiefs of Staff, General Martin E. Dempsey, recently stated, "War is discovery—we must continue to out-think and out-adapt our adversaries."[79]

INCREASING OCCURRENCE OF SIMULTANEOUS AND CONTINUOUS ENGAGEMENTS

A clear delineation of combat and post-combat operations no longer exists, and will likely become even more blurred in the future. Training must incorporate offensive, defensive, and stability operations running concurrently or changing quickly in nature, direction, and scope over an extended period of time. Our Army must learn to recognize indicators when the adversary is adapting in order to make tactical adjustments. Therefore, our training should reflect this condition to help develop skills necessary for leaders and Soldiers to adapt and respond appropriately. General George W. Casey, Jr. succinctly postulated that in order to respond to such diverse and dynamic conditions, "The Army must be expeditionary: organized, trained, and equipped to go anywhere in the world, fight upon arrival, and sustain that response for uncertain durations."[80] The Army must achieve and maintain a capability that "provides a balanced mix of multipurpose capabilities and sufficient capacity to accomplish a broad range of tasks."[81]

PREPARE FOR DECISIVE ACTION

Counterinsurgency and counterterrorist training is still important, but the scope and depth of training must expand to include the entire spectrum of potential operations. The Army must focus on preparation of conducting decisive action operations. Our OPFOR at the Combat Training Centers (CTC) must be robust to challenge decisive action mission essential task list (METL). The atrophy of our OPFOR in both equipment and personnel has placed a great training risk on our ability to provide a realistic threat against decisive action objectives. Outdated armor; a heavy reliance on augmentation to fill OPFOR ranks; and lack of wheeled combat vehicles, information warfare, and air defense capabilities must be addressed in order for our OPFOR to once again become the toughest opponent our Army will face short of actual combat.

INCREASING IMPORTANCE OF THE INFORMATION ENVIRONMENT

The force that controls the information environment or controls the perception of information has the advantage. This is true today and will be more so in the future as ICT capabilities continue to spread across the globe and into the hands of potential adversaries and other critical actors. U.S. forces must be prepared to successfully operate in and shape this environment. DOTMLPF development should focus on fully integrating all aspects of information operations (IO) at all levels and across all operations. Units must be prepared to understand their role in IO and specifically that all actions have reactions that will be captured digitally and used in the adversary's information campaign. Training and education must go beyond simply stating that IO is important; it must teach and prepare leaders and Soldiers how to operate and thrive within the information environment.

INCREASING LIKELHOOD OF A WMD EVENT AND CONSEQUENCE MANAGEMENT ACTIVITIES

The abundance of scientific, technological, and engineering (ST&E) developments has increased the possibility of WMD attacks against the U.S. or a U.S. ally. Proliferation of ST&E has helped shape the rise of the non-state threat. In many cases the non-state threat will be more capable of carrying out attacks because of its ability to remain ambiguous and thus blend within its surroundings. Although the U.S. Department of Homeland Security has mitigated the possibility of attacks to the Homeland, the lack of identity normally associated with nation-states allows the non-state threat to move across borders and within our borders almost at will. The challenge for the Army is two-fold: first, become capable of identifying and defeating this threat; second, effectively assist law enforcement, federal and state

emergency management, and other agencies in consequence management should an attack occur in the Homeland.

U.S. forces should be prepared to operate in WMD environments and in response to environmental disasters across the globe. Our Army should train to operate in contaminated areas and mitigate the effects of a WMD attack or an outbreak of a regional or global pandemic. Training should stress operating under the threat and/or occurrence of a WMD attack. Training should also include working with host-nation and domestic law enforcement, emergency relief, and humanitarian assistance agencies. This entails providing security for an area and its populace, conducting humanitarian assistance and disaster relief operations, and restoring/protecting essential services. Central to a crisis and consequence management is the populace and infrastructure. CTCs must be manned with the appropriate skilled role players and facilities equipped as per the Operational Environment Master Plan (OEMP) to replicate these conditions. Capabilities and concept developments must also adequately prepare U.S. forces to operate in such environments and provide the necessary equipment and facilities.

PREPARE FOR HOMELAND SECURITY/DEFENSE MISSIONS

Homeland defense/security, which requires shared intelligence and assistance in domestic security missions, will test traditional relationships and boundaries with law enforcement and other domestic entities. U.S. joint forces, combined with law enforcement and intelligence activities, will have to deal both with regular military and irregular forces, such as criminal organizations, terrorists, religious extremists, or individuals who seek to profit from instability. The U.S. Army must train vigorously for such operations to include Defense Support to Civil Authorities (DSCA) activities. This should include not only preparation for operations between the active component (AC) and the reserve component (RC) of the Army, but with other domestic agencies as well, particularly law enforcement. Issues of communication system interoperability and connectivity should be addressed by the Army. The collection and use of intelligence by all parties involved may require new processes and partnerships, which should be part of all Army training.

PREPARE TO DEFEND ACCESS TO THE GLOBAL COMMONS

Global commons are those areas of the world beyond the control of any one state—sea, space, air, and cyberspace—that constitute the foundation of the international system. Protection of U.S. access to the global commons will increase in importance in the coming years, specifically for space and cyberspace. U.S. forces must be prepared for degraded operations in both tactical and operational level exercises.

The 2010 Quadrennial Defense Review (QDR) states that "maintaining secure access to the global commons is of critical importance to the U.S."[82] Adversaries will continuously challenge our access to the global commons. U.S. forces will confront lower-end naval challenges in littoral waters, as well as high-end threats from missiles and advanced surface and subsurface ships.[83] Given the Army's reliance on these commons, protection of each will be critical to mission success.

Potential Global Chokepoints

Map created by TRISA-Threats OEA Team, 2012

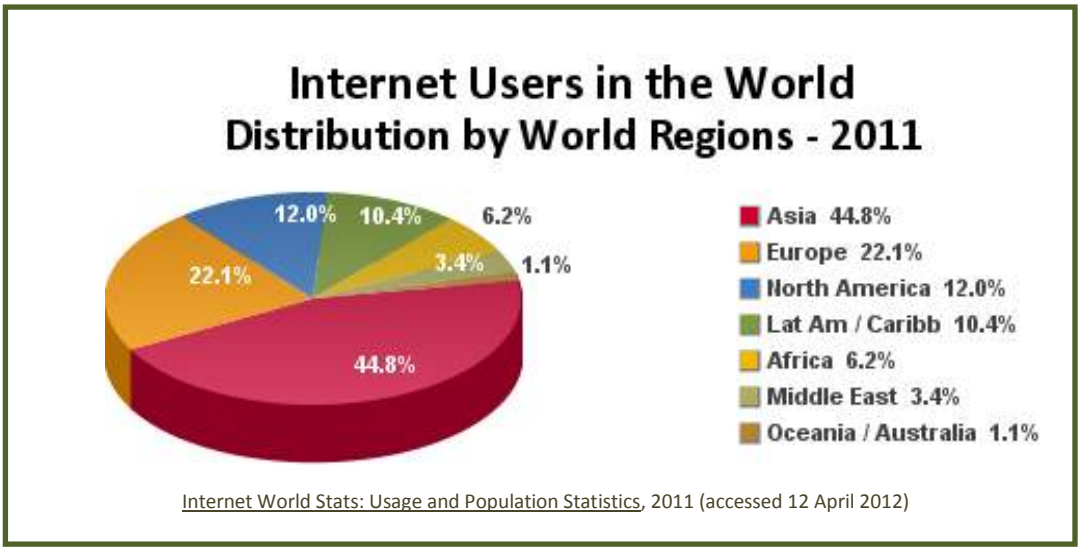
The Cyber Commons

The cyber commons provides an area of unlimited potential complicated by unlimited vulnerability. Progressively greater access to information once constrained by hierarchical organizations signals the erosion and perhaps dissolution of many organizations that once appeared immutable. To say only knowledge is power may be a misstatement; in cyberspace access to knowledge creates power. Individuals and non-state actors now exhibit ICT capabilities as powerful as most state actors'.

The importance of protecting the commons will increase in significance over the forecast period. Critical military communications and logistics systems, along with civilian financial and infrastructure networks, are now dependent on their supporting information systems, leaving them more and more exposed to crippling cyber attacks. Across the cyberspace common, potential adversaries "are employing and developing the means to deny, degrade, disrupt, deceive, and destroy the U.S. military's capability to operate, and its ability to operate effectively in other warfighting areas."[84] Current and future adversaries will relentlessly target Army information systems, data, and network links.

Critical military and civil information systems will be at risk of cyber attacks from states, non-state actors, rogue political actors, criminal networks, and terrorists. Adversaries will also employ carefully prepared perception management campaigns and targeted information events, launching surprise information attacks with false news stories, tampered or fabricated photographs and videos, spoofed Web sites and databases, false/stolen online identities, and other measures. These tactics are effective because of the growing use of the Internet worldwide. Adversaries may use these tactics to provoke

public hysteria, misdirect security efforts, create false intelligence patterns and leads, and to generate opposition to U.S. operations.



Internet World Stats: Usage and Population Statistics, 2011 (accessed 12 April 2012)

The Army will operate in this information-rich environment, and must become adept at utilizing new tools and methods for success. People today have tremendous access to a wide variety of information—some useful and some not so useful—and to tools that quicken the pace of human interaction. Phenomena like social networking and hacking are products of these easily accessible tools. In the military arena, cyber provides tremendous opportunity for those seeking ever greater efficiency in combat operations. Precise knowledge of enemy, weather, terrain, and friendly forces information rapidly disseminated allows accurate application of combat power, whether fire or maneuver. This very efficiency also creates vulnerability. With little excess capacity needed because of the multiplying effect of cyber, loss of "freedom of maneuver" in that space will tax the ability of a unit to accomplish assigned missions. The Army will need to be cognizant of such conditions and train, prepare, and educate for this environment.

Future OEs will be even more wired to cyberspace and further sensitized to its content; adversary messaging may need to be analyzed and countered in near-real time. As a hypothetical example, if adversary messaging attributed civilian casualties to host-nation or Army forces, imagery and eye witness documentation (or refutation) of these incidents could be needed within minutes to forestall the formation of flash mobs by otherwise innocent civilians. This will place greater demands on Army staff elements down to the brigade and battalion level. Enhanced real-time intelligence capabilities will be needed to offset adversary capabilities, and local culture and foreign language skills will become ever more important, along with faster and more sophisticated analysis of public attitudes, media content, and the range of effects for potential information courses of action.

The Space Commons

As with cyberspace, the protection of the common of space will rise in importance during the forecast period. Over the course of the next two decades, "space will be increasingly congested, competitive, and will likely be more reliant on partnerships and collaborations."[85] Threats to U.S. space assets and their supporting infrastructure will swell.[86] The common of space is fundamental to Army operations. As more

states and non-state actors recognize these benefits and seek their own space or counterspace capabilities, the Army will be challenged across the space common.[87]

U.S. military dependence on the space common runs the entire gamut of military operations and is one of the key reasons for our military superiority, both in conventional and strategic operations. Our current relative strength in and dependence on space operations, however, means other countries are intent upon gaining parity with the United States. It is therefore critical to continue developing both defensive and offensive space capabilities to maintain the military superiority of the U.S. Space assets will be targeted more by a "wide-range of man-made threats."[88] Adversaries will attempt electronic warfare (EW) attacks, computer network attacks, anti-satellite weapons, high energy lasers, and more conventional physical destruction methods to challenge the Army's access to space assets.[89]

In addition, the number of state actors or businesses developing space assets is rising. Space is no longer the private playground of the U.S. and Russia, according to Deputy Defense Secretary William J. Lynn who stated, "twenty-five years ago, the United States controlled two-thirds of the space market; today, that presence has slipped to below 40 percent."[90] This trend will continue into the future. New actors will present challenges to U.S. space access. In February 2011, 37 senators sent a letter to Secretary of State Hillary Clinton stating fears that the E.U. was "developing a space code of conduct that could undermine the U.S. space presence and harm security."[91]

Space itself is has also become more congested. DOD tracks approximately 22,000 man-made objects in orbit, 1,100 of which are active satellites.[92] The radiofrequency spectrum, so critical to mission command, is also crowded. Over the forecast period, the demands on the spectrum are expected to increase as global satellite services increase. By 2015, "as many as 9,000 satellite communications transponders are expected to be in orbit."[93] Greater congestion can lead to more instances of radiofrequency interference. This congestion of space and the radiofrequency spectrum will continue to increase over the forecast period.

Protection of U.S. access to the global commons will gain importance in the coming years, specifically for space and cyberspace. At a minimum, adversaries will seek to deny the U.S. access to these commons. The Army, along with the rest of the U.S., will continue to be challenged by capabilities across the commons by a host of state and non-state actors including China, Russia, and their proxies.

Humanitarian Operations in Haiti, 2010

Photo from www.army.mil, 24 April 2012

PREPARE FOR HUMANITARIAN ASSISTANCE/DISASTER RELIEF OPERATIONS

Since environmental and manmade disasters are a global constant, the Army must be prepared to conduct humanitarian assistance and disaster relief operations. The world is currently witnessing the effects of climate changes and related consequences. A condition contributing to the severity of potential

disasters is that by 2028, close to 60% of the world's population will live in and around urban areas.[94] Many of these urban areas are littoral, thus increasing their vulnerability to natural or man-made disasters. The combination of populations, stressed infrastructures, and a natural disaster produces catastrophic outcomes. Disasters are a global issue and no one is immune. Missions will range from providing security assistance to beleaguered humanitarian organizations and host-nation forces, to conducting outright humanitarian operations, to decontaminating a WMD site from a terrorist event. The likelihood that the Army will be involved in these types of operations is high over the forecast period.[95]

PREPARE FOR RECONSTRUCTION OPERATIONS

The U.S. Army Field Manual 3-07 defines reconstruction as "the process of rebuilding degraded, damaged, or destroyed political, socioeconomic, and physical infrastructure of a country or territory to create the foundation for long-term development." No matter if such destruction is caused by natural or man-made actions, U.S. forces will likely be called upon to assist in reconstruction efforts in the future. Such efforts will typically involve maintaining internal peace and stability, ensuring the rule of law, restoring or providing basic services, and repairing critical infrastructure. These conditions and missions should be stressed in training events and must be resourced with the appropriate equipment requirements.

PREPARE TO COUNTER THREAT ANTI-ACCESS CAPABILITIES

As noted in Chapter 2, the adaptive adversary is always learning and shifting strategies and tactics to counter U.S. military power. There is clear evidence that adversaries are interested in denying U.S. forces regional access. For example, Iran has a small fleet of frigates, patrol craft, submarines, mines, and advanced anti-ship cruise missiles that could be used to control access to the Strait of Hormuz.[96] Such capabilities oblige U.S. forces to train to "counter anti-access and area-denial strategies."[97]

Michele Flournoy, the former Under Secretary of Defense for Policy, stated, "The proliferation of knowledge and technology will allow an increasing number of state and non-state actors to deploy anti-access capabilities and high-end asymmetric technologies that can put allied infrastructure at risk and hamper U.S. power projection."[98] The Army must develop capabilities and strategies to counter adversarial anti-access activities.

CONCLUSION

Armed conflict will continue to be a course of action for both state and non-state actors. Any future OE will be complex and demanding. Conditions of this environment will include unprecedented amounts of information being transmitted over commercial networks, potential technological surprise, proliferation of WMD, selected conventionally advanced weapons systems, and the innovative use of highly-proliferated ones. The continued advancement of information-age technologies provides adversaries the capability to apply military force with greater precision, lethality, agility, and survivability.

Potential threats in this environment will retain hybrid capabilities and transition between traditional and adaptive constructs to counter conventional threats, add complexity to a given environment, and seek sanctuary in complex terrain. It is important to note that even as threats develop and master adaptive means, they will retain and improve traditional military capabilities.

The U.S. will remain globally engaged—called upon to execute missions across the spectrum of conflict. Increasingly interconnected economies and greater access to technology and information will challenge U.S. forces in unique and unexpected ways. To succeed will require a force that can deal with sophisticated information campaigns, integrated regular and irregular operations, and myriad improvised tools, networks, and innovation. Forces must be adaptive and master complex situations. Capabilities must be built to support decisive action operations and to take advantage of technology—especially ICT, strategic responsiveness, and joint interoperability. Only through these means will the U.S. military be able to successfully navigate any future OE.

