USAWC STRATEGY RESEARCH PROJECT

WHAT ROLE FOR DOD INTELLIGENCE IN SUPPORT OF THE HOMELAND SECURITY MISSION?

by

Lieutenant Colonel Amanda Anderson
United States Army

Colonel Joseph R. Nunez
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
19 MAR 2005		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
What Role for DOD Intelligence in Support of the Homeland Security Mission?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Amanda Anderson	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**24**	

ABSTRACT

AUTHOR: Lieutenant Colonel Amanda Anderson

TITLE: What Role for DoD Intelligence in Support of the Homeland Security Mission?

FORMAT: Strategy Research Project

DATE: 17 March 2005 PAGES: 24 CLASSIFICATION: Unclassified

The attacks of 11 September 2001 brought the emphasis for security of the homeland into sharp focus. Had the government assumed too much risk to the nation's security by not aggressively exploiting the means and ways to collect information domestically, even if it would have infringed on the liberties of United States persons? Is it time to relook the Executive Order (EO) that established provisions limiting intelligence collection on United States persons to better leverage Department of Defense (DoD) intelligence assets in support of homeland security? I will examine the basic tenets regarding the balance of security and freedom that underpin our democratic governance, the history of the EO, and how other democratic systems handle this challenge. As information is passed between different levels of agencies, to include within the DoD, greater opportunity for risks to overstep boundaries is tempered by the value that DoD intelligence assets can bring to the challenges of homeland security. Within DoD, the creation of NORTHCOM may have already blurred the line concerning use of DoD assets to collect information on U.S. persons. Lastly, potential recommendations will be provided regarding the issue to include whether policy change regarding use of DoD assets is necessary.

TABLE OF CONTENTS

WHAT ROLE FOR DOD INTELLIGENCE IN SUPPORT OF THE HOMELAND SECURITY MISSION?

> It would indeed be ironic if, in the name of national defense, we would sanction the subversion of one of those liberties which make the defense of our nation worthwhile.
>
> —Earl Warren, Jurist

Since the events of September 11, 2001, much has been discussed and written about the 9/11 Commission report on homeland security and how to best use the capabilities of the intelligence community to better protect the homeland. President Bush has made homeland security a major tenet of the National Security Strategy (NSS) and General Myers, Chairman of the Joint Chiefs of Staff has done the same with the National Military Strategy (NMS). Homeland security and the war on terrorism are linked. One of the ways that security of the nation is maintained is through collection of information or intelligence domestically, which risks infringing on the rights of United States citizens.

As President Bush noted in the National Security Strategy, "intelligence . . . is our first line of defense against terrorists"[1] and the United States government must "ensure the proper fusion of information between intelligence and law enforcement."[2] In times of war, government grows and liberty yields. The principal business of government is precisely to wage war on those who threaten our liberty and security. The question, then, is how to secure liberty consistent with liberty. And in the case of the Department of Defense (DoD), what role can or should the military have? Following September 11, 2001, the executive branch sought advice from the Justice Department on "the legality of the use of military force to prevent or deter terrorist activity inside the United States" and received the response that the question was "how the Constitution's Fourth Amendment rights against unreasonable search and seizure might apply."[3] Although many authors have written about DoD involvement in domestic issues, their focus has primarily discussed the Posse Comitatus Act and "the centralization of power that would come with domestic control managed by the commander-in-chief or the secretary of defense."[4]

The National Strategy on Homeland Security articulated the challenge that information regarding homeland security had not always been shared due to "real and perceived legal and cultural barriers."[5] If "the most serious weakness in agency capabilities were in the domestic arena,"[6] then when "creating new organizations, distributing resources, and granting new powers—we may end up creating an intelligence state very different from the United States we have had during peacetime for more than two centuries."[7] In addition to Posse Comitatus, a consideration for DoD will be its limitations on collection of information domestically in order to

protect the individual rights of U.S. persons.[8] What should be the proper role for DoD intelligence in support of homeland security, then given? Should current legal restrictions be modified—and are we operating now outside these bounds?

LIMITS ON DOD AND THEIR HISTORICAL BACKGROUND

The Department of Defense and other federal agencies are limited by Executive Order (EO) 12333 respective to what information can be collected on U.S. persons, and by whom. These rules seek to balance the individual rights versus the needs for domestic security. Provisions in EO 12333 establish prohibitions and lay out responsibilities within the United States for collection of information on U.S. persons. Derived from EO 12333, DoD further promulgated its guidance with 1981 in DoD 5240-1.R. This regulation provides limitations on the collection of information on U.S. persons within the United States and on citizens outside the country that will be used for intelligence purposes.[9] It lays out procedures under which DoD components can collect, provides guidance on certain collection techniques, and governs other aspects of DoD intelligence activities to include oversight of intelligence activities.[10] Although much interest was generated after September 11, 2001 on the procedure prohibiting assassination, the larger focus of the regulation—that of collection of information on U.S. persons—appears to be largely taken for granted, despite the impact it may have on how DoD can collect or integrate foreign and domestic information in support of both the Homeland Defense and Homeland Security mission.

