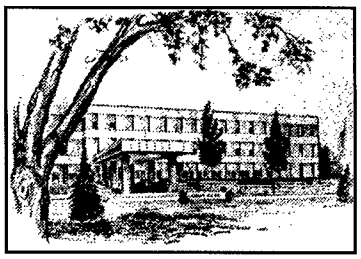
Strategic Studies Institute SSI

FROM "DEFENDING FORWARD" TO A "GLOBAL DEFENSE-IN-DEPTH": GLOBALIZATION AND HOMELAND SECURITY

Antulio J. Echevarria II
Bert B. Tussing

U.S. Army War College

STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic level study agent for the Deputy Chief of Staff for Operations and Plans, Department of the Army.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically-orientated roundtables, expanded trip reports, and quick reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

FROM "DEFENDING FORWARD" TO A "GLOBAL DEFENSE-IN-DEPTH": GLOBALIZATION AND HOMELAND SECURITY

Antulio J. Echevarria II
and
Bert B. Tussing

October 2003

*****

The views expressed in this report are those of the authors and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. This report is cleared for public release; distribution is unlimited.

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute, U.S. Army War College, 122 Forbes Ave, Carlisle, PA 17013-5244. Copies of this report may be obtained from the Publications Office by calling (717) 245-4133, FAX (717) 245-3820, or by e-mail at *Rita.Rummel@carlisle.army.mil*

*****

All Strategic Studies Institute (SSI) monographs are available on the SSI Homepage for electronic dissemination. SSI's Homepage address is: *http://www.carlisle.army.mil/ssi/*

*****

The Strategic Studies Institute publishes a monthly e-mail newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please let us know by e-mail at *outreach@carlisle.army.mil* or by calling (717) 245-3133.

ISBN 1-58487-143-1

FOREWORD

Much of today's defense literature calls for new ways of thinking, ways that appreciate the challenges of a new millennium. Yet, we find surprisingly little that is new in our nation's current strategy documents, particularly those regarding homeland security. Ideas that helped us achieve victory in the 20th century—an age marked by the Cold War and industrial-age thinking—may only hinder us as we strive for strategic success in an era shaped more and more by the forces of globalization.

With this concern in mind, Lieutenant Colonel Antulio J. Echevarria II and Professor Bert Tussing have examined the scope and substance of our *National Strategy for Homeland Security* (NSHS). Disturbingly, they find that the NSHS fails to address the challenges that globalization poses for the security of the American homeland. The NSHS focuses primarily within the nation's borders and lacks a comprehensive approach to the problem of homeland security, a problem of global proportions. To remedy these deficiencies, the authors propose a strategic way—a Global Defense-in-Depth—that, among other things, employs some of the opportunities afforded by globalization to address its challenges.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute

BIOGRAPHICAL SKETCHES OF THE AUTHORS

ANTULIO J. ECHEVARRIA II, an Army lieutenant colonel, is currently assigned as the Director of National Security Affairs at the Strategic Studies Institute. He graduated from the U.S. Military Academy in 1981, was commissioned as an armor officer, and has held a variety of command and staff assignments in Germany and Continental United States; he has also served as an Assistant Professor of European History at the U.S. Military Academy; Squadron S3 of 3/16 Cavalry; Chief of BN/TF and Bde Doctrine at the U.S. Army Armor Center at Fort Knox; as an action officer at the Army After Next project at HQ TRADOC, Ft. Monroe, VA; and as a speechwriter for the U.S. Army Chief of Staff. Lieutenant Colonel Echevarria is the author of *After Clausewitz: German Military Thinkers before the Great War*, published by the University Press of Kansas (2001). He also has published articles in a number of scholarly and professional journals to include the *Journal of Military History, War in History, War & Society*, the *Journal of Strategic Studies, Parameters, Joint Force Quarterly, Military Review*, and *Airpower Journal*. He is a graduate of the U.S. Army's Command and General Staff College, and holds M.A. and Ph.D. degrees in History from Princeton University.

BERT B. TUSSING has been Professor of National Security Affairs for the Center for Strategic Leadership at the U.S. Army War College since October 1999. Among his assignments in the United States Marine Corps during a 24-year military career, he participated in multiple humanitarian relief exercises in the Caribbean; Operation URGENT FURY in Grenada; operations as a part of the Multinational Force in Beirut; Operations PROVIDE PROMISE and DENY FLIGHT in Bosnia; and the final withdrawal of U.S. forces from Somalia. Professor Tussing also served as Marine Corps analyst to the Secretary of the Navy; as a Brookings Legislative Fellow; and as Legislative Assistant to the Chairman of the Joint Chiefs of Staff. Professor Tussing's publications include *Combating Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Strategy* (Cilluffo, Cardash and Lederman, eds.). He is a graduate (with highest distinction) with a Masters Degree in National Security and Strategic Studies from the Naval War College and has a Masters Degree in Strategic Studies from the U.S. Army War College.

SUMMARY

In July of last year, the Bush administration published the *National Strategy for Homeland Security* (NSHS) which, while commendable in many ways, failed to take into account the effects of globalization in planning for the nation's security. Safeguarding America's homeland in an era of globalization requires a more comprehensive approach based on a "global defense-in-depth."

The NSHS amounts to little more than a strategic directive for the newly formed Department of Homeland Security (DHS), rather than a national strategy. It focuses principally on activities that take place within the nation's borders, making only a brief genuflection to the need for international cooperation. Other than a passing reference to Northern Command and its envisioned responsibilities in civil support, the NSHS fails to address the roles that the U.S. military's combatant commands should play. Finally, the NSHS fails to incorporate newly emerging technologies into an overarching strategic concept, or way, that would contribute to keeping Americans safe.

To be sure, an internal focus with regard to protecting the homeland is at least partially warranted. However, the NSHS's shortsightedness overlooks the ways in which globalization—which is increasing the real and virtual mobility of people, things, and ideas worldwide—exacerbates the problem of safeguarding the homeland. The increased mobility of people, things, and ideas means that an attack against the American homeland need not take place on U.S. soil, and that the range of potential negative effects that could result from such attacks has increased. Consequently, America's homeland security challenge cannot be seen as merely a national problem; it is a problem of global dimensions.

To address homeland security in terms of today's challenges requires a global perspective. Accordingly, the NSHS should establish a "global defense-in-depth" characterized by an improved defensive coverage that uses a worldwide continuum of networked surveillance and intelligence-gathering systems to cover multiple intercept points for people, weapons, and dangerous materials, and that is linked to resources dedicated to reacting instantly to identified threats. This network must also include local law enforcement

agencies and organizations. One logical nexus for tying together these various elements is the new Terrorist Threat Integration Center (TTIC), established May 1, 2003. Much of the technology necessary to begin erecting such a continuum already exists, or is under development.