Annex A
The Operational Environment Assessment Framework of Analysis

INTRODUCTION

Once the conditions of the strategic environment have been identified (using the OE variables of PMESII-PT), the same framework of analysis can be used at the operational level with greater variable resolution. As noted, all OEs are unique and require independent analysis with strategic environment conditions manifesting differently across all OEs. The following framework provides details for PMESII-PT variables for application at the operational level.

OEA FRAMEWORK OF ANALYSIS

The framework for thoroughly and systematically analyzing and understanding any potential OE and all the challenges and opportunities inherent in it consists of the eight variables: **political**, **military**, **economic**, **social**, **information**, **infrastructure**, **physical environment**, and **time**. The memory aid for these variables is PMESII-PT.

Army forces apply the PMESII-PT variables to the specific OE in which they are conducting or plan to conduct operations. Use of the framework by Army commanders and staffs at all levels to analyze and understand their OEs:

- Enables lower commands to use their higher command's analysis of its own OE and just add details to capture the nature of variables and sub-variables in their own specific OE, which is part of that higher-level OE or the strategic environment.
- Enables higher commands to assimilate into their own OE analysis the relevant information developed by their subordinates.
- Facilitates a common operational picture (COP) at all levels of command.
- Provides compatibility with the PMESII framework used at joint level and in the Interagency Conflict Assessment Framework (ICAF).

The PMESII-PT variables are fundamental to development of a comprehensive understanding of the OE for planning and decision-making at any level, in any situation. These variables and their interrelatedness determine the nature of an OE and how it will affect or be affected by an operation. The following is a brief description of each PMESII-PT variable, along with examples (in parentheses) of questions a commander might need to have answered about each variable in his particular OE:

- **Political**: Describes the distribution of responsibility and power at all levels of governance—formally constituted authorities, as well as informal or covert political powers. (Who are the tribal leaders in the village? Which political leaders have popular support?)

- **Military**: Explores the military and/or paramilitary capabilities of all relevant actors (enemy, friendly, and neutral) in a given OE. (What is the force structure of the enemy?)

- **Economic:** Encompasses individual and group behaviors related to producing, distributing, and consuming resources. (What is the unemployment rate?)

- **Social**: Describes the cultural, religious, and ethnic makeup within an OE and the beliefs, values, customs, and behaviors of society members. (What is the ethnic composition of the OE?)

- **Information:** Explains the nature, scope, characteristics, and effects of individuals, organizations, and systems that collect, process, disseminate, or act on information. (How much access does the local population have to news media or the Internet?)

- **Infrastructure:** Details the composition of the basic facilities, services, and installations needed for the functioning of a community or society in the OE. (What are the key modes of transportation?)

- **Physical Environment:** Depicts the geography and man-made structures as well as the climate and weather in the OE. (What types of terrain or weather conditions in this area of operations favor enemy operations?)

- **Time:** Describes the timing and duration of activities, events, or conditions within an OE, as well as how the timing and duration are perceived by various actors in the OE. (What is the cultural perception of time in this OE?)

VARIABLES AND SUBVARIABLES

Each of the eight PMESII-PT variables also has associated core subvariables. These headings can be further broken down to provide the level of detail required. The degree to which each subvariable provides useful information relevant to a particular OE depends on the specific situation and echelon.

The following table gives some examples of subvariables that require consideration.

PMESII-PT Variables and Examples of Subvariables

Political Variable	Social Variable	Physical Environment Variable
- Attitude toward the United States - Centers of political power - Type of government - Government effectiveness and legitimacy - Influential political groups - International relations	- Demographic mix - Social volatility - Education level - Ethnic diversity - Religious diversity - Population movement - Common languages - Human rights - Centers of social power - Basic cultural norms and values	- Terrain - Natural resources - Climate - Weather

PMESII-PT Variables and Examples of Subvariables		
Military Variable - Military forces - Government paramilitary forces - Non-state paramilitary forces - Unarmed combatants - Nonmilitary armed combatants - Military functions	**Information Variable** - Public communications media - Information warfare - Intelligence - Information management	**Time Variable** - Knowledge of the AO - Cultural perception of time - Information offset - Tactical exploitation of time - Key dates, time periods, or events
Economic Variable - Economic diversity - Employment status - Economic activity - Illegal economic activity - Banking and finance	**Infrastructure Variable** - Construction patterns - Urban zones - Urbanized building density - Utilities present - Utility level	

CONCLUSION

Army commanders and staffs—at all levels—should use the PMESII-PT framework. TRADOC G-2 Intelligence Support Activity (TRISA-Threats) produces Operational Environment Assessments (OEAs), which are an overview of the variables operationalized to a specific OE. To date, TRISA-Threats has produced seven OEAs focused on Iraq, Afghanistan, Pakistan, North Korea, Azerbaijan, the Horn of Africa, and Iran. Each OEA contains a detailed analysis of the PMESII-PT variables, trends analysis, and an events list to show the reader the real-world manifestation of the variables in the selected OE. All OEAs and related products can be found on Army Knowledge Online (AKO).

Annex B
Asia-Pacific Regional OE Conditions and Characteristics

ASIA-PACIFIC REGION MAP

U.S. STRATEGIC INTERESTS AND GOALS

The Asia-Pacific region will become entrenched as the global economy's center of gravity over the forecast period. By 2020 the world's four largest national economies will be the U.S., China, India, and Japan; their economic interests will converge in the sea lanes and littoral areas of this region, increasing the already vital importance of mature security relationships, political stability, and the free flow of commerce in Asia. Regional security mechanisms will continue to adapt to accommodate the rising power of China and India along with concomitant military buildups throughout the region. U.S.-Asian mutual defense treaties dating from the 1950s have served as a pillar of stability in the region, but over the forecast period these are likely to be augmented by deeper U.S. bilateral and multilateral security ties with additional Asian nations.

The U.S. is committed to maintaining a significant forward military presence in Northeast Asia over the forecast period and seeks to build a comprehensive security partnership with Japan and the Republic of Korea (ROK) that enhances the capabilities of both partners. This will include transferring operational control of combined forces on the Korean peninsula to the ROK by 2015, adopting a more flexible force posture, aiding Japan's development of out-of-area capabilities, and developing Guam as a hub for future U.S. joint operations.

In Southeast Asia the U.S. will promote greater bilateral and multilateral security agreements and exercises, including both intraregional activities and those with U.S. forces. The U.S.-Australia alliance will continue to deepen and serve as a model for interoperability and collaboration in the region. The U.S. will seek greater security collaboration on counterterrorism, piracy, narcotics trafficking, and WMD proliferation with key regional partners including the Philippines, Thailand, Vietnam, Indonesia, Singapore, and Malaysia. Across the region the U.S. will work to develop a diversified and flexible set of basing agreements that will provide rapid operational access, robust sustainment capabilities, and allow a forward deployed presence as required. In addition to security missions, emphasis will be placed on the ability to support humanitarian operations.

The U.S. will seek opportunities to solidify a military-to-military (mil-mil) relationship with China, both as a trust and confidence-building measure and for collaboration on security issues such as piracy and WMD proliferation. At the same time, the U.S. will monitor China's military modernization and address regional security concerns with the country. The U.S. will also pursue greater mil-mil cooperation with India, in the expectation that India's growing capabilities in all elements of national power will serve as a pillar of stability and security throughout the Indian Ocean basin. [99]

CONDITIONS SHAPING THE REGION

POLITICAL—CHANGING INTERNATIONAL DISTRIBUTION OF POWER

China will continue to accumulate the tools associated with superpower status: a large, dynamic economic base; political and economic alliances capable of persuading or coercing other regional actors; world class technological resources; and full-spectrum military capabilities. Over the next decade, China will continue to invest enormous amounts of hard currency in joint ventures with cash-strapped Western technology firms, appropriating or reverse-engineering production methods and products, thus cutting years off of research and development cycles and leveling the technological playing field in many industries. China has already gained access to many of Russia's advanced military technologies, allowing newly profitable defense firms to reverse-engineer advanced systems such the Su-27 fighter, and facilitating development of potentially world-class platforms such as the J-20 stealth fighter ahead of expected timelines. Five- and ten-year defense technology plans are intended to elevate China's indigenous defense firms into the first tier of the global defense industry in the 2020-2025 timeframe.[100] China's rapid military modernization has prompted a military spending binge throughout Asia, as neighboring states accumulate submarines, surface warships, aircraft, and other systems to counter China's burgeoning maritime capabilities.[101]

It is unlikely that the U.S. will face China in armed conflict over the forecast period. However, China's military strength and technological prowess will manifest beyond its borders in other ways that will significantly impact the U.S. Army. A mercantilist version of the Cold War is a potential outcome from China's rise, as Beijing seeks natural resources, political influence, and strategic partners throughout the

world. China's laissez-faire approach to human rights encourages repressive regimes such as North Korea, Sudan, Iran, Burma, Venezuela, and others to pursue or deepen strategic partnerships with Beijing. This will contribute significantly to the proliferation of anti-access capabilities including ballistic and cruise missiles, air defense systems, and nuclear weapons technology that will threaten the ability of the U.S. Army to deploy and sustain in key regions of the world.[102]

Although Beijing's ambitions appear to be purely economic, China will use the full range of incentives—including military equipment and training—in developing bilateral relationships throughout Central and Southern Asia, South America, and Africa, altering regional security dynamics and creating the potential for ground conflicts between U.S. allies and regional rivals. Countries wishing to counter the military capabilities of Chinese client states may look to the U.S. for security relationships that will preserve regional stability. In recent history, China has preferred to employ economic leverage and information campaigns to achieve its ends, however future leaders of the Chinese Communist Party may choose a more muscular foreign policy. Therefore, the possibility of proxy conflicts should be anticipated.

India's international status is increasing rapidly due to its economic growth, democratic governance, technological prowess, and military strength. If India maintains its current 9% economic growth rate it will become the world's third largest economy by 2020.[103] While Indian-Chinese relationships remain cordial and their bilateral trade has grown rapidly, Indian leaders frankly comment on the potentially destabilizing effects of China's advancing military capabilities. Even as China establishes bases and conducts naval operations in the Indian Ocean, India's maritime strategy now cites the South China Sea, Western Pacific, and neighboring littoral regions as areas of national interest; the Indian Navy has conducted joint exercises in the China Sea with the U.S., Japan, Singapore, and Vietnam. India is expending significant resources to extend its military capabilities and has recently surpassed China as the world's largest importer of weapons systems.[104] A deeper U.S.-India, mil-mil relationship would be a positive development for each country's navy and for regional maritime security. However, the Indian government has refused to sign logistics support and communication interoperability agreements that the U.S. has lobbied intensively for since 2005, maintaining an independent security stance that—among other considerations—protects India's easy access to Iranian energy supplies.[105]

MILITARY—WEAPONS OF MASS DESTRUCTION

The nuclear rivalry between India and Pakistan will continue to threaten South Asia's stability; as India's economic and technical means grow apace, Pakistan's political and military leaders will struggle with the perception of an inferior military position vis-à-vis India. Transfers of nuclear and missile equipment, technologies, and expertise among North Korea, China, Pakistan, Iran, Russia, and other actors will continue to create dangerous opportunities for proliferation of WMD capabilities into the hands of rogue state and non-state actors.

INFORMATION—PROLIFERATION OF ICT

China's military is making increasing ICT investments and placing doctrinal emphasis on the use of information warfare, including robust cyber and EW capabilities. Drawing on a large domestic talent pool of hackers, China's cyber capabilities have been tested against Army and other U.S. government systems. At the same time China has built a virtual "Great Wall," fencing off Chinese cyberspace from international social networking, communications, and search engines. India, Japan, Korea, Taiwan, and other regional states also have deep reservoirs of expertise in this field. Continued economic development may eventually lead to this region becoming the world's leading source of innovations in

the ICT industry; cyber competition driven by business, military, social, or other rivalries is likely to make it a source of cyberspace threats worldwide, and a dangerous environment for U.S. military information systems. Deployed U.S. forces will find themselves operating in an environment where information systems are under continuous threat of penetration and cyber attack.

SOCIAL—DEMOGRAPHICS

Demographics will increasingly affect the security calculations of regional powers including China and Japan; both will face major challenges in maintaining a labor force capable of producing economic growth, providing for increasing numbers of retirees, and manning their military forces. Similar pressures will affect their military budgets. In China the prevailing gender gap (over 120 males per 100 females by some estimates) caused by selective abortions may contribute to increased social tensions and large-scale emigration of young males.

PHYSICAL ENVIRONMENT—NATURAL RESOURCES

China's rapid economic growth has created surging demand and prices for energy, metals, and other raw materials worldwide. Rapid growth throughout the Asia/Pacific region has also contributed to this global commodity market's boom. Price movements in global equity, bond, and product markets are increasingly driven by automated electronic trading, leading to major swings in raw material prices and the financial fortunes of key business elites. If the global economy continues in its current state of fragility for an extended period—a very real possibility—the financial markets will become increasingly sensitized to risk. Even small changes in risk perceptions associated with access to raw materials could have severe political and economic impacts in Asian markets. These risk perceptions can arise unpredictably in source regions for raw materials in Africa and the Middle East due to local political instability, military conflict, commercial competition, or natural events. In a tense economic and information environment, adverse market adjustments due to events in politically unstable regions could trigger further destabilizing actions by Asian governments: strong diplomatic pressure, aggressive financial sanctions, or military deployments focused on securing access to critical natural resources.

FUTURE ARMY MISSION AREAS

PEACETIME MILITARY ENGAGEMENT

The Army will be committed to combined training and exercises on the Korean Peninsula for the duration of the forecast period. This will involve assisting the ROK Army to develop the skills for employing combined arms teams in high-intensity conventional combat. The North Korean threat will also mandate training that realistically simulates WMD contaminated environments. Coalition-building is a critical objective in this theater; deployed Army leaders may find themselves uniquely placed to promote collaboration and interoperability between the Korean and Japanese militaries.

The Army may be called on for a higher tempo of combined training and exercises with Southeast Asian militaries. Light infantry training for counterterrorism, counter-piracy, and counterinsurgency missions will predominate. Another important activity will be the creation of a flexible basing structure that will allow U.S. forces to rapidly surge into the theater for crisis response. Vietnam is in the process of refurbishing the port at Cam Rahn Bay with the intent to reopen its facilities to transiting foreign navies

in 2014; a mil-mil relationship between Vietnam and the U.S. is an important contingency for the next decade.[106]

LIMITED INTERVENTION

The Asia-Pacific region is extremely prone to earthquakes, and many of its coastal areas and river plains are vulnerable to deadly flooding. A recent United Nations (UN) report documents the lack of disaster response capabilities in the region and the disproportionate death tolls that result.[107] China, Japan, Indonesia, India, and Taiwan have experienced over 1/3 of the world's major earthquake disasters (death tolls over 1,000) since 1900, while Bangladesh, Burma, and India remain especially vulnerable to massive losses of life from tropical cyclones.[108] As the Army increases its peacetime engagement activities in Southeast Asia, it becomes more likely that deployed units will be in the path of natural disasters and/or be called on as first responders. Important provisions for such contingencies may include early-warning services; logistics support agreements, communications interoperability with host-nation forces, and knowledge of local culture, climate, and geography.

PEACE OPERATIONS

The deployable security capabilities of regional actors such as Australia, combined with the overall stability of the region, make it unlikely that the U.S. would be involved in Asia-Pacific peacekeeping missions. The only current peace operation in the region is the United Nations Integrated Mission in Timor-Leste (UNMIT), established in 2006. U.N. Resolution 1704 authorized 34 military liaison and staff officers to this mission.

IRREGULAR WARFARE

Over the past decade, India, Indonesia, Thailand, the Philippines, and Bangladesh have all experienced insurgent and terrorist violence from Islamist extremist groups that continue to operate in Southeast Asia and receive support from Persian Gulf extremists.[109] Although these threats are largely contained at present, the U.S. will need to be prepared to assist any democratic nation in the region whose stability is threatened by future growth of extremist violence via the deployment of special operations forces (SOF), light infantry, and support forces, as has occurred in the Southern Philippines since 2002.