The constraints of EO 12333 resulted from the perception in the mid-1970s that the balance between individual rights versus domestic security had skewed too far against those individual rights upon which this nation is based. One of the ways that national security is maintained is through collection of information or intelligence domestically, which risks infringing on the rights of United States persons. The challenge is how to conduct domestic intelligence in such a manner as to balance the collection of information on U.S. citizens and the security of the nation, while "remaining consistent with the values of a democratic society."[11] Liberty, or freedom, and security are opposing conditions in which complete freedom creates anarchy in society while complete security results in a dictatorship.[12] A balance between the two must be reached.

The Constitution provides and establishes in law a system of government that defends the security of the people while also providing the guarantee of liberty. [13] The balance between security and liberty through American history has reflected the tension between these competing goals. Underscoring this balance is the "question of whether these means reinforce

or betray the democratic identity they are supposed to defend."[14] As a democracy, the U.S. government must be concerned with both "the security of the majority and the rights of the individual."[15] The collection of information on individuals falls under this sphere of liberty protection under the Constitution. The interpretation is based on Justice Louis Brandeis' majority decision regarding the right to privacy in *Olmstead vs. U.S.* in 1928, when he defined "intrusion by the government on the privacy of the individual as a violation of the Fourth Amendment."[16] These protections of individual liberty extend beyond those of U.S. citizens under the Constitution to also give aliens rights under U.S. law.[17]

The national need for balance between liberty and security resulted in the establishment of an institutionalized separation between domestic and foreign intelligence.[18] Initially codified in the National Security Act, it was further refined in Executive Orders written in response to intelligence community involvement in domestic intelligence during the 1960s, beyond the scope believed to be allowed by the National Security Act.[19] The National Security Act of 1947 codified the roles and responsibilities of the intelligence community, most clearly stating that the FBI had the internal security function, not the Central Intelligence Agency (CIA). [20]

In the mid 1970s, journalists and legislators discovered that intelligence agencies were collecting information on U.S. citizens on the authority of the executive branch and "caught up in an anti-Communist tide that swept aside safeguards against the misuse of power."[21] Up to this time, intelligence agencies were given broad discretionary powers with little supervision under the assumption they would be directing their focus outside of the United States towards foreign threats.[22] A Senate investigative committee under Senator Frank Church was charged to look into the allegations and was surprised to discover that the FBI had files on more than one million Americans (and 500,000 investigations without one single court conviction and had harassed individuals involved in both the civil rights and anti-Vietnam War movements); the NSA had monitored every cable sent to or received from overseas by Americans from 1947 to 1975; the CIA had opened mail and generated 1.5 million names for its own database in addition to infiltrating religious, media and academic organizations inside the United States; and the U.S. Army had conducted investigations on 100,000 U.S. citizens.[23] The committee's determination that the FBI had sought authority "to act against a group or individual before a crime was committed"[24] was a break from democratic values, as it indicated a shift towards investigating expression of ideas rather than violations of law. Clearly, the balance had swung against the rights of individual rights in the United States.

The Church Committee further discovered at the root of the issue was the belief by the executive branch that dissidents were acting under the influence of a foreign government, the

Soviet Union, and that "as a result, the United States would have to move outside the framework of the Constitution and the law; the legal system had become too confining in the struggle against the Soviet Union."[25] The distinction between domestic and foreign collection of information was breached and, moreover, shook the underpinning belief that the federal government upheld the democratic value of liberty espoused by the Constitution. The intelligence agencies and the executive branch had, unbeknownst to the public or to the legislative sector and based on their belief in a great threat, swung the balance to security.

As a result of the findings of the Church Committee in 1975, successive Presidents issued Executive Orders to clearly delineate the role of the intelligence agencies and to establish the need for balance in domestic information collection. Beginning with President Ford's issuance of Executive Order (EO) 11905, *U.S. Foreign Intelligence Activities*, in 1976 "to clarify the authority and responsibilities of the intelligence departments and agencies and to establish effective oversight to assure compliance with law," [26] The Executive Orders[27] symbolized executive branch recognition that although certain types of information are essential to national security decision making, at the federal level "the measures employed to acquire such information should be responsive to the legitimate needs of our Government and must be conducted in a manner which preserves and respects our established concepts of privacy and our civil liberties."[28]

When EO 11905 was rescinded and replaced by EO 12036, it loosened the restriction on CIA activity and military counterintelligence activities within the domestic sphere, but maintained FBI primacy by requiring mutually agreed upon procedures for any operations within the United States and restricting DoD to collection of military and military-related foreign intelligence.[29] Again came the reinforcement for agencies to "ensure that information is gathered by the least intrusive means possible, and limit use of such information to lawful government activities."[30]