A global defense-in-depth would entail extending the deployment of permanent chemical, biological, and radiological sensors—such as those currently being deployed in major U.S. cities and subway systems—beyond U.S. borders to key population centers overseas. It would also involve continuous monitoring and tracking of suspected terrorists and other criminals. While legal constraints can—and should—limit the monitoring or tracking of personnel within the United States, such restrictions do not apply to monitoring physical structures, such as high-security areas and key pieces of infrastructure like bridges, tunnels, airports, and border crossings. In terms of cyber-security, a global defense-in-depth would employ a more decentralized approach based on the cooperation and vigilance of individuals worldwide in both the public and private sectors. It would also include political, economic, and socio-cultural forms of national power in critical roles aimed at crushing an immediate threat as well as bringing about changes that would prevent its resurgence. All of this will, of course, require significant international cooperation centered on a coherent agenda that includes forums through which participating nations, particularly poorer ones, have opportunities to air their concerns about the unintended consequences of a global defense-in-depth.

Recommendations.

- The DHS, the DoD, the intelligence community, and other federal agencies and organizations must think of homeland security—in all of its dimensions—in global terms. All of the regional combatant commands, for example, have geographic responsibilities under homeland security, and as a minimum their Theater Cooperation Programs (TCPs) should be integrated into the NSHS.

- The next iteration of the NSHS should feature as its centerpiece a global defense-in-depth—a seamless continuum characterized by greater intelligence capabilities, enhanced visibility of areas and objects of concern, and multiple types of rapid intercept capabilities. Such a continuum will require a reexamination of the division of responsibility between DHS and DoD to ensure command and control are transferred effectively.

- DoD should invest more in the research and development of dual-use technologies appropriate for military forces as well as law enforcement agencies. Concurrently, DoD should do a better job of informing DHS (and the other organizations that play a role in homeland security) of existing dual-use technologies as well as those currently under development.

- The NSHS and the national security strategy must complement each other. Efforts to defend the homeland against immediate threats should complement those aimed at achieving peace and stability abroad.

- The NSHS should do more than refer to the need for international cooperation; it should outline a general plan for building that cooperation.

FROM "DEFENDING FORWARD" TO "GLOBAL DEFENSE-IN-DEPTH": GLOBALIZATION AND HOMELAND SECURITY

In July of last year, the Bush administration published the *National Strategy for Homeland Security* (NSHS), which quickly became the centerpiece for domestic preparedness in the United States.[1] While commendable in many ways, the strategy's focus was noticeably insular, lacking an essential global perspective in planning for the nation's security. Not surprisingly, therefore, the NSHS's supporting documents—*The National Strategy for Combating Terrorism, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* and *The National Strategy to Secure Cyberspace*—suffer from the same deficiency.[2] Except for occasional references to information technologies such as "virtual networks" and the "internet," the NSHS appears more appropriate for addressing the threats of the 20th century than those of today. Such a narrow and outdated perspective hardly inspires confidence. Indeed, it raises doubts about the strategy's potential effectiveness in an era that experts agree is being shaped definitively by the forces of globalization.[3] For purposes of this study, globalization means the enhanced mobility of people, things, and ideas. It is a phenomenon that began not in the late-20th century, but in the mid-19th with the advent of revolutionary communication and transportation technologies such as the telegraph and the steam ship. As these technologies matured during the 20th century, they contributed to a general increase in the speed and volume of travel and communications, thereby enlarging the amount of interaction among societies and essentially making the world a "smaller place."[4]

Although the effects are more pronounced in some areas than in others, the enhanced mobility of people, ideas, and things associated with globalization means that we must think differently about homeland security. Put simply, the protection of America's homeland can neither begin nor end at the nation's borders. Like the proverbial circle that has no discernable start or end point, our strategy for homeland security must be global in perspective

and have no perceivable gap. In a phrase, safeguarding America's homeland will require a "global defense-in-depth."

Deficiencies in the National Strategy for Homeland Security.

To be sure, the NSHS is based on sound principles, as far as they go. However, in today's highly mobile "global village," they simply do not go far enough. In fact, the NSHS amounts to little more than a strategic directive for the newly formed Department of Homeland Security (DHS), rather than a national strategy.[5] The objectives—or ends—outlined in the NSHS, for example, are reasonable, if obvious: to prevent terrorist attacks within the United States, to reduce America's vulnerability to terrorism, and to minimize the damage of attacks that do occur. The strategy's concepts—or ways—are also sound, if too few in number, resting mainly on the idea of establishing the Department of Homeland Security to accomplish six critical missions: intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure and key assets, defending against catastrophic threats, and emergency preparedness and response. Finally, the resources—or means—it proposes to achieve its desired ends are also logical, if only vaguely described. They include not only the assets of any number of federal and local agencies, but the many valuable resources that derive from civil law, science and technology, information sharing and systems, and international cooperation.[6] However, the bulk of these mission areas pertain principally to activities that take place within the nation's borders.

Moreover, the document makes only a brief genuflection to the theme of international cooperation, stating that America's strategy for protecting the homeland "cannot stop at our borders" and that the United States must pursue an international agenda to counter global terrorism and to improve its homeland security.[7] Unfortunately, it stops short of saying anything of substance about the content of that agenda. This oversight is particularly egregious since the cooperation expected from many European nations in the wake of 9/11 has thus far either failed to materialize or has been much less than expected.[8] Clearly, we must take more effective measures abroad.

Furthermore, the NSHS fails to address the roles that the U.S. military's combatant commands should play. Each of the regional combatant commands, and to a certain extent even the functional combatant commands, have numerous resources that can and do contribute to the nation's homeland security efforts. A combatant commander's Theater Cooperation Program (TCP), for instance, is a plan for providing U.S. support to friends and allies, but it can also provide similar guidance to multilateral national security and law enforcement agencies for exchanging vital intelligence. Even more directly, a TCP can help generate cooperative efforts against terrorism, such as the one currently taking place between the United States and the Philippines. While the NSHS mentions Northern Command and its envisioned role in civil support, the document makes no reference to the command's responsibilities in Homeland Defense, nor how it should coordinate those responsibilities with the other combatant commands.