MAJOR COMBAT OPERATIONS

Outside the Korean peninsula there is little prospect for major combat operations in the Asia-Pacific region. Should a conventional conflict break out, it will most likely be fought by naval, air, and missile forces. The geography of the theater dictates that major international conflicts will be fought for control of SLOCs, the major port facilities they serve, and the key bases that can interdict them. In such a conflict the Army's role would be limited to defense of established basing infrastructure in Guam, Korea, Japan, or of temporary U.S. installations in Singapore, Indonesia, the Philippines, Vietnam, or Australia. Threats could come from ballistic and cruise missiles, aerial bombardment, electronic and cyber attacks, amphibious SPF missions, or terrorist attacks. In this contingency the Joint force would benefit from improved methods for physical hardening of facilities, more capable missile defenses hardened against electronic and cyber threats, and improved surveillance and monitoring capabilities to support fixed-installation defense. On the Korean peninsula the threat would also include the risk of a high-intensity conflict, combined arms maneuver, and operations in WMD-contaminated environments.

Annex C
Middle East and Southwest Asia Regional OE Conditions and Characteristics

MIDDLE EAST AND SOUTHWEST ASIA REGION MAP

U.S. STRATEGIC INTERESTS AND GOALS

Vital U.S. security goals in the Middle East and Southwest Asia include political stability, the defeat of violent extremist organizations, promotion of democracy, and the strengthening of regional security structures and non-proliferation regimes. Critical economic interests include promoting economic prosperity for the region's underdeveloped states, integration of regional economies into global markets, and access to regional energy supplies.

Iran's program to develop nuclear weapons directly threatens the states of the Gulf Cooperation Council (GCC), Israel, Russia, and the North Atlantic Treaty Organization (NATO), and may provoke a nuclear arms race in the region. This could lead to future diplomatic confrontations or conflicts between nuclear-armed states with immature security and control systems for their weapons. Iranian sponsorship of Hezbollah, Hamas, Iraqi militias, and Shia minority groups throughout the region will contribute to further mistrust, instability, and violence. U.S. policy objectives will continue to include the discontinuation of Iran's pursuit of nuclear weapons and its sponsorship of terrorist groups.

The U.S. will continue to seek the conclusive defeat of al-Qaeda in the Afghanistan-Pakistan theater and to strengthen the capacity of both states to resist violent extremist movements. This includes dedicated

support to Afghanistan's Security Forces to advise, train, and assist them in resisting a Taliban return to power and to reintegrate former insurgents into Afghan society. Similar support will be provided to Iraqi security forces to expand security and freedom in a prosperous, democratic Iraqi state.

The U.S. will remain committed to the security of Israel, while simultaneously pursuing stronger bilateral and multilateral security relationships with Egypt, Lebanon, Jordan, Yemen, and the GCC states. The current basing infrastructure, force mix, and defense posture of U.S. military forces in the region will have to be reassessed alongside these security partnerships, due to the increasing threat from ballistic missiles and WMD. The U.S. will need to develop a regional military presence that is optimized against several competing criterion: to demonstrate a credible long-term commitment to regional security; to minimize perceptions of American military "occupation"; to protect U.S. bases and provide reliable logistic support in crisis situations; and to promote regional security architectures including air and missile defenses. [110]

CONDITIONS SHAPING THE REGION

MILITARY—WMD PROLIFERATION

Iran's nuclear program, risks to Pakistan's nuclear weapons and the willingness of external actors to sell nuclear technology and components all heighten the salience of WMD proliferation for the region's future. A conventional arms race is already under way and a nuclear arms race may follow: Saudi Arabia, Kuwait, and the UAE have already signed contracts for nuclear reactors, while the Saudis are actively considering their own nuclear weapons program.[111] Israel's nuclear deterrent is often cited as justification for WMD programs in Arab states. Syria possesses the most active chemical warfare program in the region and, should the regime fall, Syria's weapon stocks would be at risk of seizure by local factions. Should the Assad regime survive, it will continue to cooperate with Iran in supplying Lebanese Hezbollah with advanced weapons systems, including medium-range missiles. Future biological weapons development by Iran and Syria is a potential threat, made more severe by their demonstrated willingness to share military capabilities with non-state actors who threaten the interests of the U.S. and its allies worldwide.

POLITICAL AND INFORMATION

During the Arab Spring of 2011, ICT-empowered social movements succeeded in ousting heads of state in Tunisia, Egypt, and Libya, spawned sustained civil conflicts in Yemen and Syria, and created a political crisis in Bahrain that was only turned back by an armed coalition response from the GCC states. Each of the uprisings in the Middle East in 2011 called for democratic reform—full participation of the people in the formation and operation of their national governments. In the short term this may contribute to greater instability, creating opportunities and threats for Iran, Saudi Arabia, Turkey, and outside actors (including the U.S., the European Union [E.U.], China, Russia, and India) seeking to influence the outcomes. By 2028 democracies could be the norm in the region, although they may include "illiberal" elected regimes that oppress minority groups and foster xenophobic attitudes toward other nations and cultures.

SOCIAL

Virulent anti-Israeli sentiments run deep in the region and the ouster of authoritarian regimes may give freer rein to these public attitudes, raising the risk of further armed conflicts driven by the Israeli-Palestinian rivalry. National foreign policies in the region may move further into opposition of the United States, its policies, presence, and interests in the region, especially with respect to U.S. support for Israel. The hegemonic aspirations of the leading Sunni and Shia nations, Saudi Arabia and Iran, may spark an armed conflict as each seeks to assume religious and political leadership in the Middle East at the expense of the other. As Iran achieves nuclear weapons capability the Sunni-Arab world could respond in kind, with Israel forming the third leg of an unstable triad of well-armed protagonists with longstanding political grievances and deeply entrenched ideological divisions.

Violent Islamist extremist groups have been at the root of many conflicts in the region over the last three decades. A future wave of Islamist movements may gain political influence or control in emerging democracies, promoting populist hostilities against Israel, international institutions, and political, economic, and security relationships with Western nations. In the future al-Qaeda, its affiliates, and/or successor terrorist movements may refine their ideological message and limit their targeting of Muslims to gain broader public support. These developments would multiply the tactical threat of terrorist attacks on deployed U.S. and allied forces, embassies, businesses, and citizens.

PHYSICAL ENVIRONMENT—NATURAL RESOURCES

Competition for natural resources will continue to be a source of instability and conflict in the region over the forecast period. Oil-importing nations in Asia, Europe, and the Americas continually vie for political influence, oil and gas investment opportunities, security relationships, and arms-export deals with the region's oil producers.

Access to water is another issue that will threaten the security and stability of the region. By 2025, "water stress will increase significantly in many locations throughout the world, including North Africa, the Middle East, and Asia."[112] Changing weather patterns are impacting the natural water cycle in the region: as of mid-2011, most of the Middle East and much of Southwest Asia has endured 7–10 years of drought. The disputed Golan Heights region of Syria (captured by Israel during the 1967 "Six Days War") is home to the headwaters of the Jordan River. Syria will continue to demand that Israel return this captured territory that is home to Israel's most important fresh water source; Israeli governments will be loathe to comply. Another flashpoint involves Turkey's Southeastern Anatolia Development Project, which centers on a series of 22 dams and 19 hydroelectric plants that will further diminish the flow of water to Syria and Iraq from the Tigris and Euphrates Rivers.[113] Both Syria and Iraq receive over half of their fresh water supplies from other countries. Most major urban areas lack sufficient water-management infrastructure to supply their increasing populations, making delivery of fresh water and the disposal of wastewater sources of popular discontent and potential drivers of conflict.

FUTURE ARMY MISSION AREAS

PEACETIME MILITARY ENGAGEMENT

The U.S. will seek to preclude the creation of new terrorist safe havens and eliminate existing havens through security assistance and cooperation with Pakistan, Afghanistan, Iraq, Yemen, and other willing

partners. This will require the Army to refine its methods for providing long-term training and material support to host-nation security forces. These operations may take place in austere and hostile environments, with host-nation forces possessing limited fires and logistics support. Greater insurgent infiltration of urban populations, host-nation security forces, and other government or NGOs may greatly increase the threat to Army personnel. U.S. training missions may also include training for defense from external conventional threats, intelligence monitoring of Iranian-sponsored terrorist and information operations, security of critical infrastructure, and the prevention of internal sectarian conflicts. Public resentment toward the presence of Western military forces may preclude large-scale joint training and exercises in the Middle East. However, small-scale multinational training exercises may continue in Iraq, Afghanistan, and other nations in the region.

LIMITED INTERVENTION

Violent extremist and insurgent groups will remain active throughout the region and low-intensity conflicts will continue. U.S. forces must increase their mastery of robotic systems as technologies advance, taking full advantage of the increasing precision, persistence, and autonomy of unmanned systems to conduct strikes against key terrorist targets. SOF raids may be required in select cases to ensure neutralization of very high-value targets, to secure intelligence, or to rescue hostages. Challenging mission profiles may require extremely close coordination of armed unmanned systems with U.S. Soldiers on the ground.

Increasingly severe drought, flooding, desertification, and urbanization of populations in economically depressed nations may combine to produce humanitarian crises in which the U.S. will join multinational efforts to provide security and contribute to humanitarian relief operations. The growing number of chemical and nuclear facilities in the region will increase the risks associated with earthquakes, terrorist attacks, missile strikes, and other events that could complicate disaster-relief efforts. Weak host-nation governments may be unable to provide security to foreign disaster-relief efforts; in such scenarios the Army could be required to provide security for evacuation efforts and relief agencies in urban environments already infiltrated by terrorist groups and other political organizations with anti-Western agendas.

PEACE OPERATIONS

U.S. forces could be called on to participate in multinational peacekeeping efforts in the Middle East and South Asia. For example, any future Middle East peace process that moves toward a resolution of Israeli-Palestinian territorial disputes may require an international force to occupy neutral security zones between Israeli and Palestinian areas. As part of a United Nations peacekeeping force operating under restrictive rules of engagement, the Army could be placed in close proximity to Iranian-backed Hezbollah and Hamas forces equipped with a range of standoff weapons including modern short-range ballistic missiles, Katyusha rockets, UAVs, and successive generations of Improvised Rocket Assisted Munitions (IRAMs), along with terrorist wings well-versed in IED and suicide tactics.

IRREGULAR WARFARE

The sovereignty and security of the Afghan and Iraqi governments will remain at risk as these nations face multiple internal and external threats in the coming decades. In both countries, ethno-sectarian factions will remain significant centers of local authority, challenging or preempting the authority of the national governments. Sectarian factions such as Iraq's Kurdish Peshmerga and the Hezb-e Islami

Gulbuddin in Afghanistan include highly-organized, well-trained and well-armed militias devoted to protecting the political interests and territorial integrity of their ethnic group. Al-Qaeda will continue terrorist attacks to spark sectarian conflict in Iraq and support the Taliban's efforts to overthrow the Afghan government. Iran's Quds Force will continue arming and training insurgent groups and performing clandestine operations in Afghanistan and Iraq. In this environment the Army may be tasked with supporting domestic security forces against evolving multiple threats with declining coalition resources.

Islamist terrorist organizations will continue honing their methods for exploiting weak and failed states to establish and maintain bases of operation. Despite successful targeting of al-Qaeda leaders and an overall decline in its global capabilities, such places will still include conditions favorable to Islamist militant groups seeking to maintain their presence in Afghanistan, Pakistan, Central Asia, the Arabian Peninsula, and Africa over the forecast period.[114] A successful mass-casualty terrorist attack on U.S. citizens or installations would compel the U.S. to initiate a decisive response; if the attack issued from a terrorist safe haven, this could involve conventional forces conducting joint forced-entry operations to capture/kill terrorist leaders and destroy their base infrastructure. The adversary may employ IEDs and suicide tactics that have advanced well beyond current capabilities, employing miniaturization, robotics, more powerful explosives, improved electronic components, and prepared ground to inflict maximum casualties on U.S. forces.

MAJOR COMBAT OPERATIONS

Over the forecast period the Israeli-Palestinian confrontation may become tenser, the Saudi-Iranian rivalry and arms race may grow, and domestic challenges to authoritarian regimes could continue. In consequence, the Middle East may be the most likely theater for future major combat operations. These operations may involve large-scale aerial and missile attacks, high-intensity mechanized ground combat, and mid-intensity conflicts involving adversaries along the lines of the 2006 Israel-Hezbollah clash. These conflicts could escalate to the point of U.S. involvement if U.S. allies are attacked, if critical oil infrastructure such as the Abqaiq oil processing facility are at risk, or if maritime chokepoints vital to the global economy are threatened. In this type of contingency the Joint Force could face a spectrum of anti-access capabilities including WMD, missiles, submarines, swarming UAVs and small boats, suicide attacks on bases and critical infrastructure, and cyber and EW attacks.

Annex D
Europe and Russia Regional OE Conditions and Characteristics

EUROPE AND RUSSIA REGION MAP

U.S. STRATEGIC INTERESTS AND GOALS

The NATO alliance (along with America's non-NATO democratic allies in Europe) will remain a central pillar of U.S. international security and a priority for mil-mil engagement over the forecast period. NATO's new strategic concept is focused on strengthening capabilities for ballistic missile defense, space and cyber security, interdiction of illicit trafficking, non-proliferation regimes, and increasing NATO's capabilities by mission specialization among its members. The U.S. will maintain a few brigade combat teams (BCTs) stationed in Europe alongside an enhanced naval presence, providing an in-theater capability to meet the Article 5 requirements of the North Atlantic Treaty, as well as a flexible forward posture that supports combined operations both inside and outside the continent.

The U.S. will seek to build on collaboration with European allies to combat violent extremism in Afghanistan and to leverage NATO capabilities to act as a stabilizing force across the Middle East, North Africa, the Balkans, and the Caucasus. Other important areas of NATO cooperation will include addressing emerging security issues in the Arctic and developing closer mil-mil relationships with non-NATO Europe. The U.S. will work with European partners (especially the U.K. and France) to share facilities in Africa and to collaborate on capacity-building and contingency responses there. The U.S. will pursue an expanded security dialogue and mil-mil relationship with Russia, encouraging Moscow to play a more active role in promoting security and stability in Asia (especially in Afghanistan), developing closer cooperation on counterterrorism, counter-proliferation, space and ballistic missile defense initiatives, and negotiating the future of the Arctic. [115]

CONDITIONS SHAPING THE REGION

POLITICAL—CHANGING INTERNATIONAL DISTRIBUTION OF POWER

Demographics and economics are gradually weakening the military capabilities of the NATO alliance; over the last decade average defense spending in NATO's European member states shrank to 1.7% of

gross domestic product (GDP) and total military personnel fell by 50%. These downward trends are driven by factors—including reduced perceptions of military threats and increased demands for social spending—that may continue. However, Europe's great powers will retain significant advanced military capabilities augmented by newer NATO members such as Poland, whose wealth and national power will continue to rise relative to Europe's core states.

Russia is also facing a general decline in military capabilities and is struggling to fund and implement a sweeping set of military reforms that would slash the size of ineffective reserve forces, stockpiles of antiquated equipment, a bloated officer corps, and military bureaucracy, while simultaneously transforming the armed forces into a professional force with modern weapons, doctrine, and enhanced readiness. Russian military doctrine is still focused on the core mission of a large Asian land war, with China gradually supplanting NATO as the principal threat. However the de facto primary mission is maintaining an adequate security structure in the Caucasus and Central Asia. To that end, Russia has mutual defense pacts with Armenia, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan under the auspices of the Collective Security Treaty Organization (CSTO), and has recently established or renewed long-term leases on military bases in Abkhazia, South Ossetia, Sevastopol (Ukraine), Armenia, and Kyrgyzstan.