The enactment of EO 12333 in 1982 by President Reagan, under which DoD 5240-1R serves, gives balance to both the need for individual rights and security. It does so by issuing a blanket statement that collection would be done "consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded"[31] rather than listing restrictions in the hope that would enhance "collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers."[32] While providing for domestic information collection concerns, it concentrates on emphasizing collection outside the United States while still incorporating controls on retention of any U.S. person information to such a degree as to limit infringements on domestic liberty. It did

so by authorizing agencies to collect, retain, and disseminate information on U.S. persons, but only based on procedures each agency had approved by the Attorney General.[33] These are the intelligence collection constraints on U.S. persons under which the federal government operates today.

The United States shares with other democratic nations the challenge of conducting domestic intelligence collection for counterterrorism capabilities. Britain, France, Canada and Australia all share similar characteristics with the United States including "(1) liberal democratic traditions, (2) a common concern with stemming threats to domestic stability through robust internal security infrastructures, and (3) acceptance of the need to balance operational effectiveness in the fight against terrorism with the concomitant requirement to respect fundamental norms integral to the effective functioning of an open society."[34] How these countries have chosen to organize their counterterrorism capabilities is different than current U.S. methods. In these countries, "law enforcement agencies fight crime and a single intelligence agency in each of the four countries monitors, tracks, and evaluates terrorist activity 'at home'"[35] to allow these separate entities to focus efforts on what they do best, whether it be enforcing the law or providing intelligence regarding terrorist threats.[36] In these countries, "the establishment of dedicated domestic intelligence agencies vested with unique powers of covert surveillance has helped to 'bureaucratically normalize' state security infrastructures that have considerable authority over the individual"[37] which has resulted in cases where, in the name of counterterrorism, democratic values have been violated.[38]

In the United States, the FBI attempts to do both law enforcement and intelligence, even while other federal agencies, to include DoD, also conduct counterterrorism domestically within their jurisdictions. These democratic countries models do provide a methodology to examine as the U.S. crafts its next steps in domestic intelligence, even though U.S. guidelines for domestic intelligence gathering also impose "a far more restrictive definition of permissible areas of domestic intelligence gathering"[39] than those of foreign nations. Of note, however, is that these foreign nations have enacted a state system rather than one that relies on the military.

POST 9/11—A GROWING REALIZATION OF NEW REALITY

The attacks of 11 September 2001 brought the emphasis on security of the homeland into sharp focus. As stated in the 2002 National Security Strategy, "Defending our Nation against its enemies is the first and fundamental commitment of the Federal Government."[40] The 9/11 commission echoed a call of the Hart-Rudman report that organization changes were necessary to ensure the security of the American homeland, specifically to better use the full capabilities of

the U.S. homeland security (intelligence) community. [41] The attacks revealed gaps in threat identification based on definitional boundaries that hampered proper collection of intelligence information in the domestic sphere. First, the perception of the homeland security threat shifted from one strongly focused externally to a one that could be based domestically that could involve collection of information on U.S. citizens. Federal agencies that had restricted themselves from collecting U.S. person information needed to determine how to best incorporate all domestic and foreign information for a complete intelligence picture. Second, the amorphous boundary between homeland defense and homeland security blurs lead proponency for DoD and affects what DoD can collect and retain regarding intelligence for these two spheres. Third, because the boundary between critical DoD infrastructure and critical homeland infrastructure can be blurred, the information DoD can collect to protect these assets increases the need for domestic authority.

In the aftermath of the September 11, 2001 attacks controversy arose when it was learned that government agencies did not collect aggressively collect information because an EO, currently 12333, dating back to the 1970s had established provisions limiting intelligence collection of information on United States persons.[42] Both DoD and federal agencies restricted themselves in order to meet perceived legal barriers to information collection. Although the Church Committee "demonstrated how United States security objectives could have been achieved through legal means"[43] to show how security and liberty can be compatible in a democracy, the reaction of the intelligence community appeared to be to cease any activities that might be misconstrued.