Finally—and perhaps most critically—the NSHS fails to incorporate newly emerging technologies, many of which are associated with the ongoing revolution in information technology, into an overarching strategic concept that would contribute to keeping Americans safe. While its ends are imminently agreeable, without viable ways they are merely a wish list. Indeed, in many respects, the ends and means are the least complex elements of any strategy. They amount to a statement of the desirable in the first case and an assessment of the available in the second. The real substance of any strategy lies in the ways, or the concepts; that is, *how* the responsible parties expect to get things done. Here a strategy's designers reveal whether they appreciate the challenges they must address to achieve their aims. Without coherent ways, a strategy runs the risk of degenerating into a host of *ad hoc* actions that will undoubtedly fail to make the best use of limited resources. Effective ways can pull the ends and means of a strategy together into a series of coherent actions and inspire confidence at the same time.

To be sure, an internal focus with regard to protecting the homeland is at least partially warranted. After all, the United States is the richest, most open, and most developed nation on earth with over 4.5 million square miles of territory, 95,000 miles of shoreline, 7,500 miles of land borders, and 286 million citizens to protect.[9] It has the

world's most extensive critical infrastructure, with some 1.4 million miles of oil and natural gas pipelines, 104 nuclear reactor facilities, 300 major seaports, and 400 major airports.[10] The dramatic drop in air travel after the events of September 11, 2001, demonstrated how an attack against any major portion of this infrastructure could have significant economic consequences.[11] Similarly, an attack against the U.S. agriculture and livestock infrastructures would likely result in severe repercussions for the nation's economy.[12] Likewise, an attack against the country's vast recreation and entertainment industries—which include thousands of sports arenas, amusement parks, shopping malls, and other public places—would also result in a severe psychological and economic blow to Americans.[13] Overlooking such vulnerabilities in favor of an external focus would be tantamount to trading one form of myopia for another.

However, the NSHS's particular form of myopia overlooks the ways in which globalization—or the increased real and virtual mobility of people, things, and ideas worldwide—exacerbates the problem of safeguarding the homeland. This enhanced mobility means two things. First, the sheer volume of traffic passing through the nation's borders renders it impractical to stop all but a few vehicles long enough to perform detailed security checks. In 2000, for example, some 489 million people, 139 million motor vehicles, 2.2 million rail cars, 289,000 aircraft, 7.5 million maritime cargo containers (or 1 container every 20 seconds), and 211,000 sea vessels entered the United States or were processed at U.S. ports of entry.[14] And, more than $9 billion in goods pass through U.S. points of entry every day.[15] Notably, this flow of people, vehicles, and goods cannot be interrupted without adversely affecting the nation's economy. Moreover, America's economy sets the pace for the rest of the world, producing 30-50 percent of the world's food exports and 19 percent of its energy.[16] It must, therefore, remain open to commerce, not only because the nation's vital interests are at stake, but because any significant stoppage of trade would undoubtedly have a serious economic effect globally.

Second, terrorists or other nefarious actors need not strike America directly in order to cause harm to U.S. citizens within the homeland. The greater speed of travel that has fed globalization

means that an attack against the American homeland need not take place on U.S. soil. A biological attack against Canada or Mexico, for instance, could quickly put U.S. citizens at risk, as well as people in many other parts of the world.[17] Likewise, an attack against certain kinds of Canadian infrastructure would also have a disruptive effect on various types of U.S. infrastructure.[18] Thus, as the world becomes more interconnected due to globalization, the range of negative effects that might result from such attacks will undoubtedly increase, giving new meaning to the so-called strategy of the indirect approach. Consequently, America's homeland security challenge cannot be seen as simply a national problem; it is a problem of global dimensions.

Toward a Global Defense-in-Depth.

To address homeland security as a global challenge, the NSHS must have a global perspective. Put differently, it must regard homeland security in terms of a "global defense-in-depth" rather than the more linear—and still dominant—concept of "defending forward" made popular in the 1940s. The current notion of defending forward essentially divides the globe into two geographic and spatial zones: 1) the Homeland Zone, which includes the land, sea, air, and space areas of all states, territories, possessions, and surrounding waters out to 500 nautical miles; and 2) the Forward Zone, which encompasses all remaining air, land, sea, and space areas.[19]

Unfortunately, this idea reflects 20th century thinking in which threats came primarily in the form of aircraft, missiles, and ground troops, and in which the United States maintained a forward presence to deter its adversaries and would-be aggressors. The increasing speed of travel and access afforded by globalization mean that dividing the world into forward and homeland (or rear) areas makes little sense. Terrorists are no longer as limited by space and time as they once were; nor should we assume that they will base themselves in distant geographic regions, that is, in the Forward Zone. They are already "within the wire," so to speak. While most of Al Qaeda's recruits still come from so-called source countries located in the Forward Zone, others come from areas within or adjacent to the Homeland Zone.[20] In addition, as a number of homeland security

experts have pointed out, many of the materials that terrorists required to execute their designs did not come from remote areas. The explosive devices used in the 1993 attack on the World Trade Center, the 1995 bombing of the Murrah Federal Building in Oklahoma City, and the 2001 destruction of the World Trade Center all came from within the United States and were carried out by terrorists already in our country.[21] Therefore, effective homeland security in the 21st century requires a perspective that sees defense in terms of a fully integrated and seamless global continuum—that is, a global defense-in-depth.

The essential difference between the concept of defending forward and that of a global defense-in-depth is that the latter is predicated on achieving enhanced visibility and improved defensive coverage throughout a global continuum. The former, by contrast, conveys the sense that the threat is located somewhere along a forward "crust" beyond U.S. borders, and that defeating it *there* equates to security *here*. The new Container Security Initiative (CSI) being implemented by Bureau of Customs and Border Patrol (BCBP), the U.S. Coast Guard, and the U.S. Navy for the inspection of container ships illustrates the idea of enhanced visibility more clearly.[22] CSI enables increased (some would say total) visibility of shipping containers—of which nearly 7.5 million arrive at U.S. seaports annually—from their point of origin to their final destination.[23] Satellites and other communications equipment continuously track a ship's progress, transmitting its identity, speed, position and course until it arrives at its port of delivery along with its cargo. Currently, 15 of the 25 major international ports that have agreed to participate are already operational.[24] CSI not only allows for continuous tracking of the cargo, thereby ensuring it is not tampered with in transit; it also greatly reduces inspection and processing time at sea ports, since the system can verify that the containers remained sealed until arriving at the destination port. If the ship arrives with some seals broken in transit or visibility of it was lost, the cargo is not off-loaded and the ship is turned away.