PHYSICAL ENVIRONMENT—NATURAL RESOURCES

An emerging area of strategic interest will be the Arctic Ocean. As ice floes melt and oil-recovery methods advance, the Arctic will become increasingly accessible to maritime traffic and oil exploration/production. Five nations—Russia, Canada, Norway, Denmark, and the U.S.—border the Arctic and have territorial claims there. Other nations seek access to the energy resources in international waters. Russia, whose territory rings almost half the Arctic Circle, has placed "a naval infantry and an army brigade on the Kola Peninsula," setting the conditions for a potential increase in military operations in the Arctic. [116]

SOCIAL—DEMOGRAPHICS

The Europe/Russia region faces the demographic challenges of an aging, shrinking native population confronted with increasing numbers of less affluent, culturally diverse immigrants. The UN Population Division forecasts that Europe's population will rise less than 1% through 2020, and then decline to its present level of 738 million by 2035. The elderly will increase from 16% to 24% of the population, with a corresponding increase in healthcare and other social spending burdens, while Europe's proportion of the world's 15-24 year olds will fall from 7.7% to 6.5%. The size of the E.U. labor force is spiraling downward. Labor shortages, combined with massive debt implications, will retard economic growth for decades and have a long-term impact on European defense budgets and, by extension, NATO.[117]

POLITICAL

Russia's semi-autocratic "managed democracy" is characterized by pervasive corruption, economic inefficiencies, crumbling infrastructure, declining social services, entrenched organized crime, and rising inter-ethnic and religious violence. Governance is further complicated by the economic dominance of the oil industry and the corrupting influence of competition for control of oil-export revenues. Russia's manufacturing exports have been undermined to the point of collapse due to their poor quality and low demand. The corrosive economic climate contributes to a brain drain of young, tech-savvy professionals, with as many as 1.25 million having emigrated in the 2008-2011 timeframe to seek opportunities

outside of Russia.[118] The ability to reverse these trends will depend critically on the leadership qualities of key national leaders over the next decade. The return of Vladimir Putin to the presidency for another six years does not bode well for major changes in Russian governance. While Russia faces serious security threats along its southern borders (for which NATO assistance could be extremely helpful), Mr. Putin appears bent on erecting barriers against the West to protect the flagging legitimacy of his decades-long rule. Failure to improve Russia's governance could eventually contribute to more breakaway regions (e.g. new nations) in the Caucasus, early dominance of Central Asia by China, accession into the E.U. and/or NATO applications by the Ukraine and Georgia, and an expansion of Chinese influence/territory in Eastern Siberia.

FUTURE ARMY MISSION AREAS

PEACETIME MILITARY ENGAGEMENT

The primary mission areas for the U.S. Army in Europe will be to strengthen the existing bilateral and multilateral ties with NATO's member states, to develop closer mil-mil relations with Europe's non-NATO states, and to maintain a forward basing presence that enables rapid force projection into neighboring regions. The Army will participate in combined training and exercises with European partners to facilitate mission specialization among NATO members. For NATO's capabilities to improve through specialization, the Army may be required to provide focused training and tutelage to NATO partners in critical mission-specialization areas such as rotary-wing ground support and airlift, logistics, and field medicine. The mil-mil relationship with Turkey will become increasingly important, due to the country's role as a hub for a European missile defense network and the growth of its national power and regional influence across the Middle East. Future deterioration in Russia's security environment could eventually (post-2020) lead to increased dialogue and mil-mil relations with Russia, potentially leading to combined training or small-scale combined operations with Russian ground forces in the Arctic, the Caucasus, or Central Asia.

The U.S. Army's presence in Europe will entail continuing security risks due to the ability of terrorist operatives to transit Europe's open borders to access U.S. military targets. Since the Madrid and London bombings in 2004-2005, European law enforcement agencies had been successful in preventing further mass-casualty attacks; ironically this success ended in Norway in 2011 at the hands of an anti-Islamist extremist. Al-Qaeda and other extremist groups will continue to pursue opportunities to target U.S. installations, while European law enforcement organizations and U.S. counterterrorism intelligence programs maintain robust capabilities to defeat such plots. However, isolated attacks on U.S. military personnel in transportation hubs, restaurants, and social gatherings will remain a threat and may become more frequent if Europe experiences heightened cultural clashes between native populations and growing Muslim immigrant communities. Continuing financial crises could lead to defunding of critical European law enforcement and intelligence activities, creating greater scope for terrorist operations.

LIMITED INTERVENTION

There are no likely scenarios requiring a U.S. limited intervention over the next decade. Later in the forecast period (2025-2030) there is a possibility that population declines and continuing financial weakness will seriously erode social and economic conditions in some European states, leading to

widespread collapse in civil order, failure of national governments, or humanitarian crises due to natural disasters that weakened states are unable to contend with.

PEACE OPERATIONS

U.S. involvement in peace operations may be limited to background support to European military forces in the Balkans, including transport, logistics, and communications and intelligence support. This will continue as long as the yearly UN mandate is renewed.

IRREGULAR WARFARE

U.S. Army involvement in irregular warfare in the Europe/Russia region during the forecast period appears unlikely. Only the Balkans and the Caucasus exhibit the potential for insurgent movements, and neither region currently harbors vital U.S. interests that would justify the Army being committed in a counterinsurgency role. One exception that could arise late in the forecast period would involve a request by a weakened Russia for NATO assistance to stabilize key oil producing regions upon which Europe depends.

Annex E
Africa Regional OE Conditions and Characteristics

AFRICA REGION MAP

U.S. STRATEGIC INTERESTS AND GOALS

U.S. national security objectives in Africa focus on building governance capacity to deal with its manifold threats to human security, political stability, and international commerce. The U.S. will encourage willing African partners to assume leadership roles in regional security and will work collaboratively with extra-regional partners to build security capacity.

U.S. security assistance will focus on: South Africa, a critical partner with the greatest extant capacity for assisting other states; linchpin states such as Nigeria and Kenya, where terrorist and criminal organizations pose the greatest threats to stability and U.S. interests; regional security organizations including the African Union and Regional Economic Communities (RECs); and weak and failed states such as the Central African Republic, the Democratic Republic of Congo, Liberia, Somalia, South Sudan, Sudan, and Zimbabwe. In addition to developing military capabilities, these efforts will seek to improve civil-military relations within African society by emphasizing civilian control of the military, professionalism, and the rule of law.

The U.S. military will work more closely with European allies, seeking to improve contingency response capabilities by sharing facilities, developing logistics agreements, and improving African-owned infrastructure. These measures will enable rapid deployment for security activities in theater, and a correspondingly light external military footprint via short-term deployments in theater. [119]

CONDITIONS SHAPING THE REGION

POLITICAL

The number of African countries considered electoral democracies increased from four in 1991 to eighteen in 2011.[120] Yet African governments, including new democracies, are frequently crippled by widespread corruption, legal restrictions on civil society, entrenched political leaders who repeatedly amend constitutions to extend their rule, and the historical absence of a democratic political culture. A recent wave of coups, civil conflicts, and political stalemates between opposing factions suggest a trend of democratic backsliding across the region. Weak and failed states throughout the continent contain ungoverned spaces that provide operational bases for Africa's numerous irregular threats.

SOCIAL—DEMOGRAPHICS

There are two demographic regimes at work in Africa: the first in Northern Africa (countries bordering the Mediterranean Sea) where birth rates have been declining for a generation and youth bulges are currently near or at their maximum size, creating conditions ripe for social unrest and revolt, as has taken place in Tunisia, Libya, and Egypt. By 2035 Northern Africa's under-25 population will fall from 51% to 40% of total population; this should lead to greater political stability and higher economic growth. The second demographic regime is in Sub-Saharan Africa, where UN population growth forecasts exceed 2.0% per annum through 2035, with the majority of the population under age 25 through the year 2050. Sub-Saharan Africa's global share of 15-24 year olds will increase from 14.3% to 23.3% over the forecast period.[121] Under these circumstances, mega-cities will continue to grow rapidly, poverty will persist, and governments will struggle to provide basic services. Insurgent and terrorist groups will seek to exploit these conditions: competing with the state to provide social services; employing violence to intimidate political opposition; using terror attacks to provoke external actors into delegitimizing military interventions; and aggressively recruiting among the region's youth.

MILITARY

Irregular threats in Africa include standing militias and insurgent groups with conventional military capabilities, well-organized and well-equipped terrorist groups, pirate groups deeply embedded in local communities, and drug-trafficking organizations (DTOs) and other smuggling organizations with a broad range of land, maritime, and aviation mobility assets. These threat groups catalyze and participate in interstate conflicts such as the Second Congo War, which eventually involved eight African nations and claimed over five million lives from 1998-2003.

Islamist terrorist groups are a persistent, evolving threat to security and stability in the Trans-Sahel and the Horn of Africa. Al-Qaeda in the Islamic Maghreb (AQIM) has been contained by a decade-long Algerian COIN campaign, but still maintains approximately 1,000 fighters operating in Algeria, Mali, Mauritania, and Niger.[122] AQIM employs small arms and IEDs in ambushes on Algerian government security forces, while its southern battalions operate across wide reaches of the Sahara and the Sahel in

machine gun-armed civilian trucks. The group continues to finance itself with criminal activities including provision of safe passage for smugglers and kidnapping for ransom. Western hostages seized in the poorly-policed Sahel states have been especially lucrative for AQIM, allowing it to provide support to other terrorist groups, such as Boko Haram. This homegrown Nigerian group, also known as the Nigerian Taliban, maintains a political goal of overthrowing the government and imposing *Sharia* law across the country. A heavy-handed crackdown by the Nigerian military caused serious losses to the group in 2009 but generated sympathy and support from conservative social elements in the Muslim community. In 2010-2011 Boko Haram rebounded, greatly increasing its operational tempo and targeting police officers, government officials, and Nigerian Christians.

Al-Shabaab is a clan-based Islamist militant group that employs conventional, insurgent, and terrorist tactics against the weak Somali government, African Union peacekeeping forces, and Western civilian targets in the Horn of Africa. In 2006, al-Shabaab took over most of southern Somalia and the capital of Mogadishu; five years later it still controls large swaths of the country. Al-Shabaab also has ties to al-Qaeda, many of its members are believed to have trained and fought in Afghanistan, and it has several hundred foreign fighters within its ranks.

Despite significant international commitment, pirate groups in the Horn of Africa comprise a major threat to shipping, and the extent of their predations has grown. Somali pirates are attacking along the Kenyan and Tanzanian coasts, extending their operations into the Mozambique Channel, and striking as far east as India's exclusive economic zone. In April 2011, at least 50 hijacked vessels were in pirate hands, along with over 750 hostages.[123] Piracy has also grown into a thriving business in the Gulf of Guinea, placing the flow of important oil exports at risk. The Gulf of Guinea produces more than three million barrels of oil a day (roughly 4% of global production) and, together with Angola and the waters off Congo, is expected to supply up to one-quarter of all the United States' imported oil by 2015.[124] In 2009, 28 pirate incidents were reported in Nigerian waters and smaller numbers of incidents (one-three per country) occurred off the coasts of Guinea, Cote d'Ivoire, Ghana, Togo, Benin, Cameroon, and the Democratic Republic of the Congo.[125]

Transnational DTOs have expanded their operations in Africa over the past decade in response to growing narcotics demand in Europe and increasing interdiction of alternative routes. DTOs now manage a sophisticated "portfolio" of trafficking platforms, routes, and methods, constantly adapting to law enforcement efforts. In Africa these include: maritime platforms including cargo vessels, fishing boats, and high-speed powerboats; aviation assets ranging from single-engine light aircraft to multi-engine jetliners; land-based shipments moved by trucks across traditional Saharan caravan routes; and large numbers of drug "mules"—individuals who carry or ingest small amounts of drugs for transport via airlines or passenger vessels. Insurgent and terrorist groups are increasing their involvement with DTOs, receiving payments for drugs transiting their operating areas or actively providing security for drug shipments.

POLITICAL—CHANGING INTERNATIONAL DISTRIBUTION OF POWER

China, India, and several other external powers have dramatically increased their economic, political, and military involvement in Africa as a means to expand their access to important strategic resources. Over the last decade China has signed a string of multibillion-dollar deals with African nations to build highways, schools, hospitals, and other infrastructure in return for rights to African minerals and oil reserves. China's investments and mineral-rights agreements span the continent, supported by a rapidly expanding volume of financing targeted by the Chinese government's five year plans.[126] India's

economic ties with Africa have largely been led by the private sector, with the Indian government focused on diplomatic initiatives designed to gain African support for a permanent Indian seat on the United Nations Security Council while also posturing itself for access to the natural resources it needs to fuel its economic development.

China has developed close military ties with many African states, including Chad, the Central African Republic, Congo, Liberia, Nigeria, Senegal, Sudan, and Zimbabwe. From 2003 to 2006, China's arms sales to Africa made up 15.4% ($500 million) of all conventional arms transfers to the continent, including weapons sales to Burundi, Equatorial Guinea, Eritrea, Ethiopia, Sudan, Tanzania, and Zimbabwe.[127] From 2007 to 2009, China was the largest source of arms exports to sub-Saharan Africa; 72% of Sudan's arms imports come from China.[128] In recent years, Sudan has built several weapons factories with assistance from China, and its domestic arms production has become a major source of small arms and light weapons for other African countries such as Chad, Eritrea, Ethiopia, Somalia, and Uganda.[129] India has also begun to expand its military presence in Africa by signing defense cooperation agreements with Kenya, Madagascar, Mozambique, and the Seychelles, due in part to concerns over Chinese expansionism.[130] Over the past decade, U.S. mil-mil relationships have expanded in many of the countries listed above. For example, the U.S. has made significant investments in Nigeria's security forces, seeking to develop their capacity to lead regional stabilization efforts, perform counterterrorism missions, and secure Nigeria's oil industry. Any future crisis response in Nigeria would require careful analysis of China's interests, presence, and role in the crisis.

PHYSICAL ENVIRONMENT

African nations with large concentrations of exportable mineral wealth often find themselves cursed by it; natural resources have been a causal factor in many armed conflicts over the last decade, both as a motive and as a funding source for violence. Revenues from mineral wealth are used to build the personal fortunes of corrupt leaders, to buy political support that entrenches corruption, and to finance armies and insurgents that fight for control of the resources. Throughout Africa, the potential for conflict over access to water will continue to increase over the forecast period, as populations grow and scarce water sources shrink. The most prominent example is the Nile River, where Egypt will advance its claims for a majority of the river's flow, while Sudan and other upstream nations will have increasing needs to develop the Nile for local economic advantage.

Africa's vulnerability to drought and famine, along with the decline in fresh water availability and arable land, has led to numerous humanitarian crises in recent decades. These crises are frequently initiated or exacerbated by armed conflicts that disrupt agricultural cycles and/or create large refugee populations. Continued violence in Darfur can be traced back to climate change and water shortages, as disappearing pasture and evaporating water holes sparked deadly disputes between nomadic Arab cattle herders and black African farmers. Approximately 27% of the world's degraded land is located in Africa, with much of the cultivable land now degraded due to erosion, deforestation, and desertification; land degradation is now of major concern to 32 countries in Africa.[131]

FUTURE ARMY MISSION AREAS

PEACETIME MILITARY ENGAGEMENT

The Army's primary mission in Africa over the forecast period will be to conduct training to develop African military capabilities for combating the wide range of irregular threats in the region. Training requirements will include basic light-infantry combat skills, communications, maintenance, logistics, and familiarization with U.S.-provided weapons, vehicles, and equipment. Training and materiel assistance must be tailored to accommodate the logistical realities facing host-nation forces, such as shortages of facilities, spare parts, fuel, ammunition, and other supplies. A recurring requirement will be to improve African forces' performance as members of regional and UN peacekeeping missions.

Coincident with these mission-focused goals, the Army will be involved in broader efforts to improve the professionalism of African militaries, including respect for civilian authority, human rights, and private property. Previous efforts to build security capacity in Sub-Saharan Africa offer few examples of durable improvement; sustained effort and innovative new methods will be required. African states require assistance in simultaneously increasing the professionalism and capabilities of military forces, border guards, police, courts, and civil administrations. Holistic reforms of this type will require Army personnel to coordinate their work with joint, interagency, intergovernmental, and multinational partners, and to integrate with interagency, bilateral, and multilateral assistance efforts.

LIMITED INTERVENTION

Humanitarian Assistance

Droughts, crop failures, civil conflicts, and other disasters will continue to trigger famines, ethnic cleansing, forced migration, and epidemics in Africa. International relief efforts may require security assistance for protection against irregular threat groups. Although deployments of Army maneuver elements to Africa for these missions would face serious political obstacles, the presence and participation of small detachments of U.S. trainers, advisors, and logistics support troops would not. In the absence of sustained improvement in African public-health measures, these Army personnel could face the threat of contact with new pathogens for which immunizations and treatments do not exist.