The FBI moved away from domestic intelligence investigations in the 1980s and 1990s, despite being the lead agency for foreign terrorist investigations within the United States.[44] As noted, the NSA assumed the FBI had lead of such items, and chose not to take proactive leads on any domestic intelligence.[45] Specifically in the case of the 9/11 attacks, the National Security Agency (NSA) did not collect information on communications with suspected terrorist facilities because it "did not want to be viewed as targeting persons in the United States."[46] The Federal Bureau of Investigation (FBI) failed to aggressively investigate one of the alleged 9/11 hijackers because of a requirement that "there must be 'probable cause' that he has actually committed, or is conspiring to commit, a terrorist act."[47]

More than just information sharing then, was the need to understand what exactly were the boundaries for domestic intelligence collection and how to best use assets to support or tip-off agencies with the proper authority. To meet the National Security Strategy for Homeland Security's strategic objective to "prevent terrorist attacks within the United States,"[48] information

from the domestic sphere must be integrated with foreign intelligence. The challenge is "to find a way of pooling intelligence and using it to guide the planning of and assignment of responsibilities for *joint operations* involving organizations as disparate as the CIA, the FBI, the State Department, the military and the agencies involved in homeland security." [49]

The boundary between Homeland Security and Homeland Defense further creates ambiguity for the DoD intelligence role. The integration of foreign and domestic information and intelligence to bridge any gaps in seams on potential threats spans the concepts of homeland security and homeland defense. Homeland defense is "the protection of U.S. sovereignty, territory, domestic population and critical defense infrastructure against external threats and aggression"[50] while homeland security is defined as "a concerted national effort to prevent terrorist attacks within the U.S., reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[51] Homeland defense is assumed to focus on foreign collection, and is considered the domain of the DoD, while other governmental agencies such as the FBI and now the DHS are responsible for homeland security, or internal domestic collection. As stated in the DoD Homeland Security Joint Operating Concept, this creates a "middle 'seam' of ambiguity where threats are clearly neither clearly national security threats (the responsibility of Department of Defense [DoD] or clearly law enforcement threats (the responsibility of the Department of Homeland Security [DHS], the Department of Justice [DOJ], or other agencies."[52] The mission overlap between DoD and DHS to defend the homeland, specifically detecting threats inherently places DoD intelligence collection on the boundary of what is acceptable, especially when time constraints force leaders on the scene to determine whether a transition between national security and law enforcement has occurred.

Another area of mission overlap between Homeland Security and Homeland Defense is the requirement for critical infrastructure protection. DoD inherently has the right to retain information necessary to protect that infrastructure critical to achieving its mission. But with the overlap between those aspects of infrastructure critical to DoD also potentially being essential to the nation, collection of information regarding threats again raises the question of whether DoD should have greater ability to collect or retain the necessary information. The importance of information sharing and the benefits therein are vital to homeland security, especially within and among agencies concerned with the protection of critical infrastructure.[53] In fact, a key recommendation of the 2003 Defense Science Board was that "DoD must do more to address the vulnerabilities of mission-critical infrastructure and services, particularly in areas outside its control."[54] The blurred responsibility lines between DoD critical infrastructure and homeland

critical infrastructure, just as with mission responsibility lines, only serves to reinforce the necessity to reclarify DoD intelligence collection boundaries.

With the growing realization of a new threat to the homeland, the question of whether to expand use of DoD intelligence capabilities in support of homeland security may necessarily increase. The Executive Order points to a focus outside of the United States, looking outward and defending forward, speaking to the American belief that conducting intelligence forward will limit the information collection required domestically. Defense is perceived to have a solely foreign intelligence bent, despite a counterintelligence role for its forces in the United States; a perception reinforced by an announcement in 2003 that the DHS and U.S. Northern Command (NORTHCOM) would have no formal relationship but rather NORTHCOM[55] would respond through DoD to DHS.[56] But the EO also clearly delineates that the DoD intelligence community can pass collected information to appropriate authorities, even though it may not target U.S. persons without a nexus to terrorism, foreign intelligence, or international narcotic trafficking. The Defense Science Board also saw this as an area in which DoD could expand its efforts beyond analysis and information sharing for an integrated homeland security effort. [57] In many ways, the increased use of DoD assets makes fiscal sense as DoD intelligence controls 80% of the federal intelligence budget.[58] The key to increased use of DoD intelligence in support of homeland security will be what information can be collected and how it can be used and maintained.

The changing nature of the threat also changed the capabilities of DoD intelligence to include collection and identification of threats in the domestic sphere, the DoD intelligence collection nexus, and whether the time constraint of DoD R 5240-1R is relevant against terrorist targets. While traditional foreign intelligence still exists, the threat of foreign cyber attacks "will allow some adversaries to locate and attack targets both overseas and in the United States."[59] This raises the question of how to determine how much information can be collected for computer network defense on individuals who attack networks, if no connection to a foreign threat can be established. Further, determining the characteristics of a cyber attacker could be considered either an offensive intelligence collection activity or a defensive activity for force protection. These questions are not clarified under current policy.

Next, due to the requirement of the EO, a link to a foreign threat is required before DoD intelligence assets can be used. Although a good prevention technique for unwarranted collection, it also serves to deter follow through. Lastly, the time limitation of 90 days in DoDR 5240-1R[60] for material that cannot be linked to a foreign nexus does not reflect that terrorist threats build slowly over time, and errant data points may help build the pattern for future

attacks. Defense intelligence assets can adapt to collect on the changing capabilities of threats to the homeland, but guidelines must also adapt to reflect these changes.