Applying the same principle of enhanced visibility to other endeavors, the concept of global defense-in-depth can assist in defeating any number of threats. For example, by reading residual

effusions in the air, laser remote optical sensing systems mounted on aircraft can determine whether chemical, biological, nuclear, and radiological weapons (as well as narcotics) are being produced at any given location.[25] They can also track the movement of such weapons or illegal substances by monitoring the effusions from a cargo container, a vehicle, or even an individual who has handled the weapons or substances. If arrayed in depth globally, such airborne lasers could provide early warning of the preparation and approach of dangerous or illegal materials, which military forces or appropriate law enforcement officials could then intercept. We should not forget that terrorists need not transport chemicals, nuclear materials, and biological agents themselves, but could simply target any one of the 38,000 facilities within the United States that store hazardous materials, or one of our more than 100 nuclear power plants.[26] Indeed, some sources report that such an attack is more likely than scenarios in which terrorists smuggle dangerous materials into the United States.[27] Such a capability could also augment our defense against cruise missiles, many of which might otherwise be launched from offshore container ships or similar types of land vehicles with little or no warning.[28]

A global defense-in-depth would entail extending the deployment of permanent chemical, biological, and radiological sensors—such as those currently being deployed in major U.S. cities and subway systems—beyond U.S. borders to key population centers overseas. Currently, in a system known as Biowatch, more than 31 U.S. cities have a system of sensors in place capable of detecting the presence of pathogens such as smallpox and anthrax.[29] Similarly, more than 250 radiation detection devices are deployed in and around major U.S. points of entry to detect and deter the entry of radiological material into the country.[30] At present, such sensors, located in and around major American cities, can provide indication of a major bioterrorism attack within 12 hours of its initiation. In terms of casualties, this means that if someone released two pounds of anthrax from a tall building in New York City, the death toll would be reduced from 120,000 to 70,000 people.[31] Clearly, Biowatch, while better than no warning system at all, has room for improvement. One way to enhance it is to expand it—thereby extending its zone of warning—by building a global network of mobile and permanent sensors,

augmented with airborne lasers that can detect the preparation and transportation of hazardous materials, all of which would be connected to multiple central command and control facilities. A global Biowatch system of this sort could enable U.S. authorities to identify an attack much earlier and would provide them more time to take the necessary prophylactic and other measures.

A global defense-in-depth would also involve applying similar concepts of continuous monitoring and tracking to suspected terrorists and other criminals. As the recent capture of Khalid Sheik Mohammed suggests, such tasks have the potential to yield the most profitable results, from the names and whereabouts of other terrorists to critical information about future attacks.[32] Fortunately, our ability to share databases and other information among our intelligence agencies, and those around the world, has improved greatly since 9/11, though we still have a long way to go.[33] Initiatives such as "Combat Zones That See" (CTS), now under development by the Defense Advanced Research Projects Agency (DARPA), will use networks of thousands of computers and cameras to track, record, and analyze every vehicle in a foreign country, as well as, in many cases, drivers and passengers.[34] Over 40 million surveillance and other types of cameras are already in use around the world, with some 300 million expected by 2005. While legal constraints can—and should—limit the use of such devices to track personnel within the United States, such restrictions do not apply to monitoring physical structures, such as high-security areas and key pieces of infrastructure like bridges, tunnels, airports, and border crossings. Other programs, such as the United States Visitor and Immigrant Status Indicator (US VISIT), that will use biometric and other technologies to help track foreign visitors as they enter and leave the country, could augment CTS.[35] Yet, as the Travel Industry Association of America warns, we must take care not to discourage international travelers—who spend billions of dollars on travel and tourism while here—from visiting the United States.[36] Also, in the area of personnel activities especially, technology alone is not the answer. Terrorists will undoubtedly attempt to find "workarounds" to carry out their plans. In this regard, bolstering our human intelligence resources worldwide through the recruitment of field operatives and analysts must remain a top priority; they will provide

critical links in any global defense-in-depth.[37]

The concept of a global defense-in-depth would also apply to cyber defense, but somewhat differently. While recent research shows that cyber attacks may prove less useful to terrorists than originally thought, they continue to pose a real threat in terms of their potential utility in crime, espionage, and as a force-multiplier when used in conjunction with physical attacks.[38] In terms of cyber-security, a global defense-in-depth would need to come from the cooperation and vigilance of individuals worldwide in both the public and private sectors. In other words, it will require a more decentralized approach. Only widespread, constant awareness and reporting of cyber intrusions and attacks can help limit the damage caused by such acts and offer data that might assist in the prevention of other attempts. As the *National Strategy to Secure Cyberspace* points out, a number of initiatives and systems are in place or are being established to facilitate the reporting of malicious cyber activity.[39] However, U.S. policymakers must learn to recognize the growing interdependence among international economies and put greater emphasis on cooperation among nations to counter cyber threats.

One logical nexus—and by no means the only one—for tying together the various components of global defense-in-depth is the new Terrorist Threat Integration Center (TTIC), established May 1, 2003. The TTIC—composed of elements from the Department of Homeland Security, the FBI's Counter-Terrorism Division, the Counterterrorism Center of the Director of Central Intelligence, the Department of Defense, the Department of State, and the larger intelligence community—serves as a "hub" for terrorist, or threat-related information collected domestically or abroad and provides threat assessments for America's national leadership.[40] However, the effective functioning of the TTIC will first require resolving a number of issues, such as which federal agency or organization should control the center. The TTIC—an all-source threat intelligence analysis entity—has been placed under the direction of the Director of Central Intelligence, but the Homeland Security Act gave the DHS responsibility for all-source terrorist threat analysis.[41] Similarly, local law enforcement agencies and organizations should be tied into the network, and standardized policies and procedures should be adopted to facilitate intelligence transfer and to assist in shortening

response times.

For obvious reasons, a global defense-in-depth requires unity of command. However, the establishment of DHS created a division of responsibility in which DoD focuses primarily beyond the nation's borders—except in emergencies or other extraordinary circumstances—and DHS concentrates principally within them, thereby creating an obvious seam in terms of command and control in what should be a seamless continuum.[42] One way to remedy this problem is to place all defense and border security functions—as carried out by the U.S. Coast Guard, the Directorate for Border and Transportation Security, and the Directorate for Information Analysis and Infrastructure Protection, for example—under DoD, which in any case traditionally has had responsibility for the nation's defense. This solution would leave incident management—as performed by the directorate for Emergency Preparedness and Response, for example—and other functions under DHS and would eliminate the seam that exists at present.[43] DoD would provide military assistance to civilian authorities in much the same way it does currently. Put differently, restoring unity of command (and control) to achieve a global defense-in-depth will require rethinking the division of responsibilities between DoD and DHS.