Counter-Piracy

Piracy threats in the Horn of Africa and the West African littoral have the potential to grow if governance and security capacity in fragile regional states deteriorate. Eventually the piracy threat could require outside intervention to eradicate pirate shore bases, requiring the Joint force to embed military advisors, conduct persistent surveillance and raids, or temporarily occupy base areas. Such operations would occur in austere, arid/jungle environments, in pursuit of elusive, irregular adversaries embedded in local clan structures.

PEACE OPERATIONS

In the aftermath of Operation Provide Relief/Restore Hope in Somalia from August 1992 to March 1994, there was a marked decline in U.S. participation in UN peacekeeping missions worldwide, especially in Africa. The failure of the Somalia mission led to a reevaluation of the proper employment of U.S. forces, as stated by Secretary of State Colin Powell in testimony to Congress; "It is often best to use American

GIs for the heavy lifting of combat and leave the peacekeeping to others."[132] However, the U.S. has provided critical airlift, sustainment, and technical support to subsequent UN peacekeeping missions, and these requirements can be expected to increase as African forces assume greater responsibility for African peacekeeping.

IRREGULAR WARFARE

Extended COIN operations on the African continent would be problematic due to the absence of direct threats to vital U.S. interests. However, a successful mass-casualty terrorist attack on the U.S. Homeland or overseas installations by an Africa-based terrorist organization could change this calculation. COIN operations in Africa would involve many of the same challenges as current operations in Afghanistan: providing sufficient force densities to secure local populations; building indigenous security forces from a very low level of capability; bolstering weak governments with little political legitimacy; protecting U.S. forces from mechanical ambushes and improvised rocket munitions; and rapidly acquiring knowledge of local culture, language, and customs.

MAJOR COMBAT OPERATIONS

There are few obvious scenarios relating to possible U.S. Army involvement in major combat operations in the Africa region, as vital U.S. interests are at minimal risk and there are few serious full-spectrum threats. The most likely case would be a government stabilization operation in Nigeria to counter an expansion of transnational terrorism in the region.

Annex F
Central and South America and the Caribbean Regional OE Conditions and Characteristics

CENTRAL AND SOUTH AMERICA AND THE CARIBBEAN REGION MAP

U.S. STRATEGIC INTERESTS AND GOALS

The U.S. security strategy in the region of Central and South America and the Caribbean is based on promoting regional security mechanisms (e.g. the South American Defense Council) and emphasizes Brazil's role as a vital U.S. security partner and leader on regional issues. The principal security threats are drug trafficking organizations (DTOs), insurgent movements, terrorist groups, and the potential for collaboration between them. Other critical security issues include border and coastal security (focused on illicit trafficking and WMD interdiction), outbreaks of social unrest and political instability, humanitarian assistance, and disaster relief. The U.S. military will seek to maintain a limited presence

throughout the region, improve mil-mil relationships, and support development of U.S. interagency capabilities to address security issues.

Through these international and interagency partnerships, the U.S. will seek to deny safe havens to narco-terrorist groups in the Northern Triangle (Guatemala, Honduras, and El Salvador), the cocaine producing regions of the Andean range, and the Tri-Border Area of Argentina, Brazil, and Paraguay. Security assistance to capable, willing partners like Colombia will be integral to U.S. efforts to enhance regional security. Efforts by hostile outside actors (i.e. Iran and its Hezbollah proxies) to disrupt regional stability and threaten U.S. interests may pose special challenges over the forecast period and require adjustments to U.S. regional strategy and force posture. [133]

CONDITIONS SHAPING THE REGION

MILITARY

The region has seen the comingling of a dangerous mix of irregular threats, including DTOs, communist insurgencies, and Islamist terrorist groups, some being supported by state sponsors such as Venezuela, Cuba, and Iran. Major DTOs generate multi-billion dollar revenue streams, leftist insurgencies maintain large formations of trained guerillas, and Islamist terrorists have access to global facilitation networks and decades of expertise in terrorist tradecraft. Future combinations of these threats could seriously threaten vital U.S. interests over the forecast period. These threats are complicated by state sponsors that provide passports and other legal documents, access to international arms markets, international transportation and communication services, public media outlets, and potential access to WMD. Finally, the mountainous jungle terrain through much of the region provides cover and concealment for illicit activities and insurgent formations while imposing additional costs and logistic challenges to security forces.

The Fuerzas Armadas Revolucionarias de Colombia (FARC) and another loosely aligned Marxist group, the Ejercito de Liberacion Nacional (ELN), have waged a decades-long insurgency against the Colombian state. In the late 1990s, Colombia was on the brink of collapse from the predations of these guerilla movements, with the Colombian Army and National Police frequently suffering the annihilation of platoon- and company-size garrisons and patrols to thousand-strong FARC columns. The guerillas were far more mobile than government forces, well-trained, and equipped with small arms and highly destructive improvised mortars originally developed by the Irish Republican Army (IRA). Countervailing violence from a coalition of right-wing paramilitaries—the Autodefensas Unidas de Colombia (AUC)—further eroded the legitimacy of the Colombian government; both left- and right-wing militants preyed on civilian populations through kidnapping, torture, and mass executions while collaborating with DTOs to supplement their finances.

A successful COIN campaign was launched against the FARC and ELN during the administration of Colombian president Alvaro Uribe (2002-2010). Previous U.S. support had been strictly limited to drug-interdiction missions, but in March 2002 the George W. Bush Administration acknowledged the linkage between the insurgents and drug trafficking, expanding U.S. assistance to support developments in the Colombian military's airmobile, riverine, intelligence, and logistics capabilities.[134] Insurgent strength declined from 20,000 to fewer than 10,000, several senior leaders of the FARC were captured or killed during this period, and large segments of the AUC were demobilized.[135] Yet the FARC has weathered this storm and maintained a steady tempo of operations, adopting a new force posture of smaller units able

to operate in close proximity to police stations and military bases, and returning to the employment of car bombings, hit-and-run attacks, and IED ambushes against security forces.[136] The FARC has developed cross-border safe havens in Venezuela and Ecuador, sought collaborative relationships with diverse terrorist groups including Hezbollah, the Basque separatists of the Eusakdi Ta Askatasuna (ETA), and the IRA and received significant assistance from the Chavez regime. [137]

The group has also pursued an aggressive international information campaign against the Colombian state and U.S. security assistance, courting public sympathies and leftist political supporters in the region, Europe, and the United States.[138]

Regional DTOs are continuously evolving in response to changing security measures, drug markets, social conditions, and technological advances. During the 1980s and 1990s, Colombian DTOs sought to avoid incidents that would provoke the United States, as extradition to the U.S. was one of the greatest threats to their leaders. The Medellin and Cali cartels sought to mitigate this threat via corruption by bribing public officials and other influential elites; directed violence and assassination was used against those who could not be bought off.[139] Eventually the government developed effective intelligence methods—with assistance from U.S. agencies—and captured or killed several generations of cartel leadership. There have been only temporary reductions in the amount of cocaine cultivation and processing, however, while DTOs have continually reconstituted and reestablished their trafficking routes and financial networks. DTOs have adopted several generations of smuggling technologies including light aircraft, powerful speed boats, long-range diesel semi-submersibles, "narco-torpedoes" towed by fishing boats, fully-functional submarines, and sophisticated tunnels beneath the U.S.-Mexican border.

The Islamist terrorist threat in the region has been slow to develop, limited by a lack of large Muslim populations to hide the activities of militants, and perhaps by strategic patience on the part of terrorist leaders. But recent events provide clear signals of a growing threat: Colombia's arrest of Hezbollah money launderers working with the FARC; Turkey's seizure of Iranian explosives manufacturing equipment bound for Venezuela; and the Iranian Quds Force plot to hire Mexican DTO assassins to target Saudi Arabia's ambassador to the United States.[140] While the nominally Shia threat of Hezbollah has garnered the most attention, extremist Sunni elements sympathetic to al-Qaeda have also engaged in sustained proselytizing and recruiting efforts in the region over the past decades. A future combination of Iranian nuclear weapon proliferation, political support from regional insurgencies or states, and DTO smuggling technology and expertise could create a threat vector to the Homeland that would require major changes to the U.S. security posture in the Western Hemisphere.

POLITICAL

At the same time these threats are developing, the corrosive effects of the drug trade are undermining governments and civil society in the region, especially in the Central American transit zone for cocaine shipments to the United States and Europe. In sharp contrast to global trends of declining violence, homicide rates in the region increased from 19.9 per 100,000 people in 2003 to 32.6 in 2008.[141] The governments of Guatemala, Honduras, and El Salvador have been gravely compromised by DTO corruption and violence. New commercial real estate in Guatemala City has an occupancy rate of 25%—a telling indicator of large-scale money laundering—while homicide rates in the Northern Triangle rose to approximately 57 per 100,000 population in 2010 (in the U.S. the rate was 4.6).[142] Although regional governments score relatively well on national-level governance indices, these metrics conceal the

existence of many localized "black holes" throughout the region where the hand of government does not extend.

Brazil's perennial status as the "next" great power is coming to an end; the country is rapidly emerging as a leader in global affairs. Major offshore oil fields have fueled a rapid growth in state resources: since 2005 Brazil's annual growth in military spending has exceeded 10%. The country's 2008 National Defense Strategy articulates an ambitious 20-year plan to modernize the armed forces: spending on new and upgraded equipment; making strategic investments in cyber, space, and nuclear technologies; and laying the foundation for power projection capabilities.[143] A further objective is to develop an autonomous domestic arms industry through strategic foreign partnerships and technology transfers; nuclear submarines are one of the priorities for domestic manufacture. Multiple-launch rocket systems, artillery, UAVs, air defense systems, and helicopters are all manufactured domestically.

From 2001 to 2010, China's trade in this area reshaped the economic landscape of the region. China's share of the region's international trade rose from less than 5% in 2001 to approximately 15% in 2010, and the country supplanted the U.S. as the leading trade partner of Brazil, Chile, Argentina, Peru, and Uruguay. China became Brazil's leading source of foreign investment in 2010, with an estimated $12-20 billion invested primarily in the steel, oil, mining, transportation, and energy sectors.[144] In support of these economic interests, the PLA is extending its influence across the region through high-level mil-mil discussions, officer training and exchange programs, military sales, and a low-level presence of military personnel. As China's defense industries continue to expand and acquire advanced technologies, it is possible that China will seek to broaden its mil-mil relationships in the region as a basis for promoting arms exports and enhancing its overall international status.[145]

FUTURE ARMY MISSION AREAS

PEACETIME MILITARY ENGAGEMENT

The principal regional threat over the next decade will continue to be DTOs; the Army will conduct training missions in this region to develop host-nation capabilities for drug interdiction and, to a lesser extent, COIN missions. Many training requirements will mirror those in the Africa region: light infantry skills, communications, maintenance, and logistics. Development of airmobile capabilities, border monitoring, and intelligence collection and sharing will also be important given the physical environment of the region. The U.S. must support host-nation forces in developing indigenous doctrine and force structure to perform these missions, in order to build sustainable security capacity that will endure beyond periods of intensive U.S. engagement.

The DOD was assigned as lead agency for the detection and monitoring of drug trafficking into the U.S. by the Defense Authorization Act of 1989; these responsibilities are best executed through joint interagency intelligence fusion centers that develop actionable intelligence for law enforcement agencies and foreign partners. Intelligence drives operations through a shifting coalition of civilian and military organizations that face the challenge of pursuing DTO operations across national and international jurisdictions, with diverse legal authorities and technical capabilities. Army personnel assigned to these activities must have a broad base of work experience and the flexibility to function collaboratively in a non-military work environment.

The 2010 signing of defense cooperation and classified information-sharing agreements between Brazil and the U.S. signals both countries' intent to help secure regional prosperity and stability through transparent and collaborative security measures by the Western Hemisphere's largest military establishments. Over time, the Army will be required to develop more robust institutional ties with its Brazilian counterparts, involving combined training and exercises, student exchanges, technology and information sharing, and the potential for more combined military operations such as the Haitian relief effort of January 2010.

LIMITED INTERVENTION

By 2020 it is possible that anti-U.S. terrorist groups will develop working relationships with insurgent groups in this region, allowing them to establish an operations infrastructure in remote jungle areas and large urban centers of the Caribbean basin from which attacks can be launched against the U.S. Homeland, the Panama Canal, and U.S. interests throughout the region. Early detection of such threats is imperative and will require thorough intelligence preparations in the region. Preemptive action would also be dictated to eliminate such threats, either unilaterally or through combined raids or strikes. Effective information operations that establish the legitimacy of preemptive counterterrorism measures by the U.S. will be vital to ensure that insurgent and terrorist groups don't gain strength due to political backlash against the U.S.

This region is vulnerable to a range of natural disasters; many states lack the capacity even to coordinate international disaster relief. SOUTHCOM has been involved in humanitarian assistance operations in more than ten regional countries in the last five years, responding to earthquakes, flooding, hurricanes, and a volcano. Due to geographic proximity, these missions may involve higher proportions of U.S. resources, longer mission durations, and more intensive joint, interagency, intergovernmental, and multinational collaboration.

PEACE OPERATIONS

Interstate conflicts have been rare in this region and there are no obvious reasons for this to change over the forecast period. However, the potential exists for a very weak or failed state to experience civil war, potentially drawing neighboring states and international organizations into peacekeeping and post-conflict stabilization missions. Potential contingencies include Central American states overcome by DTO corruption and violence, and succession crises in leftist authoritarian regimes in Cuba or Venezuela. The U.S. would encourage Brazil, other Latin democracies, and regional organizations to assume leadership roles in such sensitive, long-term missions. However, in some contingencies U.S. participation may be essential; in such cases mission success could depend critically on Army personnel's knowledge of local culture, history, and political and socioeconomic drivers of conflict.

IRREGULAR WARFARE

The events of 9/11 highlighted the dangers of ungoverned spaces inhabited by combustible mixtures of extremists, guerillas, and drug traffickers. It is possible that Colombia will face a resurgent FARC with substantial material assistance from external sponsors; the introduction of MANPADs into the FARC's arsenal would tip the scales significantly against Colombian security forces.

MAJOR COMBAT OPERATIONS

At present there are no obvious major combat operations contingencies in the region that would involve the Army.

Annex G
North America Regional OE Conditions and Characteristics

NORTH AMERICA REGION MAP

U.S. STRATEGIC INTERESTS AND GOALS

The U.S. will seek to build regional defense partnerships to disrupt the threats of illicit trafficking and transnational terrorism, to enhance the defense relationship with Canada, and to develop a joint approach toward the security of the Arctic. Stability and security in Mexico are critical to U.S. national interests; the U.S. seeks a close partnership that improves cooperation on border security, allows early identification of threats, combats violent transnational criminal organizations, and enhances capacity for joint operations.

The U.S. military will maintain a domestic force posture that supports overseas missions, disperses critical strategic assets, secures the Homeland from attack, and provides the ability to support civil authorities and manage the consequences of natural disasters, terrorist attacks, and other domestic contingencies. The Army will continue to prepare National Guard elements for Homeland defense and defense support of civil authorities (DSCA) missions, including the creation of a Homeland response force in each of the ten Federal Emergency Management Agency regions.

The DOD will support interagency efforts to secure U.S. borders and to interdict illicit trafficking. Research efforts will focus on developing technologies that comprehensively monitor air, land, maritime, space, and cyberspace domains for early detection of threats; assistance will be provided to

Mexico and Caribbean partners for developing maritime and air capabilities to monitor their territorial waters. Improved capabilities for the standoff detection of nuclear/radiological devices will be a special area of emphasis.

CONDITIONS SHAPING THE REGION

MILITARY

The Army will face increasing challenges in maintaining its force structure and readiness in the face of a sustained Federal budget crisis, along with a decline in the pool of eligible military recruits due to negative trends in U.S. public health and education. The Army will face a critical challenge in trying to retain a cadre of combat veteran officers and NCOs after the Iraq and Afghanistan conflicts wind down, as budget pressures will present difficult choices between force structure, acquisition programs, overseas deployments, training, quality of life, and military benefits. A second critical challenge will be to maintain an intake of quality recruits while competing in a tightening labor market, screening incoming Soldiers for security risks, and developing education and fitness programs as required in preparing marginal recruits for service. National-level policy considerations may also impact Army readiness in terms of securing access to energy supplies and other critical resources, such as rare earth elements, and maintaining an adequate defense industry base.

