AU/ACSC/038/2000-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

EVALUATING U.S.AIR FORCE NUCLEAR WEAPON STORAGE AREA SECURITY IN THE POST COLD-WAR ENVIRONMENT

by

Lyle W. Cary, Major, United States Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lieutenant Colonel Scotty Lewis

Maxwell Air Force Base, Alabama

April 2000

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

DISCLAIMER ii

ILLUSTRATIONS v

PREFACE vi

ABSTRACT viii

INTRODUCTION 1

BACKGROUND 3
- Cold War Environment 3
  - Threat 3
  - Security Concept 4
  - Current Nuclear Security Concept 5
  - Central Intelligence Agency Asset Risk Management Model 6

DETERMINING RISK TO NUCLEAR WEAPONS IN STORAGE 8
- Asset 9
- Threat 9
  - Terrorism 9
  - Insider 12
  - Cyberwarfare 13
- Potential Vulnerabilities 15
  - Above Ground Storage Structures 16
  - Manpower 16
  - Technology 17

COUNTERMEASURES TO MITIGATE RISK 20
- Leveraging Technology 20
  - Video Storage System 20
  - Video Motion Detection 21
  - Weapon Storage and Security System 21
  - Less than Lethal Weaponry 22
- Remove Non-Strategic Nuclear Forces From Europe 23

ADDITIONAL BENEFITS 25

CONCLUSIONS.....27

BIBLIOGRAPHY.....29

Illustrations

Page

Figure 1. Typical Nuclear Weapon Storage Area Configuration 6

Figure 2. Central Intelligence Agency Asset Risk Management Model 7

Figure 3. Notional Nuclear Weapon Storage Area Employing a Sampling of Available Technology.....23

Preface

The author began his career as a Security Police Flight Security Officer and Security Police Shift Commander at Grand Forks Air Force Base, North Dakota in 1985. The officer supervised security flight operations protecting nuclear loaded B-52s, a nuclear weapon storage area, and performed duties as a nuclear weapons convoy commander. Training to defeat potential adversaries occurred daily. The flight constantly conducted response force exercises to counter unauthorized lone individuals to larger enemy forces. Most often, the larger forces were either terrorist groups or "Soviet" special operations teams attempting to simulate destruction of nuclear assets on the ground before launch against the Soviet Union during the early stages of a simulated nuclear exchange. To counter these threats, strict physical standards were employed. Since the Soviet disintegration, the face of the enemy has changed and there has been a technological explosion that could impact security operations. Considering these changes, the author was curious if current Air Force nuclear physical security standards were adequate. Many materials reviewed to support the research were classified; however, classified information is not contained in this paper. Classified information was not necessary, as the author was able to draw conclusions from unclassified sources without compromising security. Moreover, this paper's ultimate purpose is to stimulate thought and further study of a critical subject—not to get into extensive details. Finally, other related studies need to be accomplished such as ways to enhance protection of nuclear components in-

transit and those housed in intercontinental ballistic missile silos. This manuscript focuses on nuclear components in storage; however, most of the research could be applied to weapons movements and launch facilities.

The author recognizes Lieutenant Colonel Scotty Lewis' patience and guidance. His professionalism and genuine interest in force protection issues was a tremendous asset during this process. Furthermore, the U.S. Air Force Electronic Systems Center was very helpful in providing information on available technology that could be employed to improve security of these vital resources.

Abstract

Air Force physical nuclear standards have not changed significantly since the end of the Cold War. However, since the fall of the Soviet Union, the potential threat to nuclear assets in storage is now asymmetrical in nature. Given the threat, this paper explores adequacy of physical protection afforded nuclear assets in storage. Using the Central Intelligence Asset Risk Management model, the manuscript analyzes asset value, potential threats and vulnerabilities, and proposes countermeasures to mitigate risk of unauthorized access, sabotage and theft. The author holds current security standards are adequate to prevent theft; however, serious vulnerabilities yield unacceptable risk of insider tampering, unauthorized access, and sabotage. The Air Force should leverage technology to improve the physical security posture in nuclear weapon storage areas and store nuclear components in underground facilities or vaults. Furthermore, consideration should be given to removing tactical nuclear components from Europe. Finally, because the proposed countermeasures would serve as force multipliers, a potential manpower windfall could benefit support forces for the Expeditionary Air Force.

Part 1

Introduction

The world changed dramatically with the fall of the Soviet Union. The international environment no longer resembled the bipolar structure prevalent throughout the post World War II era. The menacing Soviet conventional and nuclear threat was gone. Consequently, in the absence of the Soviet threat, new threats emerged such as weapons of mass destruction, terrorism, rogue states, and failed states.[1] These asymmetrical threats now pose significant risks to U.S. interests and resources within the continental U.S. and across the globe. Therefore, the purpose of this manuscript is to explore whether the U.S. Air Force provides adequate protection for its nuclear weapons and components in light of new threats. After review, the author concludes physical security provided for U.S. Air Force nuclear assets is adequate to prevent theft; however, current standards and procedures are vulnerable to tampering, unauthorized access, and sabotage. Off-the-shelf and emerging technology would greatly enhance the Air Force's ability to secure this nation's most sensitive military resources. First, this manuscript discusses the background of the Air Force's nuclear security concept. Second, a Central Intelligence Agency Asset Risk Management Model is used to consider current nuclear security operations adequacy. Third, the author identifies potential countermeasures and recommendations to mitigate risk to nuclear components. Lastly, other benefits

associated with the recommendations are discussed. This paper provides a broad overview of a complex subject. Due to restrictions, the paper primarily addresses nuclear components in storage, not in transit or in intercontinental ballistic missile silos. Furthermore, because of the subject's sensitive nature this manuscript contains only unclassified information. The overall objective is to generate thought and further study at major command staffs and the Air Staff.