In terms of architecture, a global defense-in-depth would consist of a series of networked surveillance and intelligence gathering systems; multiple intercept points for people, weapons and dangerous materials; and resources dedicated to reacting instantly to identified threats as the need arose. While there is a great deal of dialogue about globalization, there appears to be little genuine understanding of how the technologies associated with it can be applied to improve our security. Many of the technologies necessary to begin erecting a global defense-in-depth already exist, or are under development. For instance, the administration's "Smart Borders" initiative, which screens personnel and shipments that flow through U.S. borders daily, has a substantial technological component, and is already functional.[44] In addition, the DoD is developing a number of dual-use technologies, some of which have been discussed above, that can support any number of initiatives. Indeed, as one of the initiatives associated with Defense Transformation, the U.S. military is already revamping its global communications infrastructure. This

infrastructure can serve as the architectural foundation for global defense-in-depth. As Kathryn Condon, former Special Assistant to the Secretary of the Army for Military Support, acknowledged, "technology transfer could be DoD's biggest contribution to homeland security."[45]

To succeed, the concept of a global defense-in-depth would require more than the vague reference to international cooperation mentioned in the NSHS. Instead, the NSHS should outline a general plan that reflects where it intends to go and how it intends to get there. For example, step one of such a plan should be to build an international consensus acknowledging that all responsible nations have a stake and a role in defeating terrorism. Second, the plan should include a brief description of the concept of a global defense-in-depth, a defense that—it should be emphasized—would extend to all stakeholders. Third, it should state that various forums will be created for addressing the unintended consequences that might affect participating nations, particularly poorer ones. The CSI, for instance, might enhance security at the world's 20 largest ports while unintentionally limiting the opportunities for developing nations to export their goods to the United States, and other countries. The plan need not be so detailed and rigid as to be inflexible, but it must be coherent enough to attract other nations to participate.

A coherent plan centering on a global defense-in-depth would provide important guidance for the United States and other nations to begin developing bilateral and multilateral agreements permitting the deployment of certain systems and their supporting infrastructures in strategic locations. It would also help interested nations to begin establishing relationships that would better facilitate information-sharing and operational cooperation making intercept of dangerous personnel and cargo both more effective and more efficient. One strategic forum (among others) for laying the groundwork for such a plan and the necessary types of cooperation it entails is the Global Partnership against the Spread of Weapons and Materials of Mass Destruction, which was announced by the leaders of the Group of Eight (G-8) in June 2002.[46] The G-8 established the Global Partnership to "prevent terrorists, or those that harbor them, from acquiring or developing nuclear, chemical, radiological and biological weapons; missiles; and related materials, equipment and

technology."[47] Although most of the partnership's initial projects were focused on Russia and the other states of the former Soviet Union, new efforts are underway to expand the initiative into a broader Global Coalition against Catastrophic Terrorism around the World.

Furthermore, as previously mentioned, the NSHS should incorporate the combatant commanders' TCPs into its strategy for safeguarding America. The TCPs can help establish and expand a network of regional zones of security comprised of multiple collective-security arrangements and arms control agreements. The Organization for Security and Cooperation in Europe (OSCE) is an example of just such a collective security arrangement. Its members—some 55 states—share core values, institutions, and interests.[48] The OSCE approach to security is comprehensive and co-operative: comprehensive in dealing with a wide range of security-related issues including arms control, preventive diplomacy, confidence- and security-building measures, human rights, democratization, election monitoring and economic and environmental security; co-operative in the sense that all OSCE-participating states have equal status, and decisions are based on consensus. The OSCE has fielded dozens of advisor teams on missions across Europe and Central Asia to monitor and promote respect for human rights and democratic processes, including free elections, free speech, and the rule of law.

The day-to-day work of this type of security cooperation should become a high-priority effort for the U.S. defense establishment. Such work will undoubtedly require time and other limited resources, but can pay great dividends by building strategically valuable bilateral and multilateral relationships to assist the United States in conducting counter-terrorism operations abroad. U.S. military forces would thus not only respond to terrorist threats more effectively, they would also contribute proactively to building effective working relationships with any number of host nations.[49] The key is to have the TCPs tied to each other through a strategic document such as the NSHS and, in turn, tied to the idea of erecting a global defense-in-depth.

Political, economic, and socio-cultural forms of national power could also play a proactive role in protecting the homeland through a global defense-in-depth. Most experts agree that military action

alone will not defeat terrorism. Evidence suggests that social and economic development policies can weaken local support for terrorism activities, and social and economic development can deter terrorist recruitment.[50] However, they will probably not eliminate terrorism; in fact, if they are mismanaged, they can re-ignite it. Nonetheless, the point is that the U.S. strategy for protecting the homeland should speak to America's efforts to achieve security through diplomatic, social, and economic initiatives abroad. Such initiatives would constitute additional proactive elements in a global defense-in-depth. Successful strategies for combating terrorism seem to have two prongs: one aimed at crushing the immediate threat, and the other at bringing about changes that prevent its resurgence.[51] Such social and economic development policies—inexplicably missing from the NSHS—would ably complement a global defense-in-depth by laying the groundwork for striking at some of the roots of terrorism.

Conclusion.

The idea of establishing a global defense-in-depth represents a small, but extremely significant, shift in our thinking about homeland security; it's a perspective that is broad enough to appreciate the requirements as well as the opportunities presented by globalization. Accordingly, along with an internal focus—which, as previously mentioned, ought to remain a critical component of our homeland security strategy—the NSHS should include a strategic way involving the construction of a robust, global defensive network. As a strategic way, a global defense-in-depth would assist directly in accomplishing the first two ends outlined in the NSHS, namely, preventing terrorist attacks within the United States, and reducing America's vulnerability to terrorism. In terms of means, it would take advantage of various characteristics of globalization, especially emerging information technology, sensors and surveillance devices, and information sharing among law enforcement, the military, and the public and private sectors.

Unfortunately—and inexplicably—neither the NSHS nor any of the other documents related to homeland security pay sufficient attention to this important *way* in the discussion of ends, ways, and

means. Yet, if we consider these documents collectively, their intent can hardly be accomplished without it. Instead, they approach the challenge of securing the homeland in a compartmentalized fashion, reflecting an egregious lack of perspective, especially since homeland security becomes synonymous with national security at the strategic level. The NSHS should establish a genuinely global and strategic focus that each supporting document should emulate.