MILITARY—IRREGULAR ADVERSARIES

Irregular threat groups that operate inside the U.S. or transit its borders pose unique challenges to the Army. Direct action against these adversaries is typically a law enforcement responsibility; however, DOD responsibilities for counterterrorism and counterdrug intelligence/interdiction require seamless collaboration between the U.S. military, law enforcement, and intelligence communities. These threat groups also have the potential to enlist their members in the Army, recruit current Army personnel, and employ extortion or corruption against service members and their families.

Mexican DTOs

Open-source reporting indicates that the number of DTO “foot soldiers” may rival that of Mexican security forces.[146]. Drug-trafficking violence, according to one source, caused over 13,000 deaths in Mexico in 2010, up from approximately 2,500 deaths in 2007.[147] The death toll for the first nine months of 2011 was already at 12,903; a number approaching, if not poised to exceed, the high point in 2010.[148]Mexican DTOs are the primary transporters of South American cocaine to the U.S. and also are the largest source of marijuana for U.S. markets and a major source of methamphetamine. In December 2006, the Mexican government began a gradually escalating campaign to capture or kill DTO leadership; like the Colombian cartels of the 1990s, they have become decentralized, less hierarchical, and more violent. Removal of DTO senior leaders spawns deadly episodes of executions and reprisals as mid-level leaders and competitors vie for control of trafficking routes. Mexican DTOs now use torture, execution, and corruption as general tools for controlling populations and local authorities, in a fashion not unlike that of many insurgent groups.

U.S. and Transnational Street Gangs

The U.S. National Gang Intelligence Center (NGIC) estimates that there are over 20,000 street gangs operating across the U.S. with about one million members.[149] The largest and most violent of these include 18th Street (50,000 members), Gangster Disciples (50,000 members), MS-13 (10,000 U.S. members, 50,000 worldwide), Crips (35,000 members), Vice Lord Nations (35,000), Bloods (30,000 members), and Latin Kings (20,000 members).[150] Mexican DTOs rely on U.S. street gangs as retail networks for much of the drugs they ship to the U.S. They have also employed members of Latin gangs such as MS-13 and 18th Street for contract killings in Mexico and Central America. A 2007 NGIC report documented multiple threats from street gang members in the U.S. military: theft of military weapons and equipment, use of military training in violent crimes against rival gangs and U.S. law enforcement officers, weapons and drug smuggling, armed robberies, and recruitment of service member dependents.[151]

Terrorists

From May 2009 to October 2011, there were 32 known terrorist plots by homegrown jihadists in the U.S.[152] The impact of this upsurge in homegrown extremism fell disproportionately on the Army; the only terrorist incidents resulting from the 2009-2010 plots were Major Nidal Hasan's attack at Fort Hood, Texas and Abdulhakim Muhammed's attack on the Army-Navy Career Center in Little Rock, Arkansas. Many law enforcement actions have disrupted targeting of military installations, including the May 2007 arrest of six men planning to attack Soldiers at Fort Dix, New Jersey with small arms, and the May 2009 arrest of four individuals who planned to shoot down military aircraft at a New York Air National Guard base with Stinger missiles. These types of small group and lone wolf attacks will continue to pose a threat to military installations and personnel over the forecast period.

FUTURE ARMY MISSION AREAS

PEACETIME MILITARY ENGAGEMENT

The severity of the future threat from DTOs, terrorist groups, and street gangs will drive the scale of engagement with the Mexican military. This will continue to involve targeted training to develop counternarcotics and raid capabilities, and could expand to include regular joint exercises focused on border security. Achieving the U.S. national security goal of early threat detection through comprehensive monitoring of maritime, land, air, space, and cyberspace domains will require increasing levels of intelligence sharing, data fusion, and analysis. This mission is best performed by Joint Interagency Task Forces (JIATFs) focused on border security and counternarcotics missions. Army formations supporting these missions (e.g. National Guard or Military Police units supporting the U.S. Border Patrol) would be linked to the JIATF communications and coordination architecture to facilitate intelligence-driven joint, interagency, intergovernmental, and multinational operations.

Engagement with the Canadian military will include a focus on creating an integrated security architecture for the Arctic region. New basing infrastructure will be needed to support air defense, maritime surveillance, land patrols, search and rescue, and environmental disaster response missions.

LIMITED INTERVENTION

Over the forecast period it is possible that Mexican DTOs will present imminent threats or engage in large-scale violence against U.S. citizens within Mexico's borders. It is feasible that they could act in concert with extremist jihadist organizations or U.S. street gangs to engage in violence on U.S. soil, supported from bases in Mexico. In such contingencies the Army could be called on to conduct limited interventions, including non-combatant evacuation operations, hostage rescues, or raids against imminent armed threats. Such contingencies would involve extreme political sensitivities surrounding issues of Mexican sovereignty, legal authorities, and jurisdictions of Mexican and U.S. law enforcement agencies. Such interventions might only be allowed under the terms of explicit international agreements with the Mexican government, requiring combined operations and highly restrictive rules of engagement.

PEACE OPERATIONS

There are no obvious contingencies involving peace operations in the North America region over the forecast period.

IRREGULAR WARFARE

The only feasible irregular warfare contingency in the region would involve a request by the Mexican government for assistance in restoring government authority over Mexican territory that had fallen under DTO control.

MAJOR COMBAT OPERATIONS

There are no obvious contingencies leading to major combat operations in the North America region during the forecast period.

DEFENSE SUPPORT OF CIVIL AUTHORITIES

Defense support of civil authorities could involve the U.S. Army providing support following domestic disasters (man-made or natural) or a WMD event. A more difficult DSCA operation would involve direct support to local law enforcement during an episode of massive civil disorder, which could result from a terrorist attack or a financial and organizational collapse of local government. The 1992 Los Angeles riots (54 dead, over 2,300 injured, and over 5,000 fires set) provided an important example that required intervention by military forces under Executive Order (i.e. permitting the U.S. military to function as a posse comitatus in support of law enforcement agencies). Should such operations be required in the future, important lessons from 1992 would include: the need for a more rapid response by local National Guard forces; a clear understanding of the legal ramifications of the 1876 Posse Comitatus Act (which did not apply during the federal response to the L.A. riots due to the Executive Order); more flexibility by commanders providing direct support to law enforcement; and the potential for future interventions to face an organized armed threat from street gangs, DTOs, or other organized criminal elements.[153]

Annex H
Additional Adversarial Designs and Capabilities

In addition to implications for the U.S. Army, conditions across the strategic environment also impact adversarial designs and capabilities. This section will explore the most significant adversarial responses across U.S. warfighting functions. Two major features of the SE are the adaptation of adversary designs to counter the strengths of U.S. forces, and the gradual leveling of military capabilities across all of the warfighting functions. Over the next decade this could lead to the Army facing overmatch in multiple areas. Adversarial designs presented below are median threats that aggregate across a range of potential adversaries and therefore are not representative of any specific nation-state or non-state actor. Similarly, no single adversary is investing in all the capabilities discussed below, yet the Army must prepare for all technological threats that could adversely affect its conduct of decisive operations.

MOVEMENT AND MANEUVER

Strategically, potential adversaries will deploy a range of weapon systems and other technologies that directly threaten U.S. strategic mobility assets and staging areas. Readily available commercial imagery and omnipresent media sources provide early warning of U.S. actions that will become increasingly difficult to elude. Proliferating capabilities such as precision-guided munitions, UAVs, spaced-based sensors, anti-satellite and electronic warfare capabilities, sea mines, cruise missiles like the YJ-83 and RS SS-N-27, Akula-II and Kilo class submarines, longer-range missiles like the Chinese DH-IO and the Russian Club K, and long-range air defense systems will contribute to a greater strategic access challenge in any region.[154]

Operationally, the U.S. Army maintains overmatch in movement and maneuver, mainly as a result of investments in rotary-wing aviation and mobile protected fires; much of this capability resides in Joint partners. Potential adversaries are investing in capabilities to counter this advantage by increasing the lethality of their systems, improving their situational awareness, and increasing their own mobility, then incorporating these capabilities into operational designs such as Iran's "mosaic" defense doctrine. Adversaries will position forces to launch rapid precision attacks against sea/aerial ports of debarkation (SPOD/APOD), staging areas, and intra-theater lift platforms to interrupt the flow of logistics and follow-on forces.

Access denial depends on threat capabilities that have operational reach, such as medium-range ballistic and cruise missiles, special operations forces, WMD, and cyber capabilities. As early as 2020, the Army may face increasingly capable UAV platforms like the Chinese ASN 206 that employs a GPS jammer, long-range precision strike systems such as the Chinese DH-10, a Tomahawk-like land attack cruise missile, and the Russian AS-18 KAZOO air-to-surface missile. Proliferation of long-range air defense systems such as the Russian SA-20 and the more advanced SA-21—which has an estimated engagement range of 250 miles—could present significant challenges as adversaries attempt to exclude or limit U.S. access to areas where the Army is forced to deploy by air.[155]

At the tactical level, potential adversaries recognize U.S. strengths in ground and rotary-wing maneuver and will look to counter this advantage through employment of large under-vehicle IEDs and anti-helicopter mines. Adversaries will vary the tempo and intensity of their operations to disrupt U.S. and coalition operations and exploit unique environmental conditions that are unfavorable to our combat

systems. They will employ advanced technologies secured from third-party nation-states, like the long-range tandem warhead, Russian KORNET ATGM. Adversaries will use commercial technologies such as 2nd and 3rd generation night vision devices, similar to the French Sophie-MF handheld thermal imager, offsetting U.S. advantages in night operations. They will employ tactical UAVs similar to the Chinese BZK-005 or micro-UAVs like the Japanese TRDI to increase their situational awareness and to target U.S. and coalition forces. Threats will also employ small, portable electronic jammers, like the Russian Eksiton jammer, to degrade U.S. GPS-enabled systems.[156]

MISSION COMMAND

Potential adversaries have observed the U.S. Army's increasing reliance on communications. Therefore, part of their preclusion strategy will be the development of capabilities to deny the Army access to the global information grid. Such a capability would limit the Army's efforts to coordinate operations, provide logistics support, and conduct information operations. Adversarial conduct of strategic mission command will focus on enabling simultaneous operations, fracturing coalitions, and executing integrated and continuous information campaigns. Greater investments in cyber and electronic warfare, special-purpose forces, and space-based capabilities including anti-satellite weapons and satellite communications jammers will impact Army operations in any major overseas contingency well before 2028.

The most significant operational challenge to the Army is in the area of mission command. Adversaries will seek to disrupt and degrade joint, interagency, intergovernmental, and multinational (JIIM) unity of command through a variety of means, including cyber operations and electronic warfare. The presence of multinational corporations, NGOs, terrorist organizations, religious movements, political factions, and organized criminal enterprises will further complicate the conduct of operations. Adversaries will work to identify and attack critical linkages and seams in coalitions, in an attempt to fracture coalitions, and to deter non-coalition parties who are assisting or cooperating with JIIM operations. NGOs, U.S. military contractors, and private security forces are particularly attractive targets due to the potential IO benefits for the adversary of attacking foreigners.

Adversaries are gaining parity in the conduct of integrated information campaigns, including cyber operations. Some adversaries have already conducted progressively more complex cyber attacks integrated with military operations. Russia and China have made significant efforts to integrate cyber capability and units into their force structure at the operational level. Other challenges arise from continued U.S. reliance on commercial software, the potential for introduction of malware into U.S. systems by overseas vendors, and the ever-present threats from trusted insiders and lax security practices.[157]

Recognizing the Army's reliance on the electromagnetic spectrum, potential adversaries have invested heavily in the full spectrum of electronic warfare capabilities. Threats may exploit advances in microelectronics, digital memory, and jamming capabilities. SATCOM jamming capabilities are already fielded and have been demonstrated. Several nations are developing digital radiofrequency memory (DRFM) jammers that can take down radar and communications signals. Spread spectrum jammers that target frequency-hopping and direct sequence-encoding communications devices will become available over the next decade.

At the tactical level, adversaries will seek capabilities to intercept U.S. and coalition communications; along with spread spectrum jammers to disrupt tactical communications and degrade U.S. combined

arms synchronization. The use of short-range electromagnetic pulse weapons, artillery, and rocket-delivered radio frequency jammers will deny or degrade U.S. and coalition use of surveillance sensors, communications, and computer systems. Adversaries will use ethnic and religious opportunities—such as services at Friday mosque, painting simple slogans on building walls, and encouraging hackers to carry out cyber attacks through host-nation computers to support perception management operations—as components of an integrated information warfare campaign.[158]

INTELLIGENCE

Adversary human intelligence (HUMINT) capabilities may equal or exceed U.S. capabilities in many theaters of operations. Other methods being touted to counter U.S. technical intelligence dominance include employing commercial information technology, operating among populations, and recruiting insiders over the Internet.

Adversaries will seek to exploit cultural differences between the U.S. and host-nation populations through information operations designed to alienate the local populace from U.S. and coalition forces, and to choke off the most valuable potential sources of HUMINT. Basic low-tech counters to U.S. intelligence capabilities include counter-signal GPS jammers, radar scattering, landlines, couriers, and the use of local languages. Threat actors may purchase military and commercial technology that can easily be modified for collection or analytical purposes. Examples include UAVs with multiple sensors and weapon packages, commercially-available satellite imagery, image intensifiers, first-generation forward-looking IR, computer geographic information systems, and electronic warfare technologies.

Potential adversaries recognize that the U.S. has highly capable aerial- and space-based sensors. Camouflage, concealment, and deception operations among populations are increasingly used to counter this technological advantage; conversely, threats will exploit international and local sympathizers employing secure Internet-based communications to conduct surveillance of U.S. deployments and theater movements. Potential new capabilities will include the deployment of lasers to attack reconnaissance satellites, denial of air-breathing collection using long-range SAMs, and continuing improvements to underground facilities such as those constructed in North Korea and Iran. Threat actors will incorporate commercially-available encryption systems in order to provide mission command and deny U.S. access to their intentions and plans.

In the face of superior U.S. tactical intelligence, threats will leverage the human terrain to conduct reconnaissance and deny U.S. capabilities to observe patterns and trends via technical intelligence collection. Tactical jamming and radiofrequency (RF) weapons will be employed at critical times to disrupt U.S. monitoring capabilities, especially systems like the Distributed Common Ground System Army (DCGS-A) and Tactical Ground Reporting System (TIGRnet), thereby denying situational awareness to brigade and battalion staffs. These threat capabilities will also impact U.S. logistics support by disrupting timely communications and slowing logistics unit reactions. Long-range, precision strike munitions such as the Iranian Fatah-ll0 will provide adversaries the ability to target forward operating bases and lines of communication. Threats will recruit individuals from the host-nation population to conduct terrorist activities against U.S. logistics systems, including contamination of fuel and water and theft of supplies during transit.[159]

FIRES

U.S. investments in long range conventional fires, missile defense, theater high-altitude air defense, and associated equipment are currently unmatched. U.S. investments in technical collection for a variety of intelligence functions including Homeland defense, supporting forcible entry, and rapidly realigning assets to the point of need are also unmatched by any other nation. Adversaries understand that U.S. superiority in these areas places a premium on adaptation. Cyber attacks, shielding—including the use of human shields—and first strikes are all methods for mitigating U.S. strategic fires superiority.

The U.S. will continue to enjoy an advantage in the area of fires through 2028 due to two major sets of investment: (1) air and missile defense capabilities such as the Medium Extended Air Defense System (MEADS), the Sentinel system, and the Joint Tactical Ground Station (JTAGS), and (2) fire support capabilities such as the High Mobility Artillery Rocket System (HIMARS), improvements in the Army Tactical Missile System (ATACMS), and the Guided Multiple Launch Rocket System (GMLRS).