BYPASSING EO12333/DOD 5240-1R IMPLEMENTATION AND RISKS THEREIN

The efforts in the federal government since September 11, 2001, raise the question of whether EO 12333 and DoD 5240-1R requirements have been subsumed within the requirement for homeland security. Defense efforts to address its homeland security mission through the combatant command, NORTHCOM, may place the command in a position that limits its ability to prosecute its mission fully unless it bypasses the provisions of DoD 5240-1R. To execute the intelligence mission for Homeland Security and Homeland Defense within the most of the United States, NORTHCOM's challenge is to ensure its J2 (intelligence) section conducts operations and collects information while remaining in compliance with the regulation. NORTHCOM J2 clearly has a responsibility for the homeland defense mission to collect and retain foreign intelligence information that it may receive. However, for homeland security, NORTHCOM J2 must ensure a foreign connection exists to retain information or to conduct collection operations. The NORTHCOM J2 must rely on other federal or state agencies for threat information that may affect on DoD critical infrastructure if there is no clear link to foreign terrorists. Further, by DOD 5240-1.R NORTHCOM J2 is limited to domestic information collection and retention, even for information received from other combatant commands, because improper retention may occur.

The creation of NORTHCOM has squarely placed its J2 in a dilemma of determining where and what it can request of DoD intelligence to meet mission requirements. The J2 must balance the best way to use its access to DoD intelligence capabilities to meet mission needs until DHS and the FBI are sufficiently robust to supply the J2 with the information to meet its requirements. This same dichotomy exists within STRATCOM in its role in Global Network Operations, since there is only limited guidance that defines what or what does not constitute intelligence work in the framework of computer network defense.

The need to fuse intelligence and information for domestic homeland security has not clarified EO 12333 but established a new organization, DHS, which is not included as a member of the intelligence community. DHS, like DOJ, is classified as a law enforcement entity, which allows for the retention and collection of domestic information. DHS has the statutory authority to access all information relevant to terrorist threats to the nation and serve as the "primary provider of threat information to state and local public safety agencies."[61] Because it is not defined as a member of the intelligence community by EO 12333, it is not subject to its

provisions. This omission raises the risks that DoD intelligence capabilities, to include the NORTHCOM J2, may support DHS missions in excess of those technically allowed domestically. These issues are similar to the questions regarding oversight and responsibility for counterdrug intelligence support provided by DoD intelligence components.

The use of any intelligence or surveillance capability will inherently affect the balance between civil liberties and homeland security and may present inherent risks. In response to the perceived vulnerability of the United States, Congress passed the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, or USA PATRIOT Act, which granted "the federal government increased powers for surveillance and intelligence gathering on individuals residing in the United States."[62] The USA PATRIOT Act served as notice that it was time for loosening of restrictions on domestic collection. No changes were enacted to widen the use of DoD intelligence capabilities under the USA PATRIOT Act.

A belief that the events of September 11, 2001 and the ensuing USA PATRIOT Act does allow increased use of DoD intelligence assets to conduct homeland security missions without a lead federal agency establishes the risk that individuals may conduct inquiries without sufficient evidence. Similarly, the belief that the missions National Guard troops undertake in support of the counterdrug mission can be easily shifted to those for intelligence collection for counterterrorism fails to consider the limitations imposed by DOD 5240-1R. Regardless of status and the Posse Comitatus Act, intelligence collection is considered an inherently federal function, thereby restricting state officials from conducting military, nee foreign, intelligence missions.

RECOMMENDATIONS

The use of DoD intelligence capabilities in support of the homeland security mission reflects a historic challenge regarding balancing individual rights against security of the nation and how DoD will be used domestically. Recommendations to use DoD intelligence capabilities should be considered due to the size and scope of what DoD intelligence can bring in support of the homeland security mission. Limited policy change would serve to openly allow use of DoD intelligence capability for domestic purposes, but may too fully violate historic concern regarding use of military forces within this sphere. Also, federal agencies were established with the mission and responsibility for homeland security, so an unlimited policy change could only serve to undermine their capability.

Another possible option is a limited change to policy, similar to the sunset clause of the USA PATRIOT Act that would allow greater DoD support until such time that it is felt that appropriate federal agencies are staffed sufficiently. This method builds on the current program of assigning DoD counterintelligence assets to assist FBI field offices with counterterrorism cases and the long-standing program under Joint Task Force-6 to provide intelligence support to federal agencies for domestic missions. The risks inherent with this recommendation are the migration of domestic information between law enforcement and DoD intelligence and an increased risk of DoD intelligence assets being misused. Both these methods would require policy modification on collection of U.S. person information, at the risk of reducing individual rights within the United States.