In today's global environment, it is imperative to think of homeland security in terms that extend beyond national borders. Actions that involve the closing of U.S. borders or disrupting the flow of people and goods through them would clearly affect the United States' and the world's economies adversely. Therefore, America's homeland security strategy must go beyond the notion of defending as far forward as possible; it must reflect a defense based on a seamless, global continuum. To make homeland security work in the 21st century, America should move from a "defend forward" mentality to one based on a "global defense-in-depth." The nation's homeland security strategy must reflect an understanding of globalization not only for the challenges it poses, but also for the solutions it offers. Above all, it must inspire confidence in the American public.

Recommendations.

- The DHS, the DoD, the intelligence community, and other federal agencies and organizations must think of homeland security—in all of its dimensions—in global terms. Globalization is making many of the tasks associated with national security too complex for anything less than a global perspective. For example, all of the regional combatant commands—not just Northern Command—should have geographic responsibilities under homeland security, and as a minimum their TCPs should be integrated into the NSHS.

- The next iteration of the NSHS should have a global defense-in-depth (in spirit, if not in name) as its centerpiece. A global defense-in-depth would entail establishing a seamless defensive continuum characterized by enhanced visibility and numerous, rapid intercept capabilities.

- The division of responsibilities between DoD and DHS must be reexamined. The current division prevents achieving the unity of command necessary for a global defense-in-depth.
- DoD should invest more in the research and development of dual-use technologies capable of being employed by military forces as well as law enforcement agencies. Concurrently, DoD should do a better job of informing DHS (and the other organizations that play a role in homeland security) of existing dual-use technologies as well as those currently under development.
- The NSHS and the national security strategy must complement each other. Measures to defend against or eliminate the immediate threat of terrorism should go hand-in-hand with efforts to bring about other social, political, and economic policies aimed at preventing its resurgence.
- Finally, the NSHS should include a general outline of a plan for achieving global cooperation in reducing terrorism and the spread of weapons of mass destruction. Lack of such a plan suggests that the architects of the NSHS are not sure what kinds of assistance the United States needs (and is willing to give) to protect the homeland.

ENDNOTES

1. The White House, *The National Strategy for Homeland Security*, Washington, DC, July 2002.

2. The White House, *The National Strategy for Combating Terrorism*, Washington, DC, February 2003; The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Washington, DC, February 2003; and The White House, *The National Strategy to Secure Cyberspace*, Washington, DC, February 2003. Some analysts recommend consolidating these strategies in the National Security Strategy, the National Military Strategy, and a national defense strategy. Michael O'Hanlon, "Testimony on Counterterrorism Strategies," Subcommittee on National Security, Emerging Threats and International Relations, House Committee on Government Reform, March 3, 2003, p. 1.

3. Experts do not agree on a definition of globalization, but they do concur that it is the "dominant element in the current security environment." Sam J.

Tangredi, ed., *Globalization and Maritime Power*, Washington, DC: Institute for National Strategic Studies, 2002, p. xxv. Thomas Friedman, *The Lexus and the Olive Tree*, New York: Anchor, 2000, p. 9, offers the most popular definition of globalization: "the dispersion and democratization of technology, information, and finance." The Defense Science Board defines it as "the integration of the political, economic, and cultural activities of geographically and/or nationally separated peoples." U.S. Office of the Secretary of Defense, Defense Science Board Task Force on Globalization and Security, *Report of the Task Force on Globalization and Security*, December 1999, p. 1. Others see it as a "substantial expansion of cross-border networks and flows." Ellen L. Frost, "Globalization and National Security: A Strategic Agenda," in *Challenges of the Global Century: Report of the Project on Globalization and National Security*, eds., Stephen J. Flanagan, Ellen L. Frost, and Richard L. Kugler, Washington, DC: Institute for National Strategic Studies, 2001, p. 37.

4. As an example of the acceleration in speed of travel, in 1927 Charles Lindbergh flew from New York to Paris in 33 hours; today aircraft can cover that distance in 5 or 6 hours. As an example of the increase in volume of travel, in 1980 approximately 287 million people traveled internationally compared to 595 million in 1996. James H. Mittelman, *The Globalization Syndrome: Transformation and Resistance*, Princeton: Princeton University Press, 2000, p. 21. To offer another example, the volume of U.S. trade doubled between 1990 and 2000. The U.S. Census Bureau, *Statistical Abstract of the United States: 2001*, p. 747.

5. Dave McIntyre, "The National Strategy for Homeland Security: Finding the Path Among the Trees," *ANSER Institute for Homeland Security*, July 2002, makes a similar point, arguing that the NSHS is more a plan for who should accomplish what within federal and local governments than an actual strategy.

6. Unfortunately, many of these means have yet to receive adequate funding. O'Hanlon, "Counterterrorism Strategies," p. 4; James Jay Carafano, "Budgets and Threats: An Analysis of Strategic Priorities for Maritime Security," The Heritage Foundation, Heritage Lectures, May 21, 2003.

7. NSHS, p. xii.

8. Jonathan Stevenson, "How Europe and America Defend Themselves," Vol. 82, No. 2, *Foreign Affairs*, March/April 2003, pp. 75-90.

9. Honorable Asa Hutchinson, U.S. Undersecretary for Border and Transportation Security, Statement to the House Select Committee on Homeland Security, June 25, 2003; The Subcommittee on Coast Guard and Maritime Transportation, "Hearing on Port Security: Shipping Containers," March 15, 2002. For population data, see U.S. Census Bureau, Annex A.

10. Robert T. Marsh, *Critical Foundations: Protecting America's Infrastructure,* Washington, DC: President's Commission on Critical Infrastructure Protection, October 1997, pp. 11-20; and Critical Infrastructure Protection Research and Development Interagency Working Group, *Critical Infrastructure Protection Research and Development,* January 2001. *http://www.ciao.gov/CIAO_Document_Library/Report_on_Federal_CIP_RD.txt.*

11. U.S. airlines have cut 100,000 jobs since 9/11, and lost $10 billion in revenue last year alone in spite of the $15 billion aid package passed by Congress immediately following the attacks. MSNBC report "War Could Magnify Airlines Woes," by Jon Bonne, March 11, 2003.

12. Surprisingly, the importance of agriculture to the U.S. economy is often overlooked; it netted $215 billion in 1999. U.S. Census Bureau 2001, p. 537. U.S. crops generally lack genetic diversity and the processing methods for livestock are centralized; each is therefore vulnerable to an attack by a biological agent. "Specter of Agro-Terrorism Looms Large—Part II," *Homeland Security Monitor,* March 28, 2002, p. 4.