To mitigate this advantage, adversaries will employ a wide variety of counter-precision techniques that include camouflage, concealment, and deception; GPS jamming; terminal defenses; forcing close-in fights; advanced aircraft; and extended-range precision munitions. Adversaries will seek operational shielding by exploiting civilian populations and cultural sites to hide weapons systems and shape the battlefield. They will reduce U.S. air defense system reaction times with technology such as penetration aids on missiles, low observable aircraft, and jamming. Adversaries will increasingly employ hardened and buried facilities and multispectral decoys of key operational-level targets such as SRBMs and SAMs. Many adversaries have invested in short- and medium-range missile systems, such as the Russian Smerch and Chinese PHL-03, capable of counterfires with ranges out to 150km. Improved air defense systems including counter-TBM capabilities will provide protection to these advanced fires capabilities.

Tactically, adversaries understand and respect the highly responsive and accurate indirect fires available to U.S. forces. To counter these fires they will employ simple decoys and radar corner reflectors to confuse U.S. surveillance. Threats will employ mortars, cannon, and rocket artillery with increased range munitions, like the 122mm Grad 9M218 rocket High-Explosive (HE) and High-Explosive Anti-Tank (HEAT) submunitions and GPS to improve target finding. The longer standoff will enable adversaries to accurately target logistical and forward operating bases. Adversaries will carefully plan their tactical actions to exploit complex terrain and urban areas to obtain tactical shielding and offset U.S. artillery range advantages. More capable short-range air defense systems, like the Chinese FN-16 MANPADs or SA-11/15, will enable threats to effectively target U.S. tactical UAVs and rotary-wing assets.[160]

PROTECTION

Investments in high-tech camouflage, concealment, and deception systems and increasing use of hardened and underground facilities, lasers, and GPS jammers are technological counters to U.S. intelligence overmatch being pursued by potential adversaries.

If U.S forces attain entrance into an operational theater, most threat operations will transition to a defensive posture oriented on creating excessive U.S. and coalition casualties and eroding the political will of their governments. Opponents will generally seek to avoid U.S. military firepower, instead attacking soft targets such as mission command nodes, intelligence collection systems, logistical components (APOD/SPOD/FOB), and contracted support. To protect themselves, threats will make every attempt to create chaos among the civilian and non-combatant populations to mask their movements.

Dense urban populations, protest mobs, and refugees will be exploited to conceal and shield adversary activities, overwhelming U.S. intelligence and defense support of civil authorities (DSCA) capabilities.

Technologies to overmatch U.S. protection will focus on increased lethality; longer range/stand-off, nontraditional chemical, biological, radiological, nuclear, and explosive weapons (CBRNE) agents (including fourth-generation chemicals that challenge traditional detection and decontamination methods); toxic industrial chemicals; and the use of armed UAVs. The current range of improvised munitions will grow more sophisticated, lethal, and difficult to detect over the forecast period.

SUSTAINMENT

Logistics capabilities like the Global Combat Support System-Army (GCSS-A) gives the Army unparalleled capability to sustain anywhere that it might be required to fight. Adversary strategies to counter U.S. strategic sustainment may include disruption of vulnerable logistics nodes in the Homeland, including sea and air ports of embarkation and other critical infrastructure. Cyber attacks may be employed against U.S. military networks and civilian supply chains to disrupt the smooth functioning of production facilities and logistic nodes that supply the Army.

The U.S. will maintain dominance in sustainment capabilities over the forecast period, inviting adversaries to pursue more effective means to target the entire logistics trail. U.S. forces will remain vulnerable when conducting phased entry into a theater; threats will seek to coordinate attacks on SPOD/APODs to meter U.S. entry into the area of operations. Disrupting the flow of U.S. military capabilities sets the conditions for threats to note patterns in U.S. operations, exploit the physical environment to their favor, and adapt their operations to engage soft targets including supply convoys, base areas, and host nation infrastructure. Adversaries will attempt to employ criminal organizations to slow operations in SPOD/APODs and forward movement of U.S. and coalition logistics. They will exploit cyber attacks against U.S. computer networks to further disrupt logistics operations.[161]

CONCLUSION

At the strategic level some adversaries focus on a comprehensive anti-access strategy that aims to prevent the Army from getting involved in conflicts in the first place. Potential adversaries have noted the repositioning of Army units from overseas bases to the continental U.S., along with ongoing U.S. investments in strategic mobility and joint forcible entry capabilities. One adversary response to this evolution in U.S. global force posture has been to enhance its capabilities for strategic preclusion. The first element of this strategy seeks to deter the U.S. government from making the political decision to initiate an overseas deployment. It focuses on coercing or dissuading potential U.S. allies, coalition partners, and NGOs from offering military, logistic, and political support and basing and overflight rights, as well as undermining the will of the American people to support military operations.

At the operational level the adversary's preferred design is to deny access to U.S. forces from a theater of operations through interdiction of ingress routes, denial of bases, and undermining international support. Potential adversaries will pursue access denial through diplomacy, economic threats, military coercion, and the development of operational fires capabilities. Based on their observations of recent U.S. operations, potential adversaries will use complex and urban terrain, attempt to limit U.S. mobility, separate U.S. combat formations, and neutralize U.S. technological advantages. Although their capability investments are concentrated on countering regional foes, they pose significant threats to U.S. forces, particularly in the areas of operational movement and maneuver, mission command (particularly cyber),

and protection. Even adversaries lacking defense industries may have access to weapons and technology that allow them to achieve limited, unexpected parity or overmatch in niche technologies for short periods of time. Enemies will understand U.S. strengths, leverage their superior knowledge of local physical and human terrain, and exploit U.S. rules of engagement to their advantage.[162]

At the tactical level adversary military investments are spread across a wide range of capabilities that include precision strike, survivability, and the defeat of individual U.S. systems. Adversaries will also seek to exploit lessons learned from recent operations to negate U.S. advantages in fires, technical intelligence collection, training, and logistics. Adversaries will deploy in complex urban environments, fighting among the population to challenge U.S. and coalition forces rules of engagement, create the potential to alienate host-nation populations, and generate negative international media coverage of U.S. operations. Adversaries will mass weapons systems to launch surprise strikes that inflict large numbers of casualties, again with the intent of generating media coverage. Threats will continually transition between conventional combat formations and dispersed irregular groups, focusing effects at critical times and places to diffuse U.S. and coalition employment of force.[163]

[1]Likely OEs based upon the TRADOC Intelligence Support Activity Top 10 Project February 2012. The Top 10 Project was created to provide the Army training community with a list of the operational OEs most likely to require Army brigade operations in the near- to mid-future. The list was not an attempt to determine the next location for U.S. ground troop deployment, nor is it predictive analysis reflective of a specific political policy. Instead, the Top 10 is an aid to inform the training community on the range of potential OE conditions that U.S. ground forces are liable to encounter, thus allowing commanders and trainers to focus and tailor their efforts in these areas.
[2] Quoted in "U.S. Military and Peacekeeping Operations," in *Peace Support Operations and the U.S. Military*, Barry R. McCaffery, ed. Dennis J. Quinn (Washington D.C.: Institute for National Strategic Studies, National Defense University, 1994), 3.
[3] Joint Staff J-7, *Joint Force 2030 - Evolve, Lead, Secure: Exploring Lessons of the Past and Present to Prepare for the Future,* Draft, 23 March 2012.
[4] Joint Staff J-7, *Joint Force 2030 - Evolve, Lead, Secure: Exploring Lessons of the Past and Present to Prepare for the Future,* Draft, 23 March 2012.
[5] National Intelligence Council, *Global Trends: A Transformed World*, November 2008 (accessed February 2012).
[6] National Intelligence Council, *Global Trends: A Transformed World*, November 2008 (accessed February 2012).
[7] National Intelligence Council, *Global Trends 2025: A Transformed World*, November 2008, and National Intelligence Council, *Global Governance 2025: At a Critical Juncture*, September 2010.
[8] National Intelligence Council, *Global Trends 2025: A Transformed World*, November 2008.
[9] BBC, "New Greece austerity move prompts strikes and protests," 22 September 2011 (accessed 23 March 2012); BBC, "Greece brought to standstill by anti-austerity strike," 20 May 2010 (accessed 23 March 2012).
[10] *Note*: Zaydism is a branch of Shi'a Islam that split early from what became the mainstream branch. It is endemic to Yemen.
[11] Photo from Wikimedia Commons, Yemen Protests, 3 February 2011.
[12] Stockholm International Peace Research Institute, *SIPRI Yearbook 2012: Armaments, Disarmaments and International Security Summary*, pp. 8-9 (accessed 18 June 2012).
[13] Stockholm International Peace Research Institute, *SIPRI Yearbook 2012: Armaments, Disarmaments and International Security Summary*, pp. 8-9 (accessed 18 June 2012).
[14] Joint Staff J-7, *Joint Force 2030 - Evolve, Lead, Secure: Exploring Lessons of the Past and Present to Prepare for the Future*, Draft, 23 March 2012, 2.
[15] *USSOCOM Strategic Appreciation 2: Global Synthesis, Meta-Trends and Strategic Challenges*, 5 March 2012.
[16] ARCIC, "Army 2020 Operational Environment," 23 March 2012, Briefing.
[17] ARCIC, "Army 2020 Operational Environment," 23 March 2012, Briefing.
[18]Joint Staff J-7, *Joint Force 2030 - Evolve, Lead, Secure: Exploring Lessons of the Past and Present to Prepare for the Future,* Draft, 23 March 2012, 2.
[19] Matthew Quirk, "Private Military Contractors," *The Atlantic*, September 2004 (accessed 26 March 2012); Peter W. Singer, "Peacekeepers, Inc.," Brookings Institute, June 2003 (accessed 26 March 2012).
[20] Peter W. Singer, "Humanitarian Principles, Private Military Agents: Some Implications of the Privatized Military Industry for the Humanitarian Community," Brookings Institute, 1 February 2006 (accessed 26 March 2012).
[21] Peter W. Singer, "Peacekeepers, Inc.," Brookings Institute, June 2003 (accessed 26 March 2012).
[22] Director of National Intelligence (DNI) James R. Clapper, *Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence*, 10 February 2011.
[23] Joint Staff J-7, *Joint Force 2030 - Evolve, Lead, Secure: Exploring Lessons of the Past and Present to Prepare for the Future*, Draft, 23 March 2012, 12.
[24] Joint Staff J-7, *Joint Force 2030 - Evolve, Lead, Secure: Exploring Lessons of the Past and Present to Prepare for the Future*, Draft, 23 March 2012, 12.
[25] Director of National Intelligence (DNI) James R. Clapper, *Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence*, 10 Feb 2011.

[26] Abraham M. Denmark, "Managing the Global Commons," *The Washington Quarterly*, July 2010, 167.
[27] Joint Staff J-7, Joint Force 2030 - Evolve, Lead, Secure: Exploring Lessons of the Past and Present to Prepare for the Future. 23 March 2012.
[28] Bruce W. MacDonald, *Testimony before the U.S.-China Economic and Security Review Commission on The Implications of China's Military and Civil Space Programs*, (accessed 23 March 2012).
[29] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011 (accessed 1 November 2011).
[30] National Intelligence Council, *Global Trends 2025: A Transformed World*, November 2008, 47-48 (accessed 26 March 2012); United States Secretary of Defense, *Unmanned Systems Roadmap 2007-2032*, 10 December 2007 (accessed 26 March 2012); United Kingdom Ministry of Defence, "Strategic Trends Programme Global Strategic Trends – Out to 2040, 4th Edition, 12 December 2010, 78-79, 92, 97, 132, 135-138, 141, 143-148, 154-155; U.S. Army Via Defence Talk, "Army Exploring Emerging Technologies," 14 January 2011, (accessed 26 March 2012).
[31] Rachel Morarjee, "Russia's Raw Deal Among the BRIC Countries," Telegraph, 7 February 2012.
[32] Training and Doctrine Command (TRADOC) G-2, *Army Strategic Environment 2012*, 2012.
[33] Foreign Military Studies Office (FMSO), *Economic Trends Analysis*, February 2012.
[34] National Intelligence Council, *Global Trends 2025: A Transformed World*, November 2008 (accessed February 2012), 7.
[35] United Kingdom Ministry of Defense, *Strategic Trends Programme: Global Strategic Trends – Out to 2040*, 12 January 2012 (accessed February 2012), 10.
[36] Dr. Daniel Goure, "Global Challenges in the 21st Century," Presentation to the Lockheed Martin LEAD Graduation, 6 December 2010.
[37] Population Reference Bureau, "2011 World Population Data Sheet," July 2011, 3.
[38] Population Reference Bureau, "2011 World Population Data Sheet," July 2011, 6.
[39] Population Reference Bureau, "2011 World Population Data Sheet," July 2011, 8.
[40] National Intelligence Council, *Global Trends 2025: A Transformed World*, November 2008, 19.
[41] National Intelligence Council, *Global Trends 2025: A Transformed World*, November 2008, 19.
[42] Director of National Intelligence (DNI) James R. Clapper, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence*, 31 January 2012, 9.
[43] National Intelligence Council, *Global Trends 2025: A Transformed World*, November 2008 (accessed 19 March 2012), 21.
[44] Dr. Christopher Rice, *Demographic Analysis of the Operational Environment*, TRADOC G-2.
[45] USAID, *Nigeria Strategy 2010 - 2013*, 4.
[46] Lucy Sherriff, "Germans claim first programmable computer," The Register, 2 June 2004 (accessed 23 March 2012).
[47] BBC, "India census: Half of homes have phones but no toilets," 14 March 2012 (accessed 23 March 2012).
[48] *USSOCOM Strategic Appreciation 2: Global Synthesis, Meta-Trends and Strategic Challenges*, 5 March 2012. 47.
[49] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011 (accessed 1 November 2011), 1-2.
[50] Mathew J. Schwartz, "Iran Hacked GPS Signals to Capture U.S. Drone," InformationWeek, 16 December 2011 (accessed 23 March 2012); Jeff Hecht, "Did Iran capture U.S. drone by hacking its GPS signal?" One Per Cent, 16 December 2011 (accessed 23March 2012).
[51] National Intelligence Council, *Global Trends 2025: A Transformed World*, November 2008 (accessed February 2012), 7.
[52] Kerri Shannon, "China's Highway System Growth Paves the Way to a Stronger Economy," Money Morning, 1 April 2011 (accessed 5 April 2012).
[53] BBC, "China opens coffers for minerals," 18 September 2007 (accessed 5 April 2012).
[54] USDA, "Southeastern Anatolia Project (GAP)," 20 November 2003 (accessed 22 March 2012); Julia Harte, "Turkish Water Projects Stirring Resentment Around The Region," Green Prophet, 1 November 2011 (accessed 22

March 2012); BBC, "Chile court rules in favour of Patagonia HidroAysen dam," 04 April 2012 (accessed 5 April 2012).
[55] Sahr Morris Jr, "Sierra Leone: Information Ministry Launches Fiber Optic Cable Project Today," AllAfrica, 2 September 2011 (accessed 5 April 2012).
[56] Ed Barnes, "Chavez Seals Arms-for-Oil Deal With 'Europe's Last Dictator'," FOX News, 21 March 2010 (accessed 21 March 2012); Bruno Waterfield, "European Union to lift ban on Zimbabwe's 'blood diamonds' despite torture claims," The Telegraph, 08 August 2011 (accessed 21 March 2012); Stephanie Ginter, "WTO Lawsuit Over China's Rare Earths," Energy & Capital, 15 March 2012 (accessed 21 March 2012).
[57] John Vidal, "Warning: extreme weather ahead," The Guardian, 13 June 2011 (accessed 22 March 2012); Justin Gillis, "Scientists perplexed by weird weather patterns," The Seattle Times, 23 January 2011 (accessed 22 march 2012).
[58] USDA, "Southeastern Anatolia Project (GAP)," 20 November 2003 (accessed 22 March 2012); Julia Harte, "Turkish Water Projects Stirring Resentment around the Region," Green Prophet, 1 November 2011 (accessed 22 March 2012).
[59] U.S. Energy Information Administration, "Arctic Oil and Natural Gas Potential," 19 October 2009 (accessed 22 March 2012); Shigeki Toriumi, "The Potential of the Northern Sea Route," ChuoOnline, 28 February 2011 (accessed 22 March 2012).
[60]Likely OEs based upon the TRADOC Intelligence Support Activity Top 10 Project February 2012. The Top 10 Project was created to provide the Army training community with a list of the operational OEs most likely to require Army brigade operations in the near- to mid-future. The list was not an attempt to determine the next location for U.S. ground troop deployment, nor is it predictive analysis reflective of a specific political policy. Instead, the Top 10 is an aid to inform the training community on the range of potential OE conditions that U.S. ground forces are liable to encounter, thus allowing commanders and trainers to focus and tailor their efforts in these areas.
[61] Director of National Intelligence, James R. Clapper, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community or the Senate Select Committee on Intelligence*, 31 January 2012.
[62] Director of National Intelligence, James R. Clapper, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community or the Senate Select Committee on Intelligence*, 31 January 2012.
[63] Remarks by Ambassador Harry K. Thomas, Jr. at the National Renewable Energy Program Launch, 14 June 2011.
[64] Director of National Intelligence, James R. Clapper, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community or the Senate Select Committee on Intelligence*, 31 January 2012.
[65] Director of National Intelligence, James R. Clapper, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Committee on Armed Services*, 16 February 2012.
[66] Director of National Intelligence, James R. Clapper, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Committee on Armed Services*, 16 February 2012.
[67] Director of National Intelligence, James R. Clapper, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Committee on Armed Services*, 16 February 2012.
[68] Director of National Intelligence, James R. Clapper, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Committee on Armed Services*, 16 February 2012
[69] Michael C. Horowitz and Dan A. Shalmon, *The Future of War and American Military Strategy*, 23 February 2009.
[70] *USSOCOM Strategic Appreciation 2: Global Synthesis, Meta-Trends and Strategic Challenges*, 5 March 2012.