A better method than policy change might be to use DoD intelligence capabilities to target systems vice U.S. persons. This different focus would allow use of the depth of DoD intelligence analysis capability against those means associated with terrorist activities rather than with individuals. The ability of federal agencies to be vested with the proper domestic authority would then allow them to use their assets more productively, rather than focusing on surveillance operations with their limited assets. Since "surveillance of means raises far fewer civil liberties issues than does surveillance of persons,"[63] it conceivably could be the best marriage of DoD capability with homeland security requirements.

The NSA provides an example of similar mechanism, albeit under a different operating model, and demonstrates how effective oversight can works to ensure collection capabilities are not diminished when effective controls are established. In the NSA model, its databases are populated from its collectors located worldwide and therefore include U.S. citizen information in the aggregate. These databases are available for use by intelligence analysts but filters and access approvals ensure that only certain information is accessible through data retrieval, for the most part blocking access to unauthorized U.S. person information.[64] Training, certification, and reporting procedures ensure oversight is maintained. Limiting access to the databases also ensures that only a limited number of analysts can access information. Rather than policy change, perhaps a better method is effective use of resident DoD intelligence capabilities through effective informational sharing and clearly articulated missions for support of federal agencies in the conduct of their domestic mission. This serves to meet the requirements of support for homeland security while keeping DoD out of the risks inherent in domestic operations.

CONCLUSION

The constant struggle between balancing security and domestic rights will always be present as long as there are threats to the nation's homeland security. The Department of Defense has always reinforced the efforts of federal agencies with homeland security responsibilities . We should continue to calculate the best way for the Pentagon to support the nation, within the measure of trust and confidence reposed by the populace. The response to the terrorist attacks of 9/11 presented the greatest challenge to the concept espoused by the current EO, that of balancing the values of the democratic state with the need for security to maintain the state. Any decision for new imperatives on how we determine the best way to conduct information collection for homeland security is vested in how it may reorient the balance between liberty and security. The failure of agencies to not exercise this use of their resources speaks to a larger challenge within the intelligence community and not to a need to restructure the balance towards security at the price of liberty when the question of domestic information collection is broached. Executive Order 12333 should be revisited to ensure it reflects the current construct of the IC effective with the passage of the Intelligence Bill. Defense should also examine the DOD 5240-1R to determine whether limitations are consistent with threats today that build up over time, are transnational, and which inherently may involve computer networks. Lastly, DoD and NORTHCOM should determine the best way to use capabilities resident in Defense intelligence architecture to support homeland security mission through targeting of systems and tailored use of available databases to support DHS in its mission. By doing so, the Department of Defense can marshal those resources provided to defend the nation against threats both at home and abroad without risking the confidence and trust endowed by the American people in its soldiers, sailors, airmen, or marines.

WORD COUNT=5099

ENDNOTES

[1] George W. Bush, *National Security Strategy of the United States of America* (Washington D.C.: The White House, September 2002), 30.

[2] Ibid.

[3] Tim Goldman, "After Terror, a Secret Rewriting of Military Law," *New York Times*, 24 October 2004, sec. A, p 12.

[4] Philip B. Heymann, *Terrorism, Freedom, and Security: Winning without War.* (Cambridge, MA: MIT Press, 2003), 32-3.

[5] George W. Bush, *The National Strategy for Homeland Security*, 30 April 2002; available from <http://www.whitehouse.gov/homeland/book/index.html>; Internet; accessed 26 September 2004.

[6] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: W.W. Norton, 2004), 352.

[7] Heymann,135.

[8] A U.S. person means U.S. citizens, aliens admitted to the United States for permanent residence and corporation or other organizations incorporated or organized in the United States. This definition was first established in EO 11905 and has been promulgated through succeeding EOs and in the DoD Regulation 5240.1R. This definition is wider in scope and extends protections to more than U.S. citizens. Ford, EO 11905, p 98.

[9] U.S. Department of Defense, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons* , Department of Defense Regulation 5240.1-R, December 1987; available from <http:www.dtic.mil/whs/directives/corres/html/52401r.htm>; Internet; accessed 26 September 2004.

[10] Ibid.

[11] Heymann,159.

[12] Roger Dean Golden, "What Price Security? The USA Patriot Act and America's Balance between Freedom and Security," in *The Homeland Security Papers: Stemming the Tide of Terror,* eds. Michael W. Ritz, Ralph G. Hensley, Jr., and James C. Whitmire (Maxwell Air Force Base, AL: USAF Counterproliferation Center, February 2004), 7.

[13] Golden, 9.

[14] Michael Ignatieff, *The Lesser Evil: Political Ethics in an Age of Terror (*Princeton, NJ: Princeton University Press, 2004), 21.

[15] Ignatieff, 8.

[16] Golden, 10.

[17] Ignatieff, 7.

[18] Heymann, 156.

[19] Ibid.