13. The recreation and entertainment industries were not considered part of the nation's critical infrastructure by the President's Commission on Critical Infrastructure Protection in 1997. But, income from these industries is significant; it was $535 billion in 1999, for example, nearly twice the defense budget for that year. U.S. Census Bureau 2001, pp. 753, 755.

14. Containers come in several common lengths, including 20, 40, and 45 feet, but are counted in 20-foot equivalent units (TEUs). Total (in- and outbound) TEU in 2000 was 29 million. James M. Loy and Robert G. Ross, "Global Trade: America's Achilles' Heel," *Defense Horizons,* No. 7, February 2002, note 5.

15. Sea trade accounts for 95 percent of non-North American foreign trade; almost $737 billion in trade passed through U.S. seaports in 2000. "An Assessment of the Marine Transportation System: A Report to Congress," U.S. Department of Transportation, September 2001, p. 2.

16. The United States also consumes 25 percent of energy produced. U.S. Census Bureau 2001, p. 853.

17. This is not to say that the United States is adequately prepared for a more direct biological attack. A recent report, *Homeland Insecurity: Building the Expertise to Defend America from Bioterrorism,* published in July 2003 by the Partnership for Public Service, concluded that the nation remains unprepared for a biological attack due to a shortage of scientists and medical experts.

18. The recent black-out that affected New York City, Detroit, Cleveland, Toronto, and Ottawa illustrates the interconnectedness of U.S. and Canadian

electrical infrastructure. Barton Gellman and Dana Milbank, "Blackout Causes Mass Disruption: Millions Struggle Without Power From N.Y. to Detroit to Toronto," *Washington Post*, August 15, 2003, p. 1. Steve Rinaldi, Director, National Infrastructure Simulation Agency, briefing delivered at the U.S. Army War College, January 2003. He points out that the interconnectedness of much of the world's infrastructure is still poorly understood.

19. TRADOC Pamphlet 525-3-07, DRAFT, *Operations in the Homeland: A Concept of Army Employment*, Ft. Monroe, VA: U.S. Army Training and Doctrine Command, 2003, pp. 10-11.

20. The Toronto-based Mackenzie Institute recently issued a report stating that 15 of 80 identified international terrorist groups have members or significant supporters in Canada. Kim Bolan, "Canada a Haven for Terrorism: Report, Violent Groups Banned in Other Countries Thrive Here, New Study Says," *Vancouver Sun*, June 30, 2003. Richard Paddock, "From Canada to Kandahar: The Making of a Terrorist," *Los Angeles Times*, January 22, 2003, p. 1, describes how one Al Qaeda terrorist was born in Kuwait, but grew up in Canada. While in Canada he became attracted to radical Islam.

21. Randall Larsen, "The Greatest Threat: Not What You Might Think," *ANSER Institute for Homeland Security*, Institute Commentary, March 7, 2003.

22. Stephen E. Flynn, "America the Vulnerable," *Foreign Affairs*, Vol. 81, No. 1, January/February 2002, pp. 60-74. One analyst maintains that this initiative remains under-funded by an "order of magnitude" in the 2004 budget proposal. O'Hanlon, "Counterterrorism Strategies," p. 5. Still, the concept shows promise: a component of the system, called RISK Alert, was tested in the Philadelphia area in May 2003. Henry Holcomb, "Area Officials Have Adapted A Tracking System To Watch Over U.S. Ships In An Age Of Terrorism," *Philadelphia Enquirer*, March 12, 2003.

23. Flynn, pp. 1-62.

24. Approximately two-thirds of the goods coming into the United States come from only 25 major international ports. Asa Hutchison, U.S. Undersecretary for Border and Transportation Security, "The Progress, Status ands Plans for the Department of Homeland Security's Directorate of Border and Transportation Security," *Homeland Security Intelwatch*, August 2003, Vol. 1, No. 2, p. 5.

25. "Laser Remote Optical Sensing, LROS," briefing by Lieutenant Colonel Walter Fink, Chief, Active Remote Sensing Branch, Air Force Research Lab, delivered February 24, 2003. Assistant Secretary of State for Non-proliferation recently reported that despite the provisions of the Nuclear Non-proliferation Treaty and the Chemical and Biological Weapons conventions, proliferation

of chemical, biological, nuclear, radiological and high explosive weapons continues worldwide. Press briefing by John S. Wolf, Assistant Secretary of State For Nonproliferation Issues, at the Foreign Press Center, Washington, DC, April 16, 2002. Eleven countries currently have nuclear weapons programs; and thirteen more are actively seeking them. *http://www.cdi.org/issues/nukef&f/database/nukearsenals.html.*

26. More than 15,000 chemical sites remain unprotected and still represent attractive targets for terrorists. The Environmental Protection Agency reports that more than 100 chemical plants are large enough to endanger a million or more Americans if attacked. Gary Hart, "Business as Usual for Chemical Plants," *Washington Post,* August 11, 2003.

27. Deirdre Fulton, "Dangerous Targets on U.S. Soil," *Long Island Newsday,* March 11, 2003. The director of the International Atomic Energy Agency recently reported that there have already been 280 confirmed cases of criminal trafficking of radioactive material; he warned that stricter security measures were needed to keep radioactive material out of the hands of terrorists who could use it to make "dirty bombs." Louis Charbonneau, *Washington Post,* March 12, 2003.

28. Over 75 countries currently possess some 75,000 cruise missiles. More than 80,000 are expected by 2010. The Institute for Foreign Policy Analysis, *Assessing the Cruise Missile Puzzle: How Great a Defense Challenge?,* Washington, DC: IFPA, November 2000.

29. Judith Miller, "U.S. Is Deploying a Monitor System for Germ Attacks," *The New York Times,* January 22, 2003. Essentially, Biowatch converts many of the Environmental Protection Agency's 3,000 air quality monitoring stations throughout the country from monitoring only air pollution to also being capable of detecting anthrax, smallpox, and other deadly germs. "Secret Sensors Scout Air for Bioterrorism," *Boston Globe,* July 21, 2003, p. C6. Critics maintain that the cost of Biowatch will be high and that the system will be prone to false positives in some areas due to pollution.

30. Hutchinson, "Progress," p. 4.

31. "Secret Sensors," p. C6.

