STRATEGY RESEARCH PROJECT

CRITICAL INFRASTRUCTURE PROTECTION

BY

MR. JOHN S. TOMKO, JR.
Department of the Army

USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

CRITICAL INFRASTRUCTURE PROTECTION

by

Mr. John S. Tomko, Jr.
Department of the Army Civilian

COL Frank Hancock
Project Advisor

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

ABSTRACT

AUTHOR: Mr. John S. Tomko, Jr.

TITLE: Critical Infrastructure Protection

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 49 CLASSIFICATION: Unclassified

The infrastructures addressed in this paper represent a framework of inter-dependent networks and systems comprising industries, institutions, functions, and distribution capabilities. They provide a continual flow of goods and services essential to the economic well-being and security of the United States, as well as to its defense. On the National and commercial side, the infrastructure is defined by nine areas or sectors. These are: Banking and Finance; Transportation; Electric and Gas (Power); Information and Communications (Telecommunications); Law Enforcement; Government Services; Fire; Emergency Health Services; and the Water Supply. On the Defense side they are: Financial Services; Transportation; Public Works; Defense Information Infrastructure and Command, Control, and Communications; Intelligence, Surveillance and Reconnaissance; Health Affairs; Personnel; Logistics; and Space. And while the commercial side doesn't necessarily depend on the Defense side for its survival, with the exception of Public Works, the same cannot be said for the Department of Defense.

The reader should gain a sense that, in general, critical infrastructure protection is not insurmountable. In fact, protecting the infrastructure is something we do daily, especially in the Department of Defense for those infrastructures that we own and operate. And the reader should take away the knowledge that there is considerable thought and debate going into the subject.

TABLE OF CONTENTS

PREFACE

In the opening months of the Third Millennium, the United States enjoys an economic, military, and political preeminent position globally. Despite a lagging economy, the "war on terrorism," and other factors, the United States finds itself in an enviable position vis a vis the other nations of the world. This position was achieved during the 20th Century as the United States established markets, took advantage of technology, and established or strengthened its infrastructures both at home and abroad. This latter area has become not only a boon but also a burden. A boon because the infrastructures facilitate unprecedented growth. A burden because the infrastructures are increasingly dependent upon one another not only for local operations but also for survival within the global community.

The infrastructures addressed in this paper represent a framework of inter-dependent networks and systems comprising identifiable industries, institutions, functions, and distribution capabilities. They provide a continual flow of goods and services essential to the economic well-being, security, and defense of the United States. On the National and commercial side, the infrastructure is defined by nine areas or sectors. These sectors are Banking and Finance, Transportation, Electric and Gas (Power), Information and Communications (Telecommunications), Law Enforcement, Government Services, Fire, Emergency Health Services, and the Water Supply. On the Defense side these infrastructures are Financial Services; Transportation; Public Works; Defense Information Infrastructure and Command, Control, and Communications; Intelligence, Surveillance, and Reconnaissance; Health Affairs; Personnel; Logistics; and Space. And while the commercial side doesn't necessarily depend upon the Defense side for its survival, with the exception of Public Works, the same cannot be said for the Department of Defense.

Therein lies the problem for the policy makers not only at the National-level but also within the Department of Defense. For the Department of Defense the issue is one of dependency and reliance upon the commercial sector to deliver goods and services when and where needed. As Defense drew down forces, closed installations, and contracted more of its operations, it created a greater dependency upon the private sector. The private sector itself went through similar changes; the most important of which were the consolidation of operations, increased foreign ownership of once U.S stalwarts, the closing of plants in the Continental United States, and the movement of operations to foreign countries. Thus, the United States and the Department of Defense are also dependent upon the infrastructures of foreign countries. This, of course is a significant issue when developing military campaign plans.

The reader should gain the sense that, in general, critical infrastructure protection is not insurmountable. In fact, protecting the infrastructure is something we do daily, especially in the Department of Defense for those infrastructures that we own and operate. What the reader should take away is the knowledge that there is considerable thought and debate going into the subject. Additionally, there are those who have provided approaches and solutions that capitalize on existing programs as a means of reducing redundancy and cost. The difficulty, however, is the lack of a clear way ahead not only at the National level but also within the Department of Defense. This becomes more important as we define not only the meaning the meaning of Homeland Security but also the functions, systems and assets associated with that mission.

The author is grateful to Colonel Frank R. Hancock for his excellent insights on improving the content of this paper and Dot Overcash for her editing suggestions. Don Bennett deserves mention for his patience and perseverance while I developed and refined the Army Infrastructure Assurance Program. Additionally, Thomas Burrell and Doug Gaskell of Booz-Allen and Hamilton note mention for their tireless effort and assistance as we set out to discover what critical infrastructure protection meant not only for the Army but also for the Department of Defense. Also Carol Corbin (USACW Class of 2001) who continued the work back in the Pentagon while I struggled with the Strategy Research Paper. Finally, a tip of the hat to all of the Department of Defense and Inter-agency personnel involved in the critical infrastructure protection journey.

If you browse through the bibliography you will note that I have referenced a number of excellent books, articles, and papers. I am grateful to the authors who have contributed to my learning and I thank them for their scholarship. I must also inform the reader that any and all comments, interpretations, and errors of fact within this paper are entirely my own.

LIST OF TABLES

CRITICAL INFRASTRUCTURE PROTECTION

> *America's critical infrastructures underpin every aspect of our lives. They are the foundations of our prosperity, enablers of our defense, and the vanguard of our future. They empower every element of our society. There is no more urgent priority than assuring the security, continuity, and availability of our critical infrastructure.*
>
> *...the nation is so dependent on our infrastructures that we must view them through a national security lens. They are essential to the nation's security, economic health, and social well being. In short, they are lifelines on which we as nation depend.*
>
> —Critical Foundations Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection, October 1997, p vii.

The images of the events of September 11, 2001 are burned into the memory of all Americans both at home and abroad. The pictures viewed on the cable news and major television networks and in newspapers worldwide brought home to all the vulnerability of the American homeland. In the aftermath we ask ourselves how this happened and if it will happen again. We question, given the extent of the attack, why we weren't better prepared for it. We also question if we are prepared for the potential of other such attacks. And we wonder if the Executive and Legislative branches of the Federal government are prepared to take the necessary steps to resolve related issues. The President and his Cabinet are attempting to answer these questions. The concerns of the American people will be answered with statements of policy. Some related policy [antiterrorism, force protection, combating terrorism, and critical infrastructure protection] was debated, drafted, and promulgated in the previous administration. It is this policy and its execution that warrants our attention; for it is the underpinning of thought and action related to homeland security.

A review of each of the related policies is not within the scope of this paper. However, one policy, critical infrastructure protection, bears mention in that it is a vital national interest and is at the heart of how this country operates and upon which this country survives. Any antiterrorism or force protection actions under the umbrella of territorial security, homeland defense, or homeland security will focus on the infrastructures of the United States as potential centers of gravity.

In 1996 the Clinton Administration published Executive Order 13013, *Critical Infrastructure Protection.*[1] It established the President's Commission on Critical Infrastructure Protection; an organization chartered to explore the national-level ramifications of the protection or lack thereof

of the nation's infrastructure. The effort bégan as an attempt to determine the cyber infrastructure protection requirements relating to cyber war, information operations, encryption initiatives and, tangentially, the Year 2000 problem. The preamble to Executive Order 13010, in fact, establishes "critical infrastructures" as vital U.S. interests. That is, they are immediately connected to national survival, safety and vitality. As provided in the preamble these critical infrastructures include: "telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government."[2] The work of the Commission resulted in the publication of Presidential Decision Directive 63, *Critical Infrastructure Protection*, in both a classified and unclassified version. The White House published, for general public distribution, an unclassified White Paper[3] describing "the key elements of the Clinton Administration's policy on critical infrastructure protection." It established the objective and the concept that the Federal government would adhere to in order to assure a reliable infrastructure supporting enduring constitutional government.

The White Paper focused on two aspects of national power: economic and military. It described them as "mutually reinforcing and dependent"[4] and "increasingly reliant upon certain critical infrastructures and upon cyber-based information systems."[5] These infrastructures, mentioned previously, are found in the preamble to Executive Order 13010. For the Commission and for the Nation the issue is the increasing automation and interlinking of these infrastructures as a result of "advances in information technology and the necessity of improved efficiency,"[6] thus, rendering them increasingly vulnerable to human error, failure in equipment, acts of nature, and attacks both physical and cyber. The Paper suggested that "future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States."[7] It states further "our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy."[8]

President Clinton's intent was clear: "take all necessary measures to swiftly eliminate significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[9] The President established the following objective:

> No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved

and shall maintain the ability to protect our nation's critical infrastructure from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety.
- state and local governments to maintain order and to deliver minimum essential public services.
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.[10]

The concept included a "Public-Private Partnership to Reduce Vulnerability."[11] That is, the public and private sectors, in close coordination, should work to eliminate potential vulnerabilities to facilities in the economy and in the government. The concept, to the extent practicable, should neither include increased government regulation nor "unfunded government mandates to the private sector."[12] Additionally, the concept required the establishment of a National Coordinator, Lead Agencies, and Sector Liaison Officials who shall contribute to a "sectoral National Infrastructure Assurance Plan."[13] Their task was to develop a plan for "assessing the vulnerabilities of the sector to cyber or physical attacks; recommending a plan to eliminate significant vulnerabilities; proposing a system for identifying and preventing attempted major attacks; developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack."[14] Further, the "National Coordinator, in conjunction with the Lead Agency Sector Liaison Officials and a representative of the National Economic Council, shall ensure their overall coordination and integration of the various sectoral plans, with a particular focus in interdependencies."[15] Additional detail was provided in terms of guidelines and structure and organization. The objective and the concept were presented in detail.