Notes

[1] The White House. *A National Security Strategy for a New Century*, October 1998. P 1-7.

Part 2

Background

We still protect our aircraft and resources the same way Hannibal protected his elephants.

— Colonel James J. Mecsics

Cold War Environment

Nuclear deterrence was a key ingredient in our national military strategy in the Cold War environment. The Air Force owned two-thirds of the nuclear triad consisting of the bomber and missile; therefore, the Air Force was custodian for large stockpiles of nuclear weapons. Adversaries analyzed nuclear weapons as profitable targets for attack. The loss of a nuclear weapon from attack would hold serious political and military implications.[1] Protection of these weapons from enemy attack and sabotage was a top priority.

Threat

It is not uncommon to hear Cold War veterans lament about not knowing who the enemy is anymore; however, for nearly 50 years following World War II era, there was little doubt about the adversary's identity. During the 1980s, the author served as a Flight Security Officer in the Minuteman missile complex operated by the 321st Strategic Missile Wing, a B-52 nuclear alert area owned by the 319th Bombardment Wing, and nuclear storage at Grand Forks Air Force Base, North Dakota. Anecdotal tales of Soviet

special forces teams posing as North Dakota farmers attempting to penetrate restricted areas to sabotage our weapons contributed to a near paranoid culture. With benefit of hindsight, this mindset seems incredibly naïve, yet this attitude largely drove the concept of operations to secure nuclear resources. Moreover, the "threat" was institutionalized in training, exercises, and inspections.[2] Strategic Air Command's infamous Wing Security Evaluations consisted of inspectors emerging from wheat and sunflower fields to attempt to penetrate restricted areas. To this day, the question remains how the "enemy" expected to penetrate tons of concrete covering missiles to gain access. Perhaps more worrisome was the possibility of attacking a convoy, alert area or weapon storage area (WSA).

Security Concept

Although the threat appears to have derived from near paranoia, the basic concept was appropriate. The physical security concept for a WSA consisted of a layered security approach. Strict personnel and vehicle entry control, exterior and interior structure alarms, electronic sensors and lighting was designed to detect a clandestine approach to storage structures. Once the threat was detected, an alarm monitor or security controller would dispatch assigned area patrols to assess. Many times, this assessment capability was enhanced by military working dogs. If the threat persisted and penetrated fencing then response forces would destroy it before it accessed structures.[3] Figure 1 represents a notional WSA. One may conclude that even a large special forces team would have had a difficult task if they attempted to penetrate a structure housing nuclear weapons. This overarching concept remained largely intact with a few modifications.

Current Nuclear Security Concept

The Air Force nuclear security concept remains nearly the same as during the Cold War years. The Department of Defense (DoD) and Air Force still recognize the importance of protecting nuclear resources. DoD and Air Force publications assert that nuclear weapons require special protection because of their political and military importance, their destructive power, and the consequences of an unauthorized, or inadvertent prearming, launching, firing, or detonation. Contemporary security concept of operations are designed to protect weapons from unauthorized access, damage or sabotage, unauthorized destruction, loss of custody, capture or theft. The security-in-depth approach using sensors, fencing, lighting and heavy reliance on manpower is still evident.[4] [5] This may not be all bad, as some advances have been made. For instance, detection has been enhanced through addition of closed circuit television technology. Further storage vault technology such as the Weapon Storage and Security System incorporated delayed entry into the physical security concept at several locations. Regardless of modest improvements security planners should ponder whether current operations provide optimal protection against current threats.

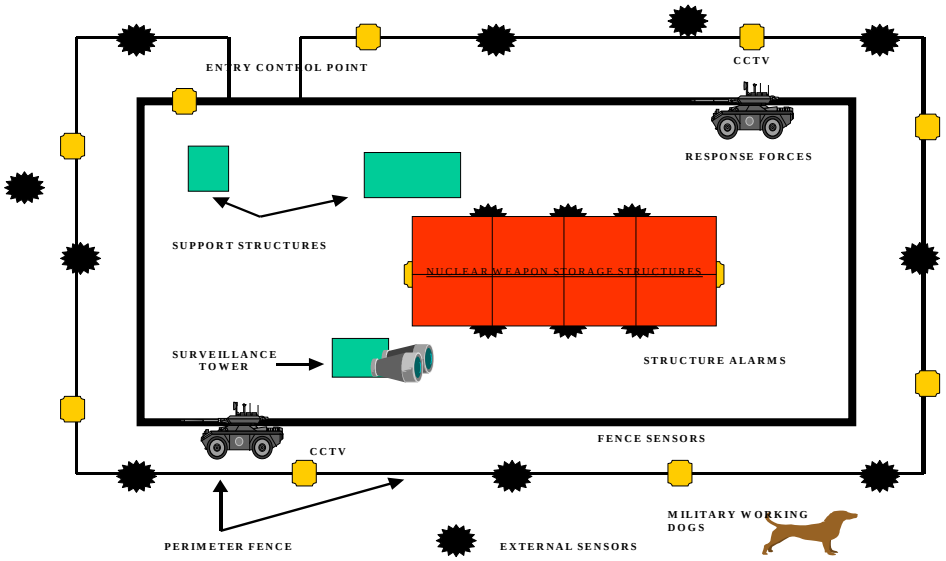

Figure 1. Typical Nuclear Weapon Storage Area Configuration

Central Intelligence Agency Asset Risk Management Model

The risk management process is useful to explore whether Air Force nuclear security standards adequately protect assets in WSAs from contemporary threats. There are many models to choose from, but the Central Intelligence Agency Asset Risk Management (ARM) model, also used by Air Mobility Command, is particularly suited to conduct an unclassified threat assessment and explore potential areas for improvement. The ARM model (figure 2), represents a five-step process. First, the value of the asset is identified. Second, potential threats are discussed. Third, potential vulnerabilities posed by the threat to the assets are identified. Fourth, associated risks are determined. Finally, countermeasures and recommendations to mitigate the risk are proposed.