[71] It is important to note that even when U.S. military capabilities eventually overwhelm threat capabilities at SPODs and APODs, adversaries will still maintain a viable capability through paramilitary and guerrilla organizations to conduct raids at such locations.
[72] DIA, 8 April 1997; *Military Power of the People's Republic of China*, Office of the Secretary of Defense, 2006; "S-400 Triumf/SA-21 Growler: New Threat Emerging," Defense Media Network, 8 April 2011; "China news tagged with: electronic warfare," China Digital Times, May 2007; "Global Combat Support System-Army (GCSS-Army)," Defense Update, 1/26/2005; *Military Capabilities Of The People's Republic Of China*, Defense Intelligence Agency (DIA) report to Congress,8 April 1997; "Cruise Missiles of the World," The Claremont Institute, 23 May 2011.
[73] Chief of Staff of the Army Gen, Raymond T. Odierno, "CSA Remarks at AUSA Institute of Land Warfare Breakfast," Jan. 2012.
[74] Department of the Army, *TC 7-100: Hybrid Threat*, November 2010.
[75] Human Security Report Project, *Human Security Report 2009/2010: The Causes of Peace and the Shrinking Cost of War*, Simon Fraser University, 2010.
[76] Human Security Report Project, *Human Security Report 2009/2010: The Causes of Peace and the Shrinking Cost of War*, Simon Fraser University, 2010.
[77] Chief of Staff of the Army White Paper Slides, *Shifting Our Aim: A Balanced Army for a Balanced Strategy*, 2011.
[78] Chief of Staff of the Army White Paper Slides, *Shifting Our Aim: A Balanced Army for a Balanced Strategy*, 2011.
[79] Joint Chiefs of Staff, *Chairman's Strategic Direction to the Joint Force*, 6 February 2012.
[80] Chief of Staff of the Army White Paper Slides, *Shifting Our Aim: A Balanced Army for a Balanced Strategy*, 2011.
[81] Chief of Staff of the Army White Paper Slides, *Shifting Our Aim: A Balanced Army for a Balanced Strategy*, 2011.
[82] Abraham M. Denmark, "Managing the Global Commons," The Washington Quarterly, July 2010, 169.
[83] Abraham M. Denmark, "Managing the Global Commons," The Washington Quarterly, July 2010, 169.
[84] United States Air Force, *Strategic Planning 2010-2030: Strategic Environment Assessment*, 11 March 2011.
[85] United States Air Force, *Strategic Planning 2010-2030: Strategic Environment Assessment*, 11 March 2011.
[86] Director of National Intelligence, James R. Clapper, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community or the Senate Select Committee on Intelligence*, 31 January 2012.
[87] Department of Defense and the Office of the Director of National Intelligence, *National Security Space Strategy*, January 2011.
[88] United States Air Force, *Strategic Planning 2010-2030: Strategic Environment Assessment*, 11 March 2011.
[89] United States Air Force, *Strategic Planning 2010-2030: Strategic Environment Assessment*, 11 March 2011.
[90] American Forces Press Service, "New Strategy Shows Importance of Space Domain, Lynn Says," 16 February 2011.
[91] American Forces Press Service, "New Strategy Shows Importance of Space Domain, Lynn Says,"16 February 2011.
[92] Department of Defense and the Office of the Director of National Intelligence, *National Security Space Strategy*, January 2011.
[93] Department of Defense and the Office of the Director of National Intelligence, *National Security Space Strategy*, January 2011.
[94] People and the Plant, "Urban population trends," 26 January 2008.
[95] Joint Staff J-7, *Joint Force 2030 - Evolve, Lead, Secure: Exploring Lessons of the Past and Present to Prepare for the Future,* Draft, 23 March 2012, 120.
[96] Abraham M. Denmark, "Managing the Global Commons," The Washington Quarterly, July 2010, 168.
[97] Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership*, 8 February 2011, 8.
[98] Flournoy, Michele and Shawn Brimley, "The Contested Commons," U.S. Department of Defense (accessed 2 November 2010).
[99] The White House, *The National Security Strategy of the United States*, 2010, 42-44; The Office of the Secretary of Defense, *The National Military Strategy of the United States*, 2011, 13-14; The Office of the Secretary of Defense, *The Quadrennial Defense Review Report*, February 2010, 59-67.

[100] International Institute for Strategic Studies (IISS), *The Military Balance 2011*, 2011.
[101] Amol Sharma, Jeremy Page, James Hookway, Rachel Pannett, "Asia's New Arms Race," Wall Street Journal, 12 February 2011.
[102] Stephen Johnson, "Balancing China's Growing Influence in Latin America," The Heritage Foundation, October 2005.
[103] Viral Dholakia, *India's GDP to touch 205 Trillion Rupees by 2020: Edelweiss Report*, 21 March 2010.
[104] Guy Ben-Ari, Nicholas Lombardo, *India's Military Modernization*, Center for Strategic and International Studies, 1 April 2011.
[105] Teresita C. Schaffer, "The United States and India 10 Years Out," from the U.S.-India Initiative Series, Center for a New American Security, October 2010.
[106] AFP News Agency, "Vietnam to Reopen Cam Ranh Bay to Foreign Fleets: PM," Bangkok Post, 31 October 2010.
[107] UN News Service, "Asia-Pacific Most Prone to Natural Disasters But Lacks Preparedness – UN Report," UN News Center, 26 October 2010.
[108] Earthquake Hazards Program, "World Earthquake Information by Country/Region," United States Geological Survey (accessed 1 September 2011).
[109] Leslie Evans, "ASEAN and Terrorism in Southeast Asia," Center for Southeast Asian Studies, UCLA International Institute, 20 May 2004.
[110] The White House, *The National Security Strategy of the United States*, 2010, 20-26, 45; The Office of the Secretary of Defense, *The National Military Strategy of the United States*, 2011, 3, 5, 11-12;The Office of the Secretary of Defense, *The Quadrennial Defense Review Report*, February 2010, 5, 25, 31, 60-61, 67.
[111] U.S.-Saudi-Arabian Business Council, "Saudi Arabia to Create First Nuclear City in Kingdom," 18 April 2010, (accessed 29 March 2012); MSN News, Saudi Arabia mulls nuclear cooperation with Pak: Report," 8 September 2011, (accessed 29 March 2012).
[112] Intelligence Community Assessment, Global Water Security, 2 February 2012.
[113] USDA, "Southeastern Anatolia Project (GAP)," no date.
[114] Dr. Jacquelyn K. Davis "Radical Islamist Ideologies and the Long War – Implications for U.S. Strategic Planning and U.S. Central Command's Operations", Institute for Foreign Policy Analysis, Jan. 2007; see also the transcript of the conference, "The Global Spread of Wahhabi Islam: How Great a Threat," Pew Forum on Religion & Public Life – particularly the remarks of James Woolsey, Former Director of CIA.
[115] The White House, *The National Security Strategy of the United States*, 2010, 41, 44; The Office of the Secretary of Defense, *The National Military Strategy of the United States*, 2011, 12; The Office of the Secretary of Defense, *The Quadrennial Defense Review Report*, February 2010, 57-58, 64-65, 68.
[116] Siemon T. Wezeman, *Military Capabilities in the Arctic*, SIPRI Background Paper, March 2012.
[117] IHS Jane's, *Jane's World Armies: Russian Federation*, 2 September 2011.
[118] Paul Goble, "Middle Class 'Fleeing' Russia, Moscow Expert Says," The New Times, 24 May 2011.
[119] The White House, *The National Security Strategy of the United States*, 2010, 21, 34, 39, 45; The Office of the Secretary of Defense, *The National Military Strategy of the United States*, 2011, 6, 12; The Office of the Secretary of Defense, *The Quadrennial Defense Review Report*, February 2010, 61, 64.
[120] USAID, "Democracy and Governance: A Critical Foundation for Sustainable Development," 13 December 2011 (accessed July 2011).
[121] UN Department of Economic and Social Affairs, Population Division (2011), (accessed April 2012).
[122] Philippe Leymarie, "The Sahel falls apart," Le Monde Diplomatique, English Edition, April 2012, (accessed April 2012).
[123] Save Our Seafarers, "Status of seized vessels and crews in Somalia as of the 26 Aril 2011," 9 May 2011.
[124] Scott Baldauf, "Pirates take new territory: West African Gulf of Guinea," The Christian Science Monitor, 15 January 2010.
[125] *ASI Global Maritime Response*, 2010.
[126] Deborah Brautigam, "Chinese Development Aid in Africa," *Rising China: Global Challenges and Opportunities*, The Australia University E Press, eds. Jane Golley and Ligang Song, June 2011.
[127] Onyi Udegbunam, "How China is Taking Over Africa," The Afropolitan Experience, 20 April 2011.

[128] Onyi Udegbunam, "How China is Taking Over Africa," The Afropolitan Experience, 20 April 2011; Richard F. Grimmett, *Conventional Arms Transfers to Developing Nations, 2002–2009,* United States Congressional Research Service, 2010, 32.
[129] *The Militarization of Sudan*, Small Arms Survey, April 2007, 2.
[130] Daniel Volman, "The Military Dimensions of Africa's New Status in Global Geopolitics," September 2008; J. Peter Pham, *India in Africa: Implications of an Emerging Power for AFRICOM and U.S. Strategy*, Strategic Studies Institute, March 2011.
[131] *Challenges to Agricultural Development in Africa*, Economic Report on Africa, 2008, 13.
[132] Colin Powell, *Statement for the Record to the Senate Foreign Relations Committee*, Federal Document Clearing House, 5 Feb 2002.
[133] The White House, *The National Security Strategy of the United States*, 2010, 43-44; The Office of the Secretary of Defense, *The National Military Strategy of the United States*, 2011; The Office of the Secretary of Defense, *The Quadrennial Defense Review Report*, February 2010, 61-62, 68-69.
[134] Robert D. Ramsey III, *From El Billar to Operations Fenix and Jaque: The Colombian Security Force Experience, 1998-2008*, Occasional Paper 34, Combat Studies Institute Press, December 2009, 79.
[135] BBC, "Colombia forces kill 'key rebel'," 23 September 2008; William Lloyd George, "Colombia's indigenous communities caught in the middle," CNN World, 02 August 2011.
[136] BBC, "Colombia's FARC Rebels: Retreating or Resurgent?" 19 July 2011.
[137] Rory Carroll, "Venezuela attacks report suggesting ties between Chavez and FARC rebels," The Guardian, 10 May 2011, (accessed 29 March 2012); *The International Exploitation of Drug Wars and What We Can Do About It*, Testimony of Douglas Farah Before the House Committee on Foreign Relations Subcommittee on Oversight and Investigations, 12 October 2011, (accessed 29 March 2012), 9; Jeremy McDermott, "'IRA influence' in Farc attacks," BBC, 9 May 2005 (accessed 29 March 2012); Michael Martinez, "Study: Colombian rebels were willing to kill for Venezuela's Chavez," CNN, 10 May 2011, (accessed 29 March 2012).
[138] International Institute for Strategic Studies, "The FARC Files: Venezuela, Ecuador and the Secret Archive of 'Raul Reyes'," May 2011.
[139] Shannon K. O'Neil, "Drug Cartel Fragmentation and Violence," Council on Foreign Relations, 9 August 2011, (accessed 26 March 2012).
[140] Chris Kraul and Sebastian Rotella, "Drug Probe Finds Hezbollah Link," Los Angeles Times, 22 October 2008; Selcan Hacaoglu, "Turkey Holds Suspicious Iran-Venezuela Shipment," Associated Press, 6 January 2009; James Vicini, "Timeline: Key Dates in Alleged Iran Assassination Plot in U.S.," Reuters, 11 October 2011.
[141] Congressional Research Service, *Latin America and the Caribbean: Illicit Drug Trafficking and U.S. Counterdrug Programs*, 12 May 2011 (accessed 21 March 2012).
[142] Bob Killebrew and Jennifer Bernal, "Crime Wars: Gangs, Cartels and U.S. National Security," Center for a New American Security, 28 September 2010, 34; Jill Replogle, "In Guatemala, a Village that Cocaine Built," TIME World, 16 April 2009.
[143] Nonproliferation for Global Security (NPSG), "Brazil Launches its National Defense Strategy," 18 December 2008.
[144] Council on Foreign Relations, *Global Brazil and U.S.-Brazil Relations*, 12 July 2011, 16.
[145] R. Evan Ellis, *China-Latin America Military Engagement: Good Will, Good Business, and Strategic Position*, Strategic Studies Institute, August 2011.
[146] "100,000 foot soldiers in Mexican cartels," Washington Times, 3 March 2009 (accessed 21 March 2012).
[147] Diana Washington Valdez, "Mexico's Drug Killings Soar Above U.S. Figures," El Paso Times, 28 March 2012 (accessed 29 March 2012).
[148] Edwin Mora, "47,515 Drug-War Murders in Mexico in Just 5 Years," CNS News, 12 January 2012 (accessed 29 March 2012).
[149] National Gang Intelligence Center, *National Gang Threat Assessment 2009*, January 2009.
[150] National Gang Intelligence Center, *National Gang Threat Assessment 2009*, January 2009.
[151] National Gang Intelligence Center, *Gang-Related Activity in the U.S. Armed Forces Increasing*, 12 January 2007.

[152] Jerome P. Bjelopera, *American Jihadist Terrorism: Combating a Complex Threat*, Congressional Research Service, 15 November 2011, (assessed 29 March 2012).
[153] Matt Matthews, *The Posse Comitatus Act and the United States Army: A Historical Perspective* (Fort Leavenworth: Combat Studies Institute Press, 2006).
[154] "Global Combat Support System-Army (GCSS-Army)," Defense Update, 26 January 2005; *Military Capabilities Of The People's Republic Of China*, Defense Intelligence Agency (DIA) report to Congress, 8 April 1997; "Cruise Missiles of the World," The Claremont Institute, 23 May 2011.
[155] DIA, 8 April 1997; *Military Power of the People's Republic of China*, Office of the Secretary of Defense, 2006; "S-400 Triumf/SA-21 Growler: New Threat Emerging," Defense Media Network, 8 April2011; China news tagged with: electronic warfare, China Digital Times, May 2007.
[156] "PHL03 300mm Multiple Launch Rocket System," SinoDefence.com, 14 March 2008.
[157] The Claremont Institute, 23 May 2011.
[158] HighBeam Research, October 2006.
[159] "SCL Spread Spectrum Communications Tactical Countermeasures Systems (SCL-SSCTS) (India), Jamming and Miscellaneous," IHS Jane's, September, 2010.
[160] "FN-16 (China), Man-portable surface-to-air missile systems," IHS Jane's, June 2010.
[161] HighBeam Research, October 2006.
[162] Defense Update, 26 January 2005.
[163] HighBeam Research, October 2006.