32. Peter Finn and Kamran Khan, "Bold Tracks Of Terrorism's Mastermind: Khalid Shiek Mohammed Carried Al Qaeda's Hope For Revenge, Renewal," *Washington Post,* March 9, 2003. The recent capture of another senior al-Qaeda operative, Riduan Isamuddin, aka Hambali, may also yield useful information. John Lumpkin, "Al-Qaida Operative Accused of Recruiting," *Chicago Tribune,* August 15, 2003.

33. Two years after the attacks of September 11, 2001, federal agencies still have not consolidated several dozen terrorist watch lists. Mimi Hall, "Terrorist Risk Lists Leave Gap, Even Now U.S. Hasn't Resolved 9/11 Vulnerability," *USA Today*, August 15, 2003, p. 1A.

34. Michael J. Sniffen, "Pentagon Designing System to Track Every Vehicle in a City: Program Would Use Cameras, Software to ID Cars, Drivers," *The Morning Call*, July 6, 2003, p. A13. Although the system is designed primarily to assist U.S. troops in urban fighting, it has obvious uses for the war on terrorism.

35. More than 28 million foreign visitors enter the United States each year. Currently, over 8 million people are in the country illegally. Bruce Finley, "U.S. Scrambles for System to Track Foreigners: Deadline Looms for Tracing Entries, Exits," *Denver Post*, August 15, 2003.

36. The U.S. Department of Commerce Travel and Tourism Promotion Advisory Board was recently established to make recommendations for promoting tourism in the United States. In 2001, the United States lost $12 billion in tourist dollars. Jonathan Tisch, "Be Safe, But Don't Roll Up the US Welcome Mat," *The Christian Science Monitor*, August 13, 2003.

37. "Searching for Answers, US Intelligence After September 11: A Conversation with [Senator] Bob Graham," *Harvard International Review*, Vol. XXIV, No. 3, Fall 2002, pp. 40-43.

38. National Infrastructure Protection Center, "Cyber Protests Related to the War on Terrorism: The Current Threat," November 2001, at *www.nipc.gov/publications/nipcpub/cyberprotests1101.pdf*. James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War, and Other Cyber Threats," Center for Strategic and International Studies, December 2002, argues that most national infrastructures rely on technologies that are not easily disrupted by network attacks and they have multiple redundancies. To cause more than a temporary disruption in services, hackers would need to attack multiple targets simultaneously for long periods of time to create terror, achieve strategic goals, or to have any noticeable effect. "Cyber Attacks During the War on Terrorism: A Predictive Analysis," Institute for Security and Technology Studies, September 22, 2001, p. 1, indicates that cyber-attacks are increasingly following physical attacks.

39. *National Strategy to Secure Cyberspace*, pp. x-xiii. This document outlines five priorities for promoting cyberspace security: a cyberspace security response system, a threat and vulnerability reduction program, a security awareness and training program, security of government cyberspace, a system of international cooperation.

40. White House Fact Sheet: *www.whitehouse.gov/news/releases/2003/01/print20030128-12.html.* Winston P. Wiley, "Consolidating Intelligence Analysis: Governmental Affairs Committee Hearing on the President's Proposal for a Terrorism Threat Integration Center," Joint Statement of the Terrorist Threat Integration Center Senior Steering Group, February 26, 2003. *www.fas.org/irp/congress/2003_hr/022603wiley.html.* Another problem is that the TTIC still remains woefully understaffed. John Mintz, "At Homeland Security, Doubts Arise Over Intelligence: Unit is Underpowered, Outmatched in Bureaucratic Struggles With Other Agencies, Critics Say," *Washington Post,* July 21, 2003, p. A12.

41. Diane Frank, "Threat Center Draws Praise, Questions," *Federal Computer Week,* February 14, 2003; *www.fcw.com.* Mark Sawyer, "Connecting the Dots: The Challenge of Improving the Creation and Sharing of Knowledge About Terrorists," *Homeland Security Journal,* July 2003.

42. Defense Secretary Rumsfeld stated that DoD's role within the United States is limited to "extraordinary" or "emergency" situations in which formal requests for assistance are made. Secretary of Defense Donald H. Rumsfeld, Testimony on Homeland Security before the Senate Appropriations Committee, May 7, 2002, pp. 2-3. This division of labor is also reflected in current military doctrine; see Joint Pub 3-26, *Joint Doctrine for Homeland Security* (Draft).

43. The other directorates—Science and Technology, Management, Secret Service, Citizenship and Immigration Services, and Inspector General—currently under DHS would remain there.

44. U.S. Department of State Fact Sheet, "Border Security, Smart Borders for the 21st Century," January 25, 2002. Some of the "new" technologies are not new at all, at least not entirely. Emma Schwartz, "Up, Up And Away In a High-Tech Surveillance Balloon: New Optical System Could Return Blimps to Forefront Of U.S. Defense," *USA Today,* August 18, 2003.

45. Interview with Kathryn A. Condon, Office of the Secretary of the Army, Special Assistant for Military Support, March 7, 2003.

46. Robert J. Einhorn and Michèle A. Flournoy, *Protecting Against the Spread of Nuclear, Biological, and Chemical Weapons: An Action Agenda for the Global Partnership,* 4 Vols., Washington, DC: Nuclear Threat Initiative and Center for Strategic and International Studies, 2003.

47. Einhorn and Flournoy, p. vii.

48. *http://www.osce.org/general.*

49. Unfortunately, at present, the U.S. military—and the U.S. Army in

particular—is not adequately resourced to conduct the war on terror and to maintain a meaningful presence abroad. Michael E. O'Hanlon, "Do the Math: We Need More Boots on the Ground," *Los Angeles Times*, August 12, 2003; Niels C. Sorrells and Colin Clark, "Undermanned And Overdeployed? Congress Debates Expanded Army," *Congressional Quarterly Weekly*, August 2, 2003, p. 1978.

50. Kim Cragin and Peter Chalk, *Terrorism and Development: Using Social and Economic Development to Inhibit a Resurgence of Terrorism*, Santa Monica, CA: RAND, 2003.

51. Paul K. Davis and Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism: A Component in the War on al Qaeda*, Santa Monica, CA: RAND, 2003.

U.S. ARMY WAR COLLEGE

Major General David H. Huntoon, Jr.
Commandant

*****

STRATEGIC STUDIES INSTITUTE

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven Metz

Author
Lieutenant Colonel Antulio J. Echevarria II
Professor Bert B. Tussing

Director of Publications
Ms. Marianne P. Cowling

Publications Assistant
Ms. Rita A. Rummel

*****

Composition
Ms. Gretchen S. Smith