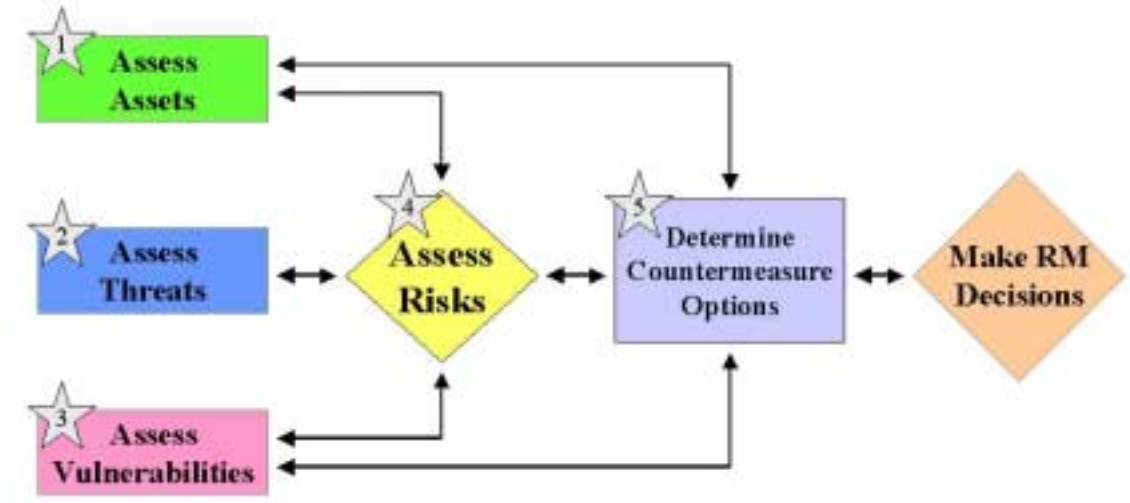

Figure 2. Central Intelligence Agency Asset Risk Management Model

Notes

[1] Air Force Regulation (AFR) 207-10. *Nuclear Weapons in Storage, Surface Movement and Logistics Transport Status*, 13 December 1974. Chapter 1, p 1.

[2] Ibid, p 3-6

[3] Ibid, chapter 2, p 1-6.

[4] Department of Defense (DoD) Manual 5210.41 (C), *Nuclear Weapon Security Manual*, April 1994. chapter 2, p 1-4.

[5] Air Force Instruction (AFI) 31-101. *The Air Force Physical Security Program*, September 1998. p 83-91.

Part 3

Determining Risk to Nuclear Weapons in Storage

It appears the threat imposed by enemy special forces units, if indeed ever a realistic threat has greatly diminished. The National Security Strategy notes broad threats to U.S. interests as regional or state-centered threats, foreign intelligence collection, transnational threats including terrorism and transnational crime, spread of dangerous technologies, and failed states.[1] Also, Michael A. Vatis, Chief, National Infrastructure Protection Center, Federal Bureau of Investigation, testified before Congress that information and cybercrime pose significant threats to U.S. infrastructure. [2] Narrowing further and more relevant to the nuclear security question, DoD Manual 5210.41M identifies four general unclassified threat categories: 1) Insider; 2) Terrorist; 3) Special Purpose Forces; 4) External Adversaries.[3] None of these lists are comprehensive. In summary, there are many threats to U.S. interests and assets. Indeed, many categories overlap. For example, the U.S. government, through the Federal Bureau of Investigation (FBI), actively investigates and prosecutes acts of terrorism and those who perpetrate the act. Therefore, the terrorist is also a criminal. However, to facilitate analysis, the author holds there are three significant threats to consider in conducting a risk analysis of Air Force nuclear weapons in storage. The categories are 1) Terrorist; 2) Insider; 3) Cyber/Information.

Before analyzing these potential threats, the importance of nuclear assets must be discussed.

Asset

Nuclear components are arguably America's most sensitive assets. The consequences of destruction or detonation are astronomical. Moreover, a nuclear weapon need not be sabotaged or stolen to have an impact. Imagine the political fallout if a terrorist or criminal merely gained unauthorized access. Undoubtedly, media attention would focus on security shortfalls, leading to erosion of public support for the weapons and lack of confidence in the Air Force's ability to secure nuclear components. The DoD and Air Force accurately assessed the uncompromising need for special protection of these weapons because of their political and military importance.[4] Therefore, the Air Force must provide state of the art physical security countermeasures, regardless of cost, to mitigate risk.

Threat

The most significant threats to Air Force nuclear weapons in storage are terrorists, the insider, and the information threat (cyberwarfare). This section discusses the nature of these threats and how they may create risks.

Terrorism

Terrorism could pose a significant threat to nuclear storage areas. Defining terrorism is problematic because there is no single definition. Perhaps the most comprehensive is the definition used by the FBI. According to the FBI, terrorism is defined as, "the unlawful use of force or violence against persons or property to intimidate or coerce a

government, the civilian population, or any segment thereof, in furtherance of political or social objectives.[5] Terrorists use violence, or the threat of violence to induce fear. Furthermore, the FBI describes terrorism as either domestic or international. Either category could use the threat of attack, or actual attack in attempt to intimidate the U.S. government or further the group's objectives. Additionally, terrorist groups are improving their ability to gain financial support and carry out complex operations. Advanced technology has allowed to communicate more efficiently and securely. Also, terrorists have learned from mistakes in past operations such as the World Trade Center and Oklahoma City bombings. Future attacks will be planned with greater care.[6] Finally, most terrorist organizations are well trained. Many organizations, domestic and international, use military models for training. Members are trained in small unit tactics, explosives and firearms.[7]