A National Security Strategy For A Global Age was published in December 2000.[16] It established "the protection of our critical infrastructures" as a vital national interest. The National Security Strategy details, to some extent, the means with which the United States attains its objective to "take all necessary measures to swiftly eliminate significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems"[17] through the concept of Public and Private partnerships. These means included new budget proposals and specific new proposals for "Federal Cyber Systems Training and Education program to offer IT [explanation added: Information Technology] education in exchange for federal service; an intrusion detection network for the Department of Defense and for federal civilian agencies; and the institute for Information Infrastructure Protection"[18] touted as "an innovative public and private partnership to fill key gaps in critical infrastructure protection

R&D."[19] An increase of 32 per cent in Research and Development was proposed in computer security research for the fiscal year 2001 budget.[20] Other resources mentioned are the *National Plan for Information Systems Protection* and the National Infrastructure Protection Center (NIPC) established in 1998.

The Clinton Administration policy for protecting critical infrastructure recognizes infrastructure as a vital national interest. The policy establishes an objective, provides a concept, and furnishes resources. While the Clinton Administration could neither foresee the devastation nor anticipate the affect of that destruction on the national and global economy resulting from the September 11th attack, its critical infrastructure protection policy provides a starting point for homeland security actions. In the wake of the September 11th terrorist attack, the Bush Administration will fine-tune this policy. Considering the current will of the people and the mood in Congress, it appears that the Administration will receive the necessary resources to carry its homeland security and critical infrastructure protection programs. The difficulty facing the current Administration is in determining infrastructure "criticality" in terms of what to protect, when to protect it, and how to protect it. This will be done in the face of competing private sector and Congressional interests. Keeping in mind the admonition that if you protect everything you protect nothing, the Administration will walk a fine line in balancing the concept, objectives, and resources relating to critical infrastructure protection.

BACKGROUND[21]

The antecedents of the current Department of Defense Critical Infrastructure Protection Program are the "Key Asset Protection Program" and the "Critical Asset Assurance Program." Initiated in 1989, the former concentrated on the protection of those off-post non-military assets (privately owned assets supporting the Department or government owned and contractor operated assets) within the Continental United States. The U.S. Army Corps of Engineers was the executive agent and the U.S. Army Forces Command was the action agent for this program and the Defense Investigative Service also played a role.

In 1998, the Department of Defense expanded the protection program renaming it the "Critical Asset Assurance Program." This focused on the protection of *critical* assets both on and off post and both within and outside of the Continental United States. For the next year the Secretary of the Army was the program executive agent. His program action agent was the Director of Operations, Readiness and Mobilization, Office of the Deputy Chief of Staff for Operations, Headquarters Department of the Army. The role of other organizations, namely U.S. Army Forces Command and the Defense Security Service (formerly the Defense

Investigative Service) remained undefined although each maintained cognizance of the ever-evolving program.

In August 1999, program executive agency was transferred to the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). The transfer resulted from action initiated by the Army because of the ever-changing nature of the program and the need to have the requisite policy written in the highest levels of the Defense establishment. With the change in executive agency also came a change in program name – "Critical Infrastructure Protection Program." The current program extended the Critical Asset Assurance Program by focusing on both cyber and physical infrastructures although, because of the nature of the business of the new executive agent, the Critical Infrastructure Protection Office emphasized the cyber infrastructures. The Army did not back away from the problem just because it handed policy responsibility to the Office of the Secretary of Defense. The Army embarked on a re-tooling of its internal program; resulting in the "Army Infrastructure Assurance Program."

ARMY INFRASTRUCTURE ASSURANCE[22]

The Army Infrastructure Assurance Program derives its authority from Sections 117, 3013 and 3962 of Title 10 – Armed Forces, United States Code, Presidential Decision Directive 63, *Critical Infrastructure Protection*, and Department of Defense Directive 5160.54, *The Critical Asset Assurance Program*.[23]

STRATEGIC PLANNING ENVIRONMENT

PRINCIPLES AND RELATIONSHIPS

Army infrastructure assurance is designed to ensure the continued performance of the functions required for mobilization, deployment, sustainment, redeployment, and reconstitution missions in support of a unified combatant command's operations and contingency plans. It leverages existing Army protection programs (physical security, personal security, information systems security, antiterrorism and force protection, and operations security); however, it is more than just protection of assets and personnel. Headquarters Department of the Army, Army Major Commands, and Army installation commanders assure Army infrastructure through plans, operations, force protection and contracts that preserve the capability to perform the functions required to support the warfighter across the full operational spectrum. These plans, operations, and contracts emphasize not only protection activities but also alternative courses of action and contingency plans to ensure that the Army can mobilize, deploy, sustain, re-deploy, and reconstitute forces. The natural consequences of these activities in today's environment

are that, in the absence of a major theater war, Army infrastructure assurance actions must also ensure the viability of the communications zone in the Continental United States.

Army infrastructure assurance is guided by two fundamental principles: leverage existing programs and ensure support to the warfighter. By leveraging existing programs, the Army incorporates active and passive measures to protect and preserve Army infrastructure (cyber and physical), equipment and personnel potentially reducing redundancy and cost. The Army ensures support to the warfighter through analysis of potentially vulnerable systems, functions, and assets and linking these to the warfighter through an analytical process (discussed later in this paper) based on the unified combatant commander's operations or contingency plan(s). These foregoing actions are also linked to current and future readiness programs in order to maintain awareness of risk management efforts associated with the Army's power projection platforms. Additionally, the Army ties these efforts to the Planning, Programming, Budgeting and Execution System in order to provide an additional level of visibility tied to resources used to mitigate vulnerabilities. This allows for the prudent application of resources against those deficiencies threatening the continuance of functions supporting the execution of the unified combatant command's operations and contingency plans. Likewise, it allows for similar support to Homeland Security.

ENVIRONMENT

The growing complexity and interdependence of Army, Department of Defense, national and international infrastructures, coupled with an increase in outsourcing and privatization of Army and Department of Defense functions, directly affect the Army's readiness and its ability to conduct operations. These factors, along with a more computer literate population and the emergent asymmetrical capabilities of its adversaries, increase the risk to the Army's ability to undertake its Title 10 – *Armed Forces* United States Code missions in support of the warfighter. Constrained resources complicate mitigation of these risks. Nonetheless, as the Army enters the Third Millennium, it must look beyond traditional protection programs to strategies that assure the capability to perform missions required to execute the National Military Strategy.

The United States exists in a complex and potentially dangerous environment that includes terrorist threats and on-going cyber attacks. The free and open nature of our society makes it increasingly vulnerable to terrorist and asymmetric attacks. A growing population increases the vulnerability to the effects of manmade and natural disasters. As a major source of Homeland Security resources, the Army must be prepared to respond to increasing calls for capabilities within this complex, danger-filled environment.

Threats of both a natural and manmade nature are increasingly capable of causing mass casualties and infrastructure damage within the United States and within the combatant commander's area of operations. They can disrupt the planning and conduct of military operations and represent a significant challenge to public, private, Federal, and host nation supporting resources.

The battle space for Army infrastructure assurance is primarily the United States, its territories, possessions, and all potential areas of operations within which any one of the Unified Combatant Commanders operates. Unlike the continental battle space for Homeland Security, ships in international waters, aircraft in international airspace, U.S. embassies and overseas military bases, remain part of the battle space. Host nation assets supporting the execution of mission essential functions in foreign countries are also included. The foregoing describes a massive physical space, with extreme varieties in facilities, weather, and terrain. Infrastructure assurance planning and execution is required for the entire spectrum of operations. This, coupled with the enormity of the battle space, makes detailed advance planning difficult, but nonetheless required.

Another portion of the operational environment is the understanding of the concept of functions, systems, and assets. This understanding is essential for successful execution and support to the combatant commander. Functions are high-level aggregations of mission-focused tasks. Systems are various mechanisms used to perform the functions. Functions can be accomplished by using the two types of systems that are categorized as either process systems or information systems. Process systems capture how work is accomplished from a conceptual perspective irrespective of the tools used to perform the work. An information system represents the interconnection of communication networks, computers, and databases that make information available to users. Finally, assets are military, public or private, on- or off-post, domestic or foreign resource, real property (land, buildings, or other structures, etc.) supplies, equipment, and software.

CAPABILITIES AND CONSTRAINTS

The Army brings a number of tangible capabilities to bear on the infrastructure assurance mission. These are the Army's existing protection, reporting and resource management programs. These mature programs ensure the overall protection of soldiers and property as well as the management and resourcing of the force. These programs must be synchronized in order to prioritize efforts for ensuring support to the warfighter.

The Army is also faced with three significant constraints to its effort to support the warfighter through infrastructure assurance. The first is the fusion of existing assessments. Currently, there is no focal point for the fusion of vulnerability and risk management information. Information from vulnerability assessments (Balanced Survivability Assessments, Joint Staff Integrated Vulnerability Assessments, Transportation Infrastructure Criticality and Vulnerability Assessments, and Service-directed vulnerability assessments) and other related reports and inspections are not readily available while others are restricted. Additionally, there are currently no efforts to correlate the results of these and related assessment and "Red Team" reports to determine the overall infrastructure vulnerability of an Army power projection platform or supporting Army installation. Most notable is the lack of an ability to determine overall vulnerability trends and to correlate these with trends both within the Federal government and the private sector.

The second constraint is outsourcing and privatization. Today, the increased number of privatized and outsourced functions complicates the Army's ability to assure the infrastructure required to support the execution of combatant command operations and contingency plans. The availability, under an all hazards scenario, of privatized or outsourced personnel, equipment, and services is essential to the accomplishment of the Army's mission Title 10 – *Armed Forces* United States Code missions. Procedures governing these privatized and outsourced functions and activities require detailed review to ensure that they fully support Army infrastructure assurance activities.

The final constraint is in the realm of support to civil authorities concurrent with the execution of a Unified Combatant Command operations plan. Because of its flexibility, the Army is able to respond to general-purpose requests for support if other missions are not also a current requirement. When responding to situations requiring the full implementation of the National Military Strategy, support to civil authorities could be severely constrained. Events that call for the use of Army forces in conjunction with, or as a precursor to, a major theater war, could easily exceed current capabilities. In addition, a series of coordinated attacks, independent of a major theater war, can exhaust the Army's ability to respond. Of course, the events of September 11th, 2001, now add another element to the mix. That is, the emphasis on Homeland Security. The Army will surely be called upon to contribute forces to a greater degree than those now guarding airports and nuclear power plants. It is possible to see major changes in the role of the National Guard. The question for the leadership is: "How do we allay the fears of the American public relative to military support to civil authorities in the case of natural disasters?"

STRATEGIC PLANNING DYNAMCS

Army infrastructure assurance, like warfighting, is conducted on three levels: strategic, operational, and tactical. The strategic level equates to the Headquarters Department of the Army. The operational level is the Army major commands and the tactical level is the Army installations (posts, camps, and stations). Each level supports infrastructure assurance through different means. However, the sum total of work performed at these levels creates a synergism to assure Army infrastructure in support of the warfighter at all levels.

Within the strategic, operational, and tactical levels of infrastructure assurance commanders and staffs execute distinct planning activities. They accomplish these activities with differing methods based upon experience, responsibilities, and needs. There are three principle and four supporting activities relevant to Army infrastructure assurance. The three activities used to analyze the combatant commander's requirements in order to identify, assess, and mitigate risks are analysis, assessment, and mitigation. The Army uses a structured mission-based analysis to identify those infrastructure functions, systems, and assets that are essential to the accomplishment of the Army's Title 10 mission in support of the warfighter. As required by existing protection programs, Headquarters, Department of the Army, Army Major Commands, and Army installations all conduct assessments. These assessments provide an objective evaluation of the vulnerabilities and risks associated with a specific installation, system, or asset. Commanders and staffs conduct mitigation in response to the vulnerabilities and risks identified through the assessment process. Mitigation reduces or eliminates long-term risk to people and property from hazards and their effects. The intent is to focus on actions that produce repetitive benefits over time, not on those actions that might be considered emergency planning or emergency preparedness.

The Army relies on five supporting planning activities (indications, warning, incident response, remediation, and reconstitution) to assure Army infrastructure. These activities are developed and provided independently of Army infrastructure assurance. However, the Army leverages these existing activities to provide a complete program that assures Army infrastructure, before, during and after an event.

The Army Staff provides indications of possible threat and natural events to Army Major Commands and Army installations through the existing force protection program and command channels. This provides installation commanders with indications of events that may directly threaten Army or commercial infrastructures supporting the execution of Unified Combatant Command operations or contingency plan(s). State and local governments also provide

installation commanders with indications that assist in adjusting mitigation procedures in response to a threat or natural conditions.

The Army Staff provides warning of threat and natural events to Army Major Commands and Army installations using the existing command and control systems. These warnings provide installation commanders the information needed to make mitigation decisions.

Incident response seeks to eliminate the cause or source of an event and is conducted primarily by installation commanders. The Army Staff and Army Major Commands support incident response by providing resources that allow subordinate commanders to eliminate the cause or source of an event.

Army installation commanders conduct remediation activities to minimize or alleviate the negative impact of a hazardous situation on people, facilities, operations, or services, and by quickly restoring the functions required to support a unified combatant command operation or contingency plan(s). The Army Staff supports remediation by providing resources to ensure Army Major Command and Army installation commanders can facilitate immediate response. The Army Staff also supports remediation through the Joint Staff and the Office of the Secretary Defense to coordinate remediation efforts of the national, public, and private infrastructures.

Reconstitution is conducted at all levels and seeks to rebuild or restore an infrastructure after it has been damaged or compromised. The Army Staff and Army Major Commands support incident response by providing resources to rebuild or restore an infrastructure after it has been damaged or compromised.

PLANNING ACTIVITIES (TACTICAL AND OPERATIONAL)

At the tactical level, commanders assure Army infrastructure through implementation of Army protection programs. At the operational level, Army Major Command staffs and commanders ensure these protection programs are implemented and sustained with adequate resources to ensure the Army installation has the capability to perform the functions required to support the warfighter.

PLANNING ACTIVITIES (STRATEGIC)

At the strategic level, the goal is to assure the capability of the United States Army to perform the functions required to support the operations and contingency plan(s) of the unified combatant commands. To do this, the Army Staff focuses on three principle activities: strategic analysis, strategic assessment, and strategic mitigation.

Strategic Analysis. The Army Staff develops and provides a mission-based analysis capability to Army Major Commands and Army installation commanders in order to identify

those functions that, when not assured, will result in a negative impact on the installation commanders' ability to execute their missions as well as the Army's ability to support the unified combatant command operations and contingency plan(s). A mission-based analysis also helps department-level planners and policy makers identify intra- and interdependencies between and among supporting infrastructures, both public and private.

Strategic Assessment. The Army Staff uses a variety of existing assessment programs to identify and understand the vulnerabilities and risk associated with a specific installation, system or asset. These assessments include Joint Staff Integrated Vulnerability Assessments, Balanced Survivability Assessments, physical security assessments, information systems security assessments, the Installation Status Report, other reports, and reports from the Inspector General. Based on these assessments, the Army Staff provides subordinate commanders an integrated assessment of vulnerabilities that affect their ability to support execution of unified combatant Command operations or contingency plan(s).

Strategic Mitigation. The Army Staff supports mitigation programs by providing strategies and resources to Army subordinate commanders as a part of existing programs. The Army Staff also supports mitigation through the Joint Staff and the Office of the Secretary Defense to coordinate mitigation with national public and private infrastructures.

FUSION ACTIVITIES.

The convergence of the strategic, operational, and tactical levels is the fusion of the eight infrastructure assurance planning activities. However, the focus is on the fusion of mission-based analysis with existing vulnerability and risk assessments. The capability to fuse and synthesize this information provides an Army-level view of vulnerabilities, trends, and mitigation priorities. Fusion activities assist each level in planning and programming resources and they provide the capability to monitor the expenditure of resources used to mitigate vulnerabilities and manage risk. Additionally, fusion activities offer a consolidated infrastructure vulnerability assessment report to the Army installation commander assisting in his infrastructure vulnerability mitigation management efforts. The next section provides a proposal for the mission, organization, and capabilities required for a fusion activity.

MISSION ANALYSIS METHODOLOGY[24]

> *Real vulnerabilities...exist. Infrastructures have always been subject to local or regional outages resulting from earthquakes, storms, and floods. Their owners and operators, in cooperation with local, state, and federal emergency services, have demonstrated their capacity to restore services efficiently. Physical vulnerabilities to man-made threats, such as arson and bombs, are likewise not*

new. But physical vulnerabilities take on added significance as new capabilities to exploit them emerge, including chemical, biological, and even nuclear weapons. As weapons of mass destruction proliferate, the likelihood of their use by terrorists increases.

--Critical Foundations Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection, October 1997, p 5.

BACKGROUND

Army infrastructure assurance, like warfighting, is conducted at the strategic, operational, and tactical levels. The Army, as the predominant land force, is required under Title 10 – *Armed Forces*, United States Code, to man, equip, train, deploy, sustain, re-deploy, and reconstitute a force in order to support the unified combatant commander. To meet these responsibilities, the Army depends on public, private, and Department of Defense infrastructure both in the Continental United States and outside of the Continental United States. In order to determine the relative value of an infrastructure on an Army asset the Army requires a methodology for analyzing the unified combatant commander's operations plan or contingency plan and the time-phased force deployment list. The methodology proposed below fulfills the requirement for an analytical process to identify functions, systems, and assets by which the Army supports the execution of the unified combatant commander's operations plan. This analytical process identifies supporting infrastructures, both public and private, and intra- and inter-dependencies between and among infrastructures. It also serves as a way to fine-tune plans. Identifying the functions supporting the warfighter and integrating these results into existing vulnerability and risk assessment processes provides the basis for focused mitigation of infrastructure vulnerabilities. The Army achieves this objective by synchronizing the results of the analysis of the operations or contingency plans with existing protection programs (Army and other) to ensure a holistic program addressing mitigation strategies across the full spectrum of hazards.

At the tactical (installation) level, commanders assure Army infrastructure through the implementation of Army protection and security programs. At the operational (Army Major Command) level, commanders and staff ensure that these protection and security programs are implemented and sustained with adequate resources to ensure that the Army installation (posts, camps, and stations) has the capability to perform the functions required to support the warfighter. At the strategic (Headquarters Department of the Army) level, the goal is to assure the capability of the United States Army to perform those functions required to support the plans of the unified combatant commands. To accomplish this, the Army requires an analysis methodology and provides it to the Army Major Commands and the Army installations so that

they can identify those functions, systems, and assets that, when not assured, result in a negative impact on the Army commander's ability to execute his mission. This methodology also helps the department-level planners and policy makers to identify intra- and inter-dependencies between and among supporting infrastructures, both public and private.

Problem

The Army does not currently have a process to identify mission essential functions that are in direct support to the unified combatant commander. Likewise, the Army does not currently have a process through which mission essential functions, systems and assets can be vetted against existing vulnerability assessment processes in order to perform focused risk management.

Facts Bearing on the Problem

There are four significant facts that, the inability to deal with any one of them, cause the Army to fail in its responsibilities under Title 10 – *Armed Forces*, United States Code. These are as follows:

- Scarce mitigation resources require the development of a focused ability to identify mission essential functions.
- The Unified Combatant Commander's operations plans, the time-phased force deployment lists, and high demand low density assets are all crucial to identifying mission essential functions, systems, and assets in support of the warfighter.
- The correlation of information derived from a mission-based analysis and existing vulnerability assessments and studies is essential in determining the Army's ability to support the warfighter.
- Multiple agencies and organizations perform vulnerability assessments.

MISSION ANALYSIS METHODOLOGY

As previously stated, Army Infrastructure Assurance concentrates on assuring functional capability as opposed to concentrating specifically on the protection of individual assets. This concept is never more important than when attempting to determine the "criticality" of systems, functions, or assets as they support the Title 10 – *Armed Forces*, United States Code, responsibilities of the Army in relation to its support of the warfighter. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) has wrestled for over two years in attempting to determine infrastructure "criticality" in terms of infrastructure "vulnerability" of a given asset. The approach has concentrated on vulnerability assessments relating to assets "owned" by the commanders of the combatant commands. Unfortunately, it has turned out to be nothing more than these commanders submitting wish lists of vulnerable assets that are "owned" by others. That is, the Services, the Host Nations, and contractors. This approach allows for no rigor nor does it consider the Commanders-in-Chief's

requirements as articulated in the operation plan(s) and time-phased force deployment lists. Additionally, it does not allow for determining how another operation or contingency may affect the outcome of the war fight because of the potential dependence by other warfighters on similar infrastructure assets.

The author searched for alternative means for determining what the Army had to do in order to ensure that it could support the warfighter through the full spectrum of operations. The methodology finally agreed upon was a basic input / output model with feedback mechanisms covering four processes of analysis. These processes are: Identify the Army resources provided to the warfighter; Link the warfighter's Army resources to Army and Defense infrastructure functions; Array intra- and inter-dependent systems and assets by owner(s); and Identify vulnerable mission essential systems and assets. The analysis associated with these processes encompasses Mobilization and Deployment; Army Assessment, Mitigation and Protection Processes; and Reports and Studies. The desired end state of the analysis is an Army capable of supporting the warfighter under all conditions. The methodology described below may not be the only one allowing the Army or another Service, for that matter, to conduct a capability analysis; this one worked to a degree that was not found in other methodologies tried.

Process I, Identify the Army resources provided to the warfighter.

In *Process I* planners require an understanding of how the warfighter intends to accomplish the described mission. In other words we are looking for his requirements and his intent and we are identifying Army warfighting requirements of the unified combatant commander so that they can be linked to the supporting Army infrastructure. These become the basic input with which our analysis starts. We find these requirements in the Time-phased Force Deployment List, the list of War Reserve Stocks, and the operations plan. The process step is to identify Army units, Army support functions, Army supporting assets, and Army required supplies from both the operations plan or the contingency plan and the Army War Reserve Stocks. The Time-phased Force Deployment List tells us when these "assets" are required in theater, the mode of transport, and the aerial port or seaport of debarkation. This information in-turn allows us to determine Army personnel and equipment and Army War Reserve Stocks in both the Continental United States and those outside of the Continental United States. The output from this basic review yields a list of the overall requirements of the warfighter in terms of Army personnel and equipment, Army War Reserve Stocks, warfighter "critical assets" as found in Appendix 16 of the operations plan, Flexible Deterrent Options,

functions, systems, and assets, and Army personnel and equipment already in the theater of operations.

Process II, Link the warfighter's Army resources to Army and Defense infrastructure functions.

In *Process II* the output from Process I carry over to become input for the Process II analysis. Two additional inputs are added at this stage. The first is the Army Mobilization Operations and Execution System and the Forces Command Mobilization and Deployment System. This set of documents gives the analyst a better understanding of how the Army mobilizes itself to support the warfighter. It also contains details pertaining to the functions of the mobilization stations and other mobilization requirements. However, while these sets of documents cover the vast majority of the Army and how it mobilizes, each Army Major Command has its own documents relating to mobilization and deployment. When required, these documents also become another input to Process II. The second form of input is the Defense Sector infrastructure characterizations. Described earlier in this paper, these characterizations provide a view of how the infrastructure within a Defense Sector is arrayed, its intra-dependencies, and its potential inter-dependencies with the other Defense Sectors. The process involved in this step is to establish relationships between and among all of the available information contained in the input as described. Three outcomes result from this procedure. First, we find the inter- and intra-dependent systems and assets required to mobilize and move personnel, equipment, and supplies owned and provided for by the Army and the Department of Defense. Second, we find inter- and intra-dependent systems and assets required to mobilize and move personnel, equipment, and supplies owned and provided for by the agencies of the Federal Government and by commercial enterprises. Third, we find the functions required to provide strategic, operational, and tactical command, control, communications, and intelligence support. This output forms the input for Process III. It also completes the Mobilization and Deployment Assessment.

Process III, Array intra- and inter-dependent systems and assets by owner(s).

Process III is the beginning of the Army Assessment, Mitigation and Protection Processes. During this step sorting is the primary action. Taking the output of Process II, and reintroducing the Defense sector characterizations as a baseline, the analyst sorts the information based upon organization asset ownership and organization mitigation responsibilities. Two outcomes result from this sorting. The first provides feedback to the Defense infrastructure sector lead with a verified list of required functions, systems, and assets. This list supports revision of the Defense Infrastructure Sector Assurance Plan. The second, provides feedback to various Army, Joint, and National organizations in the form of a verified list

of functions, systems, and assets in order to assist in vulnerability assessments, risk management, and mitigation efforts.

Process IV, Identify vulnerable mission essential systems and assets.

Process IV takes all of the previous information (lists of mission essential functions and their associated systems and assets) and some new information (in the form of reports and studies) for the purpose of identifying vulnerable mission essential assets. These reports are reviewed in a process that we call "Fusion Activities" (these activities are covered in detail later on in this paper). These reports and studies may be:

- Joint Staff Integrated Vulnerability Reports (conducted by the Joint Staff);
- Balanced Survivability Assessments (conducted by the Defense Threat Reduction Agency); Commercial Reports;
- Transportation Infrastructure Criticality and Vulnerability Assessments (conducted by the U.S. Army Transportation Engineering Agency);
- National Industrial Security Program Assessments (conducted by the Defense Security Service);
- Defense Security Service Arms and Explosives Security Support:
- Information Assurance Readiness Reviews (conducted by the Defense Information Systems Agency);
- Joint Program Office - Special Technical Countermeasures Infrastructure Assurance Program Assessments;
- National Security Agency Information Security Vulnerability Assessments (conducted by the National Security Agency);
- SECRET Internet Protocol Router Network Compliance Validations (conducted by the Defense Information Systems Agency);
- Security Readiness Reviews (conducted by the Defense Information Systems Agency);
- Vulnerability Assessments (conducted by the Defense Logistics Agency in conjunction with the U.S. Army Corps of Engineers);
- Inspector General Reports addressing process or procedural vulnerabilities;
- Federal Bureau of Investigation reports and assessments;
- Other assessment reports addressing vulnerabilities.

Three things take place during this process. First, a comparison is made of systems and assets associated with mission essential functions against results from the reports, studies, and assessments addressing vulnerabilities. Second, a determination is made of the quality and quantity of the information available on assessed systems and assets. Third, an analysis is made of Army-wide vulnerabilities, trends, and resources to assure Army infrastructure. This results in the following output.

- One, a list of vulnerable mission essential systems and assets that can be sorted by function, geographical location, region, and owner.
- Two, a list of vulnerable mission essential systems and assets that can be sorted by function, geographical location, region, and owner *requiring reassessment.*

- Three, a list of trends and resources associated with mission essential systems and asset vulnerabilities that can be sorted by function, geographical location, region, and owner.

These outputs can serve as the basis for developing a mitigation strategy or strategies by function, by geographical location, by region, or by owner. Additionally, the results of the analysis can be fed back to the warfighter and the Joint Staff in order to fine-tune the operations plan and or the time-phased force development list.

Example

The Commander-in-Chief Pacific is told that a vulnerability exists at a bridge in the Pacific Northwest. This bridge, he is told, conveys the only road into an ammunition supply facility. Additionally, he is told that not only does the bridge convey the road it also conveys all of the fuel and power lines, not to mention the water main, into the facility. He is further told that, if a terrorist were to drop the bridge a war fight would be in jeopardy in a designated region of his area of operation. The Commander-in-Chief is concerned. He cannot believe that this single "critical" infrastructure could affect the outcome of a campaign. He wonders who would draw up a plan that allowed for such a vulnerability. However, his background and experience tell him that what he really needs to do is to attack the problem from two angles. The first is to determine how much a delay there will be in moving ammunition to the theater if the bridge is destroyed. Second, to determine how he can work around the problem. Using the mission analysis methodology he determines that the in-theater commander has significant stock of ammunition in depots in country. Based upon the calculations he has enough ammunition of all kinds to fight the campaign for ninety days without re-supply. Additionally, the engineers tell the Commander-in-Chief Pacific that they can have the bridge back in operation in less than two weeks. However, if the engineers are incorrect in their assessment, he has the ability to coordinate movement of ammunition from other deep port facilities on the West Coast and still meet ammunition requirements in theater. What the mission analysis told the Commander-in-Chief Pacific was that the bridge, while vulnerable, was not "critical" to the execution of the plan.

FUSION ACTIVITY[25]

> *...sharing information isn't enough; we need the analytic tool to examine information about intrusions, crime, and vulnerabilities and determine what is actually going on in the nation's infrastructures. Deciding whether a set of cyber or physical events is coincidence, criminal activity, or a coordinated attack is not a trivial problem. In fact, without a central information repository and analytic capability, it is virtually impossible to make such assessments until after the fact.*
>
> --Critical Foundations ***Protecting America's Infrastructures*: The Report**

of the President's Commission on Critical Infrastructure Protection, October 1997, p 28

The concept of operations for the Army Infrastructure Assurance Fusion Activity is designed to express as abstract idea relating to infrastructure assurance risk management. Specifically, it outlines a proposal to establish, within the Army, a method for analyzing multiple vulnerability assessments and reports as they relate to the combatant commander's operations plan. The result is comprehensive infrastructure assurance risk management plans with associated cost.

The need for an infrastructure assurance fusion activity is demonstrated by the fact that the Army does not have a means of correlating the disparate reports and vulnerability assessments, provided by numerous organizations both inside the Army and the Department of Defense and external to the Department of Defense, in order to determine risk to its ability to support the unified combatant commander. A fusion activity, as described herein, provides that capability. The fusion activity is seen as a value added organization providing another tool for infrastructure assurance risk management activities supporting strategic readiness.

The need for a fusion activity is based upon experience gained over the last two years. It is built on conclusions drawn from various mission-based analysis studies and the inability of the critical infrastructure protection community to determine an acceptable meaning of and standard for "criticality."

The author recognizes the difficulty in establishing new organizations at any time but especially in today's environment. However, the Army cannot afford not to regard an organization of this type, considering the possibilities for a focused and coordinated infrastructure assurance risk management strategy.

The concept and ideas expressed may appear threatening to some stakeholders. This is always true when innovation is proposed. However, there are significant long-term benefits to be gained militating against perceived parochialism. It is the best interests of National Security that stakeholders share ideas about improving the concept, specifically in the areas of policy related to the sharing of various types of vulnerability assessments and reports across the inter-agency.

PROBLEM

From an infrastructure assurance (critical infrastructure protection) standpoint, the Army does not have a means of correlating mission essential functions supporting operations or

contingency plan execution with the disparate reports and vulnerability assessments.

Specifically, the Army does not have an organization chartered to:

- Manage the identification of all strategic, operational, and tactical functions, systems and assets required to support Army execution of a unified combatant command operations or contingency plan.
- Oversee and act as a catalyst for the fusion of Army infrastructure assurance analytical activities with existing assessment and mitigation activities.

FACTS BEARING ON THE PROBLEM

- No central clearing house exists within the Army for the express purpose of correlating infrastructure information in order to provide a comprehensive risk management information to installation commanders and the unified combatant commander.
- There are numerous reports, studies, and assessments concerning infrastructure vulnerabilities developed by Defense and public and private organizations. These reports can be installation or asset specific.

CONCEPT

Risk Management

The essence of any decision-making is making trade-offs among very difficult and complex objectives that are often in conflict and competition with one another. Good qualitative risk assessment and management must be grounded on basic systems engineering philosophy and principles. Good risk studies must be judged against valid criteria. The Center for Risk Management of Engineering Systems, University of Virginia suggests 10 criteria for risk studies. The study must be...

- Comprehensive,
- Adherent to evidence,
- Logically sound,
- Practical and politically acceptable,
- Open to evaluation,
- Based on explicit assumptions and premises,
- Compatible with institutions,
- Conducive to learning,
- Attuned to risk communication, and
- Innovative.

Army infrastructure assurance risk management is a process that must answer the following set of questions.

- What can go wrong?
- What is the likelihood something will go wrong?
- What are the consequences if something goes wrong?
- What can be done to mitigate the consequences?
- What options are available and what are the associated trade-offs?

- What is the impact on future options of current decisions?

FUSION ACTIVITY MISSION

The fusion activity provides functional risk assessments in support of the operations planning of the Army component of the unified combatant commander through the identification of vulnerable mission essential functions, systems, and assets. Specifically, the activity shall:

- Identify strategic, operational, and tactical functions, systems and assets required to support Army execution of each approved unified combatant command operations plan or concept plan;
- Analyze the dependencies of these functions upon functions performed by the Department of Defense, Federal, state, local, or private infrastructures; and
- Match the dependent functions, systems, and assets against existing vulnerability assessments.

FUSION ACTIVITY REQUIREMENTS

The function of the fusion activity is to identify mission essential systems and assets. The identification is accomplished by performing three macro-level tasks. These tasks are:

- Compare the systems and assets associated with mission essential functions against results from, reports, studies, and assessments addressing vulnerabilities.
- Determine the quality and the quantity of the information available on assessed systems and assets.
- Analyze Army-wide vulnerabilities, tends, and resources to assure Army infrastructure.

Inherent in the macro-level tasks are two distinct sets of tasks focusing on analytical operations and business operations. The analytical operations are those tasks associated with correlating the various assessments with the output from the mission-based analysis process in order to develop risk-based management strategies and options. The business operations tasks are these tasks required to support the operation of the fusion activity.

As a minimum, the fusion activity must be able to perform the analytical operations tasks listed below. Other analytical tasks may develop over time as experience is gained. These tasks are not listed in order of importance.

- Develop an analytical methodology for correlating the various assessments with output from the mission-related analysis process for infrastructure-related risk-based analysis.
- Develop infrastructure-relate risk-based management strategies and options.
- Develop a research methodology for determining reports and materials necessary for conducting infrastructure-related risk-based analysis.
- Develop costing models and tools for infrastructure-related risk-based management.
- Develop measurements for infrastructure-related risk-based analysis and management.
- Review infrastructure-related engineering reports and assessments.

- Review infrastructure-related transportation reports and assessments.
- Review infrastructure-related telecommunications and information management reports and assessments.
- Review infrastructure-related intelligence reports and assessment.
- Review infrastructure-related logistics reports and assessments.
- Review infrastructure assurance findings contained in Department of Defense and Army Inspector General reports.
- Review infrastructure-related findings contained in Joint Integrated Vulnerability Assessments.
- Review infrastructure-related findings contained in Balanced Survivability Assessments.
- Review infrastructure-related findings private sector infrastructure vulnerability assessments.
- Review infrastructure-related findings contained in General Accounting Office, Office of Management and Budget reports, and Congressional committee reports and investigations.
- Ascertain infrastructure-related trends and conduct trend analysis.
- Conduct infrastructure-related risk-based management conferences, symposia, and workshops.
- Write and coordinate infrastructure-related risk-based management reports.
- Recommend infrastructure-related risk-based policy.

As a minimum, the fusion activity must be able to perform the business operations listed below. Other business operations tasks may develop over time as experience is gained. These tasks are not listed in order of importance.

- Receive, catalogue, and maintain all fusion activity-related documents.
- Review and edit final reports to conform to acceptable practices.
- Develop and maintain databases necessary for the operation of the fusion activity.
- Develop, defend, and manage the fusion activity budget.
- Establish and maintain a local area computer network within the fusion activity.
- Establish and maintain SIPERNET and NIPRNET connectivity for the fusion activity.
- Administer the internal information system of the fusion activity.
- Develop and maintain standing operating procedures for obtaining, cataloguing, and maintaining fusion activity-related documents.
- Develop and maintain standing operating procedures for writing and editing reports.
- Develop and maintain standing operating procedures within the fusion activity for physical security, operations security, information security, and personal security.
- Develop and maintain security classification guidance for the reports generated by the fusion activity.
- Establish and maintain standing operations for the receipt of and accounting for classified documents.
- Establish and maintain automation accounts.
- Develop and maintain standing operating procedures for the purchase, set up, operation, and maintenance of the hardware, software, and firmware required for day-to-day operations of the fusion activity.
- Develop and maintain standing operating procedures for information management within the fusion activity.

The manpower requirements for the fusion activity are those necessary to sustain and maintain the activity's operation in order to accomplish the stated mission by performing the stated tasks associated with the stated function. Manpower requirements are associated with two distinct areas. These are the aforementioned analytical and business operations.

Analytical Operations. The volume and type of analysis conducted requires a workforce grounded in basic analytical skills and experienced in both operations and planning. The nature of the analysis and its association with supporting the installation commander unified combatant commander requires a mature workforce experienced in specific fields with the ability to understand relationships between and among their field of experience and others. The analytical environment requires a workforce able to understand disparate concepts, articulate differences and similarities, and draw conclusions about risk. Initially the workforce is composed of persons representing specified combat service and combat service support branches of the Army. These branches represent a core element in the determination of risk at the strategic, operational, and tactical level. These branches are signal, transportation, military policy, intelligence, and engineer. To round out the analytical expertise, persons with experience in risk management, cost analysis, operations research, and management analysis provide additional depth. The manpower for the analytical activity is allocated to military and civilian billets and contractor support. In this case, the contractors perform specific tasks related to cost analysis and risk management. It is anticipated that the person assigned to each military and civilian billet will perform three quarters of a man-year of effort directly related to the tasks previously mentioned. Contract work is billed as a full man-year of effort for cost analysis and risk management. Modifications to the manpower requirements are anticipated as experience is gained over time.

Business Operations. The business operations team is the support element of the analytical team and the fusion activity. The volume and type of analysis conducted requires a mature workforce grounded in basic operations skills and experienced in both operations and planning. The nature of the analysis and its association with supporting the installation commander and the unified combatant commander requires a workforce capable of developing resources, conducting research, and providing innovative approaches to conducting efficient and effective business operations. Since the analytical environment requires a workforce able to understand disparate concepts, articulate differences and similarities, and draw conclusions about risk, the business operations team brings cohesion to the fusion activity. Initially, the workforce is composed of persons representing specified functional areas. These functional areas represent the core element in supporting the determination of risk at the strategic,

operational, and tactical level. These functional areas are budget, library sciences, editing, security (physical, personal, and operations) and systems administration. The manpower for the business operations team of the fusion activity is allocated civilian billets and contractor support. In this case, the contractors perform the specific tasks of library sciences, security, editing, and systems administration. It is anticipated that persons assigned to the civilian billet will perform a full man-year of effort directly related to the tasks shown above. Contract work is billed as a full man-year of effort. Modifications to the manpower requirements are anticipated as experience is gained over time.

Fusion Activity Leadership. A director heads the fusion activity. The director establishes priorities, allocates work, and provides oversight to both the analytical and business operations teams. The director directs conferences, symposia, and workshops and is the lead executive on all work generated by the fusion activity. The director also serves as the primary point of contact on matters of mutual interest to the Office of the Secretary of Defense, the Unified Combatant Commanders, the Joint Staff, Headquarters Department of the Army, the Army Major Commands and activities, the other Military Departments, and the Defense Agencies, institutions of higher learning, and the private sector. The director has original classification authority.

Manning. Proposed manning for the fusion activity has two distinct teams and is depicted in Figure 1. All billets require, as a minimum, top secret (SCI SI/TK) clearances. Some individuals may be "read on" to special access programs. Other clearance requirements may be imposed as the activity matures.

Organizational Affiliation. Because of the nature of the work, the audience of the product, and the impact on the Army, the fusion activity falls under the purview of the Under Secretary of the Army. The organization may be located within the National Capital Region but preferably not in the Pentagon. The activity may be located at an institute of higher learning, such as the U.S. Army War College, Carlisle, Pennsylvania, or co-located with the Center for Army Analysis at Fort Belvoir, Virginia. Other locations deemed conducive to the research, inquiry, analysis, information sharing, and report writing and the distribution may also be considered.

Fusion Activity Findings. The fusion activity produces detailed infrastructure risk-based reports. These reports form the basis for infrastructure assurance risk management at the installation-level. At a minimum, the reports contain mitigation options and associated costs as a means of assisting the Army installation commander in his risk management activities. Other reports focus on risk-based Defense-wide or Army-wide trends for use by the Army leadership. All reports are informational and suggestive in nature. Reports do not direct action to be taken.

That is, the Army installation commander uses the report as a tool as he formulates his risk-based management strategy. The distribution of the reports has yet to be determined. At a minimum, the Under Secretary of the Army and the Assistant Secretaries of the Army (Civil Works and Installations and Environment), The Army G3, and the Assistant Chief of Staff (Installation Management), the Army Major Command and the Army installation commander will receive copies.

Para / Ln	Position	Grade / Rank	Branch	Req'd
01	*Office of the Director*			
01 /01	Director	SES	Civilian	1
01/ 02	Deputy Director	GS-0343-15	Civilian	1
01 03	Legal Counsel	COL	JAGC	1
	Paragraph Total			**3**
02	***Analytical Operations Team***			
02 / 01	Tactical Telecommunications Analyst	LTC / MAJ	Signal	2
02 /02	Tactical Transportation Analyst	LTC / MAJ	Transportation	2
02 /03	Tactical Security Analyst	LTC / MAJ	Military Police	2
02 / 04	Tactical Intelligence Analyst	LTC / MAJ	Intelligence	2
02 / 05	Engineering Analyst	GS-0810-13	Civilian	2
02 / 06	Management Analyst	GS-0343-12/13	Civilian	2
02 /07	Operations Research Analyst		Contractor	2
02 /08	Risk management Specialist		Contractor	2
02 / 09	Cost Analyst		Contractor	2
	Paragraph Total			**20**
03	***Business Operations Team***			
03 / 01	Budget Analyst	GS-0344-14	Civilian	1
03 / 02	Librarian		Contractor	1
03 / 03	Editor		Contractor	1
03 / 04	Security officer		Contractor	1
03 / 05	Automation Systems Administrator		Contractor	1
	Paragraph Total			**5**
	Aggregate			**28**

TABLE 1 PROPOSED FUSION ACTIVITY ORGANIZATION AND MANNING REQUIREMENTS.

FUSION ACTIVITY CONCLUSIONS

The need for an infrastructure assurance fusion activity is demonstrated by the fact that the Army does not have a means of correlating the disparate reports and vulnerability assessments, provided by numerous organizations, in order to determine risk to its ability to support the unified combatant commander. A fusion activity, as described above, provides that capability. The fusion activity is a valued added organization providing a tool for risk-based management and readiness activities.

The concept of a fusion activity, while discussed in this paper in terms of Army needs, transcends the Army and the other Services. In order to have value added risk assessment support for the warfighter and in order to maintain consistent Department of Defense policy, the fusion activity is more appropriately a Department of Defense asset. It should be Defense-centric and not Service-centric. Considering the plethora of reports and assessments from within and outside of the Department of Defense, the sensitivities concerning report and assessment contents, and the requirement for unbiased review and analysis, the fusion activity is more appropriately an organization under the cognizance of the Under Secretary of Defense (Policy). Since the fusion activity is not an operational organization, it can be organized and maintained as part of the Office of the Secretary of Defense. The details of how this is accomplished and the reporting requirements require negotiation.

CONCLUSION

The contents of this paper cover critical infrastructure protection, Army infrastructure assurance, mission-based analysis, and a proposal for a fusion activity. The reader should have gained a sense that, in general, critical infrastructure protection is not insurmountable. In fact, protecting the infrastructure is something we do daily, especially in the Department of Defense for those infrastructures that we own and operate. And the reader should take away the knowledge that there is considerable thought and debate going into the subject. Additionally, the reader should understand that approaches and solutions have been provided that capitalize on existing programs as a means of reducing redundancy and cost. Finally, the reader should be aware of the lack of a clear way ahead not only at the National level but also within the Department of Defense. This lack of clear and consistent policy becomes more important as we define the meaning of and the mechanisms for supporting Homeland Security.

Another point the reader should remember is the concept of the fusion activity. This paper dealt with the issue from the Army point of view. Considering the policy implications of critical infrastructure protection relating to Homeland Security, it is important for the Office of the

Secretary of Defense to have a organization, perhaps under the cognizance of the Deputy Under Secretary of Defense (Policy) for Policy Support, focusing on interpreting assessment information and evaluations related to Department of Defense infrastructures. This can lead to clear concise policy formulation and promulgation across the broad spectrum of Department of Defense interests.

WORD COUNT: 10,610

ENDNOTES

[1] Executive Order 13010, President's Commission on Critical Infrastructure Protection, July 15, 1996. Amended three times. On November 13, 1996 by Executive Order 13025 [Changed Section 1 by modifying the first sentence of section 1 (a).]. On April 3, 1997 by Executive Order 13041 [Added the Assistant to the President for Economic policy and the Assistant to the President and Director, Office of Science and technology Policy to the Principals Committee of the Commission.]. On October 11, 1997 by Executive Order 13064 [Amended Section 1. Section 5(a). Amended Section 2. Section 6(f) and (g). Amended Section 3 by inserting a new Section 7 (a) and (b). Renumbered Sections 7 and 8 of E.O. 13010 as Sections8 and 9.].

[2] Ibid.

[3] White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998.

[4] Ibid, 1.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Ibid, 2 .

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] *A National Security Strategy for A Global Age*, The White House, December 2000.

[17] Ibid, 24.

[18] Ibid, 24.

[19] Ibid, 24.

[20] Ibid, 24.

[21] Author's unpublished working papers. The information contained in the working papers was developed over time and is drawn from original briefings and information papers developed by the author. Additional material in the manuscript is derived from internal email, meeting notes, and the author's recollection of conversations with the numerous players (Office of the Secretary of Defense, Joint Staff, Military Departments, Defense Agencies, contractors and consultants) in critical infrastructure protection and Army infrastructure assurance.

[22] Author's working papers. Unpublished "Department of the Army Strategic Planning Guidance for Infrastructure Assurance," DRAFT Version 3.0, May 7, 2001. The information contained in the working papers formed the basis for a concept to describe strategic planning guidance relative to Army Infrastructure Assurance.

[23] Section 117 Readiness Reporting System: Establishment; Reporting to Congressional Committees. Section 3013 Secretary of the Army. Section 3062 [Army] policy; Composition; Organized Peace Establishment. Department of Defense Directive 5160.54 is under revision since the Fall of 1999. It has undergone several informal and formal coordination actions. At this writing it is being prepared for another formal coordination effort. Despite this situation, the Directive has validity as related policy.

[24] Working Paper, unpublished Concept of Operation (CONOPS), "Army Infrastructure Assurance OPLAN-based Analysis Concept of Operations (CONOPS)," DRAFT Version 1.0, June 15, 2001; developed an written by the author. The term "Mission Analysis" is an improvement upon the original term in that "OPLAN-based analysis" connotes that the methodology only applies to the approved operations plan(s) of the unified combatant commander. In retrospect, it is felt that "mission analysis" is less constricting and allows for its application against contingency plans and other types of plans for which infrastructure and the dependence thereon is important.

[25] Working paper, unpublished Concept of Operations (CONOPS), "Army Infrastructure Assurance Fusion Activity Concept of Operations (CONOPS)," DRAFT Version 1.6, May 9, 2001; developed and written by the author. The term "Mission Analysis" is an improvement upon the original term in that "OPLAN-based analysis" connotes that the methodology only applies to the approved operations plan(s) of the unified combatant commander. In retrospect, it is felt that "mission analysis" is less constricting and allows for its application against contingency plans and other types of plans for which infrastructure and the dependence thereon is important.

GLOSSARY

[the terms provided in this glossary are taken from section ii terms of draft Army Regulation 525-xx, *Army Infrastructure Assurance*. They are provided here because they constitute a body of information that is required to understand the subject covered in this paper.]

Assessment (Infrastructure)
An appraisal of the military's reliance on infrastructure, the impacts of that reliance on missions, functions, and tasks, and the identification of options to mitigate vulnerabilities.

Asset (Infrastructure)
Any infrastructure facility, equipment, or resource that performs a mission essential function.

Assurance (Infrastructure)
Identifying potential actions that can be taken to restore the functions if they are lost, damaged, corrupted, or compromised; and identifying and recommending options to mitigate, protect, and improve these functions.

Command, Control, and Communications Infrastructure Sector
This defense infrastructure sector is composed of a number of assets, facilities, networks, systems, and business processes that support the command, control, and communications functions necessary for defense operations. DISA [Defense Information Systems Agency: *emphasis added.*] is responsible for coordinating the assurance of activities of this defense infrastructure sector.

Critical Infrastructure
A term used by the office of the secretary of defense to describe infrastructure so vital that its degradation or loss would have debilitating impacts on defense or economic security.

Defense Information Infrastructure (DII) Defense Infrastructure Sector
The DII is the web of communications networks, computers, software, databases, applications, weapons system interfaces, data, security services, and other services that meet the information processing and transport needs of the DOD [Department of Defense: *emphasis added.*] users across the range of military operations. It encompasses: (1) sustaining bases, tactical, DOD-wide information systems, and command, control, communications, computers, and intelligence (C4I) interfaces to weapons systems; (2) the physical facilities used to collect, distribute, store, process, and display voice, data, and imagery; (3) the applications and data engineering tools, methods, and processes to build and maintain the software that allow command and control (C2), intelligence, surveillance, and reconnaissance (ISR), and mission support users to access and manipulate, organize, and digest proliferating quantities of information; (4) the standards and protocols that facilitate interconnection and interoperation among networks; and (5) the people and assets that provide the integrating design, management and operation of the dii, develop the applications and services, construct the facilities, and train others in dii capabilities and use, (DII Master Plan Version 7.0, page 2.1). Disa [Defense Information Systems Agency: emphasis added] is responsible for coordinating the assurance activities of this defense infrastructure sector.

Financial Services Defense Infrastructure Sector
Financial institution services fall into two categories. The first category consists of servicing official DOD [department of defense: *emphasis added.*] (i.e. Appropriated fund) disbursing and paying operations and providing cash and accepting deposits for credit to officially designated treasury general accounts. The second includes servicing individuals and on-base organizations (i.e. Non-appropriated funds) with normal deposit, maintenance of accounts, safekeeping, and other financial services functions. The defense finance and accounting service (DFAS) supports official DOD activities and provides military and civilian pay, travel pay, transportation pay, vendor pay, contractor pay, dispersing, payment of foreign military sales, and general defense business operations fund accounting. DFAS is responsible for coordinating the assurance activities of this defense infrastructure sector.

Health Affairs Defense Infrastructure Sector
DOD [Department of Defense: *emphasis added.*] maintains extensive health care infrastructure across it facilities world-wide (sic). In addition, DOD manages a larger system of non-DOD care facilities within its health care network. The health care infrastructure consists of facilities and sites located at DOD installations, information systems linking those facilities, and networks of health care among the services and components. The Office of the Assistant Secretary of Defense for Health Affairs is responsible for coordinating the assurance activities of this defense infrastructure sector.

Infrastructure
The framework of inter-dependent networks and systems comprising identifiable industries, institutions, functions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States.

Installation
An aggregation of contiguous or near contiguous, common mission-supporting real property holdings under the jurisdiction of the Department of Defense controlled by and at which an army unit or activity is permanently assigned or temporarily stationed.

Intelligence, Surveillance and Reconnaissance Defense Infrastructure Sector
This defense infrastructure sector is composed of those assets, facilities, networks, and systems that support the development, production, and conduct of ISR [intelligence, surveillance, and reconnaissance: *emphasis added.*] Activities, such as intelligence production and fusion centers. DIA [Defense Intelligence Agency: *emphasis added.*] is responsible for coordinating the assurance activities of this infrastructure sector.

Logistics Defense Infrastructure
The logistics defense infrastructure sector includes all activities, facilities, networks, and systems that support the provision of supplies and service to us forces worldwide. The logistics defense infrastructure includes material acquisition and development; the storage, movement (strategic movement is the responsibility of the transportation infrastructure defense sector and USTRANSCOM [US Transportation Command: *emphasis added.*]), and distribution of supplies; maintenance of material and supplies; and the final disposition of material no longer needed by DOD [Department of Defense: *emphasis added..*] The Defense Logistics Agency is responsible for managing most consumable supplies, administering contracts, and acquiring materials and services, and coordinating the assurance activities of this defense infrastructure sector.

Mitigation
Long-term activities conducted prior to an event to minimize or alleviate the potential adverse effects of a hazardous situation on people, facilities, operations, or services.

Personnel Defense Infrastructure Sector
The personnel defense infrastructure sector includes a large number of assets hosted on component [Department of Defense components include the Military Departments and the Defense Agencies: *emphasis added.*] sites; a network of facilities within and among service components; and computational and information systems linking those sites and facilities. The personnel infrastructure is not only responsible for its own assets, but also coordinates commercial services and facilities that support the personnel function including, but not limited to, recruitment, record keeping, and general training requirements. The Defense Human Resources Agency is responsible for coordinating the assurance activities of this defense infrastructure sector.

Public Works Defense Infrastructure Sector
Public works includes five distinct physical infrastructure sectors: land and facilities, electric power, oil and natural gas, water and sewer, and emergency services (fire, medical, hazardous material handling, etc.). This defense infrastructure sector is composed of networks and systems, principally for the distribution of the associated commodities and the real property it supports. The generation, production, and transport of these commodities for and to DOD [Department of Defense: *emphasis added.*]. Real property assets are primarily the function of their respective national infrastructures. The US Army Corps of Engineers is responsible for coordinating the assurance activities of this defense infrastructure sector.

Reconstitution
Actions taken to re-establish an organization or capabilities of an organization that have been destroyed or severely damaged.

Remediation
Post event actions taken to facilitate immediate response, to minimize or alleviate the negative impact of a hazardous situation on people, facilities, operations, or services, and to quickly restore services.

Response
Activities to address the immediate and short-term effects of an emergency or disaster.

Risk
A concept used to give meaning to things, forces, or circumstances that pose a danger t people or to things that they value. Normally stated in terms of the likelihood of harm or loss from hazard.

Sector
One of two divisions of the economy (private or public); an identified group (of industries or infrastructures) which performs a similar function within a society, e.g., vital human services.

Sector (Defense Infrastructure)
Infrastructure owned, operated or provided by the Department of Defense. Defense infrastructure sectors include the DII [Defense Information Infrastructure: *emphasis added.*], C3 [command, control, and communications: *emphasis added.*], space, ISR [intelligence, surveillance, and reconnaissance: *emphasis added*], financial services, logistics, public works (includes DOD-owned or –operated utilities, roads, rails and railheads and their interface to commercial and other government systems), personnel, and health affairs.

Space Defense Infrastructure
The space defense infrastructure sector is composed of both space- and ground-based assets including launch, specialized logistics, and control systems. Facilities are located worldwide on both DOD-controlled and private sites. US Space Command is responsible for coordinating the assurance activities of this defense infrastructure sector.

Transportation Defense Infrastructure Sector
The transportation defense infrastructure sector includes resources (surface, sea and lift assets; supporting infrastructure; personnel; and related systems) and interrelationships of DOD, federal, commercial, state/local agencies, and non-US activities that support DOD global transportation needs. US Transportation Command is the single manager for DOD transportation, and responsible for coordinating the assurance activities of this defense infrastructure sector.

Unified Combatant Command
A command with a broad continuing mission under a single commander and composed of significant assigned components of two or more military departments, and which is established and so designated by the President, through the Secretary of Defense with the advice and assistance of the Chairman of the Joint Chiefs of Staff.

Vulnerability
The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in a hostile environment.

BIBLIOGRAPHY

Alberts, David S. Defensive Information Warfare. National Defense University, Washington D.C., 1996.

Arnold, H. D., J. Hukill, J. Kennedy and A. Cameron. Targeting Financial Systems as Centers of Gravity: Low Intensity and No Intensity Conflict, Defense Analysis 10, no. 2, 1994.

Armed Forces, United States Code, Section 117, Title 10. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Armed Forces, United States Code, Section 3013, Title 10. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Army Infrastructure Assurance: A Report on the Outcome of the MANHATTAN 2001 Political-Military Game, U.S. Department of the Army, Plans Branch, Military Support Division, Director of Operations readiness and Mobilization, Office of the Deputy Chief of Staff for Operations and Plans, Washington DC April 12, 2001. [Restricted distribution.]

Assignment of National Security Emergency Preparedness Responsibilities in DOD Components, U.S. Department of Defense Directive 3020.36, 1988. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Blechman, Barry M. et al. The American Military in the 21st Century. New York: S. Martin's Press, 1993.

Bush, George, Establishing the Office of Homeland Security and the Homeland Security Council, Executive Order 13228, Washington, D.C.: The White House October 8, 2001.

Cameron, Gavin, "Multi-track Microproliferation: Lessons from Aum Shinrikyo and Al Qaida," Studies in Conflict and Terrorism, vol. 22, no. 4, (October-December 1999): 227.

Carter, Aston B., "Adapting Defense to Future Needs," Survival The IISS Quarterly, Winter 1999-2000): 101.

Chairman Joint Chiefs of Staff, Chairman's Readiness System, Instruction 3401.01B.

Chairman Joint Chiefs of Staff, Global Status of Resources and Training System, Instruction 3401.02.

Chairman Joint Chiefs of Staff, Charter of the Joint Requirements Oversight Council, Instruction 5123.01.

CIP Analysis & Assessment Prototype (P1). Final After Action Report, The Joint Program Office for Special Technology Countermeasures, Dahlgren, Virginia, 15 March 2000. [Restricted distribution.]

Clinton, William Jefferson, Executive Order 13010: Critical Infrastructure Protection. Washington D.C.: The White House, 1996. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Cohen, William S., Annual Report to the President and the Congress, U.S. Government Printing office, 1998.

Cohen, William S., Report of the Quadrennial Defense Review, Washington, D.C., 1997.

Colpo, Michael. Smell the Coffee: Military Support to Civilian Authorities & Homeland Defense Here & Now, Strategy research Project. Carlisle Barracks: U.S. Army War College, 7 April, 1999.

Continuity of Operations Policy and Planning, U.S. Department of Defense Directive 3020.26, May 1996. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Department of Defense Financial Management Regulation, 7000.14-R,. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Department of Defense Trusted Computer, U.S. Department of Defense 5200.28-STD,. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

DOD Antiterrorism/Force Protection (AT/FP) Program, U.S. Department of Defense Directive 2000.12. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

DOD Combating Terrorism Program Procedures, U.S. Department of Defense Instruction 2000.12. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

DOD Combating Terrorism Program Procedures, U.S. Department of Defense Directive 2000.14. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

DOD Combating Terrorism Standards, U.S. Department of Defense Directive 2000.16. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Drell, Sidney D., Abraham D. Sofaer, George D. Wilson. "The Present Threat", Hoover Digest, no. 1 (2000): 110.

Echevarria II, Antulio J. The Army and Homeland Security: A Strategic Perspective, Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA, March 2001.

Executive Order 13010, Critical Information Infrastructure, Weekly Compilation of Presidential Documents, vol. 32, no. 29, (July 22, 1996), pp1242-1244. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Federal Acquisition Regulation. [This publication may be obtained from Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Flournoy, Michele A., et al, QDR 2001: Strategy-Driven Choices for America's Security, National Defense University Press, Washington D.C., April 2001.

General Accounting Office, HOMELAND SECURITY, A Framework for Addressing the Nation's Efforts, Statement of David M. Walker, Comptroller General of the United States, September 21, 2001.

General Accounting Office, HOMELAND SECURITY, A Risk Management Approach Can Guide Preparedness Efforts, Statement of Raymond J. Decker, Director, Defense Capabilities and Management, October 31, 2001.

Gorelick, Jamie S. National Security in the Information Age, Speech at the U.S. Air Force Academy, Colorado Springs, February 29, 1996.

Griffith, Samuel B., Sun Tzu: The Art of War, Oxford University Press, London, 1963.

Henry, Ryan and C. Edward Peartree. Military Theory and Information Warfare, Parameters 28 – no. 3 (Autumn 1998): 121-135.

House Select Committee on Terrorism and Homeland Security, Statement for the Record, On Defensive Information Operations, Larry T. Wright, Chief, Defense Science Board Task Force, October 3, 2001.

Howard, Michael and Peter Paret. Carl Von Clausewitz ON WAR, Princeton University press, Princeton, New Jersey, 1989.

Letterman, Lester H. Defense of Critical Infrastructure, Strategy Research Project. Carlisle Barracks: U.S. Army War College, 7 April 1999.

Libicki, Martin. What is Information Warfare?. National Defense University, Washington, D.C. 1995.

Marlo, Francis H. WMD Terrorism and U.S. Intelligence Collection, Terrorism and Political Violence, vol. 11, no. 3, (Autumn 1999): 53.

Mayes, Kelly L. An Analysis of Current United States Homeland Defense Policies, Strategy Research Project. Carlisle Barracks: U. S. Army War College 6 April 2000.

McNeilly, Mark. Sun Tzu and the Art of Modern Warfare, Oxford University Press, London, 2001.

McRae, Hamish. The World in 2020, Harvard Business School Press, Boston, 1994.

Military Assistance to Civil Authorities, U.S. Department of Defense Directive 3025.15, Washington D.C.: Office of the Assistant Secretary of Defense (Special Operations and Low Intensity Conflict), 1997. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Molander, Roger C., Andrew S. Riddle, and Peter A. Wilson. Strategic Information Warfare: A New Face of War, Parameters, 26 (Autumn 1996), 81-92.

National Plan for Information Systems Protection: An Invitation to Dialogue, Version 1.0, Critical Infrastructure Assurance Office, 1999. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Payne, Allan D. The Impact of Computer Network Attacks on Infrastructure Centers of Gravity, Strategy Research Project. Carlisle Barracks: US Army War College, 7April 1999.

Physical Security Equipment, U.S. Department of Defense Directive 3224.3. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Physical Security Program, U.S. Department of Defense Directive 5200.8-R. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Physical Security Technical Vulnerability Reporting System, U.S. Department of Defense Instruction 5215.2. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Presidential Decision Directive 12656, Assignment of Emergency Preparedness Responsibilities. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Presidential Decision Directive 29, Security Policy Coordination, Washington, D.C., September 16, 1994. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Presidential Decision Directive 39, U.S. Policy on Counter-Terrorism. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Presidential Decision Directive 62, Combating Terrorism. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Presidential Decision Directive / NSC-63, Critical Infrastructure Protection, Washington, D.C., May 22, 1998. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Presidential Decision Directive 56, Managing Complex Contingencies, May 1997. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

Presidential Decision Directive 67, Continuity of Government Operations. [This publication may be obtained from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.]

PriceWaterhouseCoopers. Department of Defense Critical Infrastructure Protection Plan for Logistics, Sector Defense Overview and Demonstration, June 14, 2001. [Restricted distribution.]

Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence, U.S. Department of Defense Handbook 2000.12H. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Questech, Inc. Computer Security Threats Chart, Falls Church, VA, September 1997.

Risk Assessment and Mitigation Methodologies For Force Projection Platforms, Final Report, U.S. Department of the Army, Department of Systems Engineering, United States Military Academy, West Point, New York, 4 August 2000. [Prepared for the Director of Military Support, Pentagon, Washington, D.C. [Restricted distribution.]

Ross, Mitchell P. National Information Systems: The Achilles Heel of National Security, Strategy Research Project. Carlisle Barracks: US Army War College, 3 April 1997.

Security Criteria and telecommunications Guidance System Evaluation Criteria, U.S. Department of Defense Manual 5030.58-M. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Smulian, Paul R. National Security Agency, The Effects of Presidential Decision Directive 63 on the Public, Strategy Research Project. Carlisle Barracks: US Army War College, 1 April 2000.

Snow, Donald M. The Shape of the Future the Post-Cold War World. Armonk, New York, London, England: M.E. Sharpe Inc., 1991.

Software Engineering Institute. Report to the President's Commission on Critical Infrastructure Protection, Carnegie Mellon, University, January 1997.

Senior Readiness Oversight Council (SROC), U.S. Department of Defense Directive 5149.2. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Stern, Jessica. The Ultimate Terrorist, Harvard University Press, Cambridge, Massachusetts, 1999

Taylor, Scott R., et al. Consequence Management in Need of a Time Out, Joint Forces Quarterly 22 (Summer 1999): 78-85.

The Critical Asset Assurance Program, U.S. Department of Defense Directive 5160.54. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

Toffler, Alvin and Heidi. War and Anti-War: Survival at the Dawn of the 21st Century; Little Brown, New York, 1993.

The White House. White Paper, The Clinton Administration Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. May 22, 1998; available from <http://www.fas.ord/irp/offdocs/paper598.htm>; accessed 18 Sep 01.

The White House. A National Security Strategy for a New Century, October 1998.

U.S. Attorney General Janet Reno. Critical Infrastructure Security, Memorandum to the Presidential Cabinet, Washington, D.C., March 14, 1996.

U.S. Department of the Army, The Army Physical Security Program, Army Regulation 190-13, September 30, 1993.

U.S. Department of the Army, Personal Security, Army Regulation 190-58, March 22, 1989.

U.S. Department of the Army, Information Security, Army Regulation 380.19, February 27, 1998.

U.S. Department of the Army, Anti-Terrorism Force Protection (AT/FP), Army Regulation 525-13. [Restricted distribution.]

U.S. Department of the Army, Army Infrastructure Assurance, Army Regulation 525-XX, coordination draft, Military Support Division, Office of the Director for Operations, Readiness and Mobilization, Office of the Deputy Chief of Staff for Operations and Plans, October 2001. [Restricted distribution.]

U.S. Department of the Army, Operations Security Army Regulation 530-1. [Restricted distribution.]

U.S. Department of Defense, Defense Federal Acquisition Regulation. [This publication may be obtained from Directives and Records Branch, Washington Headquarters Services, 155 Defense Pentagon, Washington, DC 20301-1155.]

U.S. Department of Defense. Report of the National Defense Panel: Transforming Defense: National Security in the 21st Century, National Defense Panel, Arlington, Virginia, December 1997.

U.S. Department of Defense. Strategic Assessment 1999: Priorities for a Turbulent World, Institute for National Strategic Studies, National Defense University 1999

U.S. Department of Defense Joint Publication 3-07.2, Joint Tactics, Techniques and Procedures for Antiterrorism.

U.S. Department of Defense Joint Publication 6-06.7, Security Policy for the GCCS Intercomputer Network.

Welch, Claude E., Jr., and Arthur K. Smith. Military Role and Rule. North Scituate, Massachusetts: Duxbury Press, 1974.

Williamitis, Gregory M., Implementing the National Security Strategy of Critical Infrastructure Protection, Carlisle Barracks, PA March 31, 2000.