[20] *National Security Act of 1947*, Section 102, 26 July 1947, Washington, D.C; available from <http:www.cia.gov/csi/book/cia_origin/Origin_and_Evolution.pdf>; Internet; accessed 26 September 2004.

[21]Loch K. Johnson, "Congressional Supervision of America's Secret Agencies: The Experience and Legacy of the Church Committee," *Public Administration Review* (January/February 2004): 3 [database on-line]; available from Pro-Quest; accessed 16 September 2004.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] Gerald R. Ford, *United States Foreign Intelligence Activities*, Executive Order 11905 18 February 1976; available from <http:www.cia.gov/csi/book/cia_origin/ Origin_and_ Evolution.pdf>; Internet; accessed 26 September 2004.

[27] EO 11905 provided intelligence definitions and clearly delineated the CIA and Department of Defense (DoD) roles to conduct foreign intelligence and foreign military intelligence, respectively, while the FBI was charged with conducting "lawful counterintelligence operations within the United States." Ford, 96-98. The EO 11905 also laid out restrictions on collection specifically tied to the abuses discovered by the committee.

[28] Ford, 99.

[29] Carter.

[30] Carter, 126.

[31] Ronald Reagan, *United States Intelligence Activities*, Executive Order 12333, 4 December 1982; available from <http:www.cia.gov/csi/book/cia_origin/ Origin_ and_Evolution.pdf>; Internet; accessed 4 December 2004.

[32] Ibid.

[33] Ibid.

[34] Peter Chaulk and William Rosenau, *Confronting the Enemy Within: Security, Intelligence, and Police and Counterterrorism in Four Democracies*, Rand, 2004; available from <http.www.rand.org/publications/MG/MG100/ >; accessed 23 September 2004.

[35] _____, the United Kingdom, France, Canada, and Australia all retain dedicated structures to collect, assess, and disseminate information on domestic terrorist challenges

within their respective territorial jurisdictions. These include the UK Security Service (also known as MI5),1 France's Direction de la Surveillance du Territoire (Directorate of Territorial Security, or DST), the Canadian Security Intelligence Service (CSIS), and the Australian Security Intelligence Organisation (ASIO). In each of these cases, the agency in question has no powers of arrest, is separated from wider law enforcement but retains a close working relationship with the police, is primarily concerned with proactive threat mitigation, and is governed by specific accountability and oversight provisions.

[36] Ibid.

[37] Ibid.

[38] Ibid.

[39] Heymann, 143.

[40] Bush, *National Security Strategy of the United States of America*, preface.

[41] Gary Hart and Warren B. Rudman, *Road Map for National Security: Imperative for Change, Phase III Report of the United States Commission on National Security/21st Century*, 15 February 2001; available from <http://www.au.af.mil/au/awc/awcgate/nssg/>; Internet; accessed 26 September 2004.

[42] Reagan.

[43] Johnson.

[44] *The 9/11 Commission Report*, 423.

[45] Ibid., 87.

[46] Ibid., 87-8.

[47] Mark Reibling, "Uncuff the FBI", *Wall Street Journal* (4 June 2004):A.20. [database on-line]; available from Pro-Quest; accessed 16 September 2004.

[48] Bush, *The National Strategy for Homeland Security*, vii.

[49] *The 9/11Commission Report*, 352.

[50] U.S. Joint Chiefs of Staff, *Department of Defense Homeland Security Joint Operating Concept,* February 2004; available from <http:www.dtic.mil/jointvision/drafthls.joc_doc>; Internet; accessed 24 September 2004.

[51] Ibid.

[52] Ibid.

[53] Defense Science Board, *2003 Summer Study on DoD Roles and Missions in Homeland Security* (Washington, D.C.: Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, November 2003), iv.

[54] Defense Science Board, ii.

[55] NORTHCOM was created after September 11, 2001 as the combatant command responsible for the United States, with the requirement to support DHS and other federal agencies through the Department of Defense.

[56] Bert B. Tussing and James Kievit, "Collins Center Senior Symposium 'DoD, NORTHCOM, and the Department of Homeland Security'," *Center for Strategic Leadership Issue Paper 03-03* (Carlisle, PA: U.S. Army War College, Center for Strategic Leadership, April 2003): 1.

[57] Defense Science Board, v-vi.

[58] *The 9/11Commission Report*, 86.

[59] Richard B. Myers, *National Military Strategy* (Washington D.C.: Pentagon, 2004), 6.

[60] U.S. Department of Defense, 21.

[61] Bush, *National Strategy for Homeland Security*, 18.

[62] Golden, 11-12.

[63] Ashton B. Carter, "The Architecture of Government in the Face of Terrorism," in *Countering Terrorism: Dimensions in Preparedness,* eds. Arnorld M. Howitt and Robyn L. Pangi (Cambridge, MA: MIT Press, 2003) 28.