Domestic terrorist organizations are often ignored because of attention international terrorist attacks gain, such as the June 1996 Khobar Towers bombing in Saudi Arabia. However, domestic groups, either right wing or left wing extremists, could present a risk to nuclear storage areas. Right wing terrorist groups generally adhere to an anti-government or racist ideology. These groups continue to attract supporters. Militia movements, many times also right wing extremists, oppose gun control legislation, United Nations involvement in international affairs, and generally believe the U.S. government is part of a conspiracy to create a "new world order." Many of these groups see a central federal government that is too powerful, and therefore illegitimate.[8] Consequently, militias are organized, equipped and trained to protect rights they view as threatened by the U.S. government. They hold that the Second Amendment to the

Constitution of the United States was written to guarantee that everyone would have the right to protect their families, their homes, and their communities. One such group, the Mountaineer Militia, headquarters in Clarksburg, West Virginia, published a Principles of Operations Manual that is similar to the U.S. Army Ranger Handbook. In fact, according to the manual, the Adjutant General of the Mountaineer Militia spent 13 years on active duty with the U.S. Army, served in Operations and Intelligence activities at Army and North Atlantic Treaty Organization headquarters in Europe, and had extensive special forces training.[9] Therefore, many of these groups could be familiar with security operations at nuclear WSAs. However, one must analyze the feasibility of targeting a heavily guarded storage area. Would a domestic terrorist organization see these structures as valuable targets? In an interview for a television documentary on extremist groups, a former member of an Aryan Nation group operating in the Northwest United States told the interviewer that his group talked many times about the possibility of acquiring a nuclear weapon. Even more disturbing, the former member related if they possessed such a weapon, they contemplated detonating it in Washington, D.C., or New York.[10] One may question the ability of a group to acquire a nuclear weapon capable of detonation, especially from an Air Force storage area, but the willingness is present even if capability is on the margin.

International terrorists have already operated in the U.S. The most prominent example is when Egyptian Shaykh Omar Abdel Rahman and nine followers conspired to bomb major New York City landmarks such as the World Trade Center and assassinate prominent politicians in 1993. As a result, the U.S. government has become increasingly concerned that terrorists will use weapons of mass destruction (WMD) in a terrorist

attack inside the nation's borders. More specific, an emerging and significant threat is represented by improvised biological, chemical, and nuclear devices that could decimate large populations, destabilize the government, and instill fear throughout the nation. The proliferation of these weapons, exacerbated by the Soviet Union's fragmentation and lack of controls, makes this a clear and present threat to U.S. security .[11] Therefore, if there is an adequate black market supply of nuclear materials, is there a need for international terrorists to attempt nuclear theft in a secure storage area? The more likely scenario would be an attack on a storage area to embarrass and create a weak image of the U.S. government.

Insider

A second significant threat to U.S. Air Force nuclear security is the insider. The insider could be an Air Force member, visitor, or contractor who has legitimate access to nuclear components. Insiders typically have special knowledge of internal controls that are unavailable to outsiders, and they have some amount of access. They are trusted. The Air Force establishes stringent entry control and access requirements through various instructions governing physical security and the Personnel Reliability Program to prevent insider sabotage.[12] With the procedures established, the concern becomes enforcement. The DOE provides an example of non-compliance with standards and the consequences. In testimony before Congress, the Government Accounting Office noted serious security deficiencies at DOE. The official report noted a lack of required background checks of visitors and contractors. Furthermore, adherence to physical security procedures was below standards. Security personnel failed tests of required skills, training records were inaccurate, or personnel were simply unable to perform their duties. As a result, there

were well-publicized problems with not only keeping threats out of the facilities, but also preventing authorized personnel from taking property and classified information off the premises.[13] Peter Probst, a specialist on international terrorism with the DoD's Special Operations and Low-Intensity Conflict Division, holds that security planners should focus on inside-the-fence threats that could come from the very people DoD employs to make up rooms, serve food, groom lawns, and perform other such services.[14] Therefore, even if standards exist, they must be enforced; otherwise, the insider could present serious risks to nuclear weapons.

Cyberwarfare

Antiterrorism planners recognize the terrorist and insider threat to resources; however, an emergent threat, cyberwarfare may also pose a significant threat to nuclear storage area security infrastructure. Until recently, there was little concern about risk to our information infrastructures because there was only a remote possibility these services could be knocked out. The physical breadth of the infrastructures made it difficult for a potential adversary to cause anything other than an isolated disturbance. Physical security measures adopted to prevent theft or sabotage also kept out those who would seek to destroy an infrastructure's ability to continue operating. A good strong fence, alarms, sensors and manpower fended off any potential terrorist or criminal. The Information Age changed things dramatically. Nearly all-critical infrastructures now rely on computers for the management and operation of their own systems, and for their interaction with other infrastructures. For example, electric power grids and natural gas pipelines are controlled by computer systems and those computer systems may be linked

to other publicly accessible telecommunications systems.[15] President Clinton summarized the potential threat effectively

> As we approach the 21st century, our foes have extended the fields of battle from physical space to cyberspace, from the world's vast bodies of water to the complex workings of our own human body. Rather than invading our beaches or launching bombers, these adversaries may attempt cyber attacks against our critical military systems and our economic base.[16]

The potential ability of terrorist or criminal organizations to use cyberattacks against military installations should give security planners cause for concern. Specifically, one should think about how an adversary might employ cyberattack against U.S. information systems to disable physical security measures in nuclear storage areas. Although systems have back-up generators and redundant capability, the potential remains for alarms and sensors to fail, thereby facilitating unauthorized entry and access to nuclear components. Ironically, as security systems seek to improve asset protection by employing advanced technology, the potential vulnerability to cyberattack may increase.[17]

Considering the author's three potential categories of threats to Air Force nuclear resources, the most likely scenario does not involve an enemy forces squad or large terrorist force attempting entry to a storage area in an attempt to steal a nuclear weapon. A more realistic possibility is that an insider could sabotage a nuclear component. A second scenario would be for a terrorist organization to conduct a cyberattack on electronic detection systems, then follow with a small unit attack to destroy a weapon in storage. Again, theft would not be objective. Embarrassment of the U.S. government, media attention, and instilling fear throughout the American public would surely be achieved if such an attack were successful. Perhaps even more frightening is the

potential for an alliance of convenience between domestic terrorist organizations and international sponsors of terrorism. Consider the possibility of a right wing militia group receiving financial backing from Osama Bin Ladin. This arrangement would eliminate Bin Ladin's logistical challenges of smuggling foreign operatives or explosives into the United States, while the domestic terrorist group would acquire resources needed to carry out terrorist attacks. The jewel in the crown would be destruction of a nuclear weapon. Such a scenario is not impossible and has precedence. On March 9, 1995, U.S. law enforcement indicted and convicted several members of the El Rukns street gang for conspiring to commit terrorist acts on behalf of Libya. As part of the conspiracy, an El Rukns member purchased an inert light anti-tank weapon from a FBI undercover agent.[18] Given the nature of the contemporary threat, U.S. Air Force nuclear WSAs may be vulnerable to attack.

Potential Vulnerabilities

Once asset criticality and possible threats are identified, the next step in the ARM process is to highlight potential vulnerabilities. Vulnerability assessments aid security planners in identifying weaknesses in the physical security plans, programs, and structures. Vulnerabilities include methods or avenues adversaries might take to gain access to protected DoD assets and the resulting adverse consequences in terms of diminution of capability to carry out assigned missions [19] The following short list of nuclear WSA potential vulnerabilities is intended to be descriptive and thought provoking. The list is not a complete and definitive. The reader will not find these weaknesses identified in any classified documents, but result from the author's application of the ARM model.

Above Ground Storage Structures

Security planners agree that nuclear weapons in storage are far less vulnerable than those in transit or exposed. Hardened above ground structures equipped with multiple layers of alarms and sensors and high security locks are thought to provide adequate protection. However, given the author's proposed threat scenarios, a cyberattack on alarms and sensors could render detection capability null and void. Consequently, the ability to detect and assess threats before they are in proximity to actual storage structures would be greatly diminished. Given the right amount of explosives and tools, a perpetrator could be inside the structure with access to weapons before adequate response forces could eliminate the threat. Moreover, with above ground structures an adversary need not access the fenced perimeter. Stand-off weapons such as rocket propelled grenades or shoulder fired missiles could possibly breach the doors to a structure housing nuclear components.

Manpower

The days of large manpower intensive response forces are history. In the past, more manpower usually meant better security and defense. With the technological explosion in physical security, many of the latest safeguards act as force multipliers. In fact, the author holds large response forces and reliance on manpower is a liability. For instance, poor training and lack of adherence to established procedures led to serious security violations at DOE national laboratories.[20] Furthermore, adversaries have the capability to use chemical and biological agents against their targets. The materials needed to produce these agents are relatively easy to acquire. For example, in April 1991, several members of a domestic extremist group, The Patriot's Council of Minnesota

manufactured the biological agent ricin from castor beans and discussed using it against federal law enforcement officers. The amount of ricin produced could have killed over 100 people if effectively delivered. Furthermore, in May 1995, an U.S. citizen illegally obtained three vials of bubonic plague from a firm in Maryland. He was arrested and charged with fraud. It is still unclear why he ordered the vials. [21] The ability for adversaries to acquire chemical and biological agents, then employ them against security personnel has tremendous ramifications. Security forces may not have the appropriate protective gear in place without advance warning of an attack. Consequently, the attackers would effectively neutralize initial and follow-on responding forces. Without personnel to prevent entry, the perpetrators could gain access to multiple storage bunkers. If the attackers were capable of executing a more complex operation, they could use cyberattack to disable electronic security systems in advance of deploying chemical agents.

Technology

Ironically, while advances in physical security technology may be able to improve asset protection it may also foster an opportunity for cyberattack. Again, terrorists or criminals could use information warfare against nuclear storage area power grids.[22] A catastrophic alarm and sensor failure would result in reliance on more manpower to secure structures. The previous section highlighted the manpower vulnerability and potential impact. Consequently, the best concept would be to use security systems that could be adequately protected against cyberattack while also reducing manpower.

Notes

[1] The White House. *A National Security Strategy for a New Century*, October 1998. p 1-7.

[2] Vatis, Michael A. Cybercrime, Transnational Crime, and Intellectual Property Theft Statement for the Record, 24 March 1998. On-line. Internet, 24 November 1999, n.p. Available from http://www.fbi.gov/pressrm/congress/98archives/vatis.htm.

[3] Department of Defense (DoD) Manual 5210.41 (C), *Nuclear Weapon Security Manual*, April 1994. chapter 2, p 1-4.

[4] Ibid

[5] "Terrorism in the United States 1995, Federal Bureau of Investigations Report, 1995, n.p. On-line. Internet. 31 December 1991, Available from http://www.fbi.gov/publish/terror/terrusa.htm.

[6] "Terrorism Current Trends in the United States, Federal Bureau of Investigations Report, 1995, n.p. On-line. Internet, 24 November 1999, Available on http://www.fbi.gov/library/terror/95report/trends.htm.

[7] "Principles of Operations," The Mountaineer Militia.

[8] Terrorism Current Threat, Federal Bureau of Investigations Report, 1995, n.p., On-line. Internet. 24 November 1999, Available on http://www.fbi.gov/library/terror/95report/current.htm.

[9] Principles of Operations," The Mountaineer Militia.

[10] Hartevold, Allison. *Extreme Tolerance*. KSPS TV, Spokane, Wa. 24 September 1999. TV documentary.

[11]Responding to Terrorism, Chapter 9 of the U.S. Department of Defense's 1997 Annual Defense Report. *The Terrorism Research Center Report*, 1997, n.p. On-line Internet, 24 November 1999. Available from http://www.terrorism.com/terrorism Responding.html.

[12] Air Force Instruction (AFI) 31-101. *The Air Force Physical Security Program*, September 1998. p. 18.

[13] US General Accounting Office. *Key Factors Underlying Security Problems at DOE Facilities*, 20 April 1999. p. 2-7.

[14] Gilbert, Douglas J. "Terrorism Expert Sounds Battle Cry." *American Forces Press Service*, September 1997, n.p. On-line. Internet, 24 November 1999. Available from http://www.defenselink.mil:80/news/Sep1997/n09121997_9709124.html.

[15] Vatis, Michael A. Cybercrime, Transnational Crime, and Intellectual Property Theft Statement for the Record, 24 March 1998. On-line. Internet, 24 November 1999, n.p. Available from http://www.fbi.gov/pressrm/congress/98archives/vatis.htm

[16] Clinton, William J., President of the United States, Address. United States Naval Academy Commencement Ceremony, Annapolis, Md., 22 May 1998.

[17] Vatis, Michael A. Cybercrime, Transnational Crime, and Intellectual Property Theft Statement for the Record, 24 March 1998. On-line. Internet, 24 November 1999, n.p. Available from http://www.fbi.gov/pressrm/congress/98archives/vatis.htm.

[18] "Terrorism, Current Trends in the United States." *Federal Bureau of Investigations Report*, 1995, n.p. On-line. Internet, 24 November 1999. Available from http://www.fbi.gov/library/terror/95report/trends.htm.

Notes

[19] Department of Defense (DoD) Directive, 0-2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*, February 1993. Chapter 6, p. 6-11.

[20] US General Accounting Office. *Key Factors Underlying Security Problems at DOE Facilities*, 20 April 1999. p. 2-7.

[21] "Terrorism, Current Trends in the United States." *Federal Bureau of Investigations Report*, 1995, n.p. On-line. Internet, 24 November 1999. Available from http://www.fbi.gov/library/terror/95report/trends.htm.

[22] Vatis, Michael A. Cybercrime, Transnational Crime, and Intellectual Property Theft Statement for the Record, 24 March 1998. On-line. Internet, 24 November 1999, n.p. Available from http://www.fbi.gov/pressrm/congress/98archives/vatis.htm.

Part 4

Countermeasures to Mitigate Risk

The next step in the ARM process is to consider countermeasures capable of mitigating risk potential threats present to Air Force nuclear weapons in storage facilities. The advantages of underground storage structures were discussed in previous sections. Beyond underground storage, there are two broad countermeasure categories that could be employed to improve security operations. Two proposals are to invest in technology and remove non-strategic nuclear forces (NSNF) from Europe.

Leveraging Technology

Availability of existing and emerging technology presents an opportunity to improve physical security of nuclear assets in storage. Technology will be a significant force multiplier that will decrease reliance on security personnel. Detection, assessment, and denial of access may all be enhanced. Because of the criticality of nuclear weapons, financial cost should not be prohibitive. A sampling of technologies appropriate for the nuclear security mission follows.

Video Storage System

The video storage system (VSS) is currently available with vendor delivery in 45 days. This system videotapes images and stores them electronically. The video system is

electronically linked to automated intrusion detection sensors. This system was specifically designed for nuclear weapon storage areas, flightlines, and other security areas. Employment of this system would greatly improve the detection and assessment capability in storage areas.[1]

Video Motion Detection

The video motion detection system is currently available through commercial vendors. This system would dramatically improve threat detection and assessment before the threat is proximate to the storage area. Closed Circuit Television coupled with thermal imagers is capable of motion and detection assessment in daylight and darkness. Probability of detection approaches the 90 percent range. Additionally, the system stores an image of the event causing the alarm.[2] This early detection and assessment capability would improve the security in-depth concept.

Weapon Storage and Security System

The weapon storage and security system (WS3) is designed to store and protect special weapons within a protective aircraft shelter. The WS3 vault is a below ground structure that may be raised when weapons need to be accessed. This system has several advantages over open bay storage. First, it incorporates a system of sensors and tamper switches that activate alarms in monitoring facilities. Upon receipt of an alarm immediate assessment is achieved through a close-circuit television system. Furthermore, the delayed entry technology would prevent a clandestine perpetrator from immediately accessing weapons.[3] An unauthorized attempt to access weapons would give response forces ample time to respond and eliminate the threat. The WS3 has been successfully employed at four main operating bases and five munitions support squadrons throughout

Europe. Although the system is designed for specific types of special weapons in aircraft shelters, the possibility for application to other nuclear weapon storage facilities should be pursued.

Less than Lethal Weaponry

Currently, the only force alternatives available for response forces protecting nuclear weapons are firearms and explosives. Deadly force is authorized to protect nuclear weapons, and in many cases would be appropriate; however, the security forces airman should have more tools in the kit bag to subdue a perpetrator. Less than lethal technology provides opportunities to fill the need. Not all scenarios require deadly force—even in nuclear weapon storage areas. Today's capabilities largely consist of blunt trauma weapons, stick foams, and oleoresin capsicum (pepper) spray. One example of new generation capability is use of concentrated light. These lights are safe, yet so intense that they temporarily "blind" and disable a potential adversary. This would preempt the need for security forces to make immediate physical contact to restrain a perpetrator. This light technology is applicable for storage areas because it is effective at significant ranges; thus, the security forces troop could engage the subject while maintaining safe standoff distance from the protected resource.[4] Furthermore, the next generation of non-lethal weaponry holds great promise. The next generation of non-lethals includes acoustics, electromagnetic pulse, and other directed energy weapons. [5]Imagine establishing perimeters employing magnetic pulse fields or directed energy around storage sites that could disable a perpetrator without exposing personnel to danger—the possibilities are exciting.

These technologies will improve the ability to detect, assess, delay, and ultimately defeat a potential terrorist or insider threat; however, technology is not a panacea. As adversaries improve their ability to wage cyberattack on information systems, technologies reliant on power grids and telecommunications may become vulnerable. Therefore, the best approach is to use "defendable" physical security systems.

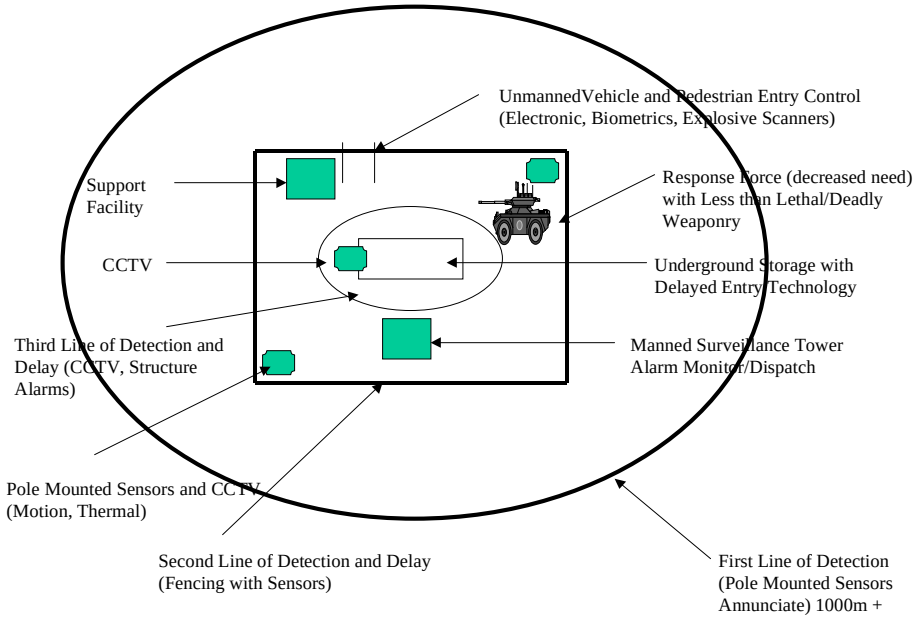

Figure 3. Notional Nuclear Weapon Storage Area Employing a Sampling of Available Technology

Remove Non-Strategic Nuclear Forces From Europe

Up to this point, this paper addressed the criticality of nuclear components in storage, the potential threat, and likely vulnerabilities. Next, the ARM model allowed the author to explore countermeasures that could decrease risk imposed by the threat. In Europe, an additional countermeasure could be imposed to not just decrease the threat, but eliminate the threat. American nuclear weapons in Europe were designed to counter the large

Soviet military threat. When the Soviet Union dissolved, the threat dissolved along with it. Clearly, there are political reasons and implications for keeping nuclear weapons in Europe; however, policy makers should consider whether benefits provided to the North Atlantic Treaty Organization (NATO) outweigh associated security risks. Crochet argues that non-strategic nuclear forces are no longer required for the security of Western Europe. The number of U.S. tactical nuclear weapons in Europe is already relatively small. It is estimated that the U.S. retains about 200 B-61 free-fall nuclear bombs, distributed among several sites.[6] Redeploying the remaining tactical nuclear weapons from Europe to storage sites in the continental United States would remove them from a higher threat area to a more benign threat environment.

Notes

[1] Electronic Systems Center Brochure. *Video Storage System*, 1999.
[2] Electronic Systems Center Brochure. *Video Motion Detection*, 1999.
[3] Electronic Systems Center Brochure, *Weapon Storage and Security System*, 1999.
[4] Electronic Systems Center Brochure, *HALT*, 1999.
[5]Herbert, Dennis B. "Non-Lethal Weaponry: From Tactical to Strategic Applications." *Joint Force Quarterly*, no. 21 (Spring 1999): 87-91.
[6] Crochet, Captain John M. *The Case for Removal of U.S. Non-Strategic Nuclear Forces From Europe*. Strategy Research Project. Carlisle Barracks, Penn.: Army War College, 1998. p 2-12.

Part 5

Additional Benefits

Potential costs and benefits have been considered throughout the paper. There is one other benefit associated with modifying U.S. Air Force nuclear security concepts. This paper attempted to show that leveraging technology could serve as a force multiplier. Therefore, a manpower windfall may be realized. At first glance, the possibility of saving manpower appears to be a good result. However, there are probably Air Force leaders that would disagree, holding that the security forces career field has been downsized too much to meet current taskings. The author does not propose that manpower be eliminated. The saved manpower could be transferred to units supporting the Expeditionary Air Force or the new breed of contingency operations units such as the 820th Security Forces Group or the 786th Security Forces Squadron. Could this be feasible? In nuclear security forces units that employ the WS3 and other advanced sensor, alarm, and delayed entry technology, DoD area response force requirements were drastically reduced.[1]

Consider the following hypothetical manpower drill as an example of the potential windfall. Squadron X, a nuclear security unit, employs a combination of the proposed countermeasures outlined in this paper. As a result, 10 duty positions are no longer needed. When multiplied by the post manning factor (5.489 personnel per 24-hour PRP

post) the total savings would be over 50 personnel.[2] These "spaces" have faces that would no longer be required to perform duties in subzero temperatures and hazardous driving conditions. Further, these personnel could be transferred to Air Expeditionary Force Wings for needed security forces support, or to contingency operations units. Moreover, consider the number of units that would be able to achieve similar results. The security forces support for the EAF concept would be greatly enhanced, while the quality of nuclear security also improved.

Notes

[1] Department of Defense (DoD) Directive 5210.41M, *Nuclear Weapon Security Manual, April 1994*, Chapter 4, p 1-7, Chapter 5, p 1-7.

[2] Air Force Manpower Standard (AFMS) 43XX (draft), 1995. Although a draft, Security Forces units are allocated manpower using the draft standard. Current revisions are estimated to be completed and published in 2000. Manpower savings are conservative by author's estimation.

Part 6

Conclusions

Overall, the Air Force nuclear security standards have not changed much since the days of the Cold War. The Soviet threat posed to U.S. nuclear stockpiles disappeared with the Soviet disintegration. The face of the enemy drastically changed. Asymmetrical threats now present the greatest challenge to U.S. interests, infrastructure, and Air Force assets—including nuclear components in storage. Therefore, an evaluation of nuclear security standards in storage areas is appropriate. The author concludes that current nuclear security standards are adequate, especially to prevent theft of nuclear components; however, much could be done to improve the current posture. Using the CIA Asset Risk Management model, research confirmed nuclear assets are the most critical resources in the U.S. military inventory. Further, the new adversary includes terrorists, insiders, and cyberwarfare. These threats create vulnerabilities especially to weapons stored in above ground structures. Reliance on large manpower-intensive response forces and physical security technology dependent on electric power grids and telecommunications are also weaknesses. Given the nature of the threat and vulnerabilities to the nuclear assets in storage, the Air Force should consider leveraging defendable off-the-shelf and emerging technology as well as decreased reliance on manpower. Furthermore, U.S. policymakers must ponder the benefit of maintaining

tactical nuclear weapons in the higher European threat environment. These weapons should be redeployed to continental U.S. storage structures. Finally, aside from improved physical security, leveraging technology to secure nuclear storage areas may pay a valuable manpower dividend for the security forces career field and more importantly the EAF.

Bibliography

Air Force Instruction (AFI) 31-101. *The Air Force Physical Security Program*, September 1998.

Air Force Manpower Standard (AFMS) 43XX (draft), 1995.

Air Force Regulation (AFR) 207-10. *Nuclear Weapons in Storage, Surface Movement and Logistics Transport Status,* 13 December 1974.

Clinton, William J., President of the United States, Address. United States Naval Academy Commencement Ceremony, Annapolis, Md., 22 May 1998.

Crochet, Captain John M. *The Case for Removal of U.S. Non-Strategic Nuclear Forces From Europe*. Strategy Research Project. Carlisle Barracks, Penn.: Army War College, 1998

Department of Defense (DoD) Directive, 0-2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence,* February 1993.

Department of Defense (DoD) Manual 5210.41 (C), *Nuclear Weapon Security Manual*, April 1994. Information extracted is unclassified.

Electronic Systems Center Brochure. *Video Storage System*, 1999.

Electronic Systems Center Brochure. *Video Motion Detection*, 1999.

Electronic Systems Center Brochure, *Weapon Storage and Security System*, 1999.

Electronic Systems Center Brochure, *HALT*, 1999.

Gilbert, Douglas J. "Terrorism Expert Sounds Battle Cry." *American Forces Press Service*, September 1997, n.p. On-line. Internet, 24 November 1999. Available from http://www.defenselink.mil:80/news/Sep1997/n09121997_9709124.html.

Hartevold, Allison. *Extreme Tolerance*. KSPS TV, Spokane, Wa. 24 September 1999. TV documentary.

Herbert, Dennis B. "Non-Lethal Weaponry: From Tactical to Strategic Applications." *Joint Force Quarterly*, no. 21 (Spring 1999): 87-91.

Payne, Keith B. "Post-Cold War Requirements for U.S. Nuclear Deterrence Policy." *Comparative Strategy* 17, no. 3 (July-September 1998): 227-278.

"Principles of Militia Operations." The Mountaineer Militia, Clarksburg, WV.

"Responding to Terrorism, Chapter 9 of the U.S. Department of Defense's 1997 Annual Defense Report. *The Terrorism Research Center Report*, 1997, n.p. On-line. Internet, 24 November 1999. Available from http://www.terrorism.com/terrorism/Responding.html.

"Terrorism, Current Threat." Federal Bureau of Investigations Report, 1995, n.p. On-line. Internet, 24 November 1999. Available from http://www.fbi.gov/library/terror/95report/current.htm

"Terrorism, Current Trends in the United States." *Federal Bureau of Investigations Report*, 1995, n.p. On-line. Internet, 24 November 1999. Available from http://www.fbi.gov/library/terror/95report/trends.htm

"Terrorism in the United States 1995." Federal Bureau of Investigations Report, 1995, . n.p. On-line. Internet, 31 December 1999. Available from http://www.fbi.gov/publish/terror/terrorism.htm

"Terrorism, the Year in Review." Federal Bureau of Investigations Report, 1995, n.p. On-line. Internet, 24 November 1999. Available from http://www.fbi.gov/library/terror/95report/year.htm

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

US General Accounting Office. *Key Factors Underlying Security Problems at DOE Facilities*, 20 April 1999.

Vatis, Michael A. Cybercrime, Transnational Crime, and Intellectual Property Theft Statement for the Record, 24 March 1998. On-line. Internet, 24 November 1999, n.p. Available from http://www.fbi.gov/pressrm/congress/98archives/vatis.htm