[64] Joel F. Brenner, "Information Oversight: Practical Lessons from Foreign Intelligence," *Heritage Lectures*, 30 September 2004; available from <www.heritage.org/research/nationalsecurity/hl851.cfm>; Internet; accessed 25 October 2004.

BIBLIOGRAPHY

Brenner, Joel. Information Oversight: Practical Lessons from Foreign Intelligence. *Heritage Lectures*, 30 September 2004. Available from <http://www.heritage.org/research/nationalsecurity/hl851.cfm>. Internet. Accessed 25 October 2004.

Bush, George W. *National Security Strategy of the United States of America*. Washington D.C.: The White House, September 2002.

Bush, George W. *The National Strategy for Homeland Security*. 30 April 2002. Available from <http:www.whitehouse.gov/homeland/book/ index.html>. Internet. Accessed 26 September 2004.

Carter, Ashton B. "The Architecture of Government in the Face of Terrorism." In *Countering Terrorism: Dimensions in Preparedness*, eds. Arnold M. Howitt and Robyn L. Pangi. Cambridge, MA: MIT Press, 2003.

Carter, Jimmy. *United States Intelligence Activities*. Executive Order 12036. 24 January 1978. Available from <http://www.cia.gov/csi/books/cia_origin/Origin_and_Evolution.pdf >. Internet. Accessed 26 September 2004.

Chaulk, Peter, and William Rosenau. *Confronting the Enemy Within: Security, Intelligence, and Police and Counterterrorism in Four Democracies.* Rand. 2004. Available from <http.www.rand.org/publications/MG/MG100/ >. Accessed 23 September 2004.

Defense Science Board. *2003 Summer Study on DoD Roles and Missions in Homeland Security*. Washington, D.C.: Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, November 2003.

Ford, Gerald R. *United States Foreign Intelligence Activities*. Executive Order 11905. 18 February 1976. Available from <http:www.cia.gov/csi/book/ cia_origin/Origin_and_ Evolution.pdf>. Internet. Accessed 26 September 2004.

Golden, Roger Dean. "What Price Security? The USA Patriot Act and America's Balance between Freedom and Security." In *The Homeland Security Papers: Stemming the Tide of Terror,* ed. Michael W. Ritz, Ralph G. Hensley, Jr., and James C. Whitmire. Maxwell Air Force Base, AL: USAF Counterproliferation Center, February 2004.

Goldman, Tim. "After Terror, a Secret Rewriting of Military Law." *New York Times*, 24 October 2004, sec. A, p. 12-13.

Hart, Gary, and Warren B. Rudman. *Road Map for National Security: Imperative for Change*. *Phase III Report of the United States Commission on National Security/21st Century.* 15 February 2001. Available from <http://www.au.af.mil/au/awc/awcgate/nssg/>. Internet. Accessed 26 September 2004.

Heymann, Philip B. *Terrorism, Freedom, and Security: Winning without War*. Cambridge, MA: MIT Press, 2003.

Ignatieff, Michael. *The Lesser Evil: Political Ethics in an Age of Terror.* Princeton, NJ: Princeton University Press: 2004.

Johnson, Loch K. "Congressonal Supervision of America's Secret Agencies: The Experience and Legacy of the Church Committee." *Public Administration Review* (January/February 2004): 3. Database on-line. Available from Pro-Quest. Accessed 16 September 2004.

Myers, Richard B. *National Military Strategy.* Washington D.C.: Pentagon, 2004.

National Security Act of 1947, Section 102, 26 July 1947. Washington D.C. Available from <http:www.cia.gov/csi/book/cia_origin/Origin_and_Evolution.pdf>. Internet. Accessed 26 September 2004.

Reagan, Ronald. *United States Intelligence Activities*. Executive Order 12333. Available from <http:www.cia.gov/csi/book/cia_origin/Origin_and_Evolution.pdf>. Internet. Accessed 4 December 1982.

Reibling, Mark, "Uncuff the FBI." *Wall Street Journal*, 4 June 2004, sec. A, p.20. Database on-line. Available from Pro-Quest. Accessed 16 September 2004.

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States. New York: W.W. Norton, 2004.

Tussing, Bert B., and James Kievit. "Collins Center Senior Symposium 'DoD, NORTHCOM, and the Department of Homeland Security'." Center for Strategic Leadership Issue Paper 03-03. Carlisle, PA: U.S. Army War College, Center for Strategic Leadership, April 2003:

U.S. Department of Defense. *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*. Department of Defense Regulation 5240.1-R. December 1987. Available from <http:www.dtic.mil/whs/directives / corres/html/52401r.htm>. Internet. Accessed 26 September 2004.

U.S. Joint Chiefs of Staff. *Department of Defense Homeland Security Joint Operating Concept.* February 2004. Available from <http:www.dtic.mil/jointvision/drafthls.joc_doc>. Internet. Accessed 24 September